802656S ALGEBRALLISET LUVUT

ALGEBRAIC NUMBERS

Tapani Matala-aho

MATEMATIIKKA/LUTK/OULUN YLIOPISTO

Autumn 2017, translated by Václav Košík 2018

Commentary on the translation

This is a translation of lecture notes for the course Algebraic Numbers taught at the University of Oulu written by Tapani Matala-aho. The translation was made from Finnish.

I did not always keep the exact wording of the original document, but the meaning should be always preserved.

I tried to use English notions/terms which are commonly used, but since I did the translation primarily for passing the exam and I was quite in a hurry, I did maybe not always succeed.

A few parts were already written in English in the original document. These parts were usually kept untouched.

The translation was made so that I tried to understand what Google Translator returned. Therefore, the text could include mistakes and misunderstandings, but I hope and presume there is not so many of them.

Václav Košík, FNSPE CTU in Prague; December 10, 2018

Sisältö

1 ABSTRACT

The theory of algebraic numbers is an important part of Number Theory.

2 INTRODUCTION

2.1 Course overview (Finnish)

Aluksi kerrataan renkaiden ja kuntien perusteita, joista edetään kuntalaajennuksiin. Erityiseen tarkasteluun otetaan jaollisuus kokonaisalueessa, jonka sovelluksiin törmätään polynomialgebrassa ja kokonaisten algebrallisten lukujen teoriassa.

Algebrallisten lukujen teoria lepää vahvasti polynomialgebraan, josta käsitellään polynomien nollakohtia ja jaollisuutta.

Algebrallisen luvun määritelmä yleistetään kuntalaajennuksien algebrallisiin alkioihin, joista edetään algebrallisiin kuntiin. Tärkeinpinä algebrallisina kuntina saadaan lukukunnat, jotka ovat äärellisesti generoituja kompleksisten algebrallisten lukujen kunnan A alikuntia. Erityisesti tutkitaan neliökuntia.

Edelleen tarkastellaan kokonaisten algebrallisten lukujen jaollisuutta ja tekijöihinjakoa, joita sovelletaan Diofantoksen yhtälöiden ratkaisemiseen.

2.2 Course overview

First we revise some basics of rings and fields which are needed to proceed ahead field extensions. In particular, divisibility in an integral domain is carefully studied yielding to applications in the theory of polynomial algebra and algebraic integers. The theory of algebraic numbers is strongly based on polynomial algebra, where the properties of zeros and divisibility of polynomials are considered. The definition of an algebraic number will be generalized to the algebraic elements of field extensions going forward to algebraic fields.Considered as most important algebraic fields we get number fields which are finitely generated subfields of the field A of all complex algebraic numbers. In particular, we study quadratic number fields.

Further, we shall consider the divisibility and factorization of algebraic integers with some applications to Diophantine equations.

802656S ALGEBRALLISET LUVUT/NOPPA LINK.

802656S ALGEBRAIC NUMBERS/NOPPA LINK.

2.3 BASICS

Prerequisites:

Algebra, Linear Algebra and Basics in Number Theory courses.

The course uses the notation of Basics in Number Theory.

2.4 REFERENCES

I.N. Stewart and D.O. Tall: Algebraic number theory.

Daniel Marcus: Number fields.

J.B. Fraleigh: Abstract algebra.

Michael Artin: Algebra.

Number Theory Web/LINK
American Mathematical Monthly/LINK

2.5 Algebraic numbers

Definition 1. Algebraic numbers are zeros of non-constant polynomials with rational coefficients.

Example 1.

Numbers

$$-1; \tag{2.1}$$

$$i; \tag{2.2}$$

$$2^{1/3} + 3^{1/2} \tag{2.3}$$

are algebraic numbers.

Example 2.

$$e^{i\pi/m}, \quad m \in \mathbb{Z} \setminus \{0\}; \tag{2.4}$$

$$\sin(\pi/m),\ \cos(\pi/m),\ \tan(\pi/m), \quad m \in \mathbb{Z} \setminus \{0\}; \tag{2.5}$$

are algebraic numbers.

Example 3.

Also roots of the polynomial equation

$$2^{1/3}x^4 + 3^{1/2}x + 1 = 0 \tag{2.6}$$

are algebraic numbers.

Remark 1. Let $f : A \to B$ and $C \subseteq B$. Then the pre-image of C is the set

$$f^{-1}(C) = \{x \in A |\ f(x) \in C\}. \tag{2.7}$$

For instance

$$f^{-1}(\{0\}) = \{x \in A |\ f(x) = 0\}. \tag{2.8}$$

Gauss proved that the number of zero points of a non-constant polynomial with complex coefficients is equal to the degree of this polynomial.

Theorem 1. FUNDAMENTAL THEOREM OF ALGEBRA.
Let $d = \deg p(x) \in \mathbb{Z}^+$ and

$$p(x) = p_0 + p_1 x + ... + p_d x^d \ \in \mathbb{C}[x], \tag{2.9}$$

then

$$\#p^{-1}(\{0\}) = \deg p(x) = d \tag{2.10}$$

or

$$p(x) = p_d(x - \alpha_1) \cdots (x - \alpha_d), \quad \alpha_1, ..., \alpha_d \ \in \mathbb{C}. \tag{2.11}$$

This course focuses on complex algebraic numbers.

3 Basics

Let K be a field and $d \in \mathbb{Z}^+$. A polynomial

$$p(x) = p_0 + p_1 x + ... + x^d \ \in K[x], \quad d = \deg p(x) \geq 1, \tag{3.1}$$

is called a *monic polynomial.* We use the following notation

$$K[x]_d = \{p(x) = p_0 + p_1 x + ... + x^d \ \in K[x]\}. \tag{3.2}$$

We define (complex) algebraic numbers using the field of rational numbers.

Definition 2. The elements of the set

$$\mathbb{A}_d = \{\alpha \ \in \mathbb{C} |\ p(\alpha) = 0,\ p(x) \in \mathbb{Q}[x]_d\} \tag{3.3}$$

are *algebraic numbers of a degree at most d.* The set

$$\mathbb{A} = \cup_{d=1}^{\infty} \mathbb{A}_d \tag{3.4}$$

is a set of all algebraic numbers

Definition 3. Let $K \subseteq \mathbb{C}$ and $p(x) \ \in K[x]$. Then

$$Z(p) = p^{-1}(\{0\}) = \{\alpha \ \in \mathbb{C} |\ p(\alpha) = 0\} \tag{3.5}$$

is a *zero set* of the polynomial $p(x)$.

Theorem 2.

$$\mathbb{A}_1 = \mathbb{Q}. \tag{3.6}$$

Remark 2. Let $D \in \mathbb{Z}$. Then

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} |\ a, b \in \mathbb{Q}\}. \tag{3.7}$$

Theorem 3.

$$\mathbb{A}_2 = \underset{D \in \mathbb{Z}}{\cup} \mathbb{Q}(\sqrt{D}). \tag{3.8}$$

4 Rings and fields

4.1 Ring

First, this course examines commutative rings.

Let R be a set such that $\#R \geq 2$. Suppose that we defined in R a binary operation (or mapping) $+$

$$+ : R \times R \to R, \quad (a, b) \to a + b,$$

where $a+b \in R$ if $a \in R$ and $b \in R$. Moreover, we defined an operation $*$

$$* : R \times R \to R, \quad (a,b) \to a * b,$$

where $a * b \in R$ if $a \in R$ and $b \in R$.

4.1.1 Commutative ring with unity

Definition 4.

A triad $(R, +, *)$ is a *commutative ring with unity* if the following conditions are satisfied:

1) additive axioms:

1. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity).
2. $a + b = b + a$ for all $a, b \in R$ (commutativity).
3. There exists a zero element $0 \in R$ for which $0 + a = a$ for all $a \in R$.
4. For all $a \in R$ there exists an inverse $-a \in R$ for which $a + (-a) = 0$.

2) multiplicative axioms:

1. $a * (b * c) = (a * b) * c$ for all $a, b, c \in R$ (associativity).
2. $a * b = b * a$ for all $a, b \in R$ (commutativity).
3. There exists a unit element $1 \in R$ for which $1 * a = a$ for all $a \in K$.

3) distribution axiom:

1. $a * (b + c) = a * b + a * c$ for all $a, b, c \in R$.

The set R from Definition 4 is called a commutative ring with unity and the conditions are called ring axioms.

Axioms 1) say that $(R, +)$ is Abel group whose operation $+$ is called an addition.

We can say that $(R, +)$ is additive group of the ring R whose neutral element is the zero element 0.

But $R = (R, *)$ is not necessarily a multiplicative group because the inverse element is not guaranteed. The neutral element is the unit 1.

Remark 3. Usually, we omit the multiplication notation:

$$a * b = ab.$$

Definition 5. Let R be a ring with a unit. The set

$$R^* = \{\text{units}\} = \{u \in R \mid \exists\ u^{-1} \in R:\ uu^{-1} = 1\} \tag{4.1}$$

is a unit group of R.

We often use the notation

$$R^* = \{u \in R \mid \exists\ v \in R:\ uv = 1\}, \tag{4.2}$$

when it holds that

$$u \in R^* \quad \Rightarrow \quad 1 = uv, \quad u, v \in R^*. \tag{4.3}$$

If $R = K$ is a field, then $K^* = K \backslash \{0\}$.

4.2 Integral Domain

Definition 6. An element $a \neq 0$ of R is a *zero divisor* if $\exists\ b \in R \backslash \{0\}$ such that $ab = 0$ or $ba = 0$.

Definition 7. A commutative ring with unity D is an *integral domain* if D does not have a zero divisor.
i.e. if $ab = 0$, $a, b \in D$, then $a = 0$ or $b = 0$.

4.3 Field

Definition 8.

A triad $(K, +, *)$ is a field if the following conditions are satisfied:

1. **1) additive axioms**:

1. $a + (b + c) = (a + b) + c$ for all $a, b, c \in K$ (associativity).
2. $a + b = b + a$ for all $a, b \in K$ (commutativity).
3. There exists a zero element $0 \in K$ for which $0 + a = a$ for all $a \in K$.
4. For all $a \in K$ there exists an inverse $-a \in K$ for which $a + (-a) = 0$.

2) multiplicative axioms:

1. $a * (b * c) = (a * b) * c$ for all $a, b, c \in K$ (associativity).
2. $a * b = b * a$ for all $a, b \in K$ (commutativity).
3. There exists a unit-element $1 \in K$ for which $1 * a = a$ for all $a \in K$.
4. For all $a \in K^* = K \setminus \{0\}$ there exists an inverse element $a^{-1} \in K^*$ for which $a * a^{-1} = 1$.

3) distribution axiom:

1. $a * (b + c) = a * b + a * c$ for all $a, b, c \in K$.

The set K from the definition 8 is called a field and the conditions are called field axioms.

Axioms 1) say that $(K, +)$ is an Abel group whose operation $+$ is called an addition.

We can say that $(K, +)$ is an additive group of the field K whose neutral element is the zero element 0.

Axioms 2) tell us that $(K^*, *)$ is an Abel group whose operation $*$ is called a multiplication.

Therefore, it can be said that $(K^*, *)$ is a multiplicative group of the field K with the unit-element 1 as the neutral element.

BRIEFLY: The triad $(K, +, \cdot)$, $\#K \geq 2$ is a *field* if:

1. $(K, +)$ is an Abel group (additive group),
2. $(K^*, *)$ is an Abel group (multiplicative group), $K^* = K \backslash \{0\}$.
3. $a(b + c) = ab + ac, \ \forall a, b, c \in K$.

Specially, a field is a commutative ring with unity (subset).

There are always at least two elements in a field, namely $0, 1 \in K$, $0 \neq 1$.

Example 4.

A field K is an integral domain.

Proof: Let

$$ab = 0, \tag{4.4}$$

where $a, b \in K$. Antithesis: $a \neq 0$ and $b \neq 0$.

Because K is a field, then $a^{-1} \in K$. Multiplying (4.4) by a^{-1} gives

$$b = a^{-1}ab = a^{-1} \cdot 0 \quad \Rightarrow \quad b = 0. \tag{4.5}$$

A contradiction. □

Example 5.

The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$, where $p \in \mathbb{P}$, are integral domains.

Example 6.

Any subring S of a field K is an integral domain.

Example 7.

$\mathbb{Z}$ is an integral domain.

Example 8.

The set

$$\mathbb{Z}[i] = \{a + ib | \ a, b \in \mathbb{Z}\} \tag{4.6}$$

of Gaussian integers is an integral domain and its unit group is

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}. \tag{4.7}$$

Example 9.

The set

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\} \tag{4.8}$$

is an integral domain and its unit group is

$$\mathbb{Z}[\sqrt{-5}]^* = \{1, -1\}. \tag{4.9}$$

4.3.1 Characteristics

Definition 9. We define characteristics of a field K as

$$\text{char } K = \begin{cases} p \Leftrightarrow \exists\ p \in \mathbb{P} :\ p1 = 0; \\ 0 \Leftrightarrow \nexists\ n \in \mathbb{Z}^+ :\ n1 = 0. \end{cases}$$

5 Divisibility in integral domain

Let D be an integral domain.

Definition 10. Let $a, b \in D$. Then

$$b|a \quad \Leftrightarrow \quad \exists c \in D : \quad a = bc. \tag{5.1}$$

If $b|a$, we say that b divides a or b is a factor of a.

Notation: $b \nmid a$ if b does not divide a.

Example 10.

$$0|0, \quad 0 \nmid a \neq 0. \tag{5.2}$$

Remark 4. Let $d, b \in D$ and $s \in \mathbb{N}$, then

$$d^s || b \;\Leftrightarrow\; d^s | b \text{ and } d^{s+1} \nmid b. \tag{5.3}$$

Lemma 1. Let $a, b, c \in D, a \neq 0$. Then

$$ab = ac \quad \Rightarrow \quad b = c. \tag{5.4}$$

Proof.

$$ab = ac \quad \Rightarrow \quad a(b-c) = 0,\; a \neq 0, \quad \Rightarrow \quad b - c = 0. \quad \square \tag{5.5}$$

Definition 11. Elements $a, b \in D$ are associated if

$$a \sim b \quad \Leftrightarrow \quad \exists \quad u \in D^* : \; b = ua. \tag{5.6}$$

Lemma 2. The relation $\sim$ is an equivalence, in other words

$$a \sim a; \tag{5.7}$$

$$a \sim b \quad \Leftrightarrow \quad b \sim a; \tag{5.8}$$

$$a \sim b, \quad b \sim c \quad \Rightarrow \quad a \sim c. \tag{5.9}$$

Proof. 5.8:

$$\begin{aligned} a \sim b \quad \Leftrightarrow \quad b = ua,\; u \in D^* \quad \Leftrightarrow \\ \exists \quad v \in D^* : \; uv = 1,\; b = ua \quad \Leftrightarrow \quad vb = vua = a \\ \Leftrightarrow \quad a = vb,\; v \in D^* \quad \Leftrightarrow \quad b \sim a. \quad \square \end{aligned} \tag{5.10}$$

Other points on one's own.

Remark 5. The equivalence class for the element $a \in D$ it the set

$$[a] = \{b \in D |\; b \sim a\}, \tag{5.11}$$

where a is the representative of $[a]$.

