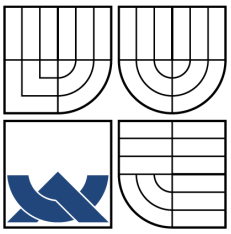
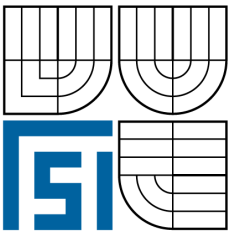


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

RINGS OF ENDOMORPHISMS OF ELLIPTIC CURVES AND MESTRE'S THEOREM

OKRUHY ENDOMORFISMŮ ELIPTICKÝCH KŘIVEK
A MESTREHO TEORÉM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

LENKA ZAVÍRALOVÁ

VEDOUCÍ PRÁCE
SUPERVISOR

doc. RNDr. MIROSLAV KUREŠ, Ph.D.

BRNO 2009

Abstrakt

Eliptické křivky jsou mocným nástrojem dnešní doby. Jednak přispěly k vyřešení mnoha matematických problémů, ale také nalezly četná uplatnění v aplikacích, jako je například kryptografie založená na eliptických křivkách (ECC). Tato metoda veřejného klíče má velkou budoucnost, neboť v mnohém doplňuje nedostatky známé RSA metody. Jedním z hlavních problémů kryptografie založené na eliptických křivkách je určení řádu eliptické křivky, tedy výpočet počtu bodů eliptické křivky nad prvočíselným polem. Tomuto zásadnímu problému je věnována tato práce. Na určení řádu eliptické křivky existuje řada algoritmů. Pro menší prvočísla (čili pro charakteristiku prvočíselného pole) se užívá metoda založená na přímém výpočtu, tzv. naivní algoritmus. Velkou pomocí v této problematice je Hasseho teorém, který omezuje řád eliptické křivky intervalem. Pro větší prvočísla se s úspěchem používají Shanksův algoritmus a jeho vylepšení Mestreho algoritmus. Oba algoritmy mají dvě části - Baby Step a Giant Step. Shanksův algoritmus je však v určitých případech nepoužitelný a tento problém řeší Mestreho algoritmus, který používá pojem twist eliptické křivky. Díky Mestreho teorému bylo dokázáno, že řád eliptické křivky nad prvočíselným polem může být spočten pro každé prvočíslo větší než 457. Důkaz, který spočívá především v isomorfismu okruhu endomorfismů nad eliptickými křivkami a imaginárního kvadratického řádu, je uveden na závěr této práce.

Summary

The elliptic curves are a powerful tool at present. First, they helped to solve many mathematical problems, but they also found their place in numerous applications, such as Elliptic Curve Cryptography (ECC). This public key encryption has a great future, because it solve the drawbacks of the famous RSA method. One of main the problems of the Elliptic Curve Cryptography is the determination of the elliptic curve's order, i.e. calculating the number of elliptic curve's points over the prime field. In this thesis we will deal with this fundamental problem. For determining of elliptic curve's order there exist several algorithms. For smaller prime numbers (i.e. the characteristics of the prime field) we have the algorithm, which uses direct calculation, called the Naive algorithm. A great assist in this issue is the Hasse's Theorem, which states that the elliptic curve's order has a bound - Hasse's interval. Shank's algorithm and its improvement Mestre's algorithm are successfully used for larger prime numbers. Both algorithms have two parts called the Baby Step and the Giant Step. Shank's algorithm is in some cases unusable, and this problem is solved by Mestre's algorithm with the twist of elliptic curve. Thanks to Mestre's Theorem, it was proved that the order of the elliptic curves over the prime field can be computed for each prime number greater than 457. The proof, which consists primarily in the isomorphism of elliptic curve's endomorphism's ring and the imaginary quadratic order, is mentioned at the end of this work.

klíčová slova
konečná pole, rozšíření polí, eliptická křivka

key words
finite fields, field extension, elliptic curve

ZAVÍRALOVÁ, L.: *Rings of endomorphisms of elliptic curves and Mestre's theorem.* Brno: Brno University of Technology, Faculty of Mechanical Engineering, 2009. 57 s. Supervisor doc. RNDr. MIROSLAV KUREŠ, Ph.D.

I declare that I have written the bachelor thesis *Rings of endomorphisms of elliptic curves and Mestre's theorem* on my own according to the instructions of my bachelor thesis supervisor doc. RNDr. Miroslav Kureš, Ph.D., and using the sources listed in references.

May 20, 2009 Lenka Zavíralová

I would like to thank my supervisor doc. RNDr. Miroslav Kureš, Ph.D. for presiding over my bachelor thesis.

Lenka Zavíralová

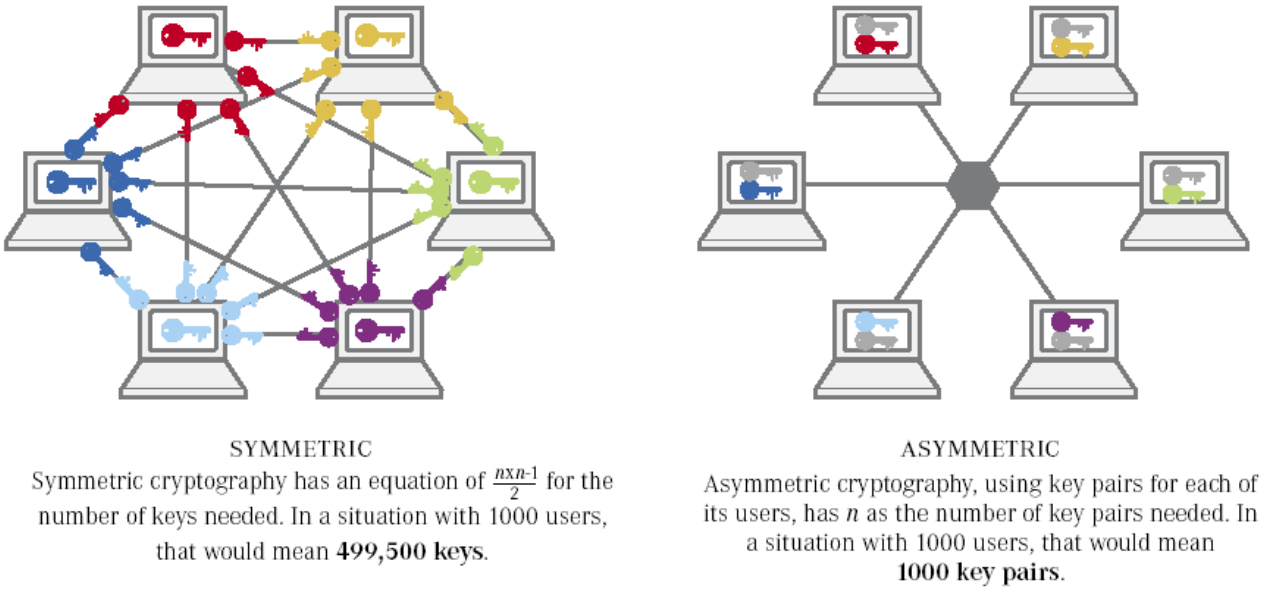
Contents

1 Introduction

Elliptic curves have been studied by mathematicians for over a century and they have been used to solve various problems. We can mention for instance the *congruent number problem*. In this, we have the area of some right-angled triangle whose lengths of sides are rational numbers, and we need the classification of the positive integers laying in this area. Another famous one is the proof of *Fermat's Last Theorem* [Andrew Wiles, 1994], which says that the equation $x^n + y^n = z^n$ has no nonzero integer solutions for x, y and z when the integer n is greater than 2. At the end of the 20th century, it turned out that it is very convenient to use the elliptic curves for designing a public-key cryptographic system.

We might not be aware of that, but we use *cryptography* every day. For example, we can buy safely on Internet or control on line bank account. Cryptography is a powerful tool in our modern life as well as a complicated issue.

We have two main approaches in cryptography - a *symmetric-key cryptography* and a *public-key cryptography* (asymmetric-key cryptography).



Picture 1.1. : *The symmetric-key and the public-key cryptography [8]*

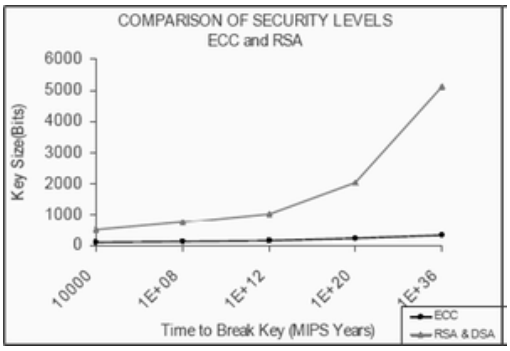
The main advantage of the symmetric-key cryptography is its high efficiency whereas there are two main drawbacks . The first is called the *key distribution problem* (a channel must be both secret and authenticated for the distribution of secured material) and the *key management problem* (each entity may have to maintain different secured material with each of the other N-1 entities). The most famous symmetric-key encryption systems are for instance Data Encryption Standard (DES), RC4 or the Advanced Encryption Standard (AES).

In contrast to symmetric-key schemes, the public-key one requires only that the communicating entities exchange keying material that is authentic (but not secret) and use the key pair - *the public and the private key*. The public key is used for encryption and the private key for decryption. The core of the public key encryption is the problem of

deriving the private key from the corresponding public key, which is equivalent to solve a computational problem that seems to be unsolvable. We have several approaches to this computational problem:

1. The integer factorization problem - *RSA public-key cryptography*
2. The discrete logarithm problem - *ElGamal public-key cryptography, Digital Signature Algorithm (DSA)*
3. The elliptic curve discrete logarithm problem - *Elliptic curve cryptography (ECC)*

RSA gets its security from the difficulty of factoring a very large product of two prime numbers, so the integer factorization problem is to factor $n = p \cdot q$. The RSA safety depends on the keys' length. It is obvious that the length must be increasingly longer and this causes several problems, which can be solved by the ECC. The ECC has a smaller key size than RSA for the same level of security (to achieve the same safety, RSA key must have 1024 bits, whereas ECC key needs only obout 160-180 bits). That means also faster cryptographic operations, running on smaller chips or more compact software.



Picture 1.2.: *The comparison of ECC and RSA [9]*

Roughly speaking, the elliptic curve discrete problem consists in the discovery of such integer k, that the equation $P = kQ$ holds for two elliptic curve's points P and Q. One of the main problems in ECC is the determination of the number of the elliptic curve's points. So we will deal with this problem in this thesis, where the most important algorithms and corollaries are mentioned.

In the § 1 we will firstly mention some basic concepts from algebra. In this paragraph we will deal mainly with algebraic structures and types of morphisms on them. The § 2 will introduce the algebraic extension. After the definition and some properties we will show and investigate some well known examples of the algebraic extension. Then in the § 4 and § 5 which are named Full module, Order and Quadratic residues we will mention the necessary concepts for understanding the following paragraphs. The remaining paragraphs constitute the main part of this thesis. In the § 6 we will explain what the elliptic curve is, we will mention its important properties and mainly the arithmetic of elliptic curve's points counting. Last § 7 mentions the most famous algorithms for determining the elliptic curve's order. The end of this chapter is devoted to the famous Mestre's Theorem and its proof, where we will avail ourselves of the knowledge from the introductory chapters. At the end of this thesis you will find the appendix which extends definitions and properties of the concepts mentioned in the previous paragraphs. We will mainly deal with the algebraic extension, its example the cyclotomic field and the application in the famous Galois Theory. After that, we will deepen the view of the module issue.

2 Algebraic Background

2.1 Algebraic Structures

Definition 2.1. A *group* $(\mathcal{G}, +)$ is a nonempty set $\mathcal{G}$ equipped with one binary operation "$+$" : $\mathcal{G} \times \mathcal{G} \to \mathcal{G}$ (where "$\times$" denotes a Cartesian product), usually called the addition. For all $a, b, c \in \mathcal{G}$ the following axioms hold:

1. $(a + b) + c = a + (b + c)$ (Associativity)
2. $\forall\ a \in \mathcal{G}\ \exists\ 0_{\mathcal{G}} \in \mathcal{G} : 0_{\mathcal{G}} + a = a + 0_{\mathcal{G}} = a$ (Identity element)
3. $\forall\ a \in \mathcal{G}\ \exists\ -a \in \mathcal{G} : a + (-a) = (-a) + a = 0_{\mathcal{G}}$ (Inverse element)

Example 2.1.

- The numerical groups are for instance $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$. Let us denote the usual multiplication as "$\cdot$" : $\mathcal{G} \times \mathcal{G} \to \mathcal{G}$. Then $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ are not groups because in $(\mathbb{Z}, \cdot)$ only the numbers 1 and -1 have the inverse element and in $(\mathbb{Q}, \cdot)$ the number 0 has no inverse element. If we denote $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ then $(\mathbb{Q}^*, \cdot)$ is a group.

Definition 2.2. A group for which the law of commutativity of addition holds, that is $\forall\ a, b \in \mathcal{G} : a + b = b + a$, is called the *Abelian group*.

Definition 2.3. The number of elements in the group $\mathcal{G}$, denoted $|\mathcal{G}|$, is called the *order of the group* $\mathcal{G}$. If the order of the group is a finite number, the group is said to be a *finite group*.

The *order of an element* $a \in \mathcal{G}$ is the smallest $n \in \mathbb{N}$ such that

$$\underbrace{a + a + \ldots + a}_{n\text{- times}} = 0_{\mathcal{G}}.$$

The group $\mathcal{G}$ is called *cyclic* if the order of any element $a \in \mathcal{G}$ has the same order as $\mathcal{G}$. Then we say that a is a *generator* of $\mathcal{G}$ and we denote this by $\mathcal{G} = \langle a \rangle$.

Let us have the smallest integer n such that it satisfies the condition $na = 0_{\mathcal{G}}\ \forall\ a \in \mathcal{G}$. Then n is an *exponent* of the group $\mathcal{G}$.

Theorem 2.1. *Lagrange's Theorem.* Let $\mathcal{G}$ be a finite group. Then the order of the group $\mathcal{G}$ is divisible by the order of every element of $\mathcal{G}$.

Definition 2.4. A *ring with a unit* (hereafter only a ring) is a nonempty set $\mathcal{R}$ equipped with two binary operations "$+$" : $\mathcal{R} \times \mathcal{R} \to \mathcal{R}$ and "$\cdot$" : $\mathcal{R} \times \mathcal{R} \to \mathcal{R}$, usually called the addition and the multiplication, such that:

- $(\mathcal{R}, +)$ is an Abelian group with the identity element 0.
- $(\mathcal{R}, \cdot)$ is a *monoid* (this means associative groupoid with the identity element 1).
- The multiplication is distributive over the addition.

Also more precisely $\forall\ a, b, c \in \mathcal{R}$ the following axioms hold:

1. $(a+b)+c = a+(b+c)$ (Associativity of addition)
2. $a+b = b+a$ (Commutativity of addition)
3. $\forall\ a \in \mathcal{R}\ \exists\ 0_{\mathcal{R}} \in \mathcal{R} : 0_{\mathcal{R}} + a = a$ (Additive identity)
4. $\forall\ a \in \mathcal{R}\ \exists\ -a \in \mathcal{R} : a + (-a) = 0_{\mathcal{R}}$ (Additive inverse)
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associativity of multiplication)
6. $\forall\ a \in \mathcal{R}\ \exists\ 1_{\mathcal{R}} \in \mathcal{R} : 1_{\mathcal{R}} \cdot a = a \cdot 1_{\mathcal{R}} = a$ (Multiplicative identity)
7. $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ (Left distributivity of multiplication over addition)
8. $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ (Right distributivity of multiplication over addition)

Example 2.2.

- The most famous are the numerical rings: $(\mathbb{Z}, +, \cdot),\ (\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot),\ (\mathbb{C}, +, \cdot)$.
- The *trivial ring* $\mathcal{R} = \{0\}$ has only one element and it serves both as the additive and the multiplicative identity.
- Among finite rings also belowng $(\mathbb{Z}_n, +, \cdot),\ n \in \mathbb{N},\ n \geq 2$ where $\mathbb{Z}_n$ is the ring of integers modulo n with n elements.
- A polynomial ring $\mathcal{R}[x]$ of polynomials over a ring $\mathcal{R}$, which means the polynomials in one indeterminate x and with coefficients in $\mathcal{R}$, form also a ring.
- Let us have $\mathcal{M}_{n\times n}(\mathbb{R})$ which is a set of all square matrices (over $\mathbb{R}$) of order n then $(\mathcal{M}_{n\times n}(\mathbb{R}), +, \cdot)$ is a ring.
- As a less common example we will investigate in detail the ring $\mathcal{R} = \{(n; P(x)) \in \mathbb{Z} \times \mathbb{F}_p[x];\ P(0_{\mathbb{F}_p}) = \overline{n}\}$. Here $\mathbb{F}_p$ is a prime field (see the Definition 2.8.), $0_{\mathbb{F}_p}$ is the additive identity of $\mathbb{F}_p$ and $\overline{n} \equiv n \pmod p$. The operations $+$ and $\cdot$ are defined "by components" and $(\mathcal{R}, +, \cdot)$ is the ring. More concretely:
  $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$,
  $(9;\ x^3 + 4x^2 + x + 4) \in \mathcal{R}$ because $P(0_{\mathbb{F}_5}) = P(0) = 4$ and $9 \equiv 4 \pmod 5$.

  Proof. We must verify the axioms of the ring. Let $(k, P(x))$, $(l, Q(x))$, $(m, R(x))$ lie in the ring $\mathcal{R}$, where k, l, $m \in \mathbb{Z}$ and $P(x)$, $Q(x)$, $R(x)$ are the polynomials defined above. We assume that the addition $\bmod p$ is associative and commutative, the multiplication $\bmod p$ is associative and the laws of distributivity hold for this arithmetic.

