ELEMENTS OF ANALYTIC NUMBER THEORY

P. S. Kolesnikov, E. P. Vdovin

Lecture course

Novosibirsk, Russia
2013

Contents

CHAPTER 1

Algebraic and transcendental numbers

§ 1.1. Field of algebraic numbers. Ring of algebraic integers

1. Preliminary information. Let us recall some basic notions from Abstract Algebra. Throughout we use the following notations:

$\mathbb{P}$ is the set of all prime numbers;
$\mathbb{N}$ is the set of positive integers (the set of natural numbers);
$\mathbb{Z}$ is the set of all integers;
$\mathbb{Q}$ is the set of all rational numbers;
$\mathbb{R}$ is the set of all real numbers;
$\mathbb{C}$ is the set of all complex numbers, $\mathbb{C} = \mathbb{R} + \iota\mathbb{R}$, $\iota^2 = -1$.

Given a field F, symbol $F[x]$ denotes the ring of polynomials in variable x with coefficients in F. If $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, $a_i \in F$, is chosen so that $a_n \neq 0$, then n is called the *degree* of $f(x)$, it is denoted by $\deg f$, while $a_n \in F$ is called the *leading coefficient* of $f(x)$, and if $a_n = 1$ then $f(x)$ is called *monic*. If $f(x) = 0$ (all coefficients are equal to zero) then the degree of $f(x)$ is said to be $-\infty$.

If $f(x), g(x) \in F[x]$, $g(x) \neq 0$, then there exist unique $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x), \quad \deg r < \deg g. \tag{1.1}$$

These polynomials (quotient $q(x)$ and remainder $r(x)$) can be found by the well-known *division algorithm*. If $r(x) = 0$ then we write $g \mid f$ (g divides f).

One may easily note the similarity between division algorithms in the ring of integers $\mathbb{Z}$ and in the ring of polynomials $F[x]$. Indeed, these are particular examples of Euclidean rings, and there are many common features and problems that can be solved in similar ways for integers and polynomials.

In particular, the greatest common divisor (gcd) d of two polynomials $f, g \in F[x]$ is defined as a monic common divisor which is divided by every

other common divisor, i.e., $d = \gcd(f, g)$ if and only if $d \mid f$, $d \mid g$, and for every $h \in F[x]$ with $h \mid f$ and $h \mid g$ it follows that h divides d.

To find gcd of f and g, one may use the Euclidean algorithm based on the following observation: If f and g are related by (1.1) then $\gcd(f, g) = \gcd(g, r)$. Moreover, if $d = \gcd(f, g)$ then there exist $p(x), s(x) \in F[x]$ such that

$$f(x)p(x) + g(x)s(x) = d(x).$$

EXERCISE 1.1. Let $f_1, \dots, f_n \in F[x]$ be a finite family of polynomials over a field F. Prove that there exists a unique monic greatest common divisor of $f_1, \dots, f_n$.

Suppose R is a commutative ring with an identity (e.g., $R = \mathbb{Z}$ or $R = F[x]$ as above). A subset $I \subseteq R$ is called an *ideal* of R if $a \pm b \in I$ for every $a, b \in I$, and $ax \in I$ for every $a \in I$, $x \in R$. For example, the set of all even integers is an ideal of $\mathbb{Z}$; the set $\{f(x) \in F[x] \mid f(\alpha) = 0\}$ is an ideal of $F[x]$, where α is an element of some extension field of F.

Since an intersection of any family of ideals is again an ideal, for every set $M \subseteq R$ there exists minimal ideal of R which contains M, it is denoted by (M). It is easy to note that

$$(M) = \left\{ \sum_i x_i a_i \mid x_i \in R,\ a_i \in M \right\}.$$

An ideal I of R is said to be *principal* if there exists $a \in R$ such that $I = (a)$, where (a) stands for $(\{a\})$.

Recall that a commutative ring R is called an integral domain (or simply a domain) if $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in R$. In particular, $\mathbb{Z}$ and $F[x]$ are integral domains. An integral domain R such that every ideal of R is principal is called a *principal ideal domain*.

EXERCISE 1.2. Prove that $\mathbb{Z}$ and $F[x]$ (where F is a field) are principal ideal domains. In particular, if $f(x), g(x) \in F[x]$ then

$$(\{f, g\}) = (\gcd(f, g)).$$

If R is a domain, then we can consider the field of fractions of R. In order to construct it we start with the Cartesian product $R \times (R \setminus \{0\})$ of R (here each pair (a, b) corresponds to fraction $\frac{a}{b}$). Now define an equivalence relation $(a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = a_2 b_1$. Let Q be the set of equivalence classes of $R \times (R \setminus \{0\})$ under this equivalence. Define the addition and multiplication on representatives by

$$(a_1, b_1) + (a_2, b_2) = (a_1 b_2 + a_2 b_1, b_1 b_2), \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

We leave for the reader to prove that all operations defined are correct and that Q is a field under these operations.