Lemma 3. Let D be an integral domain and $1, a, b \in D$. Then

$$a \sim b \quad \Rightarrow \quad a|b; \tag{5.12}$$

$$a \sim 1 \quad \Leftrightarrow \quad a|1 \quad \Leftrightarrow \quad a \in D^*; \tag{5.13}$$

$$[1] = D^*; \tag{5.14}$$

$$[a] = aD^*; \tag{5.15}$$

$$a \sim b \quad \Leftrightarrow \quad a|b \quad \text{and} \quad b|a. \tag{5.16}$$

Proof. 5.13:

$$a \sim 1 \quad \Rightarrow \quad 1 = ua,\ u \in D^* \subseteq D \quad \Rightarrow \quad a|1;$$

$$a|1 \quad \Rightarrow \quad \exists\, c \in D:\ 1 = ca \quad \Rightarrow c \in D^* \ \Rightarrow \ a \sim 1.$$

$$\rightsquigarrow \qquad a \sim 1 \quad \Leftrightarrow \quad a|1. \quad \square$$

$$a|1 \quad \Rightarrow \quad \exists\, c \in D:\ 1 = ca \quad \Rightarrow \quad a, c \in D^*;$$

$$a \in D^* \quad \Rightarrow \quad 1 = ua, u \in D \quad \Rightarrow \quad a|1.$$

$$\rightsquigarrow \qquad a|1 \quad \Leftrightarrow \quad a \in D^*. \quad \square$$

5.14:

$$b \in [1] \quad \Leftrightarrow \quad b \sim 1 \quad \Leftrightarrow \quad b \in D^*. \quad \square$$

5.15:

$$x \in [a] \quad \Leftrightarrow \quad x \sim a \quad \Leftrightarrow \quad a \sim x$$

$$\Leftrightarrow \quad x = ua,\ u \in D^* \quad \Leftrightarrow \quad x \in aD^*. \quad \square$$

5.16: First look at the case $b = 0$ which implies $a = 0$.

$$
\begin{aligned}
a \sim b \quad &\Leftrightarrow \quad b \sim a, \quad \Rightarrow \quad a|b \quad \text{and} \quad b|a; \\
a|b \quad \text{and} \quad b|a \quad &\Rightarrow \quad b = ca,\ a = db,\ c, d \in D, \\
&\Rightarrow \quad b = cdb \quad \Rightarrow \quad cd = 1 \quad \Rightarrow \quad c, d \in D^*, \\
&\Rightarrow \quad a \sim b \quad \text{and} \quad b \sim a. \quad \square
\end{aligned}
$$

Remark 1. Let $b \in D$. Then

$$b = 1 \cdot b = u(u^{-1}b) \quad \forall\ u \in D^*. \tag{5.17}$$

Therefore a unit is always a factor of an element.

Example 11.

Remember that the unit group of Gaussian integers was

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}. \tag{5.18}$$

Thus

$$2 - i \sim 1 + 2i \sim -2 + i \sim -1 - 2i \tag{5.19}$$

and the equivalence class

$$[2 - i] = \{2 - i, 1 + 2i, -2 + i, -1 - 2i\} \tag{5.20}$$

of $2 - i$ consists of four elements.

Definition 12. Trivial factors q of an element $b \in D$ are all units and associates. In other words

$$q \in [1] \quad \text{or} \quad q \in [b]. \tag{5.21}$$

An element $j \in D, j \neq 0, j \notin D^*$ is irreducible if it has only trivial factors

$$q|j \quad \Leftrightarrow \quad q \in [1] \quad \text{or} \quad q \in [j]. \tag{5.22}$$

An element $p \in D, p \neq 0, p \notin D^*$ is prime if

$$p|ab \quad \Rightarrow \quad p|a \quad \text{or} \quad p|b \quad \forall a, b \in D. \tag{5.23}$$

An element $a \in D, a \notin D^*$ is reducible if

$$\exists\, d \in D: \quad d|a \quad \Rightarrow \quad d \notin [1] \quad \text{and} \quad d \notin [a]. \tag{5.24}$$

Remark 2. The zero-element is reducible.

Remark 6. Let us denote

$$J_D = \{j \in D|\ j \text{ is irreducible}\} \tag{5.25}$$

and

$$P_D = \{p \in D|\ p \text{ is prime}\}. \tag{5.26}$$

Lemma 4. Let $a, b \in D$ and $j, h \in J_D$. Then

$$j = ab \quad \Rightarrow \quad a \sim 1 \quad \text{or} \quad b \sim 1. \tag{5.27}$$

$$j = bh, \quad \Rightarrow \quad b \sim 1. \tag{5.28}$$

Proof (5.27). Antithesis: $a \not\sim 1$ and $b \not\sim 1$

$$\Rightarrow \quad a, b \notin [1] \quad \Rightarrow \quad a, b \in [j] \tag{5.29}$$

because j is irreducible. Thus

$$a = d_1 j \quad b = d_2 j, \quad d_1, d_2 \in D^* \quad \Rightarrow \tag{5.30}$$

$$j = ab = d_1 d_2 j^2 \quad \Rightarrow \quad 1 = d_1 d_2 j \quad \Rightarrow \quad j \in D^* = [1]. \tag{5.31}$$

A contradiction. □

Definition 13. Let $a, b \in D$ be given. Then an element $d \in D$ is the greatest common divisor of a and b, denoted by $d =$syt$(a, b) =$gcd$(a, b) = (a, b)$, if

$$d|a \quad \text{and} \quad d|b; \tag{5.32}$$

$$c|a \quad \text{and} \quad c|b \quad \Rightarrow \quad c|d. \tag{5.33}$$

If $(a, b) \sim 1$, then we say that a and b are relatively prime and we write $(a, b) = 1$ or $a \perp b$.

Definition 14. Let $a, b \in D$ be given. Then an element $f \in D$ is the least common multiple of a and b, denoted by $f =$pyj$[a, b] =$lcm$[a, b] = [a, b]$, if

$$a|f \quad \text{and} \quad b|f; \tag{5.34}$$

$$a|g \quad \text{and} \quad b|g \quad \Rightarrow \quad f|g. \tag{5.35}$$

Example 12.

$$(0, 0) = 0, \quad [0, 0] = 0. \tag{5.36}$$

Lemma 5. Let $a \in D$ and $j \in J_D$. Then

$$j \not| a \quad \Rightarrow \quad (a, j) = 1. \tag{5.37}$$

Proof. Antithesis: $(a, j) \neq 1$. Therefore $(a, j) = d \not\sim 1$ and

$$d|a \quad \text{and} \quad d|j, \quad j \in J_D. \tag{5.38}$$

Because j is irreducible, then $d \sim 1$ or $d \sim j$, hence $d \sim j$. Consequently

$$d = vj, \ v \in D^* \quad \text{and} \quad a = cd = cvj \quad \Rightarrow \quad j|a. \tag{5.39}$$

A contradiction. □

Definition 15. The representation of an element $a \in D$ by irreducible elements is unique if from the condition

$$a = j_1 \cdots j_r = h_1 \cdots h_s, \quad j_l, h_k \in J_D \tag{5.40}$$

follows

$$r = s \quad \text{and} \quad h_k \sim j_l \quad \forall k = 1, ..., r \quad \text{for some } l = 1, ..., r. \tag{5.41}$$

Definition 16. An integral domain D is a unique factorization domain (UFD) if every element $a \in D, a \neq 0, a \notin D^*$ can be represented uniquely as

$$a = j_1 \cdots j_r, \quad j_i \in J_D. \tag{5.42}$$

Theorem 4. Let D be an ID. Then

$$P_D \subseteq J_D \tag{5.43}$$

(primes are irreducible.)

Proof. (5.43): Let $p \in P_D$. If $q|p$, then $p = qd_1$ for some $d_1 \in D$. Then

$$p|qd_1 \quad \Rightarrow \quad p|q \quad \text{or} \quad p|d_1 \tag{5.44}$$

because p is a prime.

If $p|q$, then $q = d_2 p$, $d_2 \in D$ and $q = d_2 q d_1$, where $q \neq 0$ by $p \neq 0$. So $1 = d_1 d_2$ meaning that $d_1, d_2 \in D^*$. Therefore $q \in [p]$.

If $p|d_1$, then (homework...) $q \in [1]$.

Thus $p \in J_D$. □

Theorem 5. Let D be an integral domain. Then

$$D = \text{UFD} \quad \Rightarrow \quad J_D \subseteq P_D \tag{5.45}$$

so UFD's irreducibles are primes and consequently $J_D = P_D$.

Proof: Let $j \in J_D$ and assume that $j|ab$ where $a, b \in D$. Since $D =$UFD, a and b has the unique representation

$$a = a_1 \cdots a_m, \quad b = b_1 \cdots b_n, \quad a_i, b_i \in J_D. \tag{5.46}$$

Hence

$$j|a_1 \cdots a_m b_1 \cdots b_n = j \cdot j_2 \cdots j_{m+n}, \tag{5.47}$$

and from here $j \sim a_i$ for some a_i or $j \sim b_i$ for b_i because $D =$UDF. Therefore $j|a$ or $j|b$.

Overally $j \in P_D$. □

Remark 3. In UFD the representation (5.42) is called prime factorization.

Definition 17. Let D be an integral domain and $a \in D$. If an irreducible element $j \in J_D$ satisfies

$$j^m \| a, \quad m \in \mathbb{Z}_{\geq 0}, \tag{5.48}$$

then m is a *multiplicity* of the factor j of a.

If $j \not| a$, then $m = 0$.

Theorem 6. Let D be an integral domain. Then

$$J_D \subseteq P_D \quad \Rightarrow \quad D = \text{UFD}. \tag{5.49}$$

Proof: Let

$$a = j_1 \cdots j_r = h_1 \cdots h_s, \quad j_l, h_k \in J_D \tag{5.50}$$

Now irreducibles j_l and h_k are primes. Thus

$$j_1|h_1 \cdots h_s \quad \Rightarrow \quad j_1|h_1 \quad \text{or} \quad j_1|h_2 \cdots h_s \ldots \tag{5.51}$$

and eventually $j_1|h_{k_1}$ implying $j_1 \sim h_{k_1}$,...,$j_r \sim h_{k_r}$ and $r = s$. □

5.1 Division and Euclidean algorithm in integral domain

5.1.1 Division algorithm/Euclidean domain

Let D be an integral domain with so called Euclidean function $E: \ D \to \mathbb{N} \cup \{-\infty\}$ and suppose that the following holds true:

Division algorithm: If $a, b \in D$ are given and $ab \neq 0$, $0 \leq E(b) \leq E(a)$, then $\exists\, q, r \in D$ such that

$$(J.A.) \quad a = qb + r \text{ and } E(r) < E(b). \tag{5.52}$$

This kind of domain is called Euclidean domain (ED). (Note that the definition of the Euclidean function varies.)

Example 13. a)$D = \mathbb{Z}, \quad E(k) = |k|$.
b)$D = K[x], \quad E(p(x)) = \deg p(x)$.

Based on division algorithm:

Euclidean algorithm=E.A.:

$$\begin{array}{ll}
r_0 = a, \ r_1 = b & E(r_1) < E(r_0) \\
r_0 = q_1 r_1 + r_2 & E(r_2) < E(r_1) \\
\vdots & \\
r_k = q_{k+1} r_{k+1} + r_{k+2} & E(r_{k+2}) < E(r_{k+1}) \\
\vdots & \\
r_{n-1} = q_n r_n & \exists\, n \in \mathbb{N}: \ r_n \neq 0, \ r_{n+1} = 0 \\
r_n = \mathrm{syt}(a, b). &
\end{array}$$

The integer $n =$ is called a length of euclidean algorithm.

Set now

$$R_k = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}, \ Q_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}, \ k \in \mathbb{N}, \tag{5.53}$$

whereupon

$$\det Q_k = -1, \quad {Q_k}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}. \tag{5.54}$$

We see that

$$\text{E.A.} \Leftrightarrow R_k = Q_{k+1} R_{k+1},\ \forall k = 0, \ldots, n-1, \tag{5.55}$$

whereupon holds

$$R_0 = Q_1 Q_2 \cdots Q_k R_k. \tag{5.56}$$

Denote

$$S_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{5.57}$$

and

$$S_k = \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = {Q_k}^{-1} \cdots {Q_2}^{-1} {Q_1}^{-1}, \tag{5.58}$$

so

$$R_k = S_k R_0. \tag{5.59}$$

We have

$$S_{k+1} = Q_{k+1}^{-1} S_k \tag{5.60}$$

so

$$\begin{pmatrix} s_{k+1} & t_{k+1} \\ s_{k+2} & t_{k+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{pmatrix} \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = \begin{pmatrix} s_{k+1} & t_{k+1} \\ s_k - q_{k+1} s_{k+1} & t_k - q_{k+1} t_{k+1} \end{pmatrix} \tag{5.61}$$

That gives us recurrent formulas:

$$\begin{cases} s_{k+2} = s_k - q_{k+1} s_{k+1},\ k = 0, 1, \ldots \\ t_{k+2} = t_k - q_{k+1} t_{k+1},\ k = 0, 1, \ldots \end{cases} \tag{5.62}$$

From formula (5.59) we get

$$r_n = s_n a + t_n b, \tag{5.63}$$

which provides us the following theorem.

Theorem 7. Let D be ED, then

$$\mathrm{syt}(a, b) = s_n a + t_n b, \tag{5.64}$$

where n is the length of EA.

Usually the following formulation is enough

Theorem 8. Let D be an ED. Then there exist $s, t \in D$ such that

$$\gcd(a, b) = sa + tb. \tag{5.65}$$

Theorem 9. Let D be an ED. Then

$$J_D \subseteq P_D \tag{5.66}$$

→ In ED, irreducibles are primes.

Therefore, Euclidean region is UFD.

Proof. Let $j \in J_D$ and let us assume, that $j|ab$, where $a, d \in D$.

We should show that $j|a$ or $j|b$.

Suppose that $j \not| a$, then $j \perp a$ by Lemma 5. Then by Theorem 8 there exist $s, t \in D$ such that

$$1 = sa + tj \quad \Rightarrow \quad b = sab + tbj \quad \Rightarrow \quad j|b. \quad \square \tag{5.67}$$

Corollary 1. .

A. $\mathbb{Z}$ is UFD where irreducibles are primes.

B. $K[x]$ is UFD where irreducibles are primes.

6 Polynomial algebra

6.1 Polynomial rings

6.1.1 Polynomial set

Let R be a ring with unity. Then a set of polynomials with coefficients from R is denoted by

$$R[x] = \{P(x) \mid P(x) = \sum_{k=0}^{n} p_k x^k;\ p_k \in R,\ n \in \mathbb{N}\}.$$

The polynomial

$$0(x) = 0 + 0 \cdot x + 0 \cdot x^2 + \dots \tag{6.1}$$

is called the *zero polynomial* and the polynomial

$$1(x) = 1 + 0 \cdot x + 0 \cdot x^2 + \dots \tag{6.2}$$

is called the unit polynomial. It is the special case of a constant polynomial

$$c(x) = c + 0 \cdot x + 0 \cdot x^2 + \dots, \quad c \in R. \tag{6.3}$$

6.1.2 Calculations

Definition 18. Let $P(x) = \sum_{k=0}^{n} p_k x^k, \quad Q(x) = \sum_{k=0}^{n} q_k x^k \in R[x]$. Then we set

$$\begin{aligned} P(x) = Q(x) &\Leftrightarrow \forall k (p_k = q_k); \\ P(x) + Q(x) &= \sum_{k \geqslant 0} (p_k + q_k) x^k; \\ P(x) \cdot Q(x) &= \sum_{k \geqslant 0} r_k x^k, \end{aligned}$$

$$r_k = \sum_{i=0}^{k} p_i q_{k-i} = \sum_{i+j=k} p_i q_j, \tag{6.4}$$

which is Cauchy's rule of thumb.

6.1.3 Polynomial ring/degree

Theorem 10. The triad $(R[x], +, \cdot)$ is a ring where $0(x)$ is the zero element of the addition and $1(x)$ is the unit-element of the multiplication.

Definition 19. If $p_n \neq 0$, then the degree of a polynomial $P(x) = \sum_{k=0}^{n} p_k x^k$ is set as

$$\deg P(x) = n, \tag{6.5}$$

$$\deg 0(x) = -\infty. \tag{6.6}$$

6.1.4 Degree formula

Remark 4.

$$\begin{aligned} &-\infty + (-\infty) = -\infty \\ &-\infty + k = -\infty, \quad \forall\ k \in \mathbb{Z}. \end{aligned} \tag{6.7}$$

Theorem 11. Degree formula.

Let D be an integral domain and $P(x), Q(x) \in D[x]$. Then

$$\deg P(x)Q(x) = \deg P(x) + \deg Q(x). \tag{6.8}$$

Theorem 12. .

A. Let $R = D$ be an integral domain. Then the ring of polynomials $D[x]$ is the integral domain.

B. Let $R = K$ be a field. Then the ring of polynomials $K[x]$ is the integral domain.

Proof: Let $a(x)b(x) = 0(x)$. According to the degree formula, we have

$$\deg a(x)b(x) = \deg a(x) + \deg b(x) = \deg 0(x) = -\infty. \tag{6.9}$$

If $a(x) \neq 0(x)$ and $b(x) \neq 0(x)$ held true, we would have

$$0 \leq \deg a(x) + \deg b(x) = -\infty. \tag{6.10}$$

$=$ contradiction □

Theorem 13. Let K be a field.