  1. Associativity of addition
     $\Big(\big(k, P(x)\big) + \big(l, Q(x)\big)\Big) + \big(m, R(x)\big) = \big(k+l, P(x)+Q(x)\big) + \big(m, R(x)\big) = \big(k+l+m, P(x)+Q(x)+R(x)\big) = \big(k, P(x)\big) + \big(l+m, Q(x)+R(x)\big) = \big(k, P(x)\big) + \Big(\big(l, Q(x)\big) + \big(m, R(x)\big)\Big)$
  2. Commutativity of addition
     $\big(k, P(x)\big) + \big(l, Q(x)\big) = \big(k+l, P(x)+Q(x)\big) = \big(l+k, Q(x)+P(x)\big) = \big(l, Q(x)\big) + \big(k, P(x)\big)$

3. Additive identity $(0, 0_{\mathbb{F}_p})$
$(0, 0_{\mathbb{F}_p}) + \big(k, P(x)\big) = \big(0 + k, 0_{\mathbb{F}_p} + P(x)\big) = \big(k, P(x)\big)$
4. Additive inverse $-\big(k, P(x)\big) = \big(- k, -P(x)\big) = \big(0 - k, 0_{\mathbb{F}_p} - P(x)\big)$
$\big(k, P(x)\big) + \Big(- \big(k, P(x)\big)\Big) = \big(k, P(x)\big) + \big(0 - k, 0_{\mathbb{F}_p} - P(x)\big) = \big(k + 0 - k, P(x) + 0_{\mathbb{F}_p} - P(x)\big) = (0, 0_{\mathbb{F}_p})$
5. Associativity of multiplication
$\Big(\big(k, P(x)\big) \cdot \big(l, Q(x)\big)\Big) \cdot \big(m, R(x)\big) = \big(k \cdot l, P(x) \cdot Q(x)\big) \cdot \big(m, R(x)\big) = \big(k \cdot l \cdot m, P(x) \cdot Q(x) \cdot R(x)\big) = \big(k, P(x)\big) \cdot \big(l \cdot m, Q(x) \cdot R(x)\big) = \big(k, P(x)\big) \cdot \Big(\big(l, Q(x)\big) \cdot \big(m, R(x)\big)\Big)$
6. Multiplicative identity $(1, 1_{\mathbb{F}_p})$
$(1, 1_{\mathbb{F}_p}) \cdot \big(k, P(x)\big) = \big(1 \cdot k, 1_{\mathbb{F}_p} \cdot P(x)\big) = \big(k, P(x)\big)$
7. Left distributivity of multiplication over addition
$\big(k, P(x)\big) \cdot \Big(\big(l, Q(x)\big) + \big(m, R(x)\big)\Big) = \big(k, P(x)\big) \cdot \big(l + m, Q(x) + R(x)\big) = \Big(k \cdot (l + m), P(x) \cdot \big(Q(x) + R(x)\big)\Big) = \big(k \cdot l + k \cdot m, P(x) \cdot Q(x) + P(x) \cdot R(x)\big) = \big(k \cdot l, P(x) \cdot Q(x)\big) + \big(k \cdot m, P(x) \cdot R(x)\big) = \Big(\big(k, P(x)\big) \cdot \big(l, Q(x)\big)\Big) + \Big(\big(k, P(x)\big) \cdot \big(m, R(x)\big)\Big)$
8. Right distributivity of multiplication over addition
$\Big(\big(k, P(x)\big) + \big(l, Q(x)\big)\Big) \cdot \big(m, R(x)\big) = \big(k + l, P(x) + Q(x)\big) \cdot \big(m, R(x)\big) = \Big((k + l) \cdot m, \big(P(x) + Q(x)\big) \cdot R(x)\Big) = \big(k \cdot m + l \cdot m, P(x) \cdot R(x) + Q(x) \cdot R(x)\big) = \big(k \cdot m, P(x) \cdot R(x)\big) + \big(l \cdot m, Q(x) \cdot R(x)\big) = \Big(\big(k, P(x)\big) \cdot \big(m, R(x)\big)\Big) + \Big(\big(l, Q(x)\big) \cdot \big(m, R(x)\big)\Big)$

□

Definition 2.5. A *characteristic* of a ring $\mathcal{R}$, denoted $\mathrm{char}(\mathcal{R})$, is defined to be the smallest number of times one must add the ring's multiplicative identity element 1 to itself to get the additive identity element 0. The ring is said to have characteristic zero if this repeated sum never reaches the additive identity. That is, $\mathrm{char}(\mathcal{R})$ is the smallest number n if it exists, and 0 otherwise.

Example 2.3. $\mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ is the set of all square matrices of degree 2 with components from an integral domain (see the Definition 2.7.) of polynomials over finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$, p-prime, $n \in \mathbb{N}$ (see the Definition 2.8.). This set $\mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ is a ring with characteristic p.

Proof. Firstly we verify the ring axioms and after we show that the characteristic for $\mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ is p. Let us have

$$\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix}, \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix}, \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{F}_q[x]),$$

where $K(x)$, $L(x)$, $M(x)$, $N(x)$, $P(x)$, $Q(x)$, $R(x)$, $S(x)$, $T(x)$, $U(x)$, $V(x)$, $W(x)$ are polynomials laying in $\mathbb{F}_q[x]$. We assume that the addition modulo q is associative and commutative, the multiplication modulo q is associative and laws of distributivity hold for this arithmetic.

1. $\mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ is a ring.

   (a) Associativity of addition

$$\left(\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} + \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix}\right) + \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)+P(x) & L(x)+Q(x) \\ M(x)+R(x) & N(x)+S(x) \end{pmatrix} + \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)+P(x)+T(x) & L(x)+Q(x)+U(x) \\ M(x)+R(x)+V(x) & N(x)+S(x)+W(x) \end{pmatrix} = Z$$

$$\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} + \left(\begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} + \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix}\right) =$$

$$= \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} + \begin{pmatrix} P(x)+T(x) & Q(x)+U(x) \\ R(x)+V(x) & S(x)+W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)+P(x)+T(x) & L(x)+Q(x)+U(x) \\ M(x)+R(x)+V(x) & N(x)+S(x)+W(x) \end{pmatrix} = Z$$

   (b) Commutativity of addition

$$\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} + \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} = \begin{pmatrix} K(x)+P(x) & L(x)+Q(x) \\ M(x)+R(x) & N(x)+S(x) \end{pmatrix} =$$

$$= \begin{pmatrix} P(x)+K(x) & Q(x)+L(x) \\ R(x)+M(x) & S(x)+N(x) \end{pmatrix} = \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} + \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix}$$

   (c) Additive identity $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} = \begin{pmatrix} 0+K(x) & 0+L(x) \\ 0+M(x) & 0+N(x) \end{pmatrix} = \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix}$$

   (d) Additive inverse $-\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} = \begin{pmatrix} -K(x) & -L(x) \\ -M(x) & -N(x) \end{pmatrix}$

$$\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} + \left(-\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix}\right) = \begin{pmatrix} K(x)-K(x) & L(x)-L(x) \\ M(x)-M(x) & N(x)-N(x) \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

   (e) Associativity of multiplication

$$\left(\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} \cdot \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix}\right) \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)\cdot P(x)+L(x)\cdot R(x) & K(x)\cdot Q(x)+L(x)\cdot S(x) \\ M(x)\cdot P(x)+N(x)\cdot R(x) & M(x)\cdot Q(x)+N(x)\cdot S(x) \end{pmatrix} \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)\cdot P(x)\cdot T(x)+L(x)\cdot R(x)\cdot T(x)+K(x)\cdot Q(x)\cdot V(x)+L(x)\cdot S(x)\cdot V(x) \\ M(x)\cdot P(x)\cdot T(x)+N(x)\cdot R(x)\cdot T(x)+M(x)\cdot Q(x)\cdot V(x)+N(x)\cdot S(x)\cdot V(x) \end{pmatrix}$$

$$\left.\begin{array}{c} K(x)\cdot P(x)\cdot U(x)+L(x)\cdot R(x)\cdot U(x)+K(x)\cdot Q(x)\cdot W(x)+L(x)\cdot S(x)\cdot W(x) \\ M(x)\cdot P(x)\cdot U(x)+N(x)\cdot R(x)\cdot U(x)+M(x)\cdot Q(x)\cdot W(x)+N(x)\cdot S(x)\cdot W(x) \end{array}\right) =$$

$$= Z$$

$$\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} \cdot \left(\begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} \right) =$$

$$= \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} \cdot \begin{pmatrix} P(x)\cdot T(x)+Q(x)\cdot V(x) & P(x)\cdot U(x)+Q(x)\cdot W(x) \\ R(x)\cdot T(x)+S(x)\cdot V(x) & R(x)\cdot U(x)+S(x)\cdot W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)\cdot P(x)\cdot T(x)+L(x)\cdot R(x)\cdot T(x)+K(x)\cdot Q(x)\cdot V(x)+L(x)\cdot S(x)\cdot V(x) \\ M(x)\cdot P(x)\cdot T(x)+N(x)\cdot R(x)\cdot T(x)+M(x)\cdot Q(x)\cdot V(x)+N(x)\cdot S(x)\cdot V(x) \end{pmatrix}$$

$$\left.\begin{array}{c} K(x)\cdot P(x)\cdot U(x)+L(x)\cdot R(x)\cdot U(x)+K(x)\cdot Q(x)\cdot W(x)+L(x)\cdot S(x)\cdot W(x) \\ M(x)\cdot P(x)\cdot U(x)+N(x)\cdot R(x)\cdot U(x)+M(x)\cdot Q(x)\cdot W(x)+N(x)\cdot S(x)\cdot W(x) \end{array}\right) =$$

$$= Z$$

(f) Multiplicative identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} = \begin{pmatrix} 1\cdot K(x)+0\cdot M(x) & 1\cdot L(x)+0\cdot N(x) \\ 0\cdot K(x)+1\cdot M(x) & 0\cdot L(x)+1\cdot N(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix}$$

(g) Left distributivity of multiplication over addition

$$\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} \cdot \left(\begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} + \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} \right) =$$

$$= \begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} + \begin{pmatrix} P(x)+T(x) & Q(x)+U(x) \\ R(x)+V(x) & S(x)+W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)\cdot P(x)+K(x)\cdot T(x)+L(x)\cdot R(x)+L(x)\cdot V(x) \\ M(x)\cdot P(x)+M(x)\cdot T(x)+N(x)\cdot R(x)+N(x)\cdot V(x) \end{pmatrix}$$

$$\left.\begin{array}{c} K(x)\cdot Q(x)+K(x)\cdot U(x)+L(x)\cdot S(x)+L(x)\cdot W(x) \\ M(x)\cdot Q(x)+M(x)\cdot U(x)+N(x)\cdot S(x)+N(x)\cdot W(x) \end{array}\right) = Z$$

$$\left(\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} \cdot \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} \right) + \left(\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} \right) =$$

$$\begin{pmatrix} K(x)\cdot P(x)+L(x)\cdot R(x) & K(x)\cdot Q(x)+L(x)\cdot S(x) \\ M(x)\cdot P(x)+N(x)\cdot R(x) & M(x)\cdot Q(x)+N(x)\cdot S(x) \end{pmatrix} +$$

$$+ \begin{pmatrix} K(x)\cdot T(x)+L(x)\cdot V(x) & K(x)\cdot U(x)+L(x)\cdot W(x) \\ M(x)\cdot T(x)+N(x)\cdot V(x) & M(x)\cdot U(x)+N(x)\cdot W(x) \end{pmatrix} = Z$$

(h) Right distributivity of multiplication over addition

$$\left(\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} + \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} \right) \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)+P(x) & L(x)+Q(x) \\ M(x)+R(x) & N(x)+S(x) \end{pmatrix} \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)\cdot T(x)+P(x)\cdot T(x)+L(x)\cdot V(x)+Q(x)\cdot V(x) \\ M(x)\cdot T(x)+R(x)\cdot T(x)+N(x)\cdot V(x)+S(x)\cdot V(x) \end{pmatrix}$$

$$\begin{pmatrix} K(x)\cdot U(x)+P(x)\cdot U(x)+L(x)\cdot W(x)+Q(x)\cdot W(x) \\ M(x)\cdot U(x)+R(x)\cdot U(x)+N(x)\cdot W(x)+S(x)\cdot W(x) \end{pmatrix} = Z$$

$$\left(\begin{pmatrix} K(x) & L(x) \\ M(x) & N(x) \end{pmatrix} \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} \right) + \left(\begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} \cdot \begin{pmatrix} T(x) & U(x) \\ V(x) & W(x) \end{pmatrix} \right) =$$

$$= \begin{pmatrix} K(x)\cdot T(x)+L(x)\cdot V(x) & K(x)\cdot U(x)+L(x)\cdot W(x) \\ M(x)\cdot T(x)+N(x)\cdot V(x) & M(x)\cdot U(x)+N(x)\cdot W(x) \end{pmatrix} +$$

$$+ \begin{pmatrix} P(x)\cdot T(x)+Q(x)\cdot V(x) & P(x)\cdot U(x)+Q(x)\cdot W(x) \\ R(x)\cdot T(x)+S(x)\cdot V(x) & R(x)\cdot U(x)+S(x)\cdot W(x) \end{pmatrix} =$$

$$= \begin{pmatrix} K(x)\cdot T(x)+P(x)\cdot T(x)+L(x)\cdot V(x)+Q(x)\cdot V(x) \\ M(x)\cdot T(x)+R(x)\cdot T(x)+N(x)\cdot V(x)+S(x)\cdot V(x) \end{pmatrix}$$

$$\begin{pmatrix} K(x)\cdot U(x)+P(x)\cdot U(x)+L(x)\cdot W(x)+Q(x)\cdot W(x) \\ M(x)\cdot U(x)+R(x)\cdot U(x)+N(x)\cdot W(x)+S(x)\cdot W(x) \end{pmatrix} = Z$$

2. $\mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ has characteristic p. We know that for finite fields $\mathbb{F}_q$, where $q = p^n$ we have the characteristic p.

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \ldots + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{p \text{ summands}} = p \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

And there does not exist any number smaller than p in $\mathbb{F}_q$, for which the equation above holds.

□

Definition 2.6. A nonzero element a of a ring $\mathcal{R}$ is a *left zero divisor* if there exists a nonzero b such that $a \cdot b = 0$. Analogously an element $a \neq 0,\ a \in \mathcal{R}$ is a *right zero divisor* if $c \neq 0$ exists such that $c \cdot a = 0$. An element that is both a left and a right zero divisor is simply called a *zero divisor*.

If multiplication in a ring is commutative (such ring is called the *commutative ring*) then the left and the right zero divisors are the same.

Definition 2.7. An *integral domain* is a commutative ring with a multiplicative identity 1 (such that the additive identity $0 \neq 1$) and with no zero divisors.

Example 2.4.

- The prototypical example is the ring $(\mathbb{Z}, +, \cdot)$, but also $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are integral domains.
- $(\mathbb{Z}_p, +, \cdot)$ where p is a prime number is an integral domain. This integral domain has also the structure of a field (see the Definition 2.8.) and we denote it $(\mathbb{F}_p, +, \cdot)$, where $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$.
- The rings of polynomials are integral domains if the coefficients come from an integral domain. For instance, the ring $\mathbb{Z}[x]$ of all polynomials in one indeterminate x with integer coefficients is an integral domain.
- For each integer $d > 1$, a set of all real numbers of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ is a subring of $\mathbb{R}$ and hence an integral domain.
- For each integer $d < 0$ a set of the form $a + bz$ with $a, b \in \mathbb{Z}$ and

$$\begin{array}{ll} z = \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \\ z = \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4 \end{array}$$

  is an integral domain.
  In the case $d = -3$ we obtain the *Eisenstein integers* $a + b\frac{1+\sqrt{-3}}{2}$ and in the case $d = -1$ we have the well-known *Gaussian integers* $a + b\sqrt{-1} = a + b\mathrm{i}$.

Definition 2.8. A *field* is a nonempty set $\mathcal{F}$ together with two binary operations "$+$" : $\mathcal{F} \times \mathcal{F} \to \mathcal{F}$ and "$\cdot$" : $\mathcal{F} \times \mathcal{F} \to \mathcal{F}$, usually called the addition and the multiplication, such that the following axioms hold:

- $(\mathcal{F}, +)$ is the Abelian group with the identity element 0.
- $(\mathcal{F}^*, \cdot)$ is the group with the identity element 1 ($\mathcal{F}^*$ means $\mathcal{F} - \{0\}$).
- The multiplication is distributive over the addition.

Also more precisely $\forall\ a, b, c \in \mathcal{F}$:

1. $(a + b) + c = a + (b + c)$ (Associativity of addition)
2. $a + b = b + a$ (Commutativity of addition)
3. $\forall\ a \in \mathcal{F}\ \exists\ 0_{\mathcal{F}} \in \mathcal{F} : 0_{\mathcal{F}} + a = a$ (Additive identity)
4. $\forall\ a \in \mathcal{F}\ \exists\ -a \in \mathcal{F} : a + (-a) = 0_{\mathcal{F}}$ (Additive inverse)
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associativity of multiplication)
6. $\forall\ a \in \mathcal{F}\ \exists\ 1_{\mathcal{F}} \in \mathcal{F} : 1_{\mathcal{F}} \cdot a = a \cdot 1_{\mathcal{F}} = a$ (Multiplicative identity)
7. $\forall\ a \neq 0_{\mathcal{F}} \in \mathcal{F}\ \exists\ a^{-1} \in \mathcal{F} : a \cdot a^{-1} = a^{-1} \cdot a = 1_{\mathcal{F}}$ (Multiplicative inverse)
8. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (Left distributivity of multiplication over addition)
9. $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (Right distributivity of multiplication over addition)

All fields are rings, but not conversely. Fields differ from rings the most importantly in the existence of the multiplicative inverse. A field is also a specific type of an integral domain. A *commutative field* is a field where the commutativity of multiplication holds.

Example 2.5.

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields.
- The integral domain $(\mathbb{Z}_p, +, \cdot)$,where p is a prime number is a field and we denote it $(\mathbb{F}_p, +, \cdot)$.
- For any field $\mathcal{F}$, the set $\mathcal{F}(x)$ of rational functions in one indeterminate x with coefficients in $\mathcal{F}$ is also a field.
- $\mathcal{F} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}; \alpha, \beta \in \mathbb{Z}_3 \right\}$ (the proof is time consuming so for that we do not mention it here).

Definition 2.9. Let $\mathcal{R}$ be a ring whose elements will be called the *scalars*. A *module* over the ring $\mathcal{R}$ is a nonempty set $\mathcal{M}$ equipped with two binary operations "$+$" : $\mathcal{M} \times \mathcal{M} \to \mathcal{M}$ usually called the *vector addition* and "$\star$" : $\mathcal{R} \times \mathcal{M} \to \mathcal{M}$, usually called the *scalar multiplication* where $a \in \mathcal{R}$; $\mathbf{v}, \mathbf{w} \in \mathcal{M}$. These operations satisfy the axioms below. $\forall\ \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{M}$; $\forall\ a, b \in \mathcal{R}$:

1. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ (Associativity of vector addition)
2. $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$ (Commutativity of vector addition)
3. $\forall\ \mathbf{v} \in \mathcal{M}\ \exists\ \mathbf{o} \in \mathcal{M} : \mathbf{v} + \mathbf{o} = \mathbf{v}$ (Identity element of vector addition - zero vector $\mathbf{o}$)
4. $\forall\ \mathbf{v} \in \mathcal{M}\ \exists\ \mathbf{w} \in \mathcal{M} : \mathbf{v} + \mathbf{w} = \mathbf{o}$ (Inverse element of vector addition)
5. $\forall\ \mathbf{v} \in \mathcal{M}\ \exists\ 1_{\mathcal{R}} \in \mathcal{R} : 1_{\mathcal{R}} \star \mathbf{v} = \mathbf{v}$ (Identity element of scalar multiplication)
6. $a \star (\mathbf{v} + \mathbf{w}) = a \star \mathbf{v} + a \star \mathbf{w}$ (Left distributivity of scalar multiplication over vector addition)
7. $(a + b) \star \mathbf{v} = a \star \mathbf{v} + b \star \mathbf{v}$ (Right distributivity of scalar multiplication over field addition)
8. $a \cdot (b \star \mathbf{v}) = (a \cdot b) \star \mathbf{v}$ (Scalar multiplication is compatible with multiplication in the field of scalars)

In other words, the module is the Abelian group with the operation of scalar multiplication (with the identity element) and the distributive laws.