Let I be an ideal of R. Then R is split into a disjoint union of congruence classes $a+I = \{a+x \mid x \in I\}$, $a \in R$, and the set of all these classes (denoted by R/I) is a ring with respect to natural operations

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = ab + I.$$

The ring R/I obtained is called a *factor ring* of R over I. For example, $\mathbb{Z}/(n) = \mathbb{Z}_n$, the ring of remainders modulo n.

A proper ideal I of R is *maximal* if there are no proper ideals J of R such that $I \subset J$. For example, if $R = \mathbb{Z}$ then (n) is maximal if and only if $n = \pm p$, where p is a prime natural number; if $R = F[x]$ then (f) is maximal if and only if the polynomial f is irreducible over F.

Note that if I is a maximal ideal of a commutative ring R then R/I is a field. Indeed, if $a + I \neq 0$ (i.e., $a \notin I$) then $J = \{xa + b \mid x \in R, b \in I\}$ is an ideal of R such that $I \subset J$. Therefore, $J = R$, and thus all equations of the form $(a + I)X = c + I$, $c \in R$, have solutions in R/I.

Exercise 1.3. Prove that $\mathbb{R}[x]/(x^2 + x + 1)$ is a field isomorphic to the field $\mathbb{C}$ of complex numbers.

2. Minimal polynomial. A complex number $\alpha \in \mathbb{C}$ is *algebraic* if there exists a nonzero polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. A non-algebraic complex number is said to be *transcendental*.

An algebraic number α is called an *algebraic integer* if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Every rational number $\alpha \in \mathbb{Q} \subset \mathbb{C}$ is obviously an algebraic one. Moreover, as we will see later, a rational number is an algebraic integer if and only if it is an integer.

Exercise 1.4. (1) Prove that $\sqrt{2}$ and $\frac{1}{2} + \iota\frac{\sqrt{3}}{2}$ are algebraic integers.

(2) Prove that if $\alpha \in \mathbb{C}$ is an algebraic number then $\operatorname{Re}\alpha$ and $\operatorname{Im}\alpha$ are algebraic numbers. Whether the same statements are true for an algebraic integer α?

(3) Show that the cardinality of the set of all algebraic numbers is countable.

Since the cardinality of the entire set of complex numbers is uncountable (continuum), transcendental numbers do exist. However, it is not so easy to show an example of such a number accompanied with reasonable proof.

Let α be an algebraic number. Denote by x a formal variable, and let

$$I(\alpha, x) = \{f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0\}.$$

It is clear that $I(\alpha, x)$ is an ideal of the ring $\mathbb{Q}[x]$.

Since $\mathbb{Q}[x]$ is a principal ideal domain, the ideal $I(\alpha, x)$ is generated by a single polynomial. Namely, the monic polynomial of minimal positive degree from $h(x) \in I(\alpha, x)$ is a generator of the ideal $I(\alpha, x)$, it is called the *minimal polynomial* for α.

Given an algebraic number α, denote its minimal polynomial by $h_\alpha(x)$ and say $\deg h_\alpha$ to be the *degree of* α.

Lemma 1.5. *Let α be an algebraic number, and let $h(x)$ be a monic polynomial from $\mathbb{Q}[x]$. Then the following conditions are equivalent:*

(1) *$h(x) = h_\alpha(x)$;*
(2) *$h(\alpha) = 0$, and h divides every $f \in I(\alpha, x)$;*
(3) *$h(\alpha) = 0$, and $h(x)$ is irreducible over $\mathbb{Q}$.*

Proof. (1) $\Rightarrow$ (2) It is obvious by definition.

(2) $\Rightarrow$ (3) Assume $h(x)$ is reducible over $\mathbb{Q}$, i.e., it can be decomposed into nonscalar factors as follows:

$$h(x) = h_1(x)h_2(x), \quad \text{where} \quad h_i(x) \in \mathbb{Q}[x],\ \deg h_i \geqslant 1.$$

Then $h(\alpha) = h_1(\alpha)h_2(\alpha) = 0$, so for either of $i = 1, 2$ we have $h_i(\alpha) = 0$. Therefore, the corresponding polynomial $h_i(x)$ belongs to $I(\alpha, x)$, hence, $h_i(x)$ is a multiple of $h(x)$, which is impossible due to $\deg h_i < \deg h$.