A. The unit group of the ring of polynomials $K[x]$ is

$$K[x]^* = K^*. \tag{6.11}$$

B. A polynomial $j(x) \in K[x] \setminus K$ is irreducible if and only if its only factors are constants k or polynomials $k \cdot j(x)$ where $k \in K \setminus \{0\}$.

C. A polynomial $a(x) \in K[x] \setminus \{0(x)\}$ is reducible if and only if it has a factor $d(x) \in K[x]$ which obeys

$$1 \leq \deg d(x) \leq \deg a(x) - 1. \tag{6.12}$$

D. Specially, one-degree polynomials are not reducible.

Proof. A: $a(x) \in K[x]^* \quad \Rightarrow \quad \exists\, b(x) \in K[x]$ such that

$$a(x)b(x) = 1 \quad \Rightarrow \quad \deg a(x) = \deg b(x) = 0 \quad \Rightarrow \quad a(x), b(x) \in K^*. \quad \square$$

Proof. B: $j(x) = a(x)b(x) \in J_{K[x]} \quad \Rightarrow$

$$a(x) \in [1] = K[x]^* = K^* \quad \Rightarrow \quad a(x) = k, \quad k \in K^*$$

or

$$a(x) \in [j(x)] = j(x)K^* \quad \Rightarrow \quad a(x) = kj(x), \quad k \in K^*. \quad \square$$

Proof. C: Let $a(x) \in K[x] \setminus \{0\}$ be reducible. Then there exists $d(x), b(x) \in K[x] \setminus \{0\}$ such that

$$a(x) = d(x)b(x), \quad d(x) \notin [1] \quad \text{and} \quad d(x) \notin [a(x)] \quad \Rightarrow$$

$$d(x) \notin K^* \quad \text{and} \quad d(x) \notin a(x)K^*.$$

If $\deg d(x) = 0$, then $d(x) \in K^*$; a contradiction.

If $\deg d(x) = \deg a(x)$, then by the degree formula $\deg b(x) = 0$ implying $b(x) = k \in K^*$. Thus $a(x) = kd(x)$ and then $d(x) \in [a(x)]$; a contradiction. $\square$

Proof. D: Homework.

6.2 The unit group of the ring $R[x]$

Let R be commutative ring with a unit. Let us study its unit group $R[x]^*$. Pick $a(x) = a_0 + a_1 x + ... + a_A x^A \in R[x]^*$, then there exists $b(x) = b_0 + b_1 x + ... + b_B x^B \in R[x]^*$ such that

$$1 = a(x)b(x) = (a_0 + a_1 x + ... + a_A x^A)(b_0 + b_1 x + ... + b_B x^B). \tag{6.13}$$

If $a_1 = ... = a_A = 0$, then $a(x) \in R^*$. Otherwise there exists an $A \geq 1$ such that $a_A \neq 0$. Then

$$\begin{aligned} & a_0 b_0 = 1 \\ & a_0 b_1 + a_1 b_0 = 0 \\ & a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \\ & \dots \\ & a_{A-2} b_B + a_{A-1} b_{B-1} + a_A b_{B-2} = 0 \\ & a_{A-1} b_B + a_A b_{B-1} = 0 \\ & a_A b_B = 0 \end{aligned} \tag{6.14}$$

Multiply the second last by a_A to get

$$a_{A-1} a_A b_B + a_A^2 b_{B-1} = 0 \quad \Rightarrow \quad a_A^2 b_{B-1} = 0 \tag{6.15}$$

$$\begin{aligned} & \dots \\ & a_{A-2} b_B + a_{A-1} b_{B-1} + a_A b_{B-2} = 0 \\ & a_{A-1} b_B + a_A b_{B-1} = 0 \\ & a_A b_B = 0 \end{aligned} \tag{6.16}$$

Multiply the third last by a_A^2 to get

$$a_{A-2} a_A^2 b_B + a_{A-1} a_A^2 b_{B-1} + a_A^3 b_{B-2} = 0 \quad \Rightarrow \quad a_A^3 b_{B-2} = 0 \tag{6.17}$$

and so on to the situation

$$\begin{aligned}
&\dots\\
&a_0 b_B + a_1 b_{B-1} + ... + a_A b_0 = 0, \quad A \leq B \qquad (6.18)\\
&a_A^A b_1 = 0
\end{aligned}$$

or

$$\begin{aligned}
&\dots\\
&a_c b_B + a_1 b_{B-1} + ... + a_A b_0 = 0, \quad A = B + c, c > 0, \qquad (6.19)\\
&a_A^A b_1 = 0.
\end{aligned}$$

Anyway, multiply now by a_A^A. Then you get

$$a_A^{A+1} b_0 = 0, \qquad (6.20)$$

where $b_0 \in R^*$ meaning that $b_0 \neq 0$. Then multiplying by b_0^{-1} we are in the situation $a_A^{A+1} = 0$.

Thus if

$$r^K \neq 0 \quad \forall\, r \in R \setminus \{0\},\ K \geq 2, \qquad (6.21)$$

then $a(x) = a_0 \in R^*$.

Otherwise: if there exists an element $r \in R \setminus \{0\}$ such that

$$r^K = 0 \quad \text{for some} \quad K \geq 2, \qquad (6.22)$$

then you may find a non-constant unit polynomial $a(x)$ i.e. $a(x) \in R[x]^* \setminus R^*$.

6.2.1 $\mathbb{Z}_m[x]^*$

Example 14.

$$\mathbb{Z}_{10}[x]^* = \mathbb{Z}_{10}^*.$$

Example 15.

$$1 + 10x \ \in \mathbb{Z}_{20}[x]^*.$$

6.3 Division algorithm

Theorem 14. Division algorithm. Let K be a field. Let $a(x), b(x) \in K[x]$, $a(x)b(x) \neq 0(x)$ and $\deg b(x) \leq \deg a(x)$.
Then $\exists\ q(x), r(x) \in K[x]$ such that

$$[J.A.] \quad a(x) = q(x)b(x) + r(x), \quad \deg r(x) < \deg b(x). \tag{6.23}$$

Moreover, $K[x]$ is the Euclidean domain!

Remark 5. If D is not a field, then the division algorithm does not work necessarily in the polynomial ring $D[x]$!!

The greatest common divisor $d(x) = \text{s.y.t.}(a(x), b(x))$ of $a(x)$ and $b(x)$ can be selected as a monic polynomial.

Based on Euclidean algorithm, there exist $s(x), t(x) \in K[x]$ such that

$$d(x) = s(x)a(x) + t(x)b(x). \tag{6.24}$$

Definition 20. A derivative $Dp(x)$ of a polynomial

$$p(x) = \sum_{k=0}^{n} p_k x^k \in K[x]$$

is the polynomial

$$Dp(x) = \sum_{k=1}^{n} k p_k x^{k-1} \in K[x]. \tag{6.25}$$

Lemma 6. Let K be a field, $p(x) \in K[x]$ and $\deg p(x) \geq 1$. Then

$$\deg Dp(x) = \deg p(x) - 1, \quad \deg p(x) \geq 1; \tag{6.26}$$

$$p(x) \not| Dp(x). \tag{6.27}$$

Theorem 15. Let K be a field and $a(x), b(x), c(x) \in K[x]$. Then

$$a = b^2 c, \quad b \not\sim 1 \quad \Leftrightarrow \quad d = \text{syt}(a, Da) \not\sim 1. \tag{6.28}$$

Proof.

Suppose $a = b^2c$, $b \not\sim 1$. Since $Da = b(2cDb + bDc)$, we have $b|\mathrm{syt}(a, Da)$ and therefore $\mathrm{syt}(a, Da) \not\sim 1$.

Let $d = \mathrm{syt}(a, Da) \not\sim 1$. Then there exists $p \in P_{K[x]}$, $p|d$. Hence $a = ps$ and $Da = pr$. Besides $Da = (Dp)s + pDs$, so $pr = (Dp)s + pDs$. Since $p \nmid Dp$ and p is prime, we have $p|s$. Hence $s = ph$ and $a = ps = p^2h$ for some h and $p \not\sim 1$. □

Claim (6.28) is equivalent to the following claim:
A polynomial is square-free if and only if it does not have common factors with its derivative.

Example 16. Let $p(x) = x^5 + 2x^3 + x \in \mathbb{Q}[x]$. By

$$syt(p, Dp) \not\sim 1 \quad \Rightarrow \tag{6.29}$$

the polynomial $p(x)$ has a multiple factor in $\mathbb{Q}[x]$.

6.4 Zero points of polynomials

Theorem 16. Let K be a field and $p(x) \in K[x]$, $1 \leq \deg p(x)$. Then

$$p(\alpha) = 0,\ \alpha \in K \Leftrightarrow (x - \alpha) \underset{K[x]}{|} p(x). \tag{6.30}$$

Proof. "◊ →": Let $p(\alpha) = 0,\ \alpha \in K$. With the division algorithm we have

$$p(x) = q(x)(x - \alpha) + r(x), \quad \deg r(x) < \deg(x - \alpha) = 1, \tag{6.31}$$

so $r(x) \in K$ is constant. Moreover

$$0 = p(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha) = r(\alpha),$$

$$\Rightarrow \quad r(x) = 0(x) \quad \Rightarrow \quad (x - \alpha) \underset{K[x]}{|} p(x). \tag{6.32}$$

"$\leftarrow \triangle$":

$$(x-\alpha) \underset{K[x]}{\mid} p(x) = (x-\alpha)h(x), \qquad \Rightarrow \quad p(\alpha)=0,\ \alpha \in K. \quad \square \tag{6.33}$$

Remark 6. Let K be a field and $p(x) \in K[x]$, $\deg p(x) = 2$ or $\deg p(x) = 3$. If $p(x)$ is reducible in $K[x]$, then it has a first degree factor and from Theorem 16 we know that $p(\alpha) = 0,\ \alpha \in K$. If there is no zero point in K, then $p(x)$ is irreducible in $K[x]$.

Extending of Definition 3.

Definition 21. Let $K \subseteq L$ be a field and $p(x) \in K[x]$. Then

$$Z_L(p) = \{\alpha \ \in L |\ p(\alpha) = 0\} \tag{6.34}$$

is a *zero set* of $p(x)$ in L.

Definition 22. Let $\alpha \in L$, $K \subseteq L$ a field and $p(x) \ \in K[x]$. If

$$(x-\alpha)^m \underset{L[x]}{\|} p(x), \quad m \in \mathbb{N}, \tag{6.35}$$

then $m = m_L(\alpha, p(x))$ is a *multiplicity of zero point* (order of zero) α of $p(x)$. The number

$$n_L(p(x)) = \sum_{p(\alpha_i)=0,\ \alpha_i \in L} m_L(\alpha_i, p(x)). \tag{6.36}$$

is the number of zeros in L.

Theorem 17. Let K be a field, char K=0, $\alpha \in K$ and $p(x) \ \in K[x]$ and $m \in \mathbb{N}$. Then

$$(x-\alpha)^m \underset{K[x]}{\|} p(x) \quad \Leftrightarrow \tag{6.37}$$

$$D^k p(\alpha) = 0 \quad \forall\ k = 0, ..., m-1 \quad , D^m p(\alpha) \neq 0. \tag{6.38}$$

Remark 7. Theorem 17 does not hold for instance in the ring of polynomials $\mathbb{Z}_p[x]$.

Example 17. Let $p(x) = (x-1)^3(x+1/2)^5$. The zeros of $p(x)$ are $\alpha_1 = 1$ and $\alpha_2 = -1/2$. Their order is

$$m_{\mathbb{Q}}(\alpha_1, p(x)) = 3, \quad m_{\mathbb{Q}}(\alpha_2, p(x)) = 5 \tag{6.39}$$

and the number of zeros

$$n_{\mathbb{Q}} = 3 + 5 = 8. \tag{6.40}$$

Example 18. Let $(x^2+1)(x^2-2) \in \mathbb{R}[x]$. Now, the number of zero points is

$$n_{\mathbb{Q}} = 0 < 4 = \deg p(x). \tag{6.41}$$

$$n_{\mathbb{R}} = m(-\sqrt{2}) + m(\sqrt{2}) = 2 < 4 = \deg p(x). \tag{6.42}$$

$$n_{\mathbb{C}} = 4 = \deg p(x). \tag{6.43}$$

Theorem 18. Let K be a field, $p(x) \in K[x]$ and $\deg p(x) \geq 1$. Then the following holds true

$$n_K(p(x)) \leq \deg p(x). \tag{6.44}$$

Proof:

1. If $\nexists$ a zero point, then $m_K(\alpha, p(x)) = 0$ for all $\alpha \in K$ and $n_K(p(x)) = 0 < 1 \leq \deg p(x)$.

2. Let $\beta_1, ..., \beta_k$ be distinct zero points and let us denote

$$m_j := m_K(\beta_j, p(x)) \geq 1 \quad \text{and} \quad (x-\beta_j)^{m_j} \underset{K[x]}{\parallel} p(x), \quad j = 1, ..., k. \tag{6.45}$$

Then

$$p(x) = (x-\beta_1)^{m_1} p_2(x), \quad p_2(\beta_1) \neq 0 \quad \Rightarrow \quad p_2(\beta_2) = 0, \tag{6.46}$$

$$p_2(x) = (x-\beta_2)^{m_2} p_3(x), \quad p_3(\beta_2) \neq 0 \quad \Rightarrow \quad p_3(\beta_3) = 0 \quad ... \tag{6.47}$$

Eventually

$$p(x) = (x - \beta_1)^{m_1} \cdots (x - \beta_k)^{m_k} p_{k+1}(x), \quad \deg p_{k+1}(x) \geq 0. \tag{6.48}$$

We get

$$\begin{aligned} \deg p(x) &= m_1 + ... + m_k + \deg p_{k+1}(x) \\ &\geq m_1 + ... + m_k = n_K(p(x)). \quad \square \end{aligned} \tag{6.49}$$

Theorem 19. Algebraic fundamental theorem.

Let $p(x) \in \mathbb{C}[x]$, deg $p(x) \geq 1$, then

$$n_{\mathbb{C}}(p(x)) = \deg p(x). \tag{6.50}$$

Theorem 20. Let $K \subseteq L$ be a field, $p(x) \in K[x]$ and $p(x) \in J_{K[x]}$. Then

$$m_L(\alpha, p(x)) \leq 1 \quad \forall \alpha \in L. \tag{6.51}$$

Proof. Since $p \in J_{K[x]}$, then $\deg p(x) \geq 1$ and therefore $p \not| Dp$. Thus according to Lemma 5 it holds that $p \perp Dp$ and according to Theorem 8 we have

$$\mathrm{syt}_{K[x]}(p, Dp) = 1 = sp + tDp, \quad s, t \in K[x] \subseteq L[x]. \tag{6.52}$$

If

$$d \underset{L[x]}{|} p \quad \text{and} \quad d \underset{L[x]}{|} Dp \tag{6.53}$$

then according to Equation (6.52) it holds that $d \underset{L[x]}{|} 1$. Hence

$$\mathrm{syt}_{L[x]}(p, Dp) = 1. \tag{6.54}$$

Then according to Theorem 15 there does not exist a square factor in $L[x]$, so $\nexists$ $\alpha \in L$ such that

$$(x - \alpha)^2 \underset{L[x]}{|} p(x). \tag{6.55}$$

Hence:

If $p(\alpha) = 0$, then $m_L(\alpha, p(x)) = 1$ and

if $p(\alpha) \neq 0$, then $m_L(\alpha, p(x)) = 0$. $\square$

Theorem 21. Let K be a field, $p(x), q(x) \in K[x]$, $p(x) \in J_{K[x]}$ and $p(\alpha) = q(\alpha) = 0$. Then

$$p(x) \underset{K[x]}{|} q(x). \tag{6.56}$$

Proof. Since p is irreducible,

$$d = \mathrm{syt}_{K[x]}(p, q) = 1 \quad \text{or} \quad p. \tag{6.57}$$

If $d = 1$, then $1 = s(x)p(x) + t(x)q(x)$ and $1 = s(\alpha)p(\alpha) + t(\alpha)q(\alpha) = 0$. contradiction.

Hence $d = p$ and consequently $p|q$. □

6.5 Polynomial division / division of factors

Note that if $p \in \mathbb{P}$, then $\mathbb{Z}_p$ is a field.