A *vector space* $\mathcal{V}$ over a field is a special case of the notion of module where instead of requiring the scalars to lie in a ring, the scalars may lie in an arbitrary field. So the axioms and the properties above also hold for the vector space.

Definition 2.10. Suppose that $\mathcal{F}$ is a field and $\mathcal{V}$ is a vector space over $\mathcal{F}$. Then we can express an element $\mathbf{v} \in \mathcal{V}$ as a *linear combination* of $\alpha_1, \ldots, \alpha_n \in \mathcal{V}$ if there exist such $c_1, \ldots, c_n \in \mathcal{F}$ that

$$\mathbf{v} = c_1\alpha_1 + \ldots + c_n\alpha_n.$$

We say that $\alpha_1, \ldots, \alpha_n$ are *linearly independent* if the equation

$$0 = c_1\alpha_1 + \ldots + c_n\alpha_n$$

holds only if $c_i = 0$ for $i = 1, \ldots, n$.

Definition 2.11. Let $\mathcal{V}$ be a vector space, a system $\alpha_1, \ldots, \alpha_n$ of generators of $\mathcal{V}$ is called the *basis* for $\mathcal{V}$ if it is linearly independent over the field $\mathcal{F}$. The number n is called the *dimension* of $\mathcal{V}$.

These definitions can be generalized also for the module $\mathcal{M}$ (see the Definition 4.1.).

2.2 Ring Homomorphisms

Definition 2.12. If $(\mathcal{R}, +, \cdot)$ and $(\mathcal{S}, \underline{+}, \underline{\cdot})$ are rings, then a *ring homomorphism* (hereafter a homomorphism) is a map $f : \mathcal{R} \to \mathcal{S}$ such that $\forall\ a, b \in \mathcal{R}$

- $f(a + b) = f(a) \underline{+} f(b)$
- $f(a \cdot b) = f(a) \underline{\cdot} f(b)$
- $f(1_{\mathcal{R}}) = 1_{\mathcal{S}}$

Definition 2.13. The map $f : \mathcal{R} \to \mathcal{S}$ is *injective* if $\forall\ a, b \in \mathcal{R}$ the equality $f(a) = f(b)$ implies $a = b$. The mapping $f : \mathcal{R} \to \mathcal{S}$ is said to be *surjective* if for every $b \in \mathcal{S}$ there is at least one $a \in \mathcal{R}$ such that $f(a) = b$. We say that the map is *bijective* if it is both injective and surjective.

Definition 2.14. Let $\mathcal{R}$ and $\mathcal{S}$ be rings and let f be a homomorphism from $\mathcal{R}$ to $\mathcal{S}$. The *kernel* of f is defined by

$$\ker f = \{a \in \mathcal{R} : f(a) = 0_{\mathcal{S}}\}.$$

The $\ker f$ is a subset of $\mathcal{R}$ whose elements are mapped to zero by the homomorphism f. The related image of the homomorphism is defined by $\mathrm{Im}(f) = \{f(a) : a \in \mathcal{R}\}$ and $\mathrm{Im}(f)$ is therefore a subset of $\mathcal{S}$.

Theorem 2.2. The homomorphism f is injective if and only if its kernel is only the singleton set $\{0_{\mathcal{R}}\}$.

Proof. We must prove that $\ker f = \{0_{\mathcal{R}}\} \Leftrightarrow f$ is injective.

1. $\ker f = \{0_{\mathcal{R}}\} \Rightarrow f$ is injective:
   $\ker f = \{0_{\mathcal{R}}\}$, this means that only for $a = 0_{\mathcal{R}}$ is $f(a) = 0_{\mathcal{S}}$. We may see that $\forall\ b, c \in \mathcal{R}\ \ f(b) = f(c) \Rightarrow b = c$.
   $f(b) = f(c) \Rightarrow f(b) - f(c) = 0_{\mathcal{S}} \Rightarrow f(b - c) = 0_{\mathcal{S}} \Rightarrow b - c = 0_{\mathcal{R}} \Rightarrow b = c \Rightarrow$ it is injective. Indeed it holds $f(0_{\mathcal{R}}) = 0_{\mathcal{S}}$ otherwise it is not possible to satisfy $f(a + 0_{\mathcal{R}}) = f(a) + f(0_{\mathcal{R}})$.

2. f is injective $\Rightarrow \ker f = \{0_{\mathcal{R}}\}$:
   $f(a) = f(b) = 0_{\mathcal{S}} \Rightarrow a = b = 0_{\mathcal{R}} \Rightarrow \ker f = \{0_{\mathcal{R}}\}$

□

Definition 2.15. Let $\mathcal{R}$, $\mathcal{S}$, $\mathcal{T}$ be rings and we denote a *composition* of mappings by "$\circ$". The homomorphisms $f : \mathcal{R} \to \mathcal{S}$ and $g : \mathcal{S} \to \mathcal{T}$ can be composed by first applying f to an argument $a \in \mathcal{R}$ and then applying g to the result. Thus one obtains the map $g \circ f : \mathcal{R} \to \mathcal{T}$ defined by $(g \circ f)(a) = g(f(a)),\ \forall\ a \in \mathcal{R}$.

Theorem 2.3. The composition of the maps is an associative operation.

Proof. Let $\mathcal{R}$, $\mathcal{S}$, $\mathcal{T}$, $\mathcal{U}$ be sets and f, g, h be the mappings: $f : \mathcal{R} \to \mathcal{S}$, $g : \mathcal{S} \to \mathcal{T}$, $h : \mathcal{T} \to \mathcal{U}$. $(r, s) \in (\mathcal{R} \to \mathcal{S})$ denotes $(r, s) \in \mathcal{R} \times \mathcal{S}, r \in \mathcal{R}, s \in \mathcal{S}$. So it must be proven $h \circ (g \circ f) = (h \circ g) \circ f$ which can be also denoted $(fg)h = f(gh)$.

Let $(r, u) \in (\mathcal{R} \to \mathcal{U})$ be an arbitrary element. Then $(r, u) \in (fg)h \Leftrightarrow \exists\, t \in \mathcal{T} : (r, t) \in fg$ and $(t, u) \in h \Leftrightarrow \exists\ t \in \mathcal{T}$ and $\exists\ s \in \mathcal{S} : (r, s) \in f, (s, t) \in g$ and $(t, u) \in h \Leftrightarrow \exists\ s \in \mathcal{S} :$ $(r, s) \in f$ and $(s, u) \in gh \Leftrightarrow (r, u) \in f(gh)$. So $(fg)h = f(gh) \Rightarrow h \circ (g \circ f) = (h \circ g) \circ f$.

□

Definition 2.16. Let $\mathcal{R}$ be a ring, the *identity homomorphism* f on $\mathcal{R}$ is defined $f\ :\ \mathcal{R} \to \mathcal{R}$ and satisfies

$$f(a) = a,\ a \in \mathcal{R}.$$

The identity map f on $\mathcal{R}$ is often denoted by $id_{\mathcal{R}}$.

Definition 2.17. An *isomorphism* is a bijective homomorphism. In other words $f\ :$ $\mathcal{R} \to \mathcal{S}$ is called an isomorphism if there exists a homomorphism $g : \mathcal{S} \to \mathcal{R}$ such that $g \circ f = id_{\mathcal{R}}$ and $f \circ g = id_{\mathcal{S}}$.

Definition 2.18. An *endomorphism* is a homomorphism from the ring to itself.

Theorem 2.4. The set of all endomorphisms of some ring $\mathcal{R}$ with the operation of composition forms a monoid and is denoted $(\mathrm{End}(\mathcal{R}), \circ)$.

Proof. $(\mathrm{End}(\mathcal{R}), \circ)$ is a monoid. This means that the composition of any two endomorphisms of $\mathcal{R}$ is closed over $\mathcal{R}$, is associative and has an identity element. Let $a, b \in \mathcal{R}$ and $f, g, h \in \mathrm{End}(\mathcal{R})$.

1. $(g \circ f)(a+b) = g(f(a+b)) = g(f(a)+f(b)) = g(f(a)) \pm g(f(b)) = (g \circ f)(a) \pm (\ g \circ f)\ (\ b\ )$
2. $(g \circ f)(a \cdot b) = g(f(a \cdot b)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b)$
3. The identity element 1: from the Definition 2.12. it follows that $f(1_{\mathcal{R}}) = g(1_{\mathcal{R}}) = h(1_{\mathcal{R}}) = 1_{\mathcal{R}}$.
4. The composition is associative: this was already proven (see the Theorem 2.3.).

□

If we consider all endomorphisms of the ring $\mathcal{R}$ with the addition by elements and the composition, we obtain $(\mathrm{End}(\mathcal{R}), +, \circ))$ which is the ring.

Definition 2.19. An *automorphism* is an endomorphism which is also an isomorphism.

2.3 Frobenius Endomorphism over Fields

Definition 2.20. Let $\mathcal{F}$ be a field of positive and prime characteristic p, we consider here the fields $\mathbb{F}_q = \mathbb{F}_{p^n},\ n \in \mathbb{N}$ or $\overline{\mathbb{F}}_q$ (see the Theorem 3.7.). A *Frobenius endomorphism* $\phi : \mathcal{F} \to \mathcal{F}$ is defined by $\phi(a) = a^p,\ \forall\ a \in \mathcal{F}$.

Theorem 2.5. The Frobenius endomorphism respects the multiplication but also the addition of $\mathcal{F}$. $\forall\ a, b \in \mathcal{F}$:

1. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ so $\phi(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p$
2. $\phi(1) = 1$
3. $\phi(a + b) = \phi(a) + \phi(b)$ so $\phi(a + b) = (a + b)^p = a^p + b^p$

Proof. $(a + b)^p$ can be expanded by using the binomial theorem:

$$\phi(a+b) = (a+b)^p = a^p + \binom{p}{1}a^{p-1}b \cdot \ldots \cdot \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p = \phi a + \phi b,$$

because for the fields of the characteristic p it holds $\binom{p}{1} = \ldots = \binom{p}{p-1} = 0$.

□

Theorem 2.6. *Fermat's little theorem.* If p is a prime and a is an integer coprime to p (so $\gcd(a, p) = 1$) then $a^{p-1} - 1$ will be evenly divisible by p. In the notation of modular arithmetic

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. The idea is to recognize that the set $\mathcal{G} = \{1, 2, \ldots, p-1\}$, with the operation of the multiplication (taken modulo p) forms the group. Let us assume that a is in the range $1 \leq a \leq p-1$ that is $a \in \mathcal{G}$. Let k be the order of a so that $a^k \equiv 1 \pmod{p}$. By Lagrange's theorem k divides the order of $\mathcal{G}$, which is $p-1$, so $p-1 = km$ for some positive integer m. Then

$$a^{p-1} \equiv a^{km} \equiv (a^k)^m \equiv 1^m \equiv 1 \pmod{p}.$$

□

Definition 2.21. Say $\mathcal{F}$ is a field. The Frobenius map *fixes* all the elements $a \in \mathcal{F}$ which satisfy the equation $a^p = a$.

Example 2.6. For finite fields $\mathbb{F}_p$, p-prime the outgrowth from the Fermat's little theorem is the property

$$a^p = a,\ \forall a \in \mathbb{F}_p.$$

These are all the roots of the equation $a^p - a = 0$ and since this equation has degree p there are at most p roots. These are exactly the elements $\{0, 1, 2, ..., p-1\}$ so the $\mathbb{F}_p$ is a *fixed point set.*

Iterating the Frobenius map $\phi^n : \mathcal{F} \to \mathcal{F}$ we have $\phi^n(a) = a^{p^n}$ which gives us a sequence of elements in $\mathcal{F}$: $a, a^p, a^{p^2}, a^{p^3}, \ldots$.

Example 2.7. It was proven above that the set $\mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ is a ring with the characteristic p (see Example 2.3.).

Let us have the Frobenius endomorphism $\varphi : \mathcal{M}_{2\times 2}(\mathbb{F}_q[x]) \to \mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ assigning $A \in \mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ a matrix $A^p \in \mathcal{M}_{2\times 2}(\mathbb{F}_q[x])$ that is $\varphi(A) = A^p$, where

$$A = \begin{pmatrix} P(x) & Q(x) \\ R(x) & S(x) \end{pmatrix} = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$$

Now we will search the fixed points for the special case of the finite field - for $\mathbb{F}_q = \mathbb{F}_2$. Let $P(x) = P$, $Q(x) = Q$, $R(x) = R$, $S(x) = S$ be the polynomials of the maximal degree 1 lying in $\mathbb{F}_2[x]$ (that is the polynomials of the form $a_0 + a_1x,\ a_0, a_1 \in \{0; 1\}$). Then Frobenius endomorphism is

$$A^2 = \begin{pmatrix} P^2 + QR & PQ + QS \\ RP + SR & RQ + S^2 \end{pmatrix} = A \Leftrightarrow \begin{array}{ll} P^2 + QR = P, & PQ + QS = Q \\ RP + SR = R, & RQ + S^2 = S \end{array}$$

From these four equations, when also the Fermat's little theorem has been used, we obtain:

$QR = 0$
$Q(P + S + 1) = 0$
$R(P + S + 1) = 0$

The solution is the following:

1. $Q = 0$, $R = 0$, P, S are arbitrary
2. $Q = 0$, $R \neq 0$, $P + S = 1$
3. $Q \neq 0$, $R = 0$, $P + S = 1$

The cardinality of the set of all matrices A is $4^4 = 256$. We obtained 40 fixed points. In the following table there are all fixed points of the Frobenius endomorphism for this example:

P	0	0	0	0	1	1	1	1
Q	0	0	0	0	0	0	0	0
R	0	0	0	1	0	0	0	0
S	0	1	x	$x+1$	0	1	x	$x+1$
P	x	x	x	x	$x+1$	$x+1$	$x+1$	$x+1$
Q	0	0	0	0	0	0	0	0
R	0	0	0	0	0	0	0	0
S	0	1	x	$x+1$	0	1	x	$x+1$
P	0	1	x	$x+1$	0	1	x	$x+1$
Q	0	0	0	0	0	0	0	0
R	1	1	1	1	x	x	x	x
S	1	0	$x+1$	x	1	0	$x+1$	x

P	0	1	x	$x+1$	0	1	x	$x+1$
Q	0	0	0	0	1	1	1	1
R	$x+1$	$x+1$	$x+1$	$x+1$	0	0	0	0
S	1	0	$x+1$	x	1	0	$x+1$	x

P	0	1	x	$x+1$	0	1	x	$x+1$
Q	x	x	x	x	$x+1$	$x+1$	$x+1$	$x+1$
R	0	0	0	0	0	0	0	0
S	1	0	$x+1$	x	1	0	$x+1$	x

3 Field Extension

Definition 3.1. Let $\mathcal{L}$ be a field. If $\mathcal{K}$ is a subset of $\mathcal{L}$ which is closed with respect to the field operations of the addition and the multiplication in $\mathcal{L}$ and the additive and the multiplicative inverses of every element in $\mathcal{K}$ lie in $\mathcal{K}$, then we say that $\mathcal{K}$ is a *subfield* of $\mathcal{L}$ and that $\mathcal{L}$ is an *extension field* of $\mathcal{K}$. $\mathcal{L}/\mathcal{K}$ read as "$\mathcal{L}$ over $\mathcal{K}$" is a *field extension.*

One of the properties of the field extension $\mathcal{L}/\mathcal{K}$ is that $\mathcal{L}$ and $\mathcal{K}$ share the same additive identity 0 and the same multiplicative identity 1. The additive group $(\mathcal{K}, +)$ is the subgroup of $(\mathcal{L}, +)$ and the multiplicative group $(\mathcal{K}^*, \cdot)$ is the subgroup of $(\mathcal{L}^*, \cdot)$.

Theorem 3.1. The set $\mathcal{L}$ can also be considered as the vector space over $\mathcal{K}$. The elements of $\mathcal{L}$ are the "vectors" and the elements of $\mathcal{K}$ are the "scalars".

Definition 3.2. The dimension of this vector space is called the *degree of the field extension*, and is denoted by $[\mathcal{L} : \mathcal{K}]$.

Proof. Let $\mathcal{L}/\mathcal{K}$ be a field extension. We can write $\mathcal{L} = \mathcal{K} + \mathcal{F};\ \mathcal{F} = \{\alpha_1, \ldots, \alpha_{n-1}\}$. So every element $a \in \mathcal{L}$ can be represented as a linear combination $a = c_1 \cdot 1 + c_2 \cdot \alpha_1 + \ldots + c_n \cdot \alpha_{n-1};\ c_1, \ldots, c_n \in \mathcal{K}$. These elements form the vector space. The basis is the set $\mathcal{B} = \{1, \alpha_1, \ldots, \alpha_{n-1}\}$ and the dimension of the vector space is $dim\ \mathcal{L} = |\mathcal{B}| = n$ so the dimension of the algebraic extension is $[\mathcal{L} : \mathcal{K}] = n$. The identity element of the vector addition is $a = 0$ and the identity element of the scalar multiplication is $1 \in \mathcal{K}$.

□

Definition 3.3. If $\mathcal{M}$ is an extension of $\mathcal{L}$ which is in turn an extension of $\mathcal{K}$, then we say $\mathcal{L}$ is a *subextension* of the field extension $\mathcal{M}/\mathcal{K}$.

3.1 Degree of Field Extension

Suppose that $\mathcal{L}/\mathcal{K}$ is a field extension. As it was said above, the dimension of the vector space $\mathcal{L}$ is denoted as the degree of the extension and we mark it $[\mathcal{L} : \mathcal{K}]$. We recognize these types of the degree of the extension:

- the finite degree
  - $[\mathcal{L} : \mathcal{K}] = 1$ is called the *trivial extension* ($\mathcal{L}$ is equal to $\mathcal{K}$)

    Proof. We must prove the equivalence $[\mathcal{L} : \mathcal{K}] = 1 \Leftrightarrow \mathcal{L} = \mathcal{K}$

    1. $[\mathcal{L} : \mathcal{K}] = 1 \Rightarrow \mathcal{L} = \mathcal{K}$:
       The basis is the singleton set $\mathcal{B} = \{1\}$, so we can't construct the elements $a \in \mathcal{L}$ as the linear combination (the basis $\mathcal{B}$ is linearly dependent) $\Rightarrow$ $\mathcal{L} = \mathcal{K} + \mathcal{F};\ \mathcal{F} = \emptyset \Rightarrow \mathcal{L} = \mathcal{K}$
    2. $\mathcal{L} = \mathcal{K} \Rightarrow [\mathcal{L} : \mathcal{K}] = 1$:
       $\mathcal{L} = \mathcal{K} + \mathcal{F};\ \mathcal{F} = \emptyset \Rightarrow$ the basis is only the singleton set $\mathcal{B} = \{1\} \Rightarrow$ $dim\ \mathcal{L} = |\mathcal{B}| = 1 \Rightarrow [\mathcal{L} : \mathcal{K}] = 1$

    □

  - $[\mathcal{L} : \mathcal{K}] = 2$ is called the *quadratic extension*

  - $[\mathcal{L} : \mathcal{K}] = 3$ is called the *cubic extension*
  - ...