(3) $\Rightarrow$ (1) Let $h_\alpha(x)$ be the minimal polynomial for α. Then $h(x) \in I(\alpha, x) = (h_\alpha(x))$, so $h_\alpha \mid h$. Since $h(x)$ is irreducible and $\deg h_\alpha > 0$, we have $h(x) = h_\alpha(x)$. □

For example, if $\alpha \in \mathbb{Q}$ then $h_\alpha = x - \alpha$. For $\alpha = \sqrt{2}$, $h_\alpha = x^2 - 2$. The number $\alpha = \dfrac{1}{2} + \iota\dfrac{\sqrt{3}}{2}$ satisfies the equation $\alpha^3 + 1 = 0$, but its minimal polynomial is $h_\alpha(x) = x^2 - x + 1$.

Exercise 1.6. Prove that a minimal polynomial does not have multiple roots.

If α is an algebraic number, and $\beta \in \mathbb{C}$ is a root of $h_\alpha(x)$ then β is said to be *conjugate* to α. Therefore, every algebraic number α of degree n has exactly n pairwise different conjugate complex numbers $\alpha_1, \ldots, \alpha_n$,

including α itself. Moreover,

$$h_\alpha(x) = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{Q}[x].$$

Given an algebraic number α, the minimal polynomial $h_\alpha \in \mathbb{Q}[x]$ is uniquely defined. If α is an algebraic integer then there also exists a monic polynomial $f \in \mathbb{Z}[x]$ of minimal degree such that $h_\alpha \mid f$. In order to prove that these f and h_α coincide, we need the following observation.

Let $h(x) \in \mathbb{Q}[x]$ be a monic polynomial with rational coefficients,

$$h(x) = \frac{p_0}{q_0} + \frac{p_1}{q_1}x + \cdots + \frac{p_{n-1}}{q_{n-1}}x^{n-1} + x^n, \quad \gcd(p_i, q_i) = 1.$$

Denote by $q(h)$ the least common multiple of the coefficients' denominators:

$$q(h) = \operatorname{lcm}(q_0, \ldots, q_{n-1}). \tag{1.2}$$

Then for $q = q(h)$ we have

$$qh(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n \in \mathbb{Z}[x],$$

where the gcd of all coefficients is equal to the identity: $(a_0, \ldots, a_n) = 1$. Indeed, assume $a_0, \ldots, a_n$ have a common divisor $d > 1$. Then $d \mid q = a_n$, and for $b = q/d \in \mathbb{Z}$ we have $bh(x) \in \mathbb{Z}[x]$. Therefore, $q_i \mid bp_i$ for all $i = 0, \ldots, n-1$, so $q_i \mid b$, and, finally, $q \mid b = q/d$, which is impossible for $d > 1$.

Polynomials with relatively prime integral coefficients are studied in Abstract Algebra, they are called *primitive*. The following statement is well-known.

Exercise 1.7 (Hauss Lemma). Prove that the product of primitive polynomials is also a primitive polynomial.

Proposition 1.8. *Let α be an algebraic integer. Then the minimal polynomial $h_\alpha(x)$ has integral coefficients.*

Proof. Suppose $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with integral coefficients such that $f(\alpha) = 0$. Then Lemma 1.5 implies $h_\alpha \mid f$, i.e.,

$$f(x) = h_\alpha(x)g(x), \quad g(x) \in \mathbb{Q}[x].$$

Since both f and h_α are monic polynomials, so is g.

Denote $q = q(h_\alpha)$, $q' = q(g)$, where the function $q(\cdot)$ is given by (1.2). According to the remark above, $qh_\alpha(x)$ and $q'g(x)$ are primitive polynomials in $\mathbb{Z}[x]$. However,

$$qq'f(x) = (qh_\alpha(x))(q'g(x)).$$

The Hauss Lemma implies $qq'f(x)$ to be primitive, while $f(x)$ has integral coefficients itself. Therefore, $qq' = 1$, i.e., all coefficients of h_α and g are integral. □

Thus, there is no need to define separately integral minimal polynomial and degree for algebraic integers. Let us also note that for every algebraic number α there exists $c \in \mathbb{N}$ such that $c\alpha$ is an algebraic integer: It is enough to consider $c = q(h_\alpha)^{\deg h_\alpha}$.

3. Algebraic complex numbers. Let us denote the set of all algebraic numbers by $\mathbb{A}$. Recall that the Fundamental Theorem of Algebra states $\mathbb{C}$ to be an algebraically closed field, i.e., every non-constant polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$. In this section, we will prove that $\mathbb{A} \subset \mathbb{C}$ is the minimal algebraically closed subfield of $\mathbb{C}$, i.e., $\mathbb{A}$ is the algebraic closure of $\mathbb{Q}$.