Definition 23. Let $n \in \mathbb{Z}_{\geq 2}$ and $a(x) = a_0 + a_1x + ... + a_dx^d \in \mathbb{Z}[x]$. The mapping

$$r_n(a_0 + a_1x + ... + a_dx^d) = \overline{a}_0 + \overline{a}_1x + ... + \overline{a}_dx^d \tag{6.58}$$

$$r_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x], \quad r_n(a(x)) = \overline{a}(x),$$

is a *reduction* (mod n).

Theorem 22. The reduction

$$r_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x], \quad r_n(a(x)) = \overline{a}(x),$$

is a morphism in the ring.

Definition 24. A vector $(a_0, ..., a_A) \in \mathbb{Z}^{m+1}$ and a polynomial $a(x) = a_0 + a_1x + ... + a_Ax^A \in \mathbb{Z}[x]$ are primitive if

$$syt(a_0, ..., a_A) = 1. \tag{6.59}$$

Sometimes, it is also required $a_A \geq 1$ for primitivism.

Lemma 7. Let $a(x) \in \mathbb{Z}[x]$ and $B, C \in \mathbb{Z}$.

A. If $a(x)$ is primitive, then

$$B \underset{\mathbb{Z}[x]}{\mid} C \cdot a(x) \quad \Rightarrow \quad B \underset{\mathbb{Z}}{\mid} C. \tag{6.60}$$

B. If $D =$syt$(a_0, ..., a_A)$, then

$$a(x) = D \cdot b(x), \quad b(x) \in \mathbb{Z}[x], \tag{6.61}$$

where the polynomial $b(x)$ is primitive.

C. Polynomials in A. and B. may be replaced by corresponding vectors.

Lemma 8. Let $b(x)$ be $c(x)$ be primitive. Then $b(x)c(x)$ is primitive

Proof. Let

$$a(x) = b(x)c(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{Z}[x] \tag{6.62}$$

and

$$syt(a_0, ..., a_A) = d \geq 2 \quad \Rightarrow \quad \exists \quad p \in \mathbb{P}, \quad p|d. \tag{6.63}$$

We apply a reduction $\pmod p$

$$\overline{a}(x) = \overline{0}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_p[x]. \tag{6.64}$$

$\mathbb{Z}_p[x]$ is the integral domain, hence

$$\overline{b}(x) = \overline{0}(x) \quad \text{or} \quad \overline{c}(x) = \overline{0}(x). \tag{6.65}$$

Hence

$$p|syt(b_0, ..., b_B) \quad \text{or} \quad p|syt(c_0, ..., c_C) \tag{6.66}$$

which is a contradiction. □

Remark 7. A. Let $B = \frac{q}{r} \in \mathbb{Q}$, $q \in \mathbb{Z}$, $r \in \mathbb{Z}^+$, $q \perp r$. Then

$$den(B) := r \tag{6.67}$$

is a denominator of rational number B.

Let $\mathrm{den}(B_j) = r_j$, $j = 1, ..., m$. Then

$$pyn(B_1, ..., B_m) := pyj(r_1, ..., r_m) \tag{6.68}$$

is the least common denominator (=lcd) of $B_1, ..., B_m$.

Lemma 9. Let

$B(x) = B_0 + B_1x + ... + B_mx^m \in \mathbb{Q}[x]$ and

$$R := pyn(B_0, B_1, ..., B_m), \quad Q := syt(RB_0, ..., RB_m). \tag{6.69}$$

Then the polynomial

$$\frac{R}{Q}B(x) := b_0 + b_1x + ... + b_mx^m \in \mathbb{Z}[x] \tag{6.70}$$

is primitive. Moreover $R \perp Q$.

Proof: Since

$$\frac{R}{Q}B_j = b_j, \quad j = 0, 1, ..., m, \tag{6.71}$$

then

$$(RB_0, ..., RB_m) = Q \cdot (b_0, b_1, ..., b_m), \tag{6.72}$$

where $Q = syt(RB_0, ..., RB_m)$. According to 7 it follows that $(b_0, b_1, ..., b_m)$ and the polynomial $b_0 + b_1x + ... + b_mx^m$ are primitive.

Now, it remains to show $R \perp Q$. Let $d = syt(R, Q)$, so $R = dr$ and $Q = dq$, $r, q \in \mathbb{Z}^+$. From (6.71) it follows that

$$Rq_j = Qr_jb_j \quad \Rightarrow \quad rq_j = qr_jb_j, \quad j = 0, 1, ..., m. \tag{6.73}$$

Since $q_j \perp r_j$, we have $r_j | r$ for $j = 0, 1, ..., m$. Hence $R = dr | r$, so $d = 1$. □

Example 19.

$$B(x) = 7 + \frac{21}{5}x + \frac{14}{3}x^2, \quad R = 15, \quad Q = 7. \tag{6.74}$$

Theorem 23. Gauss Lemma. Let $a(x) \in \mathbb{Z}[x]$ be primitive and $\deg a(x) \geq 2$. If $a(x)$ is reducible in the polynomial ring $\mathbb{Q}[x]$, then there exist primitive polynomials

$$b(x), c(x) \in \mathbb{Z}[x], \quad \text{that} \quad a(x) = b(x)c(x). \tag{6.75}$$

Proof. Suppose that

$$a(x) = B(x)C(x), \quad B(x), C(x) \in \mathbb{Q}[x]. \tag{6.76}$$

According to Lemma 9 there exist $R, Q, T, S \in \mathbb{Z}^+$ such that

$$\frac{R}{Q}B(x) := b(x) \in \mathbb{Z}[x],$$

$$\frac{T}{S}C(x) := c(x) \in \mathbb{Z}[x],$$

$$R \perp Q, \quad T \perp S, \tag{6.77}$$

where $b(x)$ and $c(x)$ are primitive. Moreover

$$RTa(x) = QSb(x)c(x). \tag{6.78}$$

Since $R \perp Q$ and $a(x)$ is primitive, then $Q|T = Qt$ and analogously $S|R = Qr$. Hence

$$rta(x) = b(x)c(x), \tag{6.79}$$

where $b(x)c(x)$ is primitive, so $rt = 1$ and finally $a(x) = b(x)c(x)$. □

According to Gauss lemma, reducible $a(x) \in \mathbb{Z}[x]$ can be factorized in $\mathbb{Z}[x]$. Thus, the polynomial is irreducible in $\mathbb{Q}[x]$ if it is prime in $\mathbb{Z}[x]$.

Theorem 24. Let $a(x) \in \mathbb{Z}[x]$. Then there exists the unique representation

$$a(x) = Aa_1(x) \cdots a_n(x), \quad A \in \mathbb{Z}, \tag{6.80}$$

where $a_1(x), ..., a_k(x) \in \mathbb{Z}[x]$ are primitive irreducible polynomials.

Theorem 25. Let $p \in \mathbb{P}$, $a(x) \in \mathbb{Z}[x]$, $\overline{a}(x) \in \mathbb{Z}_p[x]$ and $A = \deg a(x) = \deg \overline{a}(x)$. If $\overline{a}(x)$ is irreducible in $\mathbb{Z}_p[x]$, then $a(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Suppose contradiction

$$a(x) = b(x)c(x), \quad B = \deg b(x) \geq 1, \ C = \deg c(x) \geq 1. \tag{6.81}$$

Let us apply $\pmod p$:

$$\overline{a}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_p[x]. \tag{6.82}$$

Since

$$\deg \overline{b}(x) \leq B, \quad \deg \overline{c}(x) \leq C \tag{6.83}$$

and

$$\deg \overline{b}(x) + \deg \overline{c}(x) = \deg \overline{a}(x) = A, \tag{6.84}$$

then

$$\deg \overline{b}(x) = B \geq 1, \quad \deg \overline{c}(x) = C \geq 1. \tag{6.85}$$

Hence $\overline{a}(x)$ would not be irreducible in $\mathbb{Z}_p[x]$.

contradiction. □

Theorem 26. Eisenstein's criteria. Let

$$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{Z}[x], \quad \deg a(x) = A \geq 2.$$

If there exists $p \in \mathbb{P}$ such that

$$p | a_i \quad \forall\ i = 0, 1, ..., A-1, \quad p^2 \not| a_0, \quad p \not| a_A, \tag{6.86}$$

then $a(x)$ is irreducible polynomial in $\mathbb{Q}[x]$.

Proof. Let

$$a(x) = b(x)c(x) \in \mathbb{Z}[x] \tag{6.87}$$

or

$$a_0 + a_1 x + ... + a_A x^A = (b_0 + b_1 x + ... + b_B x^B)(c_0 + ... + c_C x^C) \tag{6.88}$$

and

$$B = \deg b(x) \geq 1,\ C = \deg c(x) \geq 1, \quad B + C = A. \tag{6.89}$$

We have

$$p|a_0 = b_0 c_0, \quad p^2 \not| a_0 \quad \Rightarrow \quad \text{either} \quad p|b_0 \quad \text{or} \quad p|c_0. \tag{6.90}$$

Let us suppose

$$p|b_0 \quad \text{and} \quad p \not| c_0. \tag{6.91}$$

Since

$$p|a_1 = b_0 c_1 + b_1 c_0, \quad \Rightarrow \quad p|b_1 \tag{6.92}$$

...

$$p|a_B = b_0 c_B + ... + b_B c_0, \quad \Rightarrow \quad p|b_B. \tag{6.93}$$

But

$$a_A = b_B c_C, \quad \Rightarrow \quad p|a_A. \tag{6.94}$$

contradiction. □

Theorem 27. Let

$$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{Z}[x]$$

and

$$a(r/s) = 0, \quad r, s \in \mathbb{Z}, \quad r \perp s, \tag{6.95}$$

then

$$r|a_0, \quad s|a_A, \tag{6.96}$$

This can be used to find possible rational zero-points for a polynomial.

Proof. Equation (6.95) implies

$$s^A a_0 + s^{A-1} r a_1 + ... + s r^{A-1} a_{A-1} + r^A a_A = 0 \tag{6.97}$$

The assumption $r \perp s$ implies $r | a_0$ and $s | a_A$. □

Theorem 28. Let K be a field, $p(x) \in K[x]$, $p(x) \in J_{K[x]}$, $\deg p(x) = d$ and $k \in K$. Then

$$p^*(x) = x^d p(1/x) \in J_{K[x]}, \quad \vec{p}_k(x) = p(x+k) \in J_{K[x]}. \tag{6.98}$$

Example 20.

Consider the decomposition of the polynomial

$$a(x) = 4x^3 - 2x^2 + 3x + 5 \in \mathbb{Z}[x] \tag{6.99}$$

If a polynomial of the degree 3 is reducible, it has at least one factor of the degree 1, so

$$a(x) = b(x)c(x), \quad \deg b(x) = 1. \tag{6.100}$$

Set $p = 3$ and apply the reduction $\pmod 3$:

$$\overline{a}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_3[x], \quad \deg \overline{b}(x) = 1. \tag{6.101}$$

Then

$$\overline{b}(x) \underset{\mathbb{Z}_3[x]}{|} \overline{a}(x) = x^3 + x^2 + 2, \quad \deg \overline{b}(x) = 1. \tag{6.102}$$

According to Theorem 16, $\overline{a}(x)$ has a zero point in $\mathbb{Z}_3$. But

$$\overline{a}(0) = 2, \quad \overline{a}(1) = 1, \quad \overline{a}(2) = 2. \tag{6.103}$$

contradiction. Therefore $a(x)$ is irreducible in the ring $\mathbb{Z}[x]$ and moreover in the ring $\mathbb{Q}[x]$.

Example 21. Eisenstein's criteria: $p = 7$ and

$$a(x) = 7 + 7x - 14x^3 + 2x^5 \in J_{\mathbb{Q}[x]}. \tag{6.104}$$

Using Theorem 28 we get

$$b(x) = x^5 a(1/x) = 2 - 14x^2 + 7x^4 + 7x^5 \in J_{\mathbb{Q}[x]}; \tag{6.105}$$

$$b(x-1) = 2 - 14(x-1)^2 + 7(x-1)^4 + 7(x-1)^5 \in J_{\mathbb{Q}[x]}; \tag{6.106}$$

Example 22.

Let $p \in \mathbb{P}$. Then

$$a(x) = 1 + x + x^2 + ... + x^{p-1} \in J_{\mathbb{Q}[x]}. \tag{6.107}$$

Proof. We have

$$a(x) = \frac{x^p - 1}{x - 1}, \tag{6.108}$$

and we substitute $x = t + 1$. Then

$$a(x) = a(t+1) = \frac{(t+1)^p - 1}{t} = \\ t^{p-1} + \binom{p}{p-1} t^{p-2} + ... + \binom{p}{2} t + \binom{p}{1}. \tag{6.109}$$

We should know that

$$p \left| \binom{p}{k} \right. \quad \forall\ 1 \leq k \leq p - 1. \tag{6.110}$$

We can see that assumption from Eisenstein's Theorem is satisfied, so $a(t+1)$ is irreducible and hence $a(x)$ is irreducible in the ring $\mathbb{Q}[x]$.

6.5.1 Reducibility in $\mathbb{C}[x]$ and $\mathbb{R}[x]$

Let

$$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{C}[x], \quad \deg a(x) \geq 1, \tag{6.111}$$

then

$$a(x) = a_A(x - \alpha_1) \cdots (x - \alpha_A), \quad \alpha_1, ..., \alpha_A \in \mathbb{C} \tag{6.112}$$

by the Fundamental Theorem of Algebra. Consider now

$$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{R}[x], \quad \deg a(x) \geq 1. \tag{6.113}$$

Then we have

$$a(z) = 0 \quad \Leftrightarrow \quad a(\overline{z}) = 0 \tag{6.114}$$

because

$$0 = \overline{a(z)} = a_0 + a_1 \overline{z} + ... + a_A \overline{z}^A. \tag{6.115}$$

Therefore, non-real complex roots exist in pairs:
$\beta_j \neq \overline{\beta_j}$, $\beta_j \in \{\alpha_1, ..., \alpha_A\}$. Consequently

$$\begin{aligned} a(x) = a_A(x - \alpha_1) \cdots (x - \alpha_h) \cdot (x - \beta_1)(x - \overline{\beta_1}) \cdots (x - \beta_k)(x - \overline{\beta_k}), \\ \alpha_1, ..., \alpha_h \in \mathbb{R}, \quad \beta_1, ..., \beta_k \in \mathbb{C} \setminus \mathbb{R}, \quad h + 2k = A. \end{aligned} \tag{6.116}$$

Write $\beta = a + ib$, where $a, b \in \mathbb{R}$ and compute

$$(x - \beta_1)(x - \overline{\beta_1}) = (x - a - ib)(x - a + ib) = (x - a)^2 + b^2 \in \mathbb{R}[x]. \tag{6.117}$$

Hence

$$\begin{aligned} a(x) = a_A(x - \alpha_1) \cdots (x - \alpha_h) \cdot ((x - a_1)^2 + b_1^2) \cdots ((x - a_k)^2 + b_k^2), \\ (x - \alpha_1), ..., (x - \alpha_h), ((x - a_1)^2 + b_1^2), \ldots, ((x - a_k)^2 + b_k^2) \in \mathbb{R}[x]. \end{aligned}$$

In other words: Any non-constant polynomial with real coefficients, factors in $\mathbb{R}[x]$ into first and second degree polynomials.

7 Symmetric polynomials

Definition 25. Let R be a ring. A polynomial

$$P(t_1, ..., t_m) = \sum_{Finite} p_{i_1,...,i_m} t_1^{i_1} \cdots t_m^{i_m}, \quad p_{i_1,...,i_m} \in R \tag{7.1}$$

is m variable R-coefficient polynomial, where $t_1, ..., t_m$ are polynomial variables. A degree of a polynomial P is the number

$$\deg P(t_1, ..., t_m) = \max\{i_1 + ... + i_m\}. \tag{7.2}$$

For all R-coefficient polynomials we use the notation

$$R[t_1, ..., t_m]. \tag{7.3}$$

Let $< i_1, ..., i_m >$ be exponents of a term $p_{i_1,...,i_m} t_i^{i_1} \cdots t_m^{i_m}$. Then, terms can be compared as in the case of a single variable polynomial. Thus, $R[t_1, ..., t_m]$ can be defined in a natural way by the identity and the multiplication.

It can be proved that $(R[t_1, ..., t_m], +, \cdot)$ is a ring.