- the infinite degree

3.2 Some Types of Field Extensions

Definition 3.4. Let $\mathcal{L}$ be a field extension of a field $\mathcal{K}$. Given a set A of elements lying in $\mathcal{L} - \mathcal{K}$, we denote by $\mathcal{K}(A)$ the smallest subextension which contains the elements of A. We say $\mathcal{K}(A)$ is constructed by *adjunction* of the elements of A to $\mathcal{K}$ or generated by A. If A is finite we say $\mathcal{K}(A)$ is *finitely generated*. For finite extensions $A = \{a_0, \ldots, a_n\}$ we often write $\mathcal{K}(a_0, \ldots, a_n)$ instead of $\mathcal{K}(\{a_0, \ldots, a_n\})$.

Definition 3.5. A field extension $\mathcal{L}/\mathcal{K}$ is called the *simple extension* if there exists a singleton set $A = \{a\}$ in $\mathcal{L}$ with $\mathcal{L} = \mathcal{K}(a)$. In other words the simple extension is the field extension which is generated by the adjunction of a single element a which is named a *primitive element*. We also say that $\mathcal{L}$ is generated over $\mathcal{K}$ by a. The primitive element of the finite field $\mathcal{L}$ is the generator of the field's multiplicative group $(\mathcal{L}, \cdot)$.

The statement that the field extension $\mathcal{L}/\mathcal{K}$ of finite degree n has the primitive element a means that extension $\mathcal{L}/\mathcal{K}$ is generated by the single element a satisfying the polynomial equation of degree n: $a^n + c_1 a^{n-1} + \ldots + c_n = 0$, with coefficients in $\mathcal{K}$. The primitive element a provides a *power basis* $\{1, a, a^2, \ldots, a^{n-1}\}$ for $\mathcal{L}$ over $\mathcal{K}$.

Theorem 3.2. *Primitive Element Theorem.* A field extension $\mathcal{M}/\mathcal{K}$ is finite and has a primitive element if and only if there are only finitely many intermediate fields $\mathcal{L}_i$, $i = 1, \ldots s$, with $\mathcal{K} \subseteq \mathcal{L}_i \subseteq \mathcal{M}$.

Definition 3.6. Let $\mathcal{L}/\mathcal{K}$ be a field extension. An element $a \in \mathcal{L}$ is called an *algebraic element* over $\mathcal{K}$ if there exists some non-zero polynomial $P(x)$ with coefficients in $\mathcal{K}$ such that $P(a) = 0$. Elements $a \in \mathcal{L}$ which are not algebraic over $\mathcal{K}$, i.e. which are not roots of any polynomial $P(x)$ with coefficients in $\mathcal{K}$ so that $P(a) \neq 0$, are called *transcendental* over $\mathcal{K}$.

Definition 3.7. If every element of $\mathcal{L}$ is algebraic over $\mathcal{K}$, then the extension $\mathcal{L}/\mathcal{K}$ is said to be an *algebraic extension*. The field extensions which contain some transcendental elements are called *transcendental extensions*. The field extension $\mathcal{L}/\mathcal{K}$ is *purely transcendental* if there is a subset A of $\mathcal{L}$ for which $\mathcal{L} = \mathcal{K}(A)$ and where the elements of A do not satisfy any non-trivial polynomial equation with the coefficients in $\mathcal{K}$.

Theorem 3.3. All transcendental extensions are of infinite degree.

Proof. Let us have the field $\mathcal{L}$, which is the finite extension of the field $\mathcal{K}$. The degree of the field extension is $[\mathcal{L} : \mathcal{K}] = n$. We take a as an arbitrary element of the field extension $\mathcal{L}$ of $\mathcal{K}$ so the elements $\underbrace{1, a, \ldots, a^n}_{n+1}$ are linearly dependent over $\mathcal{K}$. Then for $c_i = 0,\ i = 0, \ldots, n$ we have $c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n = 0$. This means that a is a root of the polynomial $c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n$ so a is algebraic. It follows that no

transcendental element can come from the field extension of the finite degree.

□

All finite extensions are algebraic but not conversely - there exists also an infinite algebraic extension, for example the algebraic number field (see the Example 3.1.).

Definition 3.8. An extension $\mathcal{L}$ of the field $\mathcal{K}$ is called *algebraically generated* if it is generated by some finite system of numbers algebraic over the field $\mathcal{K}$, that is if there exist numbers $a_1, \ldots, a_n$ algebraic over the field $\mathcal{K}$ such that $\mathcal{L} = \mathcal{K}(a_1, \ldots, a_n)$. If in particular $n = 1$, then the field $\mathcal{L} = \mathcal{K}(a_1)$ is called the *simple algebraic extension* of the field $\mathcal{K}$.

Definition 3.9. An extension $\mathcal{M}$ of a field $\mathcal{K}$ is called the *composite algebraic extension* if there exists a chain of subfields

$$\mathcal{K} = \mathcal{L}_0 \subseteq \mathcal{L}_1 \subseteq \ldots \subseteq \mathcal{L}_{s-1} \subseteq \mathcal{L}_s = \mathcal{M},$$

such that for any $i = 1, \ldots, s$ the field $\mathcal{L}_i$ is a simple algebraic extension of the field $\mathcal{L}_{i-1}$. If $\mathcal{L}_i = \mathcal{L}_{i-1}(a_i)$, $i = 1, \ldots, s$, then the field $\mathcal{M}$ is denoted by $\mathcal{K}(a_1)(a_2)\ldots(a_s)$.

Theorem 3.4. Let us have a field extension $\mathcal{L}/\mathcal{K}$. Then the following properties of this field extension are equivalent:

(a) The field extension is a finite extension.

(b) The field extension is a composite algebraic extension.

(c) The field extension is a algebraically generated extension.

(d) The field extension is a simple algebraic extension.

Proof. We can find this proof in [5].

Theorem 3.5. Let $\mathcal{L}$ be a finite extension of the field $\mathcal{K}$ and let $\mathcal{M}$ be a finite extension of the field $\mathcal{L}$ so

$$\mathcal{K} \subseteq \mathcal{L} \subseteq \mathcal{M}.$$

We denote $m = [\mathcal{L} : \mathcal{K}]$, $n = [\mathcal{M} : \mathcal{L}]$. Then $m \cdot n = [\mathcal{M} : \mathcal{K}]$ holds.

Proof. Let $\alpha_1, \ldots, \alpha_m$ be a basis of the field $\mathcal{L}$ and $\beta_1, \ldots, \beta_n$ be a basis of the field $\mathcal{M}$. In fact any element b of the field $\mathcal{M}$ is a linear combination of the elements $\beta_1, \ldots, \beta_n$ with coefficients from the field $\mathcal{L}$: $b = a_1\beta_1 + \ldots + a_n\beta_n$ where $a_1, \ldots, a_n \in \mathcal{L}$. On the other hand, for any $j = 1, \ldots, n$ the element a_j is a linear combination of the elements $\alpha_1, \ldots, \alpha_m$ with coefficients from the field $\mathcal{K}$: $a_j = c_{1j}\alpha_1 + \ldots + c_{mj}\alpha_m$ where $c_{1j}, \ldots, c_{mj} \in \mathcal{K}$. Substituting these expressions we obtain

$$b = \sum_{j=1}^{n} \sum_{i=1}^{m} c_{ij}\alpha_i\beta_j.$$

Thus, any element of the field $\mathcal{M}$ is a linear combination of elements of the form $\alpha_i\beta_j$ with coefficients from the field $\mathcal{K}$.

Now suppose that in the field $\mathcal{K}$ there exist elements k_{ij} such that

$$\sum_{j=1}^{n}\sum_{i=1}^{m} k_{ij}\alpha_i\beta_j = 0.$$

For any $j = 1, \ldots, n$ we shall set

$$a_j = \sum_{i=1}^{m} k_{ij}\alpha_i.$$

The elements $a_1, \ldots, a_n \in \mathcal{L}$ and satisfy the relation $a_1\beta_1 + \ldots, a_n\beta_n = 0$. Because the elements $\beta_1, \ldots, \beta_n$ form a basis of the field $\mathcal{M}$, it follows $a_1 = \ldots = a_n = 0$. Thus for any $j = 1, \ldots, n$ it holds

$$\sum_{i=1}^{m} k_{ij}\alpha_i = 0.$$

Hence, since the elements $\alpha_1, \ldots, \alpha_m$ form a basis of the field $\mathcal{L}$, then $k_{ij} = 0 \ \forall \ i, j$. Thus it is proved that the system of elements $\alpha_i\beta_j$ is linearly independent and it follows that $\mathcal{M}$ is a finite extension of the field $\mathcal{K}$ and its degree is equal to mn.

□

We can also generalize this relation:

Theorem 3.6. If

$$\mathcal{K} = \mathcal{L}_0 \subseteq \mathcal{L}_1 \subseteq \ldots \subseteq \mathcal{L}_{i-1} \subseteq \mathcal{L}_i \subseteq \ldots \subseteq \mathcal{L}_s = \mathcal{M},$$

where for any $i = 1, \ldots, s$ the field $\mathcal{L}_i$ is a finite extension of the field $\mathcal{L}_{i-1}$, then the field $\mathcal{M}$ is a finite extension of the field $\mathcal{K}$ and

$$[\mathcal{M} : \mathcal{K}] = [\mathcal{M} : \mathcal{L}_{s-1}] \cdot \ldots \cdot [\mathcal{L}_i : \mathcal{L}_{i-1}] \cdot \ldots \cdot [\mathcal{L}_1 : \mathcal{K}].$$

Proof. We can find this proof in [5].

Example 3.1. Let us have a set $\mathcal{K}(A)$ which is constructed by adjunction of the elements of the set A to the field $\mathcal{K}$. More concretely let $\mathcal{K} = \mathbb{Q}$ and $A = \{\sqrt{n};\ n \in \mathbb{N}\}$. So we can write $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n}; a, b \in \mathbb{Q}\},\ n \in \mathbb{N}$. This field extension is infinite because the set A is infinite and so the basis $\{1, \sqrt{2}, \sqrt{3}, \ldots\}$ is also infinite. This field extension is algebraic.

3.3 Algebraic Closure

Definition 3.10. Let us consider the ring $\mathcal{K}[x]$ of polynomials in one indeterminate x over the field $\mathcal{K}$. If we can express the nonconstant polynomial $P \in \mathcal{K}[x]$ as

$$P = \prod_{i=1}^{\deg P} (x - p_i)$$

where p_i are roots of the P, we say that P is *fully reducible* in $\mathcal{K}[x]$.

Theorem 3.7. *Steinitz Theorem.* For every field $\mathcal{K}$ there exists an algebraic extension $\mathcal{L}$ such that every polynomial $P \in \mathcal{K}[x]$ is fully reducible in $\mathcal{L}[x]$ and $\mathcal{L}$ is the least field with this property. We say that $\mathcal{L}$ is the *algebraic closure of* $\mathcal{K}$ and we denote it $\mathcal{L} = \overline{\mathcal{K}}$. The field for which $\mathcal{K} = \overline{\mathcal{K}}$ is called *algebraically closed.*

3.4 Examples of Field Extension

- The field of complex numbers $\mathbb{C}$, which is the algebraically closed field, real numbers $\mathbb{R}$ and rational numbers $\mathbb{Q}$:
  $\mathbb{C}/\mathbb{R}$ $[\mathbb{C} : \mathbb{R}] = 2$, the basis is $\{1, i\}$, the extension is finite, simple ($\mathbb{C} = \mathbb{R}(i)$) and algebraic (all polynomials over $\mathbb{R}$ have roots in $\mathbb{C}$)
  $\mathbb{C}/\mathbb{Q}$ $[\mathbb{C} : \mathbb{Q}] = c$, the extension is infinite and transcendental (the transcendental numbers are for example e, π, i)
  $\mathbb{R}/\mathbb{Q}$ $[\mathbb{R} : \mathbb{Q}] = c$, the extension is infinite and transcendental (the transcendental numbers are for instance $\mathrm{e}, \pi, 2^{\sqrt{2}}$)

- The extension of the field of rational numbers $\mathbb{Q}$:
  Algebraic number field (see the Definition 3.11.):
  $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3};\ a, b \in \mathbb{Q}\}$ $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, the basis is $\{1, \sqrt{3}\}$, the extension is finite, simple and algebraic

- The finite field $\mathbb{F}_p$, where p is a prime number and $n \in \mathbb{N}$:
  $\mathbb{F}_{p^n}/\mathbb{F}_p$ $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, the basis is $\{1, p, p^2, \ldots, p^{n-1}\}$, the extension is finite and algebraic

  Proof. We show that the basis of the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is $\{1, p, p^2, \ldots, p^{n-1}\}$. The elements of the fields are following: $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, $\mathbb{F}_{p^n} = \{0, 1, \ldots, p^n - 1\}$. We can construct all elements of this extension as the linear combination $a = c_1 \cdot 1 + c_2 \cdot p + \ldots + c_n \cdot p^{n-1}$ where $c_1, \ldots, c_n \in \mathbb{F}_p$ and $a \in \mathbb{F}_{p^n}$. After constructing all possible combination we obtain p^n elements which are all elements of $\mathbb{F}_{p^n}$.
  $0 \cdot 1 + 0 \cdot p + 0 \cdot p^2 + \ldots + 0 \cdot p^{n-1} = 0 \in \mathbb{F}_{p^n}$
  $\vdots$
  $(p-1)\cdot 1 + (p-1)\cdot p + (p-1)\cdot p^2 + \ldots + (p-1)\cdot p^{n-1} = p - 1 + p^2 - p + p^3 - p^2 + \ldots + p^{n-1} = p^n - 1 \in \mathbb{F}_{p^n}$

  □

- Let us consider the polynomial $x^2 + x + 1$ over the finite field $\mathbb{F}_2$. This polynomial is irreducible over $\mathbb{F}_2$. If we denote its root j, we have the extension of $\mathbb{F}_2$, which has four elements $0, 1, j, j + 1$ and is isomorphic with the field $\mathbb{F}_4$. But this polynomial is irreducible also over $\mathbb{F}_4$ so we have an infinite series of extensions

  $$\mathbb{F}_2 \subseteq \mathbb{F}_4 \subseteq \mathbb{F}_8 \subseteq \mathbb{F}_{16} \subseteq \ldots,$$

  whereas all fields are not algebraically closed, but they have the same algebraic closure, so

  $$\overline{\mathbb{F}}_2 = \overline{\mathbb{F}}_4 = \overline{\mathbb{F}}_8 = \overline{\mathbb{F}}_{16} = \ldots.$$

- Algebraic closure $\overline{\mathbb{F}}_q$ of the finite field $\mathbb{F}_q$ is infinite. $\overline{\mathbb{F}}_q = \overline{\mathbb{F}}_{p^n},\ n \in \mathbb{N}$ is the field of characteristic p and cardinality $\aleph_0$.

3.5 Algebraic Number Field

Definition 3.11. An *algebraic number field* $\mathcal{L}$ is a finite algebraic field extension of the field of rational numbers $\mathbb{Q}$. Thus $\mathcal{L}$ is the field that contains $\mathbb{Q}$ and it can be considered as a vector space over $\mathbb{Q}$ with finite dimension.

Definition 3.12. An *algebraic integer* is an element a of the algebraic number field $\mathcal{L}$ which is the root of a monic polynomial (a polynomial in which the coefficient of the highest order term is 1) with integer coefficients.

The algebraic integers in $\mathcal{L}$ form a *ring of integers* denoted by $\mathcal{O}_\mathcal{L}$ which contains no zero divisors. Therefore the ring of integers of $\mathcal{L}$ is an integral domain. The property of being an algebraic integer is independent of the choice of the basis in $\mathcal{L}$.

Definition 3.13. An *integral basis* for a number field $\mathcal{L}$ of degree n is a set $\beta = \{\alpha_1, \ldots, \alpha_n\}$ of n algebraic integers in $\mathcal{L}$ such that every element of the ring of integers $\mathcal{O}_\mathcal{L}$ of $\mathcal{L}$ can be written uniquely as a linear combination of elements of β, that is $\forall\ a \in \mathcal{O}_\mathcal{L}$ we have $a = c_1\alpha_1 + \cdots + c_n\alpha_n$ where the c_i are integers. There exists also the case that any element $b \in \mathcal{L}$ can be written uniquely as $b = c_1\alpha_1 + \cdots + c_n\alpha_n$ where now the c_i are rational numbers.

A *discriminant* of an algebraic number field is an important numerical invariant. The definition follows.

Definition 3.14. Let $\mathcal{L}$ be an algebraic number field, and let $\mathcal{O}_\mathcal{L}$ be its ring of integers. Let $\alpha_1, \ldots, \alpha_n$ be the integral basis of $\mathcal{O}_\mathcal{L}$ and let $\{f_1, \ldots, f_n\}$ be the ring of homomorphisms $\mathcal{L} \to \mathbb{C}$. The discriminant of $\mathcal{L}$ is the square of the determinant of the n by n matrix M whose (i, j)-entry is $f_i(\alpha_j)$. Symbolically

$$\Delta_\mathcal{L} = \det \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & \cdots & f_1(\alpha_n) \\ f_2(\alpha_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ f_n(\alpha_1) & \cdots & \cdots & f_n(\alpha_n) \end{pmatrix}^2$$

Among considerable theorems which are related to the discriminant, the following ones belong:

1. *Stickelberger's Theorem*: $\Delta_\mathcal{L} \equiv 0$ or $1 \pmod 4$
2. *Minkowski bound*: Let n denote the degree of the extension $\mathcal{L}/\mathbb{Q}$ then
$$|\Delta_\mathcal{L}|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$
3. *Minkowski's Theorem*: If $\mathcal{L}$ is not $\mathbb{Q}$ then $|\Delta_\mathcal{L}| > 1$ (this follows directly from the Minkowski bound).
4. *Hermite's Theorem*: Let N be a positive integer. There are only finitely many algebraic number fields $\mathcal{L}$ with $\Delta_\mathcal{L} < N$.

3.6 Quadratic Field

Definition 3.15. A *quadratic field* is an algebraic number field $\mathcal{L}$ of degree two over $\mathbb{Q}$.

The map $d \to \mathbb{Q}(\sqrt{d})$ where $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d};\ a, b \in \mathbb{Q},\ d \in \mathbb{Z}\}$ is a bijection from the set of all square-free integers d to the set of all quadratic fields. If $d > 0$ the corresponding quadratic field is called the *real quadratic field*, and for $d < 0$ the *imaginary quadratic field*.

The discriminant of the quadratic field $Q(\sqrt{d})$ is:

$$\Delta_{\mathcal{L}} = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \equiv 2, 3 \bmod 4 \end{cases}$$

4 Full Modul and Order

As mentioned before a module is a generalization of a vector space, where the scalars lie in an arbitrary ring. We can also generalize some other concepts, for instance the basis of the vector space. However the basis of the module is not uniquely given so we must consider some restrictions.