Lemma 1.9. *The following statements are equivalent for $\alpha \in \mathbb{C}$:*

(1) $\alpha \in \mathbb{A}$;
(2) $\mathbb{Q}[\alpha] := \{f(\alpha) \mid f(x) \in \mathbb{Q}[x]\}$ *is a finite-dimensional vector space over* $\mathbb{Q}$;
(3) $\mathbb{Q}[\alpha]$ *is a subfield of* $\mathbb{C}$.

Proof. (1) $\Rightarrow$ (2). Note that $f(x) = q(x)h_\alpha(x) + r(x)$ by the division algorithm, $\deg r < \deg h_\alpha$. Hence, $f(\alpha) = r(\alpha)$, and the latter is a linear combination over $\mathbb{Q}$ of $1, \alpha, \dots, \alpha^{n-1}$, where $n = \deg h_\alpha$. Therefore, $\dim \mathbb{Q}[\alpha] \leqslant n$. Moreover, $1, \alpha, \dots, \alpha^{n-1}$ are linearly independent since n is the minimal possible degree of a polynomial over $\mathbb{Q}$ annihilating α, so

$$\dim \mathbb{Q}[\alpha] = \deg h_\alpha.$$

(2) $\Rightarrow$ (1). It is enough to note that $1, \alpha, \alpha^2, \dots$ are linearly dependent, so there exist $a_0, a_1, \dots, a_n \in \mathbb{Q}$ such that

$$a_0 \cdot 1 + a_1\alpha + \dots + a_n\alpha^n = 0,$$

end at least one of a_i is nonzero. Hence, $h(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Q}[x]$ is a nonzero polynomial annihilating α.

(1) $\Rightarrow$ (3) Obviously, $\mathbb{Q}[\alpha]$ is a subring of $\mathbb{C}$. Let $0 \neq f(\alpha) \in \mathbb{Q}[\alpha]$, then $f \in \mathbb{Q}[x] \setminus I(\alpha, x)$. Therefore, h_α does not divide f. Since h_α is irreducible, we have $\gcd(f, h_\alpha) = 1$. Hence, there exist polynomials $u(x), v(x) \in \mathbb{Q}[x]$ such that

$$u(x)f(x) + v(x)h_\alpha(x) = 1.$$

Then for $x = \alpha$ we obtain $u(\alpha)f(\alpha) = 1$, i.e., $f(\alpha)^{-1} = u(\alpha) \in \mathbb{Q}[\alpha]$, i.e., $\mathbb{Q}[\alpha]$ is a field.

(3) $\Rightarrow$ (1) Suppose $\mathbb{Q}[\alpha]$ is a subfield of $\mathbb{C}$. It is enough to consider the case when $\alpha \neq 0$. Since $\alpha^{-1} \in \mathbb{Q}[\alpha]$, there exists $f(x) \in \mathbb{Q}[x]$ such that $\alpha^{-1} = f(\alpha)$, i.e., $h(\alpha) = 0$ for $h(x) = xf(x) - 1$, $\deg h \geqslant 1$. □

Corollary 1.10. *If $\alpha_1, \ldots, \alpha_n \in \mathbb{A}$ then*

$$\mathbb{Q}[\alpha_1, \ldots, \alpha_n] := \{f(\alpha_1, \ldots, \alpha_n) \mid f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]\}$$

is a finite-dimensional vector space over $\mathbb{Q}$.

Proof. For $n = 1$, it follows from Lemma 1.9. By induction, since $\dim Q[\alpha_1, \ldots, \alpha_{n-1}] < \infty$ and $\dim Q[\alpha_n] < \infty$,

$$\dim Q[\alpha_1, \ldots, \alpha_n] \leqslant \dim Q[\alpha_1, \ldots, \alpha_{n-1}] \cdot \dim Q[\alpha_n] < \infty$$

(all dimensions are over $\mathbb{Q}$). □

Exercise 1.11. Prove that $Q[\alpha_1, \ldots, \alpha_n]$ is a subfield of $\mathbb{C}$ provided that $\alpha_1, \ldots, \alpha_n \in \mathbb{A}$.

Theorem 1.12. *The set of all algebraic numbers is a subfield of $\mathbb{C}$.*

Proof. Since $1, 0 \in \mathbb{C}$ are obviously algebraic, it is enough to prove the following two statements:
(1) If α and β are algebraic numbers then $\alpha \pm \beta$ and $\alpha\beta$ are also algebraic numbers;
(2) If $\beta \neq 0$ is an algebraic number then $1/\beta$ is also an algebraic number.

(1) Since

$$\mathbb{Q}[\alpha \pm \beta], \mathbb{Q}[\alpha \cdot \beta] \subseteq \mathbb{Q}[\alpha, \beta] \subseteq \mathbb{C},$$

we have $\dim \mathbb{Q}[\alpha \pm \beta] < \infty$, $\dim \mathbb{Q}[\alpha \cdot \beta] < \infty$ by Corollary 