Let S_M be a set of permutations of $\{1, 2, ..., m\}$. If $\lambda \in S_m$, then we write

$$p^\lambda(t_1, ..., t_m) = p(t_{\lambda(1)}, ..., t_{\lambda(m)}). \tag{7.4}$$

Definition 26. A polynomial p is symmetric if

$$p(t_{\lambda(1)}, ..., t_{\lambda(m)}) = p(t_1, ..., t_m) \quad \forall\ \lambda \in S_m. \tag{7.5}$$

7.1 Elementary Symmetric Polynomials

Definition 27. Polynomials

$$s_k = s_k(t_1, ..., t_m) = \tag{7.6}$$

$$\sum_{1 \le j_1 < j_2 < ... < j_k \le m} t_{j_1} t_{j_2} \cdots t_{j_k}, \quad k = 1, ..., m,$$

are *elementary symmetric polynomials.*

Lemma 10. Elementary symmetric polynomials $s_1, ..., s_m$ are symmetric polynomials, i.e.

$$s_k(t_{\lambda(1)}, ..., t_{\lambda(m)}) = s_k(t_1, ..., t_m) \quad \forall\, \lambda \in S_m \tag{7.7}$$

for all $k = 1, ..., m$.

They look like

$$s_1 = t_1 + ... + t_m; \tag{7.8}$$

$$s_2 = t_1t_2 + t_1t_3 + ... + t_{m-1}t_m; \tag{7.9}$$

$$s_3 = t_1t_2t_3 + t_1t_2t_4 + ... + t_{m-2}t_{m-1}t_m; \tag{7.10}$$

...

$$s_m = t_1t_2 \cdots t_{m-1}t_m; \tag{7.11}$$

Theorem 29. Fundamental theorem about symmetric polynomials.

A symmetric polynomial $S(t_1, ..., t_m)$ from $R[t_1, ..., t_m]$ can be represented by elementary symmetric polynomials $s_1 = s_1(t_1, ..., t_m), ..., s_m = s_m(t_1, ..., t_m)$. In other words, there exists a polynomial $P(s_1, ..., s_m) \in R[s_1, ..., s_m]$ such that

$$S(t_1, ..., t_m) = P(s_1(t_1, ..., t_m), ..., s_m(t_1, ..., t_m)). \tag{7.12}$$

Let $S \subseteq R$ be a ring. Suppose that a polynomial $a(x) = a_0 + a_1x + ... + x^m \in S[x]$ is factorized in $R[x]$ as follows

$$a(x) = (x - \alpha_1) \cdots (x - \alpha_m), \quad \alpha_1, ..., \alpha_m \in R. \tag{7.13}$$

Theorem 30. Let $b(t_1, ..., t_m) \in S[t_1, ..., t_m]$ be a symmetric polynomial. Then

$$b(\alpha_1, ..., \alpha_m) \in S. \tag{7.14}$$

Let $K \subseteq L$ be a field. Suppose that a polynomial $a(x) = a_0 + a_1x + ... + a_mx^m \in K[x]$ is factorized in $L[x]$ as follows

$$a(x) = a_m(x - \alpha_1)\cdots(x - \alpha_m), \quad \alpha_1, ..., \alpha_m \in L. \tag{7.15}$$

Theorem 31. Let $b(t_1, ..., t_m) \in K[t_1, ..., t_m]$ be a symmetric polynomial. Then

$$b(\alpha_1, ..., \alpha_m) \in K. \tag{7.16}$$

Example 23. Let

$$x^2 + bx + c = (x - \alpha)(x - \beta) \in \mathbb{Q}[x]. \tag{7.17}$$

Then

$$\alpha^2 + \beta^2 \in \mathbb{Q}, \tag{7.18}$$

$$\alpha^3 + 2\alpha\beta + \beta^3 \in \mathbb{Q}. \tag{7.19}$$

8 Field extension

8.1 Field extension

Definition 28. A field K is a subfield of L or L is a field extension of $K \Leftrightarrow K$ and L are fields and $K \subseteq L$.

This course uses the notation:
$L : K$ and $K \leqslant L$.

If $L : K$, then we can interpret L as a vector space over K by setting addition

$$L \times L \ \to L, \quad (\alpha, \beta) \ \to \alpha + \beta; \tag{8.1}$$

and scalar $r \in K$ multiplication

$$K \times L \ \to L, \quad (r, \alpha) \ \to r\alpha \tag{8.2}$$

using the field operations.

Definition 29. A degree of a field extension or $[L : K] = \dim_K L$ is finite if $[L : K] < \infty$

8.2 Field tower

If $K \leqslant M \leqslant L$, then the field M is called a *field tower.*

$$\begin{tikzcd} L_1 & & L_2 \\ & L_3 \arrow[ul, dash] \arrow[ur, dash] & \\ & K \arrow[u, dash] & \end{tikzcd} \quad \Leftrightarrow \begin{cases} K \leqslant L_3 \leqslant L_1 \\ \text{and} \\ K \leqslant L_3 \leqslant L_2 \end{cases}$$

Theorem 32. Let $K \leqslant M \leqslant L$ be a field tower. Then

$$[L : K] = [L : M][M : K]. \tag{8.3}$$

Proof. Let

$$\begin{aligned} M = \langle \alpha_1, ..., \alpha_r \rangle_K = K\alpha_1 + ... + K\alpha_r, \quad \dim_K M = r; \\ L = \langle \beta_1, ..., \beta_s \rangle_M = M\beta_1 + ... + M\beta_s, \quad \dim_M L = s. \end{aligned} \tag{8.4}$$

Set $\gamma \in L$. Then

$$\begin{aligned} \gamma &= \sum_{j=1}^{s} m_j \beta_j, \quad m_j \in M; \\ m_j &= \sum_{i=1}^{r} k_{ij} \alpha_i, \quad k_{ij} \in K \quad \Rightarrow \\ \gamma &= \sum_{i=1}^{r} \sum_{j=1}^{s} k_{ij} \alpha_i \beta_j \in K\alpha_1\beta_1 + ... + K\alpha_r\beta_s, \\ &\#\{\alpha_i\beta_j\} = rs. \end{aligned} \tag{8.5}$$

It remains to show that $\{\alpha_i\beta_j\}$ is linearly independent.

$$\begin{aligned}
&\sum_{i=1}^{r}\sum_{j=1}^{s} h_{ij}\alpha_i\beta_j = 0, \quad h_{ij} \in K \quad \Rightarrow \\
&\sum_{j=1}^{s}\left(\sum_{i=1}^{r} h_{ij}\alpha_i\right)\beta_j = 0 \Rightarrow \\
&\sum_{i=1}^{r} h_{ij}\alpha_i = 0 \Rightarrow \\
&h_{ij} = 0, \quad \forall \quad i, j. \quad \square
\end{aligned} \tag{8.6}$$

8.3 Quotient field

We will focus on the concept of rational numbers and rational functions.

Definition 30. Let D be an integral domain and $a, b, c, d \in D$, $bd \neq 0$. Then we define

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc. \tag{8.7}$$

Theorem 33. The relation $\sim$ is the equivalence for $D \times (D \setminus \{0\}) = \mathcal{D}$.

Definition 31. The class of equivalence

$$[a, b] = \{(c, d) \in \mathcal{D} |\ (c, d) \sim (a, b)\}$$

has addition defined as

$$[a_1, b_1] + [a_2, b_2] = [a_1b_2 + a_2b_1, b_1b_2] \tag{8.8}$$

and multiplication as

$$[a_1, b_1][a_2, b_2] = [a_1a_2, b_1b_2] \tag{8.9}$$

for all $(a_1, b_1), (a_2, b_2) \in \mathcal{D}$.

We use the notation

$$a/b = \frac{a}{b} = [a,b] \quad \text{and} \quad Q(D) = \{a/b|\ (a,b) \in \mathcal{D}\}.$$

It can be proven that

Theorem 34. The triad $(Q(D), +, \cdot)$ is a field.

We say that $Q(D)$ is a *quotient field* (field of fractions) of D. Then the isomorphic result

$$\{\frac{a}{1}|\ a \in D\} \cong D, \tag{8.10}$$

holds true and hence we can write $a = a/1$. Moreover

$$ab^{-1} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1} = \frac{a}{1}\frac{1}{b} = \frac{a}{b} \tag{8.11}$$

Example 24.

Let $D = \mathbb{Z}$, which is an integral domain. Then we define the quotient field $Q(\mathbb{Z})$ which determines rational numbers

Definition 32. The set of rational numbers is the field $\mathbb{Q} = Q(\mathbb{Z})$.

Cancellation of rational numbers

$$\frac{ac}{bc} = \frac{a}{b} \tag{8.12}$$

and convert

$$\frac{a}{b} = \frac{da}{db} \tag{8.13}$$

follows from Definition 31.

Example 25.

Let K be a field, then the ring of polynomials $D = K[x]$ is the integral domain.

Definition 33. A field of rational function is the field $K(x) = Q(K[x])$.

The rules which were mentioned above hold true:

$$\frac{(x^2-1)x}{(x-1)x^2} = \frac{x+1}{x} = 1 + \frac{1}{x}. \tag{8.14}$$

Example 26.

Let K be a field. The set of series $D = K[[T]]$ is an integral domain. Then its quotient field is isomorphic to Laurent series, so in other words

Theorem 35.

$$K((T)) \cong Q(K[[T]]). \tag{8.15}$$

These structures have the following relationships:

$$K[T] \subset K(T) \subset K((T)), \tag{8.16}$$

$$K[T] \subset K[[T]] \subset K((T)). \tag{8.17}$$

Definition 34. The derivation

$$D: \ K((T)) \to K((T))$$

is a linear mapping and it satisfies

$$DT^k = kT^{k-1} \quad \forall \quad k \in \mathbb{Z}. \tag{8.18}$$

9 Algebraic numbers

9.1 Algebraic elements of subfields

Definition 35. Let $K \subseteq L$ be a field and $\alpha \in L$. If there exists $p(x) \in K[x] \setminus K$ such that

$$p(\alpha) = 0 \tag{9.1}$$

then α is algebraic over the field K.

Otherwise α is transcendental over the field K.

Example 27. A. It is known that π is transcendental over $\mathbb{Q}$.

B. Since

$$p(\pi) = 0, \quad p(x) = x - \pi \in \mathbb{R}[x], \tag{9.2}$$

it is obvious that π is algebraic over $\mathbb{R}$.

Definition 36. Let $K \subseteq L$ be a field and $\alpha \in L$. The *minimum polynomial* of the algebraic number α is a monic polynomial $M_\alpha(x) \in K[x] \setminus K$ of the lowest possible degree such that

$$M_\alpha(\alpha) = 0. \tag{9.3}$$

Let $\deg M_\alpha(x) = n$, then the degree of the algebraic number α over K is

$$\deg \alpha = \deg_K \alpha = n \geq 1. \tag{9.4}$$

Theorem 36. Let $K \subseteq L$ be a field and $\alpha \in L$. The minimal polynomial $M_\alpha(x) \in K[x]_n$ of α is unique and irreducible in the ring of polynomials $K[x]$.

Proof. If $M_\alpha(x)$ was reducible, then

$$M_\alpha(x) = A_1(x)A_2(x), \quad \deg A_1(x), \deg A_2(x) \leq n - 1. \tag{9.5}$$

Since

$$0 = M_\alpha(\alpha) = A_1(\alpha)A_2(\alpha), \tag{9.6}$$

then there would be a polynomial $A_i(x) \in K[x]$ such that

$$A_i(\alpha) = 0, \quad \deg A_i(x) \leq n - 1. \quad \text{contradiction.} \tag{9.7}$$

Uniqueness: Let $M_\alpha(x), N_\alpha(x) \in K[x]_n$ be two minimal polynomials of α. They are irreducible and $M_\alpha(\alpha) = N_\alpha(\alpha) = 0$, so according to Theorem **??** we have

$$M_\alpha(x) \underset{K[x]}{\mid} N_\alpha(x) \quad \text{and} \quad N_\alpha(x) \underset{K[x]}{\mid} M_\alpha(x). \tag{9.8}$$

Therefore $M_\alpha(x) = k \cdot N_\alpha(x)$ and moreover $M_\alpha(x) = N_\alpha(x)$. □

Definition 37. Let $\alpha \in \mathbb{C}$ be an algebraic number over $\mathbb{Q}$ (in that case, we shortly say an algebraic number) such that $\deg \alpha = n$. If $\alpha \in \mathbb{C}$ is not an algebraic number, then α is transcendental.

Let α be an algebraic number such that $\deg \alpha = n$. Then the minimal polynomial $M_\alpha(x) \in \mathbb{Q}[x]_n$ is irreducible in the polynomial ring and $\deg M_\alpha(x) = n$. Hence it is of the form

$$M_\alpha(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, \quad a_i \in \mathbb{Q}, \tag{9.9}$$

which is an irreducible monic polynomial.

9.1.1 Algebraic integer

Definition 38. Let $\alpha \in \mathbb{C}$ be an algebraic number such that $\deg \alpha = n$ and its minimal polynomial

$$M_\alpha(x) \in \mathbb{Z}[x]_n. \tag{9.10}$$

Then α is an algebraic integer of the degree n.

Thus, the minimum polynomial of the degree n is

$$M_\alpha(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, \quad a_i \in \mathbb{Z}, \tag{9.11}$$

which is an irreducible monic polynomial.

Example 28.

$$\frac{1+\sqrt{5}}{2} \tag{9.12}$$

is the algebraic integer of degree 2..

Example 29.

$$x^3 - 2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \tag{9.13}$$

According to Theorem 20 zero points of an irreducible polynomial are distinct. Let $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n \in \mathbb{C}$ be zero points of the minimal polynomial $M_\alpha(x)$. Therefore $\alpha_i \neq \alpha_j$ if $i \neq j$.

Definition 39. Conjugates of an algebraic number α are zero points of its minimal polynomial $M_\alpha(x)$, i.e.

$$\alpha_1, ..., \alpha_n \in \mathbb{C}. \tag{9.14}$$

Definition 40.

Monomorphisms associated with conjugates of algebraic number α are morphisms

$$\sigma_1, ..., \sigma_n : \ \mathbb{K} = \mathbb{Q}(\alpha) \to \mathbb{C}; \tag{9.15}$$

which satisfy:

$$\sigma_i \quad \text{is an injection;} \tag{9.16}$$

$$\sigma_i(x + y) = \sigma_i(x) + \sigma_i(y); \tag{9.17}$$

$$\sigma_i(xy) = \sigma_i(x)\sigma_i(y); \tag{9.18}$$

$$\sigma_i|_{\mathbb{Q}} = \mathrm{Id} : \mathbb{Q} \to \mathbb{Q} \quad \text{identity} \tag{9.19}$$

$$\sigma_i(\alpha) = \alpha_i, \quad i = 1, ..., n. \tag{9.20}$$

Specially

$$\sigma_1 = \mathrm{Id}|_{\mathbb{K}}, \quad \sigma_1(\alpha) = \alpha. \tag{9.21}$$

Definition 41. Let $\mathbb{Q} \leqslant \mathbb{K} \leqslant \mathbb{C}$ and $[\mathbb{K} : \mathbb{Q}] < \infty$, then $\mathbb{K}$ is a *number field.*

Theorem 37. Let $\mathbb{K}$ be a number field and $\sigma: \mathbb{K} \to \mathbb{C}$ a monomorphism. Then

$$\sigma(a) = a \quad \forall a \in \mathbb{Q}. \tag{9.22}$$

$$\sigma(a\alpha + b\beta) = a\sigma(\alpha) + b\sigma(\beta), \quad \forall a, b \in \mathbb{Q}, \alpha, \beta \in \mathbb{K}. \tag{9.23}$$

$$\sigma(p(\beta)) = p(\sigma(\beta)) \quad \forall \beta \in \mathbb{K}, \quad p(x) \in \mathbb{Q}[x]. \tag{9.24}$$

9.2 Extension by an element

Definition 42. Let $S \leqslant R$ be a ring extension and $\alpha_1, ..., \alpha_m \in R$. Then the set

$$S[\alpha_1, ..., \alpha_m] = \bigcap_{S \cup \{\alpha_1, ..., \alpha_m\} \subseteq V \leqslant R} V, \tag{9.25}$$

is the smallest subring of R containing S and $\alpha_1, ..., \alpha_m$.