Definition 4.1. A system of generators $\alpha_1, \alpha_2 \ldots, \alpha_n$ of the module $\mathcal{M}$ is called the *basis* for $\mathcal{M}$ if it is linearly independent over the ring of integers, that is if the equation

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n = 0, \ (c_i \in \mathbb{Z})$$

holds only when all c_i are zero.
Any $\mathbf{v} \in \mathcal{M}$ has a unique representation in the form $c_1\alpha_1+c_2\alpha_2+\ldots+c_n\alpha_n = \mathbf{v}, \ (c_i \in \mathbb{Z})$.

Definition 4.2. Let $\mathcal{L}$ be an algebraic number field of degree n. Let $\mathcal{M}$ be a module in $\mathcal{L}$. If $\mathcal{M}$ contains n linearly independent elements (over the field of rational numbers), then it is called the *full module*, otherwise the *non-full module*.

The number of elements n in any base of the module $\mathcal{M}$ is called the *rank* of the module $\mathcal{M}$. If the degree of the field $\mathcal{L}$ is equal to n, then the rank of the module does not exceed n and the rank of the full module is equal to n.

Definition 4.3. A full module in the field of algebraic numbers $\mathcal{L}$ which contains the number 1 and is a ring is called the *order* of the field $\mathcal{L}$.

Definition 4.4. The *maximal order* of the algebraic number field $\mathcal{L}$ is such order that all other orders in $\mathcal{L}$ are contained in it.

A basic result on orders states that the ring of integers $\mathcal{O}_\mathcal{L}$ in $\mathcal{L}$ is the unique maximal order.

All bases of the full module have the same discriminant - the *discriminant of the module* $\mathcal{M}$. Every order of the field $\mathcal{L}$ is a full module in $\mathcal{L}$, then we may also speak of the *discriminant of an order*.

A basis of the maximal order of the algebraic number field $\mathcal{L}$ is frequently called the *fundamental basis of* $\mathcal{L}$ and its discriminant is called the *discriminant of the field* $\mathcal{L}$.

5 Quadratic Residues

Definition 5.1. A nonzero integer a is called the *quadratic residue* modulo n if there is an integer $0 < y < n$ such that

$$y^2 \equiv a \pmod{n}.$$

Otherwise, this nonzero a is called the *quadratic non-residue* mod n. For $a = 0$ we obtain the trivial case $y = 0$.

For the notation whether the number is the quadratic residue or not we use the following signification.

Definition 5.2. For integer a and positive odd prime p the *Legendre symbol* $(\frac{a}{p})$ is defined by:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is the quadratic residue} \\ 0 & \text{if } a \equiv 0 \pmod{p} \\ -1 & \text{if } a \text{ is the quadratic non-residue} \end{cases}$$

Theorem 5.1. For the conguruence $y^2 \equiv a \pmod{p}$, where $a \in \mathbb{Z}$ and p is an odd prime, there is the same number of the quadratic residues and the non-residues modulo p. So there are $\frac{p-1}{2}$ quadratic residues in $\mathbb{F}_p$.

Proof. For $y \in \mathbb{Z}$ we have $(y)^2 \equiv y^2 \pmod{p}$ and $(p-y)^2 = p^2 - 2py + y^2 \equiv y^2 \pmod{p}$. We can see that y and $p - y$ have the same square modulo p so there are $\frac{p-1}{2}$ pairs.

□

6 Order of Elliptic Curves

6.1 Elliptic Curves

Definition 6.1. A *cubic curve* is an algebraic curve of curve order 3 in two variables, defined by the equation

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0$$

where A, B, C, D, E, F, G, H, I, $J \in \mathcal{F}$, $\mathcal{F}$ is an arbitrary field ($\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, algebraic extensions of $\mathbb{Q}$, finite field $\mathbb{F}_p$) and at least one of the coefficients A, B, C, D must be nonzero.

An elliptic curve over a field $\mathcal{F}$ is a special case of a cubic curve, which must be nonsingular (the condition of the nonzero discriminant must hold), coefficients $B = C = D = 0$ and $A = G$. A general form of an elliptic curve over a field $\mathcal{F}$ is called the Weierstrass equation.

Definition 6.2. An *elliptic curve* $\mathcal{E}$ over $\mathcal{F}$ is a set of all points $[x, y] \in \mathcal{F}^2$ satisfying the *Weierstrass equation*

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where a_1, a_2, a_3, a_4, $a_6 \in \mathcal{F}$. The non-singularity is assured by the nonzero *discriminant* of the elliptic curve, defined as

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where
$b_2 = a_1^2 + 4a_2$,
$b_4 = 2a_4 + a_1a_3$,
$b_6 = a_3^2 + 4a_6$,
$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_3^2a_2 - a_4^2$.

There exist several transformations of elliptic curve's equation by an appropriate change of variables.

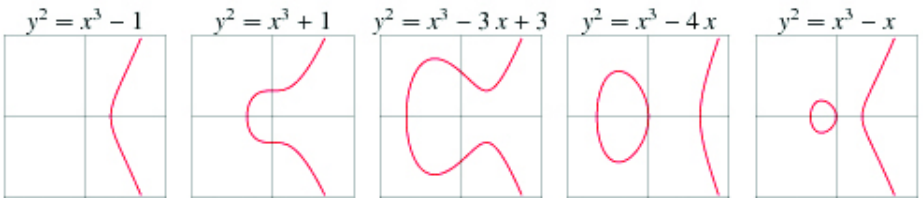
Definition 6.3. Let $\mathcal{F}$ be a field of characteristic different from 2 and 3. Let $\mathcal{E}$ be an elliptic curve defined over $\mathcal{F}$. Then there exists a transformation of the Weierstrass equation sending $\mathcal{E}$ to the form:

$$\mathcal{E} : y^2 = x^3 + ax + b,\ a, b \in \mathcal{F}.$$

The discriminant is simplified to the form

$$D = -16(4a^3 + 27b^2)$$

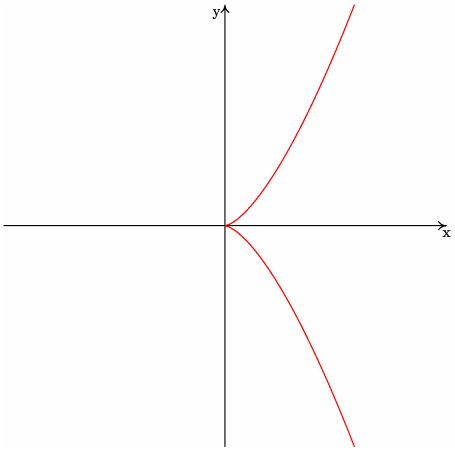
and must be nonzero.



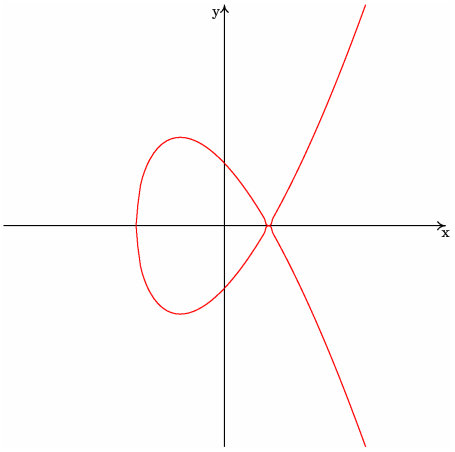
Picture 6.3.: *Elliptic curves with various coefficients* $a, b \in \mathbb{R}$ *[16]*

In the theory of elliptic curves there exist also some invariants, two of the most important are the already mentioned discriminant and a j-invariant.

The discriminant is used for testing of the curves's regularity. If the discriminant is nonzero, then the elliptic curve is regular and so it has no *cusps* and *nodes*. Pictures 6.4 and 6.5 show two non-regular elliptic curves. If $D = 0$ and $a = 0$, then the curve has a cusp singularity and if $D = 0$ and $a \neq 0$, its singularity is called the *ordinary double point* (or node).



Picture 6.4.: *cusp:* $\mathcal{E} : y^2 = x^3$



Picture 6.5.: *node:* $\mathcal{E} : y^2 = x^3 - 3x + 2$

Definition 6.4. The *j-invariant* of an elliptic curve $\mathcal{E}(\mathbb{F}_p)$ is defined by

$$j(\mathcal{E}(\mathbb{F}_p)) = 1728\frac{4a^3}{4a^3 + 27b^2} \ .$$

Hereafter we will deal only with elliptic curves $\mathcal{E}(\mathbb{F}_p)$ over a finite field $\mathbb{F}_p$ and given by the equation $\mathcal{E} : y^2 = x^3 + ax + b, \ a, b \in \mathbb{F}_p$.

Definition 6.5. *The order of an elliptic curve* $\mathcal{E}(\mathbb{F}_p)$, denoted $\#\mathcal{E}(\mathbb{F}_p)$, is the cardinality of the set of elliptic curve's points.

We can see that the number of points on $\mathcal{E}(\mathbb{F}_p)$ with given x-coordinate is 0,1 or 2. More precisely there are

$$1 + \left(\frac{x^3 + ax + b}{p}\right)$$

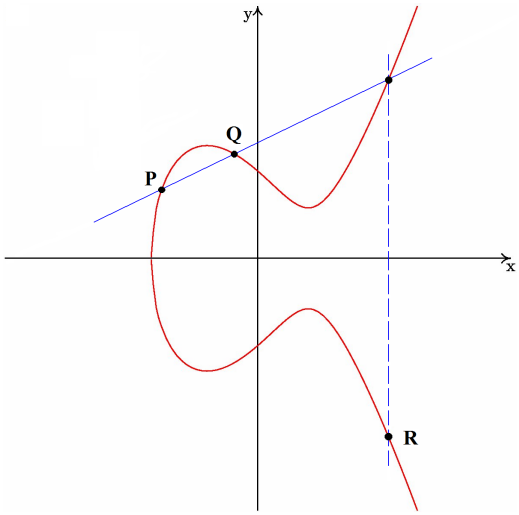
points on $\mathcal{E}(\mathbb{F}_p)$ with x-coordinate equal to x. Here $\left(\frac{\cdot}{p}\right)$ denotes the quadratic residue symbol. Then the order of the elliptic curve $\mathcal{E}(\mathbb{F}_p)$ can be evaluated in this way:

$$\#\mathcal{E}(\mathbb{F}_p) = 1 + \sum_{x\in\mathbb{F}_p}\left(1 + \left(\frac{x^3+ax+b}{p}\right)\right) = 1 + p + \sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right).$$

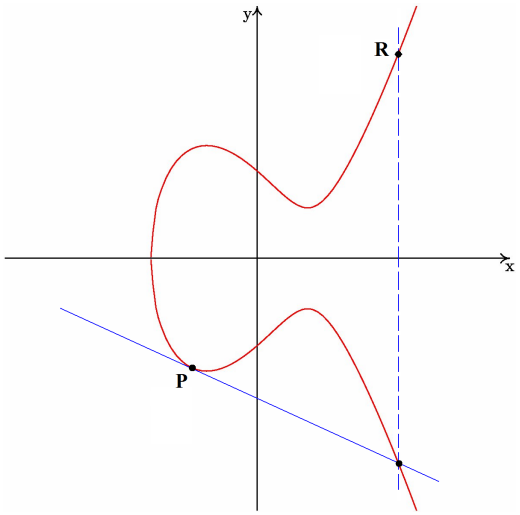
6.2 Elliptic Curve's Points Addition

At first we mention that the *opposite of a point* $P = [x_1, y_1]$ is the point $[x_1, -y_1]$ and hereafter the element, denoted ∞, will be considered as the point of an elliptic curve.

For point's addition we use the well-known *chord and tangent method*. This method is based on the construction of the chord if we want to add two distinct points on the elliptic curve and on the construction of the tangent if we double one point. Both the chord and the tangent intersect the elliptic curve and by reflecting the intersection point about the x-axis, we gain the sum of the points.



Picture 6.6.: *the addition of two distinct points on the elliptic curve over* $\mathbb{R}$



Picture 6.7.: *the double of the point on the elliptic curve over* $\mathbb{R}$

More concretely, let us have two distinct points $P = [x_1, y_1]$ and $Q = [x_2, y_2]$ which lay on the same elliptic curve. Then their addition is the point $R = [x_3, y_3]$ where

$$x_3 = -x_1 - x_2 + \lambda^2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

Here λ is the slope of the line through P and Q. We have that $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ if $P \neq Q$ and $\lambda = \dfrac{3x_1 + a}{2y_1}$ if $P = Q$ (so we double the point P).

It also holds that if the points P and Q have the same x-coordinates or we double the point with zero y-coordinate, their sum is ∞.

Finally let us observe that the set of points of an elliptic curve $\mathcal{E}(\mathbb{F}_p)$ forms an additive group and the point at infinity, denoted ∞, is the neutral element of this group.

Theorem 6.1. The group $\mathcal{E}(\mathbb{F}_p)$ is always isomorphic to the group $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, where n_2 is divisor of both n_1 and $p-1$. The numbers n_1, n_2 are determined uniquely (we permit also $n_2 = 1$, in this case we have the trivial group, the notation is simplified and we write only $\mathbb{Z}_{n_1}$). Then $\#\mathcal{E}(\mathbb{F}_p) = n_1 n_2$ under the condition that there is an element of order n_1 in the group $\mathcal{E}(\mathbb{F}_p)$.

Example 6.1. We investigate the order of the elliptic curve $\mathcal{E} : y^2 = x^3 + 3x + 3$ over the finite fields $\mathbb{F}_5$, $\mathbb{F}_7$ and $\mathbb{F}_{11}$.
At first it must be checked whether the discriminant is nonzero. By substituting in the discriminant's formula we obtain $D = -16(4a^3 + 27b^2) = -16(4 \cdot 3^3 + 27 \cdot 3^2) = -5616$, so we have

- $\mathbb{F}_5$: $-5616 \equiv 4(\mod 5)$ ✓
- $\mathbb{F}_7$: $-5616 \equiv 5(\mod 7)$ ✓
- $\mathbb{F}_{11}$: $-5616 \equiv 5(\mod 11)$ ✓

We can also compute their j-invariants. We obtain $j = \frac{6912}{13}$ so

- $\mathbb{F}_5$: $j = \frac{6912}{13} \equiv 4(\mod 5)$
- $\mathbb{F}_7$: $j = \frac{6912}{13} \equiv 4(\mod 7)$
- $\mathbb{F}_{11}$: $j = \frac{6912}{13} \equiv 2(\mod 11)$

The condition of nonzero discriminant is satisfied so now we can search for the points of elliptic curves.

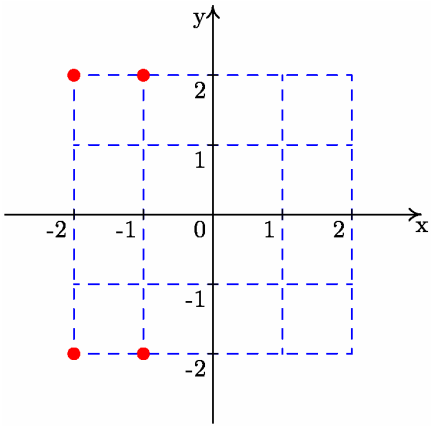
1. $\mathcal{E} : y^2 = x^3 + 3x + 3$ over $\mathbb{F}_5$

   This elliptic curve has 5 points. $\mathcal{E}_{\mathbb{F}_5} : \{\infty, [3,2], [4,2], [3,3], [4,3]\}$

   The group $\mathcal{E}(\mathbb{F}_5)$ is isomorphic with the group $\mathbb{Z}_5$ (see the Theorem 6.1.). We will find the isomorphism and we will make the tables of additive operation within both groups. It is easy to verify the isomorphism by construction of the modified addition table of $\mathbb{Z}_5$.

$+$	∞	$[3,2]$	$[4,2]$	$[3,3]$	$[4,3]$
∞	∞	$[3,2]$	$[4,2]$	$[3,3]$	$[4,3]$
$[3,2]$	$[3,2]$	$[4,3]$	$[3,3]$	∞	$[4,2]$
$[4,2]$	$[4,2]$	$[3,3]$	$[3,2]$	$[4,3]$	∞
$[3,3]$	$[3,3]$	∞	$[4,3]$	$[4,2]$	$[3,2]$
$[4,3]$	$[4,3]$	$[4,2]$	∞	$[3,2]$	$[3,3]$

Table 6.1.: *Addition table of* $\mathcal{E}(\mathbb{F}_5)$



Picture 6.8.: $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_5$

∞	$\mapsto$	0
$[3;2]$	$\mapsto$	4
$[4;2]$	$\mapsto$	2
$[3;3]$	$\mapsto$	1
$[4;3]$	$\mapsto$	3

Table 6.2.: *Isomorphism* $\mathcal{E}(\mathbb{F}_5)$ *and* $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 6.3.: *Addition table of* $\mathbb{Z}_5$

+	0	4	2	1	3
0	0	4	2	1	3
4	4	3	1	0	2
2	2	1	4	3	0
1	1	0	3	2	4
3	3	2	0	4	1

Table 6.4.: *Modified addition table of* $\mathbb{Z}_5$

Now we will search for all endomorphisms on the group $\mathcal{E}(\mathbb{F}_5)$. These endomorphisms form a group again and we can construct the addition and composition tables of them.

		h_0	h_1	h_2	h_3	h_4
∞	$\mapsto$	∞	∞	∞	∞	∞
$[3,2]$	$\mapsto$	∞	$[3,2]$	$[3,3]$	$[4,3]$	$[4,2]$
$[4,2]$	$\mapsto$	∞	$[4,2]$	$[4,3]$	$[3,2]$	$[3,3]$
$[3,3]$	$\mapsto$	∞	$[3,3]$	$[3,2]$	$[4,2]$	$[4,3]$
$[4,3]$	$\mapsto$	∞	$[4,3]$	$[4,2]$	$[3,3]$	$[3,2]$

Table 6.5.: *Endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_5$

+	h_0	h_1	h_2	h_3	h_4
h_0	h_0	h_1	h_2	h_3	h_4
h_1	h_1	h_3	h_0	h_4	h_2
h_2	h_2	h_0	h_4	h_1	h_3
h_3	h_3	h_4	h_1	h_2	h_0
h_4	h_4	h_2	h_3	h_0	h_1

Table 6.6.: *Addition table of endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_5$

∘	h_0	h_1	h_2	h_3	h_4
h_0	h_0	h_0	h_0	h_0	h_0
h_1	h_0	h_1	h_2	h_3	h_4
h_2	h_0	h_2	h_1	h_4	h_3
h_3	h_0	h_3	h_4	h_2	h_1
h_4	h_0	h_4	h_3	h_1	h_2

Table 6.7.: *Composition table of endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_5$

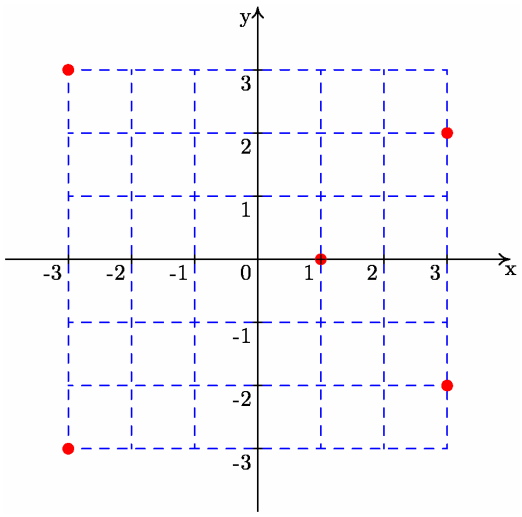
2. $\varepsilon : y^2 = x^3 + 3x + 3$ over $\mathbb{F}_7$

   This elliptic curve has 6 points. $\mathcal{E}_{\mathbb{F}_7} : \{\infty, [1,0], [3,2], [4,3], [4,4], [3,5]\}$

   The group $\mathcal{E}(\mathbb{F}_7)$ is isomorphic with the group $\mathbb{Z}_6$. We will find the isomorphism and we will construct the tables of additive operation within both groups. It is easy to verify the isomorphism by construction of the modified addition table of $\mathbb{Z}_6$.