We can see that $S[\alpha_1, ..., \alpha_m]$ consists of polynomial values in points $\alpha_1, ..., \alpha_m$. Specially,

$$S[\alpha] = \{s_0 + s_1\alpha + s_2\alpha^2 + ... + s_n\alpha^n |\ s_i \in S,\ n \in \mathbb{N}\} \tag{9.26}$$

is a single variable α polynomial ring.

Definition 43. Let $K \leqslant L$ be a field extension and $\alpha_1, ..., \alpha_m \in L$. then the set

$$\langle K, \alpha_1, ..., \alpha_m \rangle = \bigcap_{K \cup \{\alpha_1, ..., \alpha_m\} \subseteq M \leqslant L} M, \tag{9.27}$$

is the smallest subfield of L containing K and $\alpha_1, ..., \alpha_m$.

Theorem 38.

$$\langle K, \alpha_1, ..., \alpha_m \rangle = K(\alpha_1, ..., \alpha_m) := \tag{9.28}$$
$$\left\{ \frac{A}{B} |\ A, B \in K[\alpha_1, ..., \alpha_m],\ B \neq 0 \right\}.$$

Theorem 39.

$$\langle K, \alpha \rangle = K(\alpha) := \left\{ \frac{A(\alpha)}{B(\alpha)} |\ A(\alpha), B(\alpha) \in K[\alpha],\ B \neq 0 \right\}. \tag{9.29}$$

Theorem 40. If α is transcendental over K, then

$$K[\alpha] \cong K[x], \tag{9.30}$$

i.e. rings $K[\alpha]$ and $K[x]$ are isomorphic. Moreover

$$K(\alpha) \cong K(x), \tag{9.31}$$

i.e. fields $K(\alpha)$ and $K(x)$ are isomorphic.

10 Algebraic fields

Definition 44. An algebraic extension $L : K$ is algebraic if all elements of L are algebraic over K.

Remark 8.

$$K\alpha_1 + ... + K\alpha_m := \{k_1\alpha_1 + ... + k_m\alpha_m |\ k_1, ..., k_m \in K\}; \tag{10.1}$$

$$K[\beta]_n := K\beta^0 + K\beta^1 + ... + K\beta^n. \tag{10.2}$$

$$K[\beta]_n \subseteq K[\beta] = K\beta^0 + K\beta^1 + ... \tag{10.3}$$

Theorem 41. Let $L : K$ and $\beta \in L$. Then

A. $\quad \deg_K \beta = s \quad \Leftrightarrow$

$$K[\beta] = K[\beta]_{s-1} \quad \text{and} \quad \dim_K K[\beta] = s; \tag{10.4}$$

B. If β is algebraic over K, then $K[\beta]$ is a field;

$$C. \qquad [L:K] = r < \infty \quad \Rightarrow \quad \deg_K \beta = s|r; \tag{10.5}$$

D. A finite field extension $L : K$ is algebraic.

Theorem 42. Let $L : K$, $\alpha \in L$ be algebraic over K and $\deg_K \alpha = n$. Then

$$A. \qquad \langle K, \alpha \rangle = K[\alpha] = K + K\alpha + ... + K\alpha^{n-1}; \tag{10.6}$$

$$B. \qquad [\langle K, \alpha \rangle : K] = \deg_K \alpha = n; \tag{10.7}$$

$$C. \qquad \beta \in \langle K, \alpha \rangle \quad \Rightarrow \quad \deg_K \beta = k|n; \tag{10.8}$$

D. The field extension $\langle K, \alpha \rangle$ is algebraic.

Proof.

Theorem 41 A. "$\Rightarrow$": Let $\deg_K \beta = s$. First, we show that

$$K[\beta] = K[\beta]_{s-1} = K\beta^0 + K\beta^1 + ... + K\beta^{s-1}. \tag{10.9}$$

Consider the minimal polynomial of β

$$M_\beta(x) = b_0 x^0 + ... + x^s \in K[x] \qquad \text{and} \quad a(\beta) \in K[\beta], \quad a(x) \in K[x]. \tag{10.10}$$

We apply the division algorithm:

$$a(x) = q(x)M_\beta(x) + r(x), \quad \deg r(x) \leq s - 1 \quad \Rightarrow$$
$$a(\beta) = q(\beta)M_\beta(\beta) + r(\beta) = r(\beta) \in K[\beta]_{s-1} \quad \Rightarrow$$
$$K[\beta] \subseteq K[\beta]_{s-1} \quad \Rightarrow \quad K[\beta] = K[\beta]_{s-1}. \tag{10.11}$$

Next, we show that $\{\beta^0, \beta^1, ..., \beta^{s-1}\}$ forms a base. So, let us suppose that

$$k_0\beta^0 + k_1\beta^1 + ... + k_{s-1}\beta^{s-1} = 0,$$

$$k_0, ..., k_{s-1} \in K,\ k_i \neq 0,\ \text{for all } i = 0, ..., s-1 \quad \Rightarrow$$

$$\deg_K \beta \leq s-1. \quad \text{contradiction.} \quad \Rightarrow$$

$$\dim_K K[\beta] = \dim_K K[\beta]_{s-1} = s. \quad \Box \quad (10.12)$$

"$\Leftarrow$": Let $K[\beta] = K[\beta]_{s-1}$ and $\dim_K K[\beta] = s$. Hence $\dim_K K[\beta]_{s-1} = s$ and

$$K[\beta]_{s-1} = K\beta^0 + K\beta^1 + ... + K\beta^{s-1}, \quad (10.13)$$

where $\{\beta^0, \beta^1, ..., \beta^{s-1}\}$ are linearly independent over K. If

$$p(x) \in K[x], \quad 1 \leq \deg p(x) \leq s-1, \quad p(\beta) = 0, \quad \Rightarrow$$

$$\{\beta^0, \beta^1, ..., \beta^{s-1}\} \quad \text{would be linearly dependent.} \quad \text{Contradiction}$$

$$\Rightarrow \quad \deg_K \beta \geq s. \quad (10.14)$$

On the other hand

$$\beta^s \in K[\beta] = K[\beta]_{s-1} \quad \Rightarrow$$

$$\beta^s = k_0\beta^0 + k_1\beta^1 + ... + k_{s-1}\beta^{s-1} \quad \Rightarrow \deg_K \beta \leq s. \quad (10.15)$$

$$\rightsquigarrow \deg_K \beta = s. \quad \Box$$

Proof. Theorem 41 C:
We know from B. that $K[\beta]$ is a subfield of L. Since $[L : K] = r < \infty$, according to the item A, we have

$$\dim_K K[\beta] := s \leq \dim_K L = r \quad \Rightarrow \quad \deg_K \beta = s \leq r. \quad (10.16)$$

$K \leqslant K[\beta] \leqslant L$ forms a field tower. From Theorem 32 we have

$$[L : K] = [L : K[\beta]][K[\beta] : K] \quad \Rightarrow \quad r = vs, \quad v = [L : K[\beta]]. \quad (10.17)$$

Hence

$$s|r. \quad \square \tag{10.18}$$

Remark 8.

Theorem 39 says

$$\langle K, \alpha \rangle = K(\alpha) = \left\{ \frac{A(\alpha)}{B(\alpha)} | \ A(\alpha), B(\alpha) \in K[\alpha], \ B \neq 0 \right\}. \tag{10.19}$$

but 42 A. says that $K(\alpha)$ is determined just by polynomial values.

Example 30.

Consider the field extension

$$\mathbb{L} := \langle \mathbb{Q}, 2^{1/2}, 2^{1/3} \rangle = \langle \langle \mathbb{Q}, 2^{1/2} \rangle, 2^{1/3} \rangle. \tag{10.20}$$

Let us denote

$$\mathbb{M}_2 := \langle \mathbb{Q}, 2^{1/2} \rangle, \quad \mathbb{M}_3 := \langle \mathbb{Q}, 2^{1/3} \rangle. \tag{10.21}$$

At first

$$\begin{multline} M_{\alpha_1} = x^2 - 2 = (x - \alpha_1)(x - \alpha_2), \quad \alpha_1 = 2^{1/2}, \\ M_{\alpha_1} \in J_{\mathbb{Q}[x]}, \quad \deg_{\mathbb{Q}} M_{\alpha_1} = 2, \\ \Rightarrow \quad [\mathbb{M}_2 : \mathbb{Q}] = 2; \end{multline} \tag{10.22}$$

$$\begin{multline} M_{\beta_1} = x^3 - 2 = (x - \beta_1)(x - \beta_2)(x - \beta_3), \ \beta_1 = 2^{1/3}, \\ M_{\beta_1} \in J_{\mathbb{Q}[x]}, \quad \deg_{\mathbb{Q}} M_{\beta_1} = \deg_{\mathbb{Q}} M_{\beta_2} = \deg_{\mathbb{Q}} M_{\beta_3} = 3, \\ \Rightarrow \quad [\mathbb{M}_3 : \mathbb{Q}] = 3. \end{multline} \tag{10.23}$$

According to Theorem 42 C it holds that

$$\beta_1, \beta_2, \beta_3 \notin \mathbb{M}_2, \quad \alpha_1, \alpha_2 \notin \mathbb{M}_3. \tag{10.24}$$

Thus, the polynomial x^3-2 does not have zero points in the field $\mathbb{M}_2$, so x^3-2 is irreducible in the ring of polynomials $\mathbb{M}_2[x]$.

Therefore

$$[\mathbb{L}:\mathbb{M}_2]=[\langle\mathbb{M}_2,2^{1/3}\rangle:\langle\mathbb{Q},2^{1/2}\rangle]=3. \tag{10.25}$$

According to Theorem 32 it holds that

$$[\mathbb{L}:\mathbb{Q}]=[\mathbb{L}:\mathbb{M}_2][\mathbb{M}_2:\mathbb{Q}]=6. \tag{10.26}$$

Similarly as in the proof of Theorem 32, we get

$$\mathbb{M}_2=\langle 1,2^{1/2}\rangle_{\mathbb{Q}}=\mathbb{Q}\cdot 1+\mathbb{Q}2^{1/2},\quad \dim_{\mathbb{Q}}\mathbb{M}_2=2;$$
$$\mathbb{L}=\langle 1,2^{1/3},2^{2/3}\rangle_{\mathbb{M}_2}=\mathbb{M}_2\cdot 1+\mathbb{M}_2 2^{1/3}+\mathbb{M}_2 2^{2/3},\quad \dim_{\mathbb{M}_2}\mathbb{L}=3.$$

That implies

$$\begin{aligned}\mathbb{L}&=\mathbb{Q}\cdot 1+\mathbb{Q}2^{1/2}+\mathbb{Q}2^{1/3}+\mathbb{Q}2^{1/2}2^{1/3}+\mathbb{Q}2^{2/3}+\mathbb{Q}2^{1/2}2^{2/3}\\&=\langle 1,2^{1/6},2^{2/6},2^{3/6},2^{4/6},2^{5/6}\rangle_{\mathbb{Q}},\\&\dim_{\mathbb{Q}}\mathbb{L}=6.\end{aligned}$$

Hence

$$\langle\mathbb{Q},2^{1/2},2^{1/3}\rangle=\langle\mathbb{Q},2^{1/6}\rangle \tag{10.27}$$

or written in a different way

$$\mathbb{Q}(2^{1/2},2^{1/3})=\mathbb{Q}(2^{1/6}). \tag{10.28}$$

Lemma 11. Let

$$[\langle K,\alpha_i\rangle:K]=n_i,\quad i=1,...,r. \tag{10.29}$$

Then

$$[\langle K,\alpha_1,...,\alpha_r\rangle:K]\le n_1\cdots n_r. \tag{10.30}$$

Theorem 43. A field extension $L:K$ is finite if and only if $L=\langle K,\alpha_1,...,\alpha_r\rangle$ and L is algebraic over K.

11 Algebraic numbers $\mathbb{A}$

A set $\mathbb{A} \subseteq \mathbb{C}$ is the set of all algebraic numbers over $\mathbb{Q}$. The following result shows that $\mathbb{A}$ is a subfield of complex numbers.

Theorem 44.

$$\mathbb{A} \leqslant \mathbb{C}. \tag{11.1}$$

Corollary 2. If $\alpha, \beta \in \mathbb{A}$, then

$$\alpha \pm \beta,\ \alpha\beta,\ \alpha/\beta \in \mathbb{A}. \tag{11.2}$$

According to Fundamental Theorem of Algebra 19, the set $\mathbb{C}$ is algebraically closed, i.e. if τ is algebraic over $\mathbb{C}$, then $\tau \in \mathbb{C}$.

The following result tells us that if $\omega \in \mathbb{C}$ is algebraic over $\mathbb{A}$, then $\omega \in \mathbb{A}$.

Theorem 45. The set of algebraic numbers $\mathbb{A}$ is algebraically closed, i.e.

$$a(x) \in \mathbb{A}[x] \setminus \{0(x)\}, \quad a(\omega) = 0 \quad \Rightarrow \quad \omega \in \mathbb{A}. \tag{11.3}$$

12 Number field

Theorem 46. Let $\mathbb{K}$ be a number field. Then there exists $\tau \in \mathbb{K}$ such that

$$\mathbb{K} = \mathbb{Q}(\tau). \tag{12.1}$$

Thus, number fields are simple extensions of $\mathbb{Q}$, i.e. they are generated by a single element.

Proof. By induction.
We look at the case

$$\mathbb{K} = \mathbb{Q}(\alpha, \beta) \tag{12.2}$$

and show that

$$\mathbb{K} = \mathbb{Q}(\alpha + c\beta) \quad \text{where} \quad c \in \mathbb{Q}. \tag{12.3}$$

Let

$$\begin{aligned} M_\alpha(x) &= (x - \alpha_1)\cdots(x - \alpha_n) \in \mathbb{Q}[x]; \\ M_\beta(x) &= (x - \beta_1)\cdots(x - \beta_m) \in \mathbb{Q}[x]. \end{aligned} \tag{12.4}$$

Then there exists $c \in \mathbb{Q}$ such that

$$\gamma := \alpha + c\beta \neq \alpha_i + c\beta_j, \quad \forall (i,j) \neq (1,1). \tag{12.5}$$

a). Obviously

$$\gamma := \alpha + c\beta \in \mathbb{Q}(\alpha, \beta) \quad \Rightarrow \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta). \tag{12.6}$$

b). We show (not so easily) that

$$\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma). \tag{12.7}$$

Consider polynomials

$$\begin{aligned} r(x) = M_\alpha(\gamma - cx) \in \mathbb{Q}(\gamma)[x], \quad \deg r(x) = n, \\ r(\beta) = M_\alpha(\gamma - c\beta) = M_\alpha(\alpha) = 0; \\ M_\beta(\beta) = 0, \quad M_\beta(x) \in \mathbb{Q}[x], \end{aligned} \tag{12.8}$$

where zero points β_j of $M_\beta(x)$ are simple.

Let us set

$$\begin{aligned} r(\tau) = M_\beta(\tau) = 0 \quad \Rightarrow \quad \tau = \beta_k; \\ 0 = r(\tau) = M_\alpha(\gamma - c\tau) \quad \Rightarrow \quad \gamma - c\tau = \alpha_h \\ \Rightarrow \quad \gamma = \alpha_h + c\tau = \alpha_h + c\beta_k \\ \Rightarrow \quad \gamma = \alpha + c\beta \Rightarrow \quad \tau = \beta. \end{aligned} \tag{12.9}$$

Hence, a simple zero point β is the only common zero point of $r(x)$ and $M_\beta(x)$. Let us denote

$$d(x) = s.y.t(r(x), M_\beta(x)) \in \mathbb{Q}(\gamma)[x]. \tag{12.10}$$

If

$$\begin{aligned}
&\deg d(x) \geq 2 \quad \Rightarrow \\
&\qquad d(x) = (x-\beta)(x-\kappa)q(x), \quad \beta, \kappa \in \mathbb{C} \quad \Rightarrow \\
&\qquad r(\kappa) = M_\beta(\kappa) = 0 \quad \Rightarrow \quad \kappa = \beta \quad \Rightarrow \\
&\qquad\qquad (x-\beta)^2 \underset{\mathbb{C}[x]}{\|} M_\beta(x)
\end{aligned} \tag{12.11}$$

Contradiction. Therefore $\deg d(x) = 1$ and

$$\begin{aligned}
&d(x) = (x-\beta) \in \mathbb{Q}(\gamma)[x] \quad \Rightarrow \\
&\qquad \beta \in \mathbb{Q}(\gamma) \quad \Rightarrow \quad \alpha = \gamma - c\beta \in \mathbb{Q}(\gamma) \quad \Rightarrow \\
&\qquad\qquad \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma). \quad \square
\end{aligned} \tag{12.12}$$

Example 31.

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i - \sqrt{2}). \tag{12.13}$$

12.1 Conjugates, field polynomial

Theorem 47. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field and $[\mathbb{K} : \mathbb{Q}] = m$. Then, there are exactly m different monomorphisms

$$\sigma_i : \mathbb{K} \to \mathbb{C}, \quad i = 1, ..., m. \tag{12.14}$$

Remark 9. Even if $a \in \mathbb{K}$, it may happen that $\sigma_i(a) \notin \mathbb{K}$ for some i.

Example 32. Let $\mathbb{K} = \mathbb{Q}(2^{1/3})$, then

$$\sigma_2(2^{1/3}), \sigma_3(2^{1/3}) \notin \mathbb{K}. \tag{12.15}$$

Definition 45. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field and $[\mathbb{K} : \mathbb{Q}] = m$. A *field polynomial* of an element $\beta \in \mathbb{K}$ is

$$K_\beta(x) = \prod_{i=1}^{m}(x - \sigma_i(\beta)), \tag{12.16}$$

where numbers

$$\sigma_i(\beta) \in \mathbb{C} \tag{12.17}$$

are conjugates of β over $\mathbb{K}$.

Theorem 48.

$$K_\beta(x) \in \mathbb{Q}[x]. \tag{12.18}$$

Proof: Based on Fundamental Theorem About Symmetric Polynomials.

Let us recall that according to Definition 39, conjugates of $\beta \in \mathbb{A}$ are zero points of the minimum polynomial$M_\beta(x) \in \mathbb{Q}[x]$,

$$\beta_1, ..., \beta_d \in \mathbb{C}. \tag{12.19}$$

We have

$$\deg K_\beta(x) = m, \quad \deg M_\beta(x) = d. \tag{12.20}$$

Theorem 49. Let $\beta \in \mathbb{K} = \mathbb{Q}(\tau)$ and $[\mathbb{K} : \mathbb{Q}] = m$. Then

$$M_\beta(x) \underset{\mathbb{Q}[x]}{\mid} K_\beta(x); \tag{12.21}$$

$$K_\beta(x) = M_\beta(x)^{m/d}, \quad m/d \in \mathbb{Z}^+. \tag{12.22}$$

Corollary 3.

$$\{\sigma_1(\beta), ..., \sigma_m(\beta)\} = \{\beta_1, ..., \beta_d\}; \tag{12.23}$$

$$\beta \in \mathbb{Q} \quad \Leftrightarrow \quad \sigma_1(\beta) = ... = \sigma_m(\beta); \tag{12.24}$$

$$\mathbb{Q}(\beta) = \mathbb{K} \quad \Leftrightarrow \quad \sigma_i(\beta) \neq \sigma_j(\beta) \quad \forall\ i \neq j. \tag{12.25}$$

12.2 Discriminant/not required

Definition 46.

Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field and $[\mathbb{K} : \mathbb{Q}] = m$. A discriminant of numbers $\gamma_1, ..., \gamma_m \in \mathbb{K}$ is defined as

$$\Delta(\gamma_1, ..., \gamma_m) = (\det(\sigma_i(\gamma_j))_{i=1,...,m,j=1,...,m})^2 = \tag{12.26}$$

$$\begin{vmatrix} \sigma_1(\gamma_1) & \sigma_2(\gamma_1) & ... & \sigma_m(\gamma_1) \\ . & & ... & . \\ . & & ... & . \\ . & & ... & . \\ \sigma_1(\gamma_m) & \sigma_2(\gamma_m) & ... & \sigma_m(\gamma_m) \end{vmatrix}^2 .$$

A discriminant of an element $\beta \in \mathbb{K}$ is

$$\delta(\beta) = \Delta(1, \beta, ..., \beta^{m-1}) = \tag{12.27}$$

$$\begin{vmatrix} 1 & 1 & & 1 \\ \sigma_1(\beta) & \sigma_2(\beta) & ... & \sigma_m(\beta) \\ . & & ... & . \\ . & & ... & . \\ . & & ... & . \\ \sigma_1(\beta)^{m-1} & \sigma_2(\beta)^{m-1} & ... & \sigma_m(\beta)^{m-1} \end{vmatrix}^2 .$$

Theorem 50.

$$\Delta(\gamma_1, ..., \gamma_m) \in \mathbb{Q}. \tag{12.28}$$

Theorem 51. The set $\{\gamma_1, ..., \gamma_m\}$ is a base of $\mathbb{K}$ if and only if the discriminant is not zero, i.e.

$$\dim_{\mathbb{Q}} \mathbb{Q}(\gamma_1, ..., \gamma_m) = m \quad \Leftrightarrow \quad \Delta(\gamma_1, ..., \gamma_m) \neq 0. \tag{12.29}$$

Theorem 52.

$$\delta(\beta) = \prod_{i<j} (\sigma_i(\beta) - \sigma_j(\beta))^2; \tag{12.30}$$

$$\delta(\beta) \neq 0 \quad \Leftrightarrow \quad \deg_{\mathbb{Q}}(\beta) = m; \tag{12.31}$$

$$\delta(\beta) \neq 0 \quad \Leftrightarrow \quad \mathbb{Q}(\beta) = \mathbb{K}. \tag{12.32}$$

12.3 Norm and trace

Definition 47. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field and $[\mathbb{K} : \mathbb{Q}] = m$. A *norm* of an element $\beta \in \mathbb{K}$ is the number

$$N(\beta) = N_{\mathbb{K}}(\beta) = \prod_{i=1}^{m} \sigma_i(\beta) \tag{12.33}$$

and a *trace* is the number

$$T(\beta) = T_{\mathbb{K}}(\beta) = \sum_{i=1}^{m} \sigma_i(\beta). \tag{12.34}$$

Theorem 53.

$$N_{\mathbb{K}}(\beta), \quad T_{\mathbb{K}}(\beta) \in \mathbb{Q}. \tag{12.35}$$

$$N_{\mathbb{K}}(\beta) \neq 0 \quad \Leftrightarrow \quad \beta \neq 0. \tag{12.36}$$

Proof. (12.35):

$$K_\beta(x) = x^m - T(\beta)x^{m-1} + ... + (-1)^m N(\beta) \in \mathbb{Q}[x]. \tag{12.37}$$

(12.36): Since σ_i is the injection, we have

$$\sigma_i(x) = 0 \quad \Leftrightarrow \quad x = 0. \quad \square \tag{12.38}$$

Theorem 54.

$$N(\alpha\beta) = N(\alpha)N(\beta) \tag{12.39}$$

$$T(r\alpha + s\beta) = rT(\alpha) + sT(\beta); \tag{12.40}$$

$$N(r) = r^m, \quad T(r) = mr; \tag{12.41}$$

for all $\alpha, \beta \in \mathbb{K}$, $r, s \in \mathbb{Q}$.

Example 33.

Let us show by using the trace function that

$$3^{1/2} \notin \mathbb{K} = \mathbb{Q}(2^{1/2}) = \mathbb{Q}[2^{1/2}]. \tag{12.42}$$

Notice that

$$[\mathbb{Q}(2^{1/2}) : \mathbb{Q}] = [\mathbb{Q}(3^{1/2}) : \mathbb{Q}] = 2. \tag{12.43}$$

Suppose the opposite

$$3^{1/2} \in \mathbb{Q}[2^{1/2}] = \mathbb{Q} + 2^{1/2}\mathbb{Q} \tag{12.44}$$

so

$$3^{1/2} = a + b2^{1/2}, \quad a, b \in \mathbb{Q}. \tag{12.45}$$

We compute the trace

$$T_\mathbb{K}(3^{1/2}) = T_\mathbb{K}(a) + T_\mathbb{K}(b2^{1/2}) = 2a + bT_\mathbb{K}(2^{1/2}). \tag{12.46}$$

On the other hand, according to (12.22) the field polynomials

$$K_{2^{1/2}}(x) = \prod_{i=1}^{2}(x - \sigma_i(2^{1/2})) = x^2 - T_{\mathbb{K}}(2^{1/2})x + N_{\mathbb{K}}(2^{1/2});$$

$$K_{3^{1/2}}(x) = \prod_{i=1}^{2}(x - \sigma_i(3^{1/2})) = x^2 - T_{\mathbb{K}}(3^{1/2})x + N_{\mathbb{K}}(3^{1/2})$$

are powers of corresponding minimal polynomials

$$M_{2^{1/2}}(x) = x^2 - 2; \quad M_{3^{1/2}}(x) = x^2 - 3$$

Since

$$\begin{multline} x^2 - 2 = x^2 - T_{\mathbb{K}}(2^{1/2})x + N_{\mathbb{K}}(2^{1/2}); \\ x^2 - 3 = x^2 - T_{\mathbb{K}}(3^{1/2})x + N_{\mathbb{K}}(3^{1/2}), \quad (12.47) \end{multline}$$

we have

$$T_{\mathbb{K}}(2^{1/2}) = T_{\mathbb{K}}(3^{1/2}) = 0. \qquad (12.48)$$

Now, from (12.46) we get

$$\begin{multline} a = 0 \quad \Rightarrow \quad 3^{1/2} = b2^{1/2}, \quad b \in \mathbb{Q} \\ \Rightarrow \quad (3/2)^{1/2} = b \quad \Rightarrow \\ T_{\mathbb{K}}((3/2)^{1/2}) = 2b. \quad (12.49) \end{multline}$$

But if we look at the field polynomial of $(3/2)^{1/2}$:

$$\begin{multline} K_{(3/2)^{1/2}}(x) = x^2 - T_{\mathbb{K}}((3/2)^{1/2})x + N_{\mathbb{K}}((3/2)^{1/2}); \\ M_{(3/2)^{1/2}}(x) = x^2 - 3/2 \quad \Rightarrow \\ T_{\mathbb{K}}((3/2)^{1/2}) = 0 \quad \Rightarrow \quad b = 0 \\ \Rightarrow \quad 3^{1/2} = 0. \quad (12.50) \end{multline}$$

contradiction. □

Theorem 55. Not required. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field, $[\mathbb{K} : \mathbb{Q}] = m$, let $M_\tau(x)$ be the minimal polynomial of τ and $DM_\tau(x)$ its derivative. Then

$$\Delta(1, \tau, ..., \tau^{m-1}) = (-1)^{m(m-1)/2} N(DM_\tau(\tau)). \tag{12.51}$$

Theorem 56. Not required. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field, $[\mathbb{K} : \mathbb{Q}] = m$ and $\gamma_1, ..., \gamma_m \in \mathbb{K}$. Then

$$\Delta(\gamma_1, ..., \gamma_m) = \det(T(\gamma_i \gamma_j)). \tag{12.52}$$

13 Algebraic integers - $\mathbb{B}$

The set $\mathbb{B} \subseteq \mathbb{C}$ consists of all algebraic integers over $\mathbb{Q}$.

The following result shows that the set of all algebraic integers $\mathbb{B}$ is a subring of the set of all algebraic numbers $\mathbb{A}$

Theorem 57.

$$\mathbb{B} \leqslant \mathbb{A}. \tag{13.1}$$

Corollary 4. If $\alpha, \beta \in \mathbb{B}$, then

$$\alpha \pm \beta,\ \alpha\beta\ \in \mathbb{B}. \tag{13.2}$$

The set $\mathbb{B}$ is algebraically closed:

Theorem 58. Let

$$b(x) = x^n + ... + b_0 \in \mathbb{B}[x] \setminus \{0(x)\},$$

$$b(\omega) = 0 \quad \Rightarrow \quad \omega \in \mathbb{B}. \tag{13.3}$$

Example 34.

$$\alpha^2 = \alpha + 1, \quad \beta^5 + \alpha\beta^2 + 5 = 0 \tag{13.4}$$

$$\omega^2 - \beta = 0 \quad \Rightarrow \quad \omega \in \mathbb{B}. \tag{13.5}$$

Theorem 59. If $\alpha \in \mathbb{A}$, then $\exists$ the smallest $d \in \mathbb{Z}^+$ such that

$$d\alpha \in \mathbb{B}. \tag{13.6}$$

Definition 48. The number $d \in \mathbb{Z}^+$ from Theorem 59 is called the denominator of the algebraic number α. We write den $\alpha = d$.

Example 35. Let

$$5\alpha^2 + \alpha + 1 = 0, \quad \Rightarrow \quad (5\alpha)^2 + 5\alpha + 5 = 0 \quad \Rightarrow \tag{13.7}$$

$$5\alpha \in \mathbb{B}, \quad den\ \alpha = 5. \tag{13.8}$$

Definition 49. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field. Then

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{K} \cap \mathbb{B} \tag{13.9}$$

is a ring of integers of K.

Example 36.

$$\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}. \tag{13.10}$$

Example 37.

$$2^{1/7} \notin \mathbb{Q}. \tag{13.11}$$

Proof by contradiction:

$$2^{1/7} \in \mathbb{Q}. \quad \text{But} \quad 2^{1/7} \in \mathbb{B} \quad \Rightarrow \quad 2^{1/7} \in \mathbb{Z}.$$
$$\text{Obviously} \quad 1 < 2^{1/7} < 2. \quad \text{contradiction.} \quad \square \tag{13.12}$$

Example 38. Let $n \in \mathbb{Z}_{\geq 2}$. Then

$$2^{1/n} + 3^{1/n} \notin \mathbb{Q}. \tag{13.13}$$

The ring of integers is a subring of the set of algebraic integers

Theorem 60.

$$\mathbb{Z} \leqslant \mathbb{Z}_{\mathbb{K}} \leqslant \mathbb{B}. \tag{13.14}$$

Moreover

Theorem 61. Let $\beta \in \mathbb{Z}_{\mathbb{K}}$, then

$$\mathbb{Z}[\beta] \leqslant \mathbb{Z}_{\mathbb{K}}. \tag{13.15}$$

Remark 10. However, it often happens that

$$\mathbb{Z}_{\mathbb{K}} \neq \mathbb{Z}[\beta]. \tag{13.16}$$

Example 39. $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ is the number field where

$$\frac{1+\sqrt{5}}{2} \in \mathbb{Z}_{\mathbb{K}}, \quad \frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]. \tag{13.17}$$

Theorem 62. Not required. Let $\mathbb{K}$ be a number field. Then

$$\mathbb{K} = \mathbb{Q}(\lambda), \quad \lambda \in \mathbb{Z}_{\mathbb{K}}. \tag{13.18}$$

Theorem 63. Not required. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field and $[\mathbb{K} : \mathbb{Q}] = m$. If $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_{\mathbb{K}}$ is a base of $\mathbb{K}$, then

$$\Delta(\lambda_1, ..., \lambda_m) \in \mathbb{Z} \setminus \{0\}. \tag{13.19}$$

Theorem 64. Not required. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field and $[\mathbb{K} : \mathbb{Q}] = m$. Then there exists a base $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_{\mathbb{K}}$ of $\mathbb{K}$ over $\mathbb{Q}$.

Theorem 65. Not required. Let $\mathbb{K} = \mathbb{Q}(\tau)$ be a number field and $[\mathbb{K} : \mathbb{Q}] = m$. Then there exists a base $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_{\mathbb{K}}$ of $\mathbb{Z}_{\mathbb{K}}$ over $\mathbb{Z}$.

Definition 50. According to Theorem 65, a base of $\mathbb{Z}_{\mathbb{K}}$ over $\mathbb{Z}$ is formed by an algebraic integer base of $\mathbb{K}$.

Theorem 66. Not required. Let $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_{\mathbb{K}}$ be a base of a field $\mathbb{K}$. If $\Delta(\lambda_1, ..., \lambda_m)$ is square-free, then $\{\lambda_1, ..., \lambda_m\}$ is an algebraic integer base of $\mathbb{K}$.

Example 40.

$$\Delta\left(1, \frac{1+\sqrt{5}}{2}\right) = 5 \quad \Rightarrow \quad \left\{1, \frac{1+\sqrt{5}}{2}\right\} \tag{13.20}$$

is the algebraic integer base of $\mathbb{Q}(\sqrt{5})$.