+	∞	$[1,0]$	$[3,2]$	$[4,3]$	$[4,4]$	$[3,5]$
∞	∞	$[1,0]$	$[3,2]$	$[4,3]$	$[4,4]$	$[3,5]$
$[1,0]$	$[1,0]$	∞	$[4,4]$	$[3,5]$	$[3,2]$	$[4,3]$
$[3,2]$	$[3,2]$	$[4,4]$	$[3,5]$	$[1,0]$	$[4,3]$	∞
$[4,3]$	$[4,3]$	$[3,5]$	$[1,0]$	$[3,2]$	∞	$[4,4]$
$[4,4]$	$[4,4]$	$[3,2]$	$[4,3]$	∞	$[3,5]$	$[1,0]$
$[3,5]$	$[3,5]$	$[4,3]$	∞	$[4,4]$	$[1,0]$	$[3,2]$

Table 6.8.: *Addition table of* $\mathcal{E}(\mathbb{F}_7)$



Picture 6.9.: $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_7$

∞	$\mapsto$	0
$[1;0]$	$\mapsto$	3
$[3;2]$	$\mapsto$	2
$[4;3]$	$\mapsto$	1
$[4;4]$	$\mapsto$	5
$[3;5]$	$\mapsto$	4

Table 6.9.: *Isomorphism* $\mathcal{E}(\mathbb{F}_7)$ *and* $\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	0	1	2	3	5
5	5	0	1	2	3	4

Table 6.10.: *Addition table of* $\mathbb{Z}_6$

+	0	3	2	1	5	4
0	0	3	2	1	5	4
3	3	0	5	4	2	1
2	2	5	4	3	1	0
1	1	4	3	2	0	5
5	5	2	1	0	4	3
4	4	1	0	5	3	2

Table 6.11.: *Modified addition table of* $\mathbb{Z}_6$

Now we will search for all endomorphisms on the group $\mathcal{E}(\mathbb{F}_7)$. These endomorphisms form a group again and we can construct the addition and composition tables of them.

		h_0	h_1	h_2	h_3	h_4	h_5
∞	$\mapsto$	∞	∞	∞	∞	∞	∞
$[1,0]$	$\mapsto$	∞	$[1,0]$	$[1,0]$	∞	∞	$[1,0]$
$[3,2]$	$\mapsto$	∞	$[3,2]$	$[3,5]$	$[3,5]$	$[3,2]$	∞
$[4,3]$	$\mapsto$	∞	$[4,3]$	$[4,4]$	$[3,2]$	$[3,5]$	$[1,0]$
$[4,4]$	$\mapsto$	∞	$[4,4]$	$[4,3]$	$[3,5]$	$[3,2]$	$[1,0]$
$[3,5]$	$\mapsto$	∞	$[3,5]$	$[3,2]$	$[3,2]$	$[3,5]$	∞

Table 6.12.: *Endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_7$

+	h_0	h_1	h_2	h_3	h_4	h_5
h_0	h_0	h_1	h_2	h_3	h_4	h_5
h_1	h_1	h_3	h_0	h_4	h_5	h_2
h_2	h_2	h_0	h_5	h_1	h_3	h_4
h_3	h_3	h_4	h_1	h_5	h_2	h_0
h_4	h_4	h_5	h_3	h_2	h_0	h_1
h_5	h_5	h_2	h_4	h_0	h_1	h_3

Table 6.13.: *Addition table of endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_7$

$\circ$	h_0	h_1	h_2	h_3	h_4	h_5
h_0	h_0	h_0	h_0	h_0	h_0	h_0
h_1	h_0	h_1	h_2	h_3	h_4	h_5
h_2	h_0	h_2	h_1	h_5	h_4	h_3
h_3	h_0	h_3	h_5	h_5	h_0	h_3
h_4	h_0	h_4	h_3	h_1	h_2	h_4
h_5	h_0	h_5	h_3	h_1	h_2	h_4

Table 6.14.: *Composition table of endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_7$

3. $\varepsilon : y^2 = x^3 + 3x + 3$ over $\mathbb{F}_{11}$
   This elliptic curve has 8 points. $\mathcal{E}_{\mathbb{F}_{11}} : \{\infty, [5,0], [8,0], [9,0], [7,2], [0,5], [0,6], [7,9]\}$

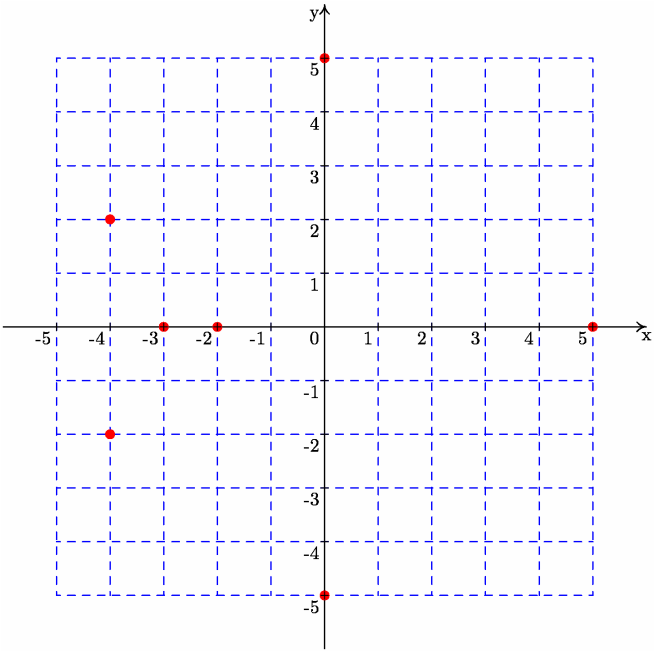
   The group $\mathcal{E}(\mathbb{F}_{11})$ is isomorphic with the group $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. We will find the isomorphism and we will make the tables of additive operation within both groups. It is easy to verify the isomorphism by construction of the modified addition table of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$.

$+$	∞	$[5,0]$	$[8,0]$	$[9,0]$	$[7,2]$	$[0,5]$	$[0,6]$	$[7,9]$
∞	∞	$[5,0]$	$[8,0]$	$[9,0]$	$[7,2]$	$[0,5]$	$[0,6]$	$[7,9]$
$[5,0]$	$[5,0]$	∞	$[9,0]$	$[8,0]$	$[0,5]$	$[7,2]$	$[7,9]$	$[0,9]$
$[8,0]$	$[8,0]$	$[9,0]$	∞	$[5,0]$	$[0,6]$	$[7,9]$	$[7,2]$	$[0,5]$
$[9,0]$	$[9,0]$	$[8,0]$	$[9,0]$	∞	$[7,9]$	$[0,6]$	$[0,5]$	$[7,2]$
$[7,2]$	$[7,2]$	$[0,5]$	$[0,6]$	$[7,9]$	$[9,0]$	$[8,0]$	$[5,0]$	∞
$[0,5]$	$[0,5]$	$[7,2]$	$[7,9]$	$[0,6]$	$[8,0]$	$[9,0]$	∞	$[5,0]$
$[0,6]$	$[0,6]$	$[7,9]$	$[7,2]$	$[0,5]$	$[5,0]$	∞	$[9,0]$	$[8,0]$
$[7,9]$	$[7,9]$	$[0,6]$	$[0,5]$	$[7,2]$	∞	$[5,0]$	$[8,0]$	$[9,0]$

Table 6.15. : *Addition table of* $\mathcal{E}(\mathbb{F}_{11})$

∞	$\mapsto$	(0,0)
$[5;0]$	$\mapsto$	(0,1)
$[8;0]$	$\mapsto$	(2,1)
$[9;0]$	$\mapsto$	(2,0)
$[7;2]$	$\mapsto$	(3,0)
$[0;5]$	$\mapsto$	(3,1)
$[0;6]$	$\mapsto$	(1,1)
$[7;9]$	$\mapsto$	(1,0)

Table 6.16. : *Isomorphism* $\mathcal{E}(\mathbb{F}_{11})$ *and* $\mathbb{Z}_4 \oplus \mathbb{Z}_2$



Picture 6.10.: $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_{11}$

+	(0,0)	(1,0)	(2,0)	(3,0)	(0,1)	(1,1)	(2,1)	(3,1)
(0,0)	(0,0)	(1,0)	(2,0)	(3,0)	(0,1)	(1,1)	(2,1)	(3,1)
(1,0)	(1,0)	(2,0)	(3,0)	(0,0)	(1,1)	(2,1)	(3,1)	(0,1)
(2,0)	(2,0)	(3,0)	(0,0)	(1,0)	(2,1)	(3,1)	(0,1)	(1,1)
(3,0)	(3,0)	(0,0)	(1,0)	(2,0)	(3,1)	(0,1)	(1,1)	(2,1)
(0,1)	(0,1)	(1,1)	(2,1)	(3,1)	(0,0)	(1,0)	(2,0)	(3,0)
(1,1)	(1,1)	(2,1)	(3,1)	(0,1)	(1,0)	(2,0)	(3,0)	(0,0)
(2,1)	(2,1)	(3,1)	(0,1)	(1,1)	(2,0)	(3,0)	(0,0)	(1,0)
(3,1)	(3,1)	(0,1)	(1,1)	(2,1)	(3,0)	(0,0)	(1,0)	(2,0)

Table 6.17.: *Addition table of* $\mathbb{Z}_4 \oplus \mathbb{Z}_2$

+	(0,0)	(0,1)	(2,1)	(2,0)	(3,0)	(3,1)	(1,1)	(1,0)
(0,0)	(0,0)	(0,1)	(2,1)	(2,0)	(3,0)	(3,1)	(1,1)	(1,0)
(0,1)	(0,1)	(0,0)	(2,0)	(2,1)	(3,1)	(3,0)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(0,0)	(0,1)	(1,1)	(1,0)	(3,0)	(3,1)
(2,0)	(2,0)	(2,1)	(0,1)	(0,0)	(1,0)	(1,1)	(3,1)	(3,0)
(3,0)	(3,0)	(3,1)	(1,1)	(1,0)	(2,0)	(2,1)	(0,1)	(0,0)
(3,1)	(3,1)	(3,0)	(1,0)	(1,1)	(2,1)	(2,0)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(3,0)	(3,1)	(0,1)	(0,0)	(2,0)	(2,1)
(1,0)	(1,0)	(1,1)	(3,1)	(3,0)	(0,0)	(0,1)	(2,1)	(2,0)

Table 6.18.: *Modified addition table of* $\mathbb{Z}_4 \oplus \mathbb{Z}_2$

Now we will search for all endomorphisms on the group $\mathcal{E}(\mathbb{F}_{11})$. These endomorphisms form a group again and we can construct the addition and composition tables of them.

	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}
$\infty \mapsto$	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
$[5,0] \mapsto$	∞	$[5,0]$	∞	∞	∞	$[9,0]$	$[9,0]$	$[9,0]$	$[9,0]$	$[5,0]$	$[5,0]$
$[8,0] \mapsto$	∞	$[8,0]$	∞	∞	∞	$[9,0]$	$[9,0]$	$[9,0]$	$[9,0]$	$[8,0]$	$[8,0]$
$[9,0] \mapsto$	∞	$[9,0]$	∞	∞	∞	∞	∞	∞	∞	$[9,0]$	$[9,0]$
$[7,2] \mapsto$	∞	$[7,2]$	$[5,0]$	$[8,0]$	$[9,0]$	$[9,0]$	∞	$[8,0]$	$[5,0]$	$[7,9]$	$[0,5]$
$[0,5] \mapsto$	∞	$[0,5]$	$[5,0]$	$[8,0]$	$[9,0]$	∞	$[9,0]$	$[5,0]$	$[8,0]$	$[0,6]$	$[7,2]$
$[0,6] \mapsto$	∞	$[0,6]$	$[5,0]$	$[8,0]$	$[9,0]$	∞	$[9,0]$	$[5,0]$	$[8,0]$	$[0,5]$	$[7,9]$
$[7,9] \mapsto$	∞	$[7,9]$	$[5,0]$	$[8,0]$	$[9,0]$	$[9,0]$	∞	$[8,0]$	$[5,0]$	$[7,2]$	$[0,6]$

	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}
$\infty \mapsto$	∞	∞	∞	∞	∞
$[5,0] \mapsto$	$[5,0]$	$[8,0]$	$[8,0]$	$[8,0]$	$[8,0]$
$[8,0] \mapsto$	$[8,0]$	$[5,0]$	$[5,0]$	$[5,0]$	$[5,0]$
$[9,0] \mapsto$	$[9,0]$	$[9,0]$	$[9,0]$	$[9,0]$	$[9,0]$
$[7,2] \mapsto$	$[0,6]$	$[0,5]$	$[7,9]$	$[7,2]$	$[0,6]$
$[0,5] \mapsto$	$[7,9]$	$[7,9]$	$[0,5]$	$[0,6]$	$[7,2]$
$[0,6] \mapsto$	$[7,2]$	$[7,2]$	$[0,6]$	$[0,5]$	$[7,9]$
$[7,9] \mapsto$	$[0,5]$	$[0,6]$	$[7,2]$	$[7,9]$	$[0,5]$

Table 6.19.: *Endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_{11}$

$+$	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}
h_0	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}
h_1	h_1	h_4	h_{10}	h_{11}	h_9	h_{13}	h_{14}	h_{15}	h_{12}	h_0	h_3	h_2	h_7	h_6	h_5	h_8
h_2	h_2	h_{10}	h_0	h_4	h_3	h_7	h_8	h_5	h_6	h_{11}	h_1	h_9	h_{14}	h_{15}	h_{12}	h_{13}
h_3	h_3	h_{11}	h_4	h_0	h_2	h_8	h_7	h_6	h_5	h_{10}	h_9	h_1	h_{13}	h_{12}	h_{15}	h_{14}
h_4	h_4	h_9	h_3	h_2	h_0	h_6	h_5	h_8	h_7	h_1	h_{11}	h_{10}	h_{15}	h_{14}	h_{13}	h_{12}
h_5	h_5	h_{13}	h_7	h_8	h_6	h_0	h_4	h_2	h_3	h_{14}	h_{15}	h_{12}	h_{11}	h_1	h_9	h_{10}
h_6	h_6	h_{14}	h_8	h_7	h_5	h_4	h_0	h_3	h_2	h_{13}	h_{12}	h_{15}	h_{10}	h_9	h_1	h_{11}
h_7	h_7	h_{15}	h_5	h_6	h_8	h_2	h_3	h_0	h_4	h_{12}	h_{13}	h_{14}	h_9	h_{10}	h_{11}	h_1
h_8	h_8	h_{12}	h_6	h_5	h_7	h_3	h_2	h_4	h_0	h_{15}	h_{14}	h_{13}	h_1	h_{11}	h_{10}	h_9
h_9	h_9	h_0	h_{11}	h_{10}	h_1	h_{14}	h_{13}	h_{12}	h_{15}	h_4	h_2	h_3	h_8	h_5	h_6	h_7
h_{10}	h_{10}	h_3	h_1	h_9	h_{11}	h_{15}	h_{12}	h_{13}	h_{14}	h_2	h_4	h_0	h_5	h_8	h_7	h_6
h_{11}	h_{11}	h_2	h_9	h_1	h_{10}	h_{12}	h_{15}	h_{14}	h_{13}	h_3	h_0	h_4	h_6	h_7	h_8	h_5
h_{12}	h_{12}	h_7	h_{14}	h_{13}	h_{15}	h_{11}	h_{10}	h_9	h_1	h_8	h_5	h_6	h_4	h_2	h_3	h_0
h_{13}	h_{13}	h_6	h_{15}	h_{12}	h_{14}	h_1	h_9	h_{10}	h_{11}	h_5	h_8	h_7	h_2	h_4	h_0	h_3
h_{14}	h_{14}	h_5	h_{12}	h_{15}	h_{13}	h_9	h_1	h_{11}	h_{10}	h_6	h_7	h_8	h_3	h_0	h_4	h_2
h_{15}	h_{15}	h_8	h_{13}	h_{14}	h_{12}	h_{10}	h_{11}	h_1	h_9	h_7	h_6	h_5	h_0	h_3	h_2	h_4

Table 6.20.: *Additive table of endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_{11}$

$\circ$	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}
h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_0
h_1	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}
h_2	h_0	h_2	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_2	h_2	h_2	h_2	h_2	h_2	h_2
h_3	h_0	h_3	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_3	h_3	h_3	h_3	h_3	h_3	h_3
h_4	h_0	h_4	h_0	h_0	h_0	h_0	h_0	h_0	h_0	h_4	h_4	h_4	h_4	h_4	h_4	h_4
h_5	h_0	h_5	h_0	h_0	h_0	h_0	h_0	h_4	h_4	h_5	h_6	h_6	h_6	h_5	h_5	h_6
h_6	h_0	h_6	h_0	h_0	h_0	h_0	h_0	h_4	h_4	h_6	h_5	h_5	h_5	h_6	h_6	h_5
h_7	h_0	h_7	h_0	h_0	h_0	h_4	h_4	h_4	h_4	h_7	h_8	h_8	h_8	h_7	h_7	h_8
h_8	h_0	h_8	h_0	h_0	h_0	h_4	h_4	h_4	h_4	h_8	h_7	h_7	h_7	h_8	h_8	h_7
h_9	h_0	h_9	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_1	h_{11}	h_{10}	h_{15}	h_{14}	h_{13}	h_{12}
h_{10}	h_0	h_{10}	h_2	h_3	h_4	h_6	h_5	h_8	h_7	h_{11}	h_1	h_9	h_{14}	h_{15}	h_{12}	h_{13}
h_{11}	h_0	h_{11}	h_2	h_3	h_4	h_6	h_5	h_8	h_7	h_{10}	h_9	h_1	h_{13}	h_{12}	h_{15}	h_{14}
h_{12}	h_0	h_{12}	h_2	h_3	h_4	h_6	h_5	h_8	h_7	h_{15}	h_{14}	h_{13}	h_9	h_{11}	h_{10}	h_1
h_{13}	h_0	h_{13}	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_{14}	h_{15}	h_{12}	h_{11}	h_1	h_9	h_{11}
h_{14}	h_0	h_{14}	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_{13}	h_{12}	h_{15}	h_{10}	h_9	h_1	h_{10}
h_{15}	h_0	h_{15}	h_2	h_3	h_4	h_6	h_5	h_8	h_7	h_{12}	h_{13}	h_{14}	h_1	h_{11}	h_{10}	h_9

Table 6.21.: *Composition table of endomorphisms on* $\mathcal{E} : y^2 = x^3 + 3x + 3$ *over* $\mathbb{F}_{11}$

7 Algorithms for Determining Order of Elliptic Curve

7.1 Naive Algorithm

In the Definition 6.5. we evaluated the order of the elliptic curve by this formula

$$\#\mathcal{E}(\mathbb{F}_p) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right).$$

Straightforward evaluation of this sum is the so-called *naive algorithm* for determining the order of elliptic curves.