14 Divisibility in $\mathbb{Z}_{\mathbb{K}}$

Theorem 67. Let $\beta \in \mathbb{Z}_{\mathbb{K}}$, then

$$N_{\mathbb{K}}(\beta), \quad T_{\mathbb{K}}(\beta) \in \mathbb{Z}; \tag{14.1}$$

$$N_{\mathbb{K}}(\beta) \neq 0 \quad \Leftrightarrow \quad \beta \neq 0. \tag{14.2}$$

Let $\mathbb{Z}_{\mathbb{K}}^*$ be the unit group of the integer ring $\mathbb{Z}_{\mathbb{K}}$.

Theorem 68. Let $a, b \in \mathbb{Z}_{\mathbb{K}}$, then

$$a \underset{\mathbb{Z}_{\mathbb{K}}}{|} b \quad \Rightarrow \quad N(a) \underset{\mathbb{Z}}{|} N(b); \tag{14.3}$$

$$a \in \mathbb{Z}_{\mathbb{K}}^* \quad \Leftrightarrow \quad N(a) = \pm 1; \tag{14.4}$$

$$a \sim b \quad \Rightarrow \quad N(a) = \pm N(b); \tag{14.5}$$

$$|N(a)| \in \mathbb{P} \quad \Rightarrow \quad a \in J_{\mathbb{Z}_{\mathbb{K}}}. \tag{14.6}$$

Proof.

14.3: Suppose

$$b = ca, \quad a, b, c \in \mathbb{Z}_{\mathbb{K}} \tag{14.7}$$

since σ_i is the homomorphism, we have

$$\sigma_i(b) = \sigma_i(c)\sigma_i(a) \quad \forall\ i = 1, ..., m \quad \Rightarrow \tag{14.8}$$

$$N(b) = \prod_{i=1}^{m} \sigma_i(b) = \prod_{i=1}^{m} \sigma_i(c) \prod_{i=1}^{m} \sigma_i(a) = N(c)N(a), \tag{14.9}$$

where

$$N(b), N(c), N(a) \in \mathbb{Z} \quad \Rightarrow \quad N(a) \underset{\mathbb{Z}}{|} N(b). \quad \square \tag{14.10}$$

14.4: First, let us suppose

$$a \in \mathbb{Z}_{\mathbb{K}}^{*} \quad \Rightarrow \quad a \underset{\mathbb{Z}_{\mathbb{K}}}{|} 1. \tag{14.11}$$

The relationship (14.3) implies

$$N(a) \underset{\mathbb{Z}}{|} N(1) = 1 \quad \Rightarrow \quad N(a) = \pm 1. \tag{14.12}$$

Now, suppose

$$N(a) = \pm 1. \tag{14.13}$$

Therefore

$$a\sigma_2(a) \cdots \sigma_m(a) = \pm 1, \quad \Rightarrow \quad c = \sigma_2(a) \cdots \sigma_m(a) \in \mathbb{K}. \tag{14.14}$$

Moreover, since

$$a \in \mathbb{Z}_{\mathbb{K}} \subseteq \mathbb{B} \quad \Rightarrow \quad \sigma_2(a), ..., \sigma_m(a) \in \mathbb{B} \quad \Rightarrow \quad c \in \mathbb{B}. \tag{14.15}$$

Hence

$$c \in \mathbb{K} \cap \mathbb{B} = \mathbb{Z}_{\mathbb{K}}, \quad \pm c \cdot a = 1 \quad \Rightarrow \tag{14.16}$$

$$a \underset{\mathbb{Z}_{\mathbb{K}}}{|} 1 \quad \Rightarrow \quad a \in \mathbb{Z}_{\mathbb{K}}^*. \tag{14.17}$$

The relationship (14.4) is proven. □

Note that even if $a \in \mathbb{Z}_{\mathbb{K}}$, it may happen that $\sigma_i(a) \notin \mathbb{Z}_{\mathbb{K}}$, look at Example 32. However, $\sigma_i(a) \in \mathbb{B}$ always holds.

14.5:

$$b = ua, \quad u \in \mathbb{Z}_{\mathbb{K}}^* \quad \Rightarrow \quad N(u) = \pm 1 \quad \Rightarrow \tag{14.18}$$

$$N(b) = N(u)N(a) = \pm N(a). \quad \square \tag{14.19}$$

14.6: Obviously $a \neq 0$. Proof by contradiction: a is reducible

$$a = bc, \quad b, c \notin \mathbb{Z}_{\mathbb{K}}^*,\ b, c \neq 0, \quad \Rightarrow \tag{14.20}$$

$$|N(b)|, |N(c)| \geq 2 \quad \Rightarrow \quad |N(a)| = |N(b)||N(c)| \notin \mathbb{P}. \tag{14.21}$$

contradiction. □

Theorem 69. Let D be a UFD, $a, b, c \in D$ and

$$ab = c^k, \quad a \perp b. \tag{14.22}$$

Then

$$a \sim d^k, \quad b \sim e^k, \tag{14.23}$$

for some $d, e \in D$.

15 A Diophantine equation

The main motive for studying algebraic numbers was originally solving Diophantine equations.

Example 41.

$$y^2+2=x^3, \quad 2 \not| y, \tag{15.1}$$

is a Diophantine equation. We are seeking integer solutions.

I. Equation splits in $\mathbb{K}=\mathbb{Q}(\sqrt{-2})$ as follows:

$$(y+\sqrt{-2})(y-\sqrt{-2})=x^3. \tag{15.2}$$

II. The ring of integers is

$$\mathbb{Z}_{\mathbb{K}}=\mathbb{Z}+\mathbb{Z}\sqrt{-2}. \tag{15.3}$$

III. Its unit group is

$$\mathbb{Z}_{\mathbb{K}}^{*}=\{\pm 1\}. \tag{15.4}$$

IV. The integral domain

$$\mathbb{Z}_{\mathbb{K}}=\mathbb{Z}+\mathbb{Z}\sqrt{-2}. \tag{15.5}$$

is Euclidean domain and thus UFD. Hence, we can operate with it as in the ring of rational integers (see Solving the Pythagorean Equation).

V. Let

$$D=syt(y-\sqrt{-2},y+\sqrt{-2}),$$
$$D=a+b\sqrt{-2}\in\mathbb{Z}_{\mathbb{K}} \quad \Rightarrow \tag{15.6}$$

$$D \underset{\mathbb{Z}_{\mathbb{K}}}{\Big|} 2y, \quad D \underset{\mathbb{Z}_{\mathbb{K}}}{\Big|} 2\sqrt{-2} \quad \Rightarrow \tag{15.7}$$

$$N(D)\underset{\mathbb{Z}}{\Big|}N(2y), \quad N(D)\underset{\mathbb{Z}}{\Big|}N(2\sqrt{-2}),$$
$$N(D)=(a+b\sqrt{-2})(a-b\sqrt{-2})=a^2+2b^2 \quad \Rightarrow \tag{15.8}$$

$$a^2+2b^2\underset{\mathbb{Z}}{\Big|}4y^2, \quad a^2+2b^2\underset{\mathbb{Z}}{\Big|}-8 \quad \Rightarrow \tag{15.9}$$

$$D=\pm 1, \pm 2, \pm\sqrt{-2}. \tag{15.10}$$

For instance

$$\begin{aligned}
&\sqrt{-2}\underset{\mathbb{Z}_{\mathbb{K}}}{\Big|}y-\sqrt{-2} \quad \Rightarrow \\
&\qquad y-\sqrt{-2}=\sqrt{-2}(e+f\sqrt{-2}), \quad e,f\in\mathbb{Z} \quad \Rightarrow \\
&\qquad\qquad 2f=-y, \quad \text{cannot happen.}
\end{aligned} \tag{15.11}$$

Similarly, we can eventually conclude that

$$D=\pm 1\underset{\mathbb{Z}_{\mathbb{K}}}{\Big|}y-\sqrt{-2}, y+\sqrt{-2}, \quad \Rightarrow \tag{15.12}$$

$$y-\sqrt{-2}\ \perp\ y+\sqrt{-2}, \quad \Rightarrow \tag{15.13}$$

$$\begin{aligned}
&y+\sqrt{-2}=(c+d\sqrt{-2})^3, \quad c+d\sqrt{-2}\in\mathbb{Z}_{\mathbb{K}}, \quad c,d\in\mathbb{Z} \\
&\qquad \Rightarrow \quad 1=d(3c^2-2d) \quad \Rightarrow \quad d=\pm 1, \quad d=1, c=\pm 1; \\
&\qquad\qquad y=c^3-6cd^2 \quad \Rightarrow \quad y=\pm 5 \\
&\qquad\qquad\qquad \Rightarrow \quad x=3,\ y=\pm 5. \quad \square
\end{aligned} \tag{15.14}$$

16 Square root fields

Square root field is of the form

$$\mathbb{K}=\mathbb{Q}(\sqrt{d}), \quad d\in\mathbb{Z}, \tag{16.1}$$

where d is square-free from now on.

Theorem 70.

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, then

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\lambda, \tag{16.2}$$

where

$$\lambda = \sqrt{d}, \quad d \equiv 2,\ 3 \pmod 4; \tag{16.3}$$

$$\lambda = \frac{1+\sqrt{d}}{2}, \quad d \equiv 1 \pmod 4; \tag{16.4}$$

$$\Delta = 4d, \quad d \equiv 2,\ 3 \pmod 4; \tag{16.5}$$

$$\Delta = d, \quad d \equiv 1 \pmod 4. \tag{16.6}$$

Proof. Consider

$$\begin{gathered}
\beta = r + s\sqrt{d} \in \mathbb{Z}_{\mathbb{K}}, \quad r, s \in \mathbb{Q} \quad \Rightarrow \\
T(\beta) = 2r \in \mathbb{Z} \quad \Rightarrow \quad r \in \frac{1}{2}\mathbb{Z} \quad \Rightarrow \quad r = \frac{a}{2},\ a \in \mathbb{Z}; \\
N(\beta) = r^2 - ds^2 \in \mathbb{Z} \quad \Rightarrow \quad d(2s)^2 = (2r)^2 - 4N(\beta) \in \mathbb{Z}, \\
\text{where} \quad 2s = \frac{k}{l}, \quad k \perp l, \quad \Rightarrow \\
d(2s)^2 = \frac{dk^2}{l^2} \in \mathbb{Z}, \quad \text{where d is square-free} \quad \Rightarrow \quad l = 1, \\
\Rightarrow \quad 2s \in \mathbb{Z} \quad \Rightarrow \quad s = \frac{b}{2},\ b \in \mathbb{Z}.
\end{gathered} \tag{16.7}$$

Hence

$$\beta = \frac{a + b\sqrt{d}}{2}, \quad a, b \in \mathbb{Z}. \tag{16.8}$$

Let us look at a form of a and b more closely.

Case 16.3, so $d \equiv 2,\ 3 \pmod 4$:

We have

$$N(\beta) = \frac{a^2 - db^2}{4} \in \mathbb{Z} \quad \Rightarrow$$

$$a^2 - db^2 \equiv 0 \pmod 4 \quad \Rightarrow$$

$$a \equiv b \equiv 0 \pmod 2 \quad \Rightarrow$$

$$\beta = \frac{a + b\sqrt{d}}{2} = A + B\sqrt{d}, \quad A, B \in \mathbb{Z}. \tag{16.9}$$

Case 16.4, so $d \equiv 1 \pmod 4$:

We have

$$N(\beta) = \frac{a^2 - db^2}{4} \in \mathbb{Z} \quad \Rightarrow$$

$$a^2 \equiv b^2 \pmod 4 \quad \Rightarrow$$

$$a \equiv b \equiv 0 \pmod 2 \quad \text{or} \quad a \equiv b \equiv 1 \pmod 2 \quad \Rightarrow \tag{16.10}$$

$$\beta = \frac{a + b\sqrt{d}}{2}, \quad a \equiv b \pmod 2, \ a, b \in \mathbb{Z}$$

$$\Rightarrow \quad \beta = A + B\frac{1 + \sqrt{d}}{2}, \quad A, B \in \mathbb{Z}. \quad \Box \tag{16.11}$$

16.1 Imaginary square root fields

16.1.1 Unit group

Let us denote

$$\omega = e^{\frac{2\pi}{3}i}. \tag{16.12}$$

Theorem 71. Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, then

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1, \pm i\}, \quad d = -1; \tag{16.13}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1\}, \quad d = -2; \tag{16.14}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1, \pm\omega, \pm\omega^2\}, \quad d = -3; \tag{16.15}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1\}, \quad d \in \mathbb{Z}_{\leq -5}. \tag{16.16}$$

For instance the case: $d = -5 \equiv 3 \pmod 4$, so integers are of the form

$$\begin{aligned}\beta = A + B\sqrt{-5}, \quad A, B \in \mathbb{Z} \quad \Rightarrow \\ N(\beta) = A^2 + 5B^2 = 1 \quad \Rightarrow \quad A = \pm 1,\ B = 0 \quad \Rightarrow \\ \mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}^* = \{\pm 1\}.\end{aligned} \tag{16.17}$$

16.1.2 UFD/Euclidean domain

Theorem 72. Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, then $\mathbb{Z}_{\mathbb{K}}$ is UFD if

$$d = -1, -2, -3, -7, -11, \tag{16.18}$$

which are imaginary Euclidean domains and moreover if

$$d = -19, -43, -67, -163. \tag{16.19}$$

These are all cases if $d \leq -1$.

Proof of the case $d = -1$ where $\mathbb{Z}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[i]$. We will show that $\mathbb{Z}[i]$ is Euclidean domain.

Let $a, b \in \mathbb{Z}[i]$ where

$$\frac{a}{b} = x + iy, \quad x, y \in \mathbb{Q}. \tag{16.20}$$

We choose $s, t \in \mathbb{Z}$ such that

$$|x - s| \leq \frac{1}{2}, \quad |y - t| \leq \frac{1}{2}. \tag{16.21}$$

Let

$$q = s + it, \quad a = qb + r, \quad r \in \mathbb{Z}[i]. \tag{16.22}$$

We compare the norms of b and r:

$$N(r) = N(b)N(x - s + i(y - t)) = N(b)((x - s)^2 + (y - t)^2) \tag{16.23}$$

$$\leq N(b)\frac{1}{2} \quad \Rightarrow \quad N(r) < N(b) \tag{16.24}$$

and we have

$$N : \ \mathbb{Z}[i] \to \mathbb{N}, \tag{16.25}$$

so N is Euclidean function. Moreover, we know from Theorem 9 that Euclidean domain is UFD. □

16.1.3 Gaussian integers/prime numbers

Definition 51. Let $\mathbb{K} = \mathbb{Q}(i)$. Elements of the integer ring

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[i] \tag{16.26}$$

are called Gaussian integers. Moreover irreducible Gaussian integers are called Gaussian primes.

Since $\mathbb{Z}[i]$ is UFD, its irreducible elements are prime, so

$$P_{\mathbb{Z}[i]} = J_{\mathbb{Z}[i]}. \tag{16.27}$$

Theorem 73.

$$\pi = a + ib \in P_{\mathbb{Z}[i]} \quad \Leftrightarrow \tag{16.28}$$

$$\pi \sim 1 + i; \tag{16.29}$$

$$\pi \sim a + ib, \quad a^2 + b^2 = p \in \mathbb{P}, \quad p \equiv 1 \pmod 4; \tag{16.30}$$

$$\pi \sim p \in \mathbb{P}, \quad p \equiv 3 \pmod 4. \tag{16.31}$$

16.2 Real square root fields

16.2.1 Unit group

Unit groups of real square root fields are infinite and in general case quite difficult to define. They are needed for solving Pell's equation.

Theorem 74. Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}_{\geq 2}$. Then

$$\mathbb{Z}_{\mathbb{K}}^* = \{x_k + y_k\sqrt{d} |\ x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k,\ k \in \mathbb{Z}\}, \tag{16.32}$$

where $(x_1, y_1) \in \mathbb{Z}^2$ is the smallest positive solution of Pell's equation

$$x^2 - dy^2 = 1. \tag{16.33}$$

The smallest solution can be studied by using continued fractions. Sign up for the course Continued Fractions!

16.2.2 UFD/Euclidean domain

Theorem 75. Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, then $\mathbb{Z}_{\mathbb{K}}$ is UFD if

$$d = 2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41, 57, 73, \tag{16.34}$$

which are real Euclidean domains and moreover if

$$d = 11, 14, 19, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67,$$

$$69, 71, 77, 83, 86, 89, 93, 94, 97. \tag{16.35}$$

That is all only if we consider $2 \leq d \leq 100$.