We used this algorithm in the Example 6.1. It is very practical to make the table of squares modulo p (see Appendix E) and then count the number of all x for which $x^3 + ax + b$ is square ($x = 0, \ldots, p-1$). This algorithm is efficient for very small primes, say $p < 200$.

7.2 Hasse's Theorem

Theorem 7.1. *H. Hasse, 1933.* Let p be a prime and $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$. Then

$$|p + 1 - \#\mathcal{E}(\mathbb{F}_p)| < 2\sqrt{p}.$$

Due to the Hasse's Theorem and the Lagrange's Theorem which says that the orders of points of elliptic curve divide the order of the elliptic curve, there is a very simple idea to find the order of the elliptic curves. We find the orders of at least two points and we compute their least multiple, let us denote it lcm. It holds that $r \cdot \text{lcm}$ is the order of the elliptic curve for some $r \in \mathbb{Z}$. If the number $r \cdot \text{lcm}$ lies in the Hasse's interval $\langle p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p} \rangle$ for only one r, then $r \cdot \text{lcm}$ is the order of the elliptic curve.

7.3 Shank's Baby Step and Giant Step Algorithm

The idea of this algorithm is to pick a random point $P \in \mathcal{E}(\mathbb{F}_p)$ and to compute an integer m in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ such that $mP = \infty$. If m is the only such number in the interval, it follows from the Theorem 7.1. that $m = \#\mathcal{E}(\mathbb{F}_p)$. This algorithm has two parts - the Baby step and the Giant step.

The algorithm:

- Baby Step
  1. Hasse's interval $\langle p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p} \rangle$.
  2. Choose a random point $P \in \mathcal{E}(\mathbb{F}_p)$, if $\exists\ i \in \mathbb{Z},\ i \leq d :\ iP = \infty$ choose another point P.
  3. $d = \lceil \sqrt{\mathcal{U} - \mathcal{L}} \rceil = \sqrt{\lceil p + 1 + 2\sqrt{p} \rceil - \lfloor p + 1 - 2\sqrt{p} \rfloor}$
     Make the sequence $BS = \{\infty, P, 2P, \ldots, (d-1)P\}$.

- Giant Step

4. $Q = dP$
   $H_j = \mathcal{L}P + jQ,\ j = 1, 2, \ldots, d$
   Make the sequence $GS = \{H_1, H_2, \ldots, H_d\}$.
5. Now we compare the sequences BS and GS. If there is only one common element $P_i = H_j,\ P_i \in BS,\ H_j \in GS$, then we have found the order of the elliptic curve as $\#\mathcal{E}(\mathbb{F}_p) = \mathcal{L} + jd - i$. If there are more common elements (let us say M), we order them to a sequence of couples according to the indexes $(i_k, j_k),\ k = 1, 2, \ldots M,\ j_1 > j_2 > \ldots > j_M$.
6. Count the order of the point P as $|P| = (j_1 - j_2)d - (i_1 - i_2)$.
   If $|P| < \sqrt{p} - 1$ repeat the whole algorithm from the beginning with another point. Otherwise take another point $R \in \mathcal{E}(\mathbb{F}_p)$ and repeat the Steps 1 - 5 with it.
7. If Step 5 has finished successfully we have the order of the elliptic curve. If not we count the order $|R|$ and we find its least divisor s such that sR is a multiple of P.
8. If $s|P| < 4\sqrt{p}$, another point R must be chosen. Otherwise we determine (the unique) n such that $ns|P|$ falls into Hasse's interval and we have $\#\mathcal{E}(\mathbb{F}_p) = ns|P|$.

This algorithm is practical for large primes. It becomes impractical when p has more than say 20 decimal digits.

If the exponent of the group $\mathcal{E}(\mathbb{F}_p)$ is very small, there is more than one m in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ such that $mP = \infty$ for every point P. This problem was solved with Mestre's improvement of this algorithm.

7.4 Mestre's Algorithm

Definition 7.1. Let the equation $y^2 = x^3 + ax + b$ denote the elliptic curve $\mathcal{E}$ and $g \in \mathbb{F}_p$ be some quadratic non-residue number. Then the *quadratic twist $\mathcal{E}'$ of an elliptic curve $\mathcal{E}$* is determined by a Weierstrass equation

$$y^2 = x^3 + ag^2x + bg^3.$$

Theorem 7.2. Let us consider all elliptic curves given by the equation

$$y^2 = x^3 + ag^2x + bg^3$$

where $0 \neq g \in \mathbb{F}_p$. It holds that all elliptic curves which satisfy $\left(\frac{g}{p}\right) = 1$ are isomorphic to each other and have the same order. Accordingly elliptic curves for which $\left(\frac{g}{p}\right) = -1$ are isomorphic to each other as well.

If we look at the Definition 6.4. we can see that the elliptic curve and its quadratic twist have the same j-invariant. There are two exceptions:

1. For $j = 0$ and $p \equiv 1 \pmod 3$ there exist six curves.
2. For $j = 1728$ and $p \equiv 1 \pmod 4$ there are four curves.

Theorem 7.3. *J.-F. Mestre.* Let $\mathcal{E}$ be an elliptic curve and $\mathcal{E}'$ be its quadratic twist than it holds

$$\#\mathcal{E}(\mathbb{F}_p) + \#\mathcal{E}'(\mathbb{F}_p) = 2(p+1).$$

This theorem is a great instrument because as we can see the sum of orders of $\mathcal{E}$ and $\mathcal{E}'$ is constant. So it holds that if the elliptic curve has small order and therefore the Shank's algorithm fails, its quadratic twist has a big order and we can apply the Shank's algorithm to it.

The algorithm:

1. Choose randomly a point $z \in \mathbb{F}_p$ and compute the Legendre symbol $\left(\frac{z^3+az+b}{p}\right) = L$
2. Now we have 3 possibilities:
   - $L = 0$ - we choose another point z
   - $L = 1$ - we work further with the elliptic curve $\mathcal{E}_z = \mathcal{E}$
   - $L = -1$ - we work further with the elliptic curve $\mathcal{E}_z = \mathcal{E}'$
3. Compute the second coordinate of the point $P = [z, y_z]$ and apply the steps 3-6 of the Shank's algorithm.
4. If we do not get the $\#\mathcal{E}_z$ choose another point z. Otherwise the order is readily obtained as

$$\#\mathcal{E} = \begin{cases} \#\mathcal{E}_z & \text{if we compute with } \mathcal{E} \\ 2(p+1) - \#\mathcal{E}_z & \text{if we compute with } \mathcal{E}' \end{cases}$$

Example 7.1. Let us have the elliptic curve defined by the equation $\mathcal{E} : y^2 = x^3 + 3x + 3$ over $\mathbb{F}_{617}$. We will compute the order of this elliptic curve using the Mestre's Algorithm.

1. $z = 7$
   $\left(\frac{x^3+3x+3}{617}\right) = \left(\frac{7^3+3\cdot 7+3}{617}\right) = \left(\frac{367}{617}\right) = -1$
2. 5 is not a quadratic residue in $\mathbb{F}_{617}$
   $\mathcal{E}_z = \mathcal{E}' : y^2 = x^3 + 3 \cdot 5^2 \cdot x + 3 \cdot 5^3 = x^3 + 75x + 375$
3. $P = [7, 3]$
   I. Hasse's interval:
   $\mathcal{L} = p + 1 - 2\sqrt{p} = 617 + 1 - 2\lfloor\sqrt{617}\rfloor = 568$
   $\mathcal{U} = p + 1 + 2\sqrt{p} = 617 + 1 + 2\lceil\sqrt{617}\rceil = 668$

   $$568 \leq \#\mathcal{E}_z(\mathbb{F}_{617}) \leq 668$$

   II. $d = \sqrt{\mathcal{U} - \mathcal{L}} = \sqrt{100} = 10$

   $$BS = \{\infty; [7,3]; [121,98]; [404,386]; [604,467]; [100,427]; [26,262];$$
   $$[93,286]; [455,589]; [574,123]\}$$

III. $Q = d \cdot P = 10P = [486, 36]$
$H_j = L \cdot P + j \cdot Q = 568P + j \cdot 10P = [524, 332] + j \cdot [486, 36]$

$$GS = \{[177, 455]; [52, 302]; [150, 594]; [78, 256]; [90, 186]; [258, 102];$$

$$[423, 579]; [535, 592]; [93, 331]; [404, 386]\}$$

IV. $P_3 = Q_{10} = [404, 386]$
$\#\mathcal{E}_z(\mathbb{F}_{617}) = \mathcal{L} + jd - i = 568 + 10 \cdot 10 - 3 = 665$

4. $\#\mathcal{E}(\mathbb{F}_{617}) = 2(p+1) - \#\mathcal{E}_z(\mathbb{F}_{617}) = 2(617+1) - 665 = 571$

7.5 Mestre's Theorem

As was said above if p is prime, than $\mathbb{F}_q$, where $q = p^n$, is a field of characteristic p. The field $\mathbb{F}_{q^k},\ k \in \mathbb{N}$ is an algebraic extension of $\mathbb{F}_q$, which has also the characteristic equal to p. If the order of the elliptic curve $\mathcal{E}(\mathbb{F}_q)$ is known, the order of the elliptic curve $\mathcal{E}(\mathbb{F}_{q^k})$ can be computed and the following relation holds

$$\#\mathcal{E}(\mathbb{F}_q) < \#\mathcal{E}(\mathbb{F}_{q^k})$$

and the elliptic curve $\mathcal{E}(\mathbb{F}_{q^k})$ contains all points of the elliptic curve $\mathcal{E}(\mathbb{F}_q)$.

This statement is also true for elliptic curves $\mathcal{E}(\overline{\mathbb{F}}_q)$ over algebraic closure $\overline{\mathbb{F}}_q = \overline{\mathbb{F}}_{p^n}$ and $\mathcal{E}(\overline{\mathbb{F}}_q)$ contains all points of $\mathcal{E}(\mathbb{F}_q)$.

Definition 7.2. Let us have an elliptic curve $\mathcal{E}(\mathbb{F}_q)$, where $q = p^n$ and let $t = q + 1 - \#\mathcal{E}(\mathbb{F}_q)$. We say that the elliptic curve $\mathcal{E}(\mathbb{F}_q)$ is *supersingular* if $p|t$ and *ordinary* if $p \not| t$.

Let $\mathcal{E}(\overline{\mathbb{F}}_q)$ be denoted as $\overline{\mathcal{E}}$. Among the ring of endomorphisms $\mathrm{End}\,(\overline{\mathcal{E}})$ there are always the endomorphisms of type $x \mapsto kx,\ \forall\ x \in \overline{\mathcal{E}},\ k \in \mathbb{Z}$, so $\mathrm{End}\,(\overline{\mathcal{E}})$ contains the duplication of $\mathbb{Z}$ and we have

$$\mathrm{End}\,(\overline{\mathcal{E}}) \supseteq \mathbb{Z}.$$

Thus $\mathrm{End}\,(\overline{\mathcal{E}})$ is isomorphic to a *complex quadratic order* with discriminant Δ. For the case of the ordinary elliptic curves it holds $\mathrm{End}\,(\overline{\mathcal{E}}) \supset \mathbb{Z}$ and so

$$\mathrm{End}\,(\overline{\mathcal{E}}) = \mathbb{Z}[\delta] = \mathbb{Z} + \mathbb{Z}[\delta]$$

where $\delta = \frac{\sqrt{\Delta}}{2}$ or $\delta = \frac{1+\sqrt{\Delta}}{2}$ depending on whether Δ is even or odd. We have also $\mathrm{End}\,(\overline{\mathcal{E}}) = \mathrm{End}\,(\overline{\mathcal{E}'})$.

The Frobenius endomorphism $\varphi \in \mathrm{End}\,(\overline{\mathcal{E}})$ is the endomorphism given by

$$\varphi(x, y) = (x^p, y^p)$$

which satisfies the quadratic equation $\varphi^2 - t\varphi + p = 0$. Here $t \in \mathbb{Z}$ and is related to the number of the elliptic curve's points by $\#\mathcal{E}(\overline{\mathbb{F}}_p) = p + 1 - t$.

Theorem 7.4. *J.-F. Mestre.* Let $p > 457$ be a prime and let $\mathcal{E}(\mathbb{F}_p)$ be an elliptic curve over $\mathbb{F}_p$. Then either $\mathcal{E}(\mathbb{F}_p)$ or its quadratic twist $\mathcal{E}(\mathbb{F}_p)'$ admits an $\mathbb{F}_p$-rational point of order at least $4\sqrt{p}$.

Proof. The endomorphism rings of $\overline{\mathcal{E}}$ and $\overline{\mathcal{E}'}$ are both isomorphic to the same quadratic order $\mathcal{O}$ of discriminant Δ, so $\mathcal{O} = \mathcal{O}_{\mathbb{Z}+\mathbb{Z}[\delta]} = \mathrm{End}\,(\overline{\mathcal{E}}) = \mathrm{End}\,(\overline{\mathcal{E}'})$. Let $\varphi \in \mathcal{O}$ denote the Frobenius endomorphism of $\overline{\mathcal{E}}$. Let n be the largest integer such that $\varphi \equiv 1 \pmod{n}$ in $\mathrm{End}\,(\overline{\mathcal{E}})$ and let $N = \frac{p+1-t}{n}$ denote the exponent of $\mathcal{E}(\overline{\mathbb{F}}_p)$. We denote $\mathbb{Z}[\varphi] : k\varphi,\ k \in \mathbb{Z}$ and we have that

$$\mathbb{Z}[\varphi] \subset \mathbb{Z}\left[\frac{\varphi - 1}{n}\right] \subset \mathcal{O}$$

which implies that n divides the index $[\mathcal{O} : \mathbb{Z}[\varphi]]$ (index $\mathbb{Z}[\varphi]$ in $\mathcal{O}$ is the number of left classes). Since $[\mathcal{O} : \mathbb{Z}[\varphi]]^2$ is equal to the quotient of the discriminants of the orders $\mathcal{O}$ and $\mathbb{Z}[\varphi]$, we see that n^2 divides $\frac{t^2-4p}{\Delta}$.

Similarly, let m be the largest integer such that $-\varphi \equiv 1 \pmod{m}$ in $\mathrm{End}\,(\overline{\mathcal{E}})$ and let $M = \frac{p+1+t}{m}$ denote the exponent of $\mathcal{E}'(\overline{\mathbb{F}}_p)$. Then

$$\mathbb{Z}[\varphi] \subset \mathbb{Z}\left[\frac{\varphi + 1}{m}\right] \subset \mathcal{O}$$

Therefore m^2 also divides $\frac{t^2-4p}{\Delta}$. Since n divides $\varphi - 1$ and m divides $\varphi + 1$, we see that $\gcd(n, m)$ divides $\gcd(\varphi - 1, \varphi + 1)$ which divides 2. Therefore

$$n^2m^2 \text{ divides } 4\frac{t^2 - 4p}{\Delta}.$$

Since $|\Delta| \geq 3$ this implies that $(nm)^2 \leq 4\frac{4p-t^2}{3}$. If both exponents N and M are less than $4\sqrt{p}$, we have that

$$\left((p+1)^2 - t^2\right)^2 = (nNmM)^2 < (4\sqrt{p})^4 4\frac{4p - t^2}{3}$$

and therefore

$$p^4 + 4p^3 < (p+1)^4 < \frac{4^6}{3}p^3 - t^4 - \left(\frac{4^5}{3}p^2 - 2(p+1)^2\right)t^2 \leq \frac{4^6}{3}p^3,$$

which implies that $p < 1362$.

A straightforward case-by-case calculation shows that the theorem also holds for the primes p with $457 < p < 1362$. This completes the proof.

□

8 Conclusion

We were concerned with several algorithms for counting the elliptic curve's points, which represents one of the most important problems in the Elliptic Curve Cryptography. Four of the most famous algorithms were mentioned. For small prime numbers it is successful to use the Naive algorithm and the algorithm which is based on the Hasse's Theorem. The Naive algorithm's principle consists of the straightforward numeration of the elliptic curve's points and for this algorithm it is appropriate to apply the table of quadratic residues. Another one uses the connection between the Hasse's Theorem and the Lagrange's Theorem. For bigger prime numbers, we use the Shank's Baby step - Giant Step algorithm or its improvement, the Mestre's algorithm. The last algorithm is based on the clever and simple idea of the elliptic curve's twist. Due to the famous Mestre's theorem, it was proven that the elliptic curve order can be computed for all elliptic curves over the finite prime field of the prime bigger than 457. The proof of this theorem is based on the isomorphism of the endomorphism's ring over the elliptic curve and the complex quadratic order.

Finally we mention some additional information and properties of the themes of the algebraic background which was used in the proof of the Mestre's Theorem.

A Additional Information about Algebraic Extension

Definition A.1. Suppose $\mathcal{L}$ is a field extension of the field of rational numbers $\mathbb{Q}$ of finite degree n, so $\mathcal{L}$ is an algebraic extension. Let us choose an *integral basis* $\alpha_1, \ldots, \alpha_n$ for $\mathcal{L}$, then any element $x \in \mathcal{F}$ has a unique representation of the form $x = \sum x_i \alpha_i$.

Definition A.2. A *regular representation* of the elements of the field $\mathcal{L}$ is a representation by n by n matrices, as follows:

$$x\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j, \quad a_{ij} \in \mathbb{Q},\ 1 \leq i, j \leq n.$$

For this formulation the multiplication in $\mathcal{L}$ was used.

The square matrix $A = A(x)$ represents the effect of multiplication by x in the basis α. Consequently $a \in \mathcal{L}$ is represented by a matrix A and $b \in \mathcal{L}$ is represented by a matrix B, then the product ab is represented by the matrix product AB.

We say that $x \in \mathcal{L}$ is an algebraic integer if and only if the characteristic polynomial p_A of the matrix A associated to x is a monic polynomial with integer coefficients, in other words if x is an algebraic integer, then $A(x)$ is an integer square matrix.

Among the most important invariants of square matrices of regular representation there belong the *trace*, the *determinant* and the *characteristic polynomial*. These invariants are independent of the choice of a basis in $\mathcal{L}$.

Definition A.3. Let $A = A(x)$ for $x \in \mathcal{L}$ be a square matrix. Then we denote the trace of the field element x as $\mathrm{Tr}(x)$ and the determinant, which is called the *norm* of x, is denoted by $\mathcal{N}(x)$.

For λ which is scalar and $x, y \in \mathcal{L}$ the following properties hold:

- $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ (The trace is a linear function of x)
- $\mathrm{Tr}(\lambda x) = \lambda \mathrm{Tr}(x)$ (The trace is a linear function of x)
- $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ (The multiplication of the norm)
- $\mathrm{N}(\lambda x) = \lambda^n \mathrm{N}(x)$ (The norm is a homogeneous function of x of degree n)

B Galois Theory

Due to *Galois theory*, named after Evariste Galois, certain problems in the *field theory* can be reduced to the *group theory*, which is in some sense simpler and better understood. Originally Galois theory used the permutation groups to describe how the various roots of a given polynomial equation are related to each other. The modern approach to Galois theory, developed by Richard Dedekind, Leopold Kronecker and Emil Artin, among others, involves studying automorphisms of field extensions.

Definition B.1. We say that a field extension $\mathcal{L}/\mathcal{K}$ is *separable*, if it is generated by adjunction of a set the roots of a separable polynomial over $\mathcal{K}$ (a separable polynomial $P(x)$ over $\mathcal{K}$ means that each irreducible factor of $P(x)$ has distinct linear factors in some large enough field extension of $\mathcal{K}$).

With the definition of the separable extension we get some important corollaries from the Primitive element theorem:

- Every finite separable extension $\mathcal{L}/\mathcal{K}$ has a primitive element.
- For non-separable extensions the following statement holds: if the degree $[\mathcal{L} : \mathcal{K}]$ is a prime number, then $\mathcal{L}/\mathcal{K}$ has a primitive element.

Definition B.2. A field extension $\mathcal{L}/\mathcal{K}$ is called *normal* if every irreducible polynomial in $\mathcal{K}[X]$ that has a root in $\mathcal{L}$ completely factors into linear factors over $\mathcal{L}$.

Definition B.3. We denote the field extension $\mathcal{L}/\mathcal{K}$ as a *Galois extension* if and only if it is normal and separable extension. This extension is important for the Galois theory.

Definition B.4. An *abelian extension* is a Galois extension whose *Galois group* (a set of automorphisms with the operation of composition denoted $\mathrm{Aut}(\mathcal{L}/\mathcal{K})$, where $\mathcal{L}/\mathcal{K}$ is Galois extension) is abelian. When the Galois group is a cyclic group, we have a *cyclic extension.*

Definition B.5. A *permutation* is a bijection from a finite set onto itself.

Theorem B.1. The number of permutations on a set of n elements is given by $n!$.

Definition B.6. A *permutation group* is a finite group $\mathcal{G}$ whose elements are permutations of a given set and whose group operation is composition of permutations in $\mathcal{G}$. Permutation groups have orders dividing $n!$.

Two permutations form a group only if one of them is the *identity element* and the other is a *permutation involution*, i.e. a permutation which is its own inverse. Every permutation group with more than two elements can be written as a product of transpositions.

For some polynomials it holds that their roots are connected by various algebraic equations. The central idea of Galois theory is to consider those permutations of the roots having the property that any algebraic equation satisfied by the roots is still satisfied

after the roots have been permuted. An important proviso is that we restrict ourselves to algebraic equations whose coefficients are rational numbers. These permutations together form a permutation group, also called the *Galois group of the polynomial*.

Example B.1. Consider the quadratic equation $x^2 - 4x + 1 = 0$ with two roots $A = 2 + \sqrt{3}$ and $B = 2 - \sqrt{3}$. Algebraic equations satisfied by A and B are $A + B = 4$ and $AB = 1$. We conclude that the Galois group of the polynomial $x^2 - 4x + 1$ consists of two permutations: the *identity permutation* which leaves A and B untouched, and the *transposition permutation* which exchanges A and B. It is a cyclic group of order two and therefore isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

In general for any quadratic polynomial $ax^2 + bx + c$ where $a, b, c \in \mathbb{Q}$ it holds:

- If the polynomial has only one root, then the Galois group is *trivial*, that is it contains only the identity permutation.
- If it has two distinct rational roots, the Galois group is again trivial.
- If it has two irrational roots (including the case where the roots are complex), then the Galois group contains two permutations, just as in the above example.

In the modern approach, one starts with a field extension $\mathcal{L}/\mathcal{K}$, and examines the group of field automorphisms of $\mathcal{L}/\mathcal{K}$. The coefficients of the polynomial should be chosen from the base field $\mathcal{K}$. The top field $\mathcal{L}$ should be the field obtained by adjoining the roots of the polynomial to the base field. Any permutation of the roots which respects certain algebraic equations gives rise to an automorphism of $\mathcal{L}/\mathcal{K}$, and vice versa. In the example above, we were studying the extension $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.

In conclusion we only mention that one of the great triumphs of Galois Theory was the proof that for every $n > 4$, there exist polynomials of degree n which are not solvable by radicals - the *Abel-Ruffini theorem*.

C Cyclotomic Field

Firstly we define an n-th root of unity and an n-th cyclotomic polynomial.

Definition C.1. An *n-th root of unity*, where $k = 1, 2, 3, \ldots$, is a complex number ζ satisfying the equation $\zeta^k = 1$.

We say that the n-th root of unity ζ is a *primitive* if the following formula holds: $\zeta^k \neq 1,\ k = 1, 2, \ldots, n-1)$. The primitive n-th roots of unity are those ζ^k where k and n are coprime. Second roots are called the *square roots* and the *third roots* are called cube roots.

Definition C.2. A *Euler's Totient function* $\varphi(n)$ of a positive integer n is defined to be the number of positive integers less than or equal to n that are coprime to n.

Definition C.3. An *n-th cyclotomic polynomial* is defined by the fact that its zeros are precisely the primitive n-th roots of unity, each with multiplicity 1:

$$\Phi_n(\zeta) = \prod_{i=1}^{\varphi(n)} (\zeta - \zeta_i)$$

where $\zeta_1, \ldots, \zeta_{\varphi(n)}$ are the primitive n-th roots of unity and $\varphi(n)$ is Euler's Totient function.

The polynomial $\Phi_n(\zeta)$ has integer coefficients and is an irreducible polynomial over the rational numbers.

Definition C.4. A *factorization* is the decomposition of an object (for example a number, a polynomial or a matrix) into the *factors*, which when multiplied together give the original.

Definition C.5. The extension field $\mathcal{L}$ of a field $\mathcal{K}$ is called the *splitting field* for the polynomial $f(x)$ in $\mathcal{K}[x]$ if $f(x)$ factors completely into linear factors in $\mathcal{L}[x]$ and $f(x)$ does not factor completely into linear factors over any *proper subfield* (this means a subfield which is strictly smaller than the field in which it is contained) of $\mathcal{L}$ containing $\mathcal{K}$.

A *cyclotomic field* $\mathbb{Q}(\zeta_n)$ (with $n > 2$) is a number field obtained by adjoining a root of unity to $\mathbb{Q}$, the field of rational numbers $\mathbb{Q}$. This field contains all n-th roots of unity and is the splitting field of the n-th cyclotomic polynomial over $\mathbb{Q}$. The field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is abelian (and therefore also Galois) with the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ given by $\varphi(n)$, where φ is Euler's Totient function.

Definition C.6. Let n be a positive integer, let ζ_n be a primitive n-th root of unity, and let $\mathcal{L}_n = \mathbb{Q}(\zeta_n)$ be the n-th cyclotomic field. The discriminant of $\mathcal{L}_n$ is given by

$$\Delta_{\mathcal{L}_n} = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}$$

where $\varphi(n)$ is Euler's Totient function, and the product in the denominator is over primes p dividing n.

A classical example of the construction of a quadratic field is to take the unique quadratic field inside the cyclotomic field generated by a primitive p-th root of unity, with p a prime number > 2. The uniqueness is a consequence of Galois theory.

D Full Modules and Their Rings of Coefficients

The *transition matrix* C from one basis $\alpha_1, \ldots, \alpha_n$ of the module $\mathcal{M}$ to another one $\alpha_1^*, \ldots, \alpha_n^*$ is of the rank n and unimodular, which means that it is integral and $\det C = \pm 1$. The rank is the same for all bases of the module $\mathcal{M}$.

Definition D.1. A number a of the algebraic number field $\mathcal{L}$ is called the *coefficient* of the full module $\mathcal{M}$ of the field $\mathcal{L}$ if $a\mathcal{M} \subset \mathcal{M}$, that is $\forall\ \xi \in \mathcal{M}$ it holds that $a\xi \subseteq \mathcal{M}$.

The set of all coefficient of a module $\mathcal{M}$ forms a ring with unit called the *ring of coefficients* of the full module $\mathcal{M}$ and denoted $\mathfrak{R}_\mathcal{M}$. For $a, b \in \mathfrak{R}_\mathcal{M}$ and for $\xi \in \mathcal{M}$ we have $a - b \in \mathfrak{R}_\mathcal{M}$ and $ab \in \mathfrak{R}_\mathcal{M}$. To discover if $c \in \mathfrak{R}_\mathcal{M}$ it suffices to check if $c\alpha_i \in \mathcal{M}\ \forall\ i = 1, \ldots, n$, where $\alpha_1, \ldots, \alpha_n$ is the basis of the module $\mathcal{M}$. $\mathfrak{R}_\mathcal{M}$ is also a full module.

Theorem D.1. The coefficient ring $\mathfrak{R}_\mathcal{M}$ for any full module $\mathcal{M}$ of the algebraic number field $\mathcal{L}$ is an order of this field.

Conversely, any order of the algebraic number field $\mathcal{L}$ is coefficient ring for some full module, for instance for itself.

Lemma D.1. If the number a belongs to the order $\mathfrak{R}_\mathcal{M}$, then its characteristic and minimum polynomials have integer coefficients. In particular, the norm $\mathrm{N}(a) = \mathrm{N}_{\mathcal{L}/\mathbb{R}}(a)$ and the trace $\mathrm{Tr}(a) = \mathrm{Tr}_{\mathcal{L}/\mathbb{R}}(a)$ are *rational integers* ("rational" is used for emphasis to distinguish it from other types of "integers").

According to Lemma D.1. the minimum polynomial of any number in any order has integer coefficients. We denote the set of all numbers of $\mathcal{L}$ whose minimum polynomial has integer coefficients as $\tilde{\mathfrak{R}}$.

Lemma D.2. If $\mathfrak{R}$ is any order of the field $\mathcal{L}$ and $a \in \tilde{\mathfrak{R}}$, then the ring $\mathfrak{R}[a]$, consisting of all polynomials in a with coefficients from $\mathfrak{R}$, is also an order of the field $\mathcal{L}$.

Corollary of the Lemma D.2 is following. If $\mathfrak{R}$ is an order and $a_1, \ldots, a_p,\ p \in \mathbb{N}$ are numbers of $\tilde{\mathfrak{R}}$, then the ring $\mathfrak{R}[a_1, \ldots, a_p]$ of all polynomials in $a_1, \ldots, a_p$ with coefficient from $\mathfrak{R}$ is also an order.

Theorem D.2. The set of all numbers of the algebraic number field $\mathcal{L}$ whose minimum polynomial has integer coefficients is the maximal order of the field $\mathcal{L}$.

Proof. Let $\mathfrak{R}$ be any order of the field $\mathcal{L}$ and let a, b be arbitrary numbers of $\tilde{\mathfrak{R}}$. By the corollary of the Lemma D.2 the ring $\mathfrak{R}[a, b]$ is an order, and hence it is contained in $\tilde{\mathfrak{R}}$ (Lemma D.1) . But then the difference $a - b$ and the product ab are also contained in $\tilde{\mathfrak{R}}$. This proves that $\tilde{\mathfrak{R}}$ is a ring. Since $\mathfrak{R} \subseteq \tilde{\mathfrak{R}}$, $\tilde{\mathfrak{R}}$ contains n linearly independent numbers. We thus only need to show that $\tilde{\mathfrak{R}}$ is a module.

Let $\alpha_1, \ldots, \alpha_n$ be any basis of the order $\mathfrak{R}$, and let $\alpha_1^*, \ldots, \alpha_n^*$ be the dual basis to it in the field $\mathcal{L}$. We shall show that the ring $\tilde{\mathfrak{R}}$ is contained in the module $\mathfrak{R}^* = \{\alpha_1^*, \ldots, \alpha_n^*\}$. Let a be any element of the ring $\tilde{\mathfrak{R}}$. Represent it in the form $a = c_1\alpha_1^* + \cdots + c_n\alpha_n^*$ with rational c_i. Multiplying by α_i and taking the trace, we obtain $c_i = \mathrm{Sp}\ a\alpha_i,\ (1 \le i \le n)$. All products $a\alpha_i$ are contained in the order $\mathfrak{R}[a]$, and therefore by the Lemma D.1 all

numbers c_i are integers, and this means that $a \in \Re^*$. Thus $\tilde{\Re} \subseteq \Re$. We finally conclude that $\tilde{\Re}$ is a module and the theorem is proved.

□

The maximal order of an algebraic number field $\mathcal{L}$ is the integral closure of the ring $\mathbb{Z}$ of rational integers in the field $\mathcal{L}$. The maximal order is therefore also called the *ring of integers of* $\mathcal{L}$ and any number in $\tilde{\Re}$ is named an *integer of* $\mathcal{L}$.

Definition D.2. Elements ε of the ring $\Re_{\mathcal{M}}$ for which ε^{-1} also belongs to $\Re_{\mathcal{M}}$ are called the *units of the ring* $\Re_{\mathcal{M}}$.

Since the inclusions $\varepsilon\mathcal{M} \subseteq \mathcal{M}$ and $\varepsilon^{-1}\mathcal{M} \subseteq \mathcal{M}$ are equivalent to $\varepsilon\mathcal{M} = \mathcal{M}$. The units of the maximal order $\tilde{\Re}$ are also called the *units of the algebraic number field* $\mathcal{L}$.

E Table of Quadratic Residues

n	number of quadratic residues	quadratic residues a
1	0	(none)
2	**1**	**1**
3	**1**	**1**
4	1	1
5	**2**	**1, 4**
6	3	1, 3, 4
7	**3**	**1, 2, 4**
8	2	1, 4
9	3	1, 4, 7
10	5	1, 4, 5, 6, 9
11	**5**	**1, 3, 4, 5, 9**
12	3	1, 4, 9
13	**6**	**1, 3, 4, 9, 10, 12**
14	7	1, 2, 4, 7, 8, 9, 11
15	5	1, 4, 6, 9, 10
16	3	1, 4, 9
17	**8**	**1, 2, 4, 8, 9, 13, 15, 16**
18	7	1, 4, 7, 9, 10, 13, 16
19	**9**	**1, 4, 5, 6, 7, 9, 11, 16, 17**
20	5	1, 4, 5, 9, 16

Table E.22. : *Table of Quadratic residues*

In this table there are the quadratic residues, i.e. the numbers a which satisfy the equation $y^2 \equiv a \pmod{n}$ for some integer $0 < y < n$, and their number for the integers $n \leq 20$. The web site [14] is very useful for searching the quadratic residues for bigger integers n.

References

[1] BOREVICH, Z.I. - SHAFAREVICH, I.R. *Number Theory*. New York: Academic Press, 1966. 435s.

[2] HANKERSON, D. - MENEZES, A. - VANSTONE, S. *Guide to elliptic curve cryptography*. New York: Springer, 2004. 311s. ISBN 0-387-95273-X

[3] KARÁSEK, J. - SKULA, L. *Obecná algebra*. Brno: Akademické nakladatelství Cerm, 2008. 64 s. ISBN 978-80-214-3794-4

[4] MUSIKER, G. *Schoof's algorithm for counting points on* $E(\mathbb{F}_q)$. 2005. 13 s.

[5] POSTNIKOV, M.M. *Foundations of Galois Theory*. New York: Dover, 2004. 128 s. ISBN 0-486-43518-0

[6] SCHOOF, R. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 1995, vol. 7, no. 1, s. 219-254

[7] TRCHALÍKOVÁ, J. *Algorithms for determining the order of the group of points on an elliptic curve with application in cryptography*. Bachelor's Thesis. Brno: Brno University Of Technology, Faculty of Mechanical Engineering, 2008. 27 s. Supervisor doc. RNDr. MIROSLAV KUREŠ, Ph.D.

[8] Certicom. *An Elliptic Curve Cryptography (ECC) Primer* [online]. last revision 20th of July 2004 [retrieved 2009-05-01]. <http: //www.deviceforge.com/articles/AT4234154468.html>

[9] Chikaradirghsa Multiply. *ECC vs RSA* [online]. last revision 24th of November 2007 [retrieved 2009-05-01]. <http: //chikaradirghsa.multiply.com/journal/item/16>

[10] In Wikipedia, The Free Encyclopedia. *Field (mathematics)* [online]. last revision 15th of February 2009 [retrieved 2009-02-17]. <http: //en.wikipedia.org/w/index.php?titleF̄ield_(mathematics)&oldid=270819174>

[11] In Wikipedia, The Free Encyclopedia. *Field extension* [online]. last revision 12th of February 2009 [retrieved 2009-02-17]. <http: //en.wikipedia.org/w/index.php?title=Field_extension&oldid=270153622>

[12] In Wikipedia, The Free Encyclopedia. *Algebraic number field* [online]. last revision 1st of December 2008 [retrieved 2009-02-17]. <http: //en.wikipedia.org/w/index.php?title=Algebraic_number_field&oldid=255207573>

[13] In Wikipedia, The Free Encyclopedia. *Quadratic field* [online]. last revision 3rd of February 2009 [retrieved 2009-02-17]. <http: //en.wikipedia.org/w/index.php?title=Quadratic_field&oldid=268217634>

[14] Michigan Technological University Department of Mathematical Sciences, W. H. Freeman and Company. *Quadratic Residues and Primitive Roots* [online]. 2001 [retrieved 2009-05-05]. <http: //www.math.mtu.edu/mathlab/COURSES/holt/dnt/quadratic4.html>

[15] ROWLAND, T. From MathWorld–A Wolfram Web Resource. *Elliptic Discriminant* [online]. last revision 20th of April 2009 [retrieved 2009-04-23]. <http://mathworld.wolfram.com/EllipticDiscriminant.html>

[16] WEISSTEIN, E.W. From MathWorld–A Wolfram Web Resource. *Elliptic Curve* [online]. last revision 20th of April 2009 [retrieved 2009-04-23]. <http://mathworld.wolfram.com/EllipticCurve.html>

[17] WEISSTEIN, E.W. From MathWorld–A Wolfram Web Resource. *Quadratic Residue* [online]. last revision 3rd of May 2009 [retrieved 2009-05-05]. <http://mathworld.wolfram.com/QuadraticResidue.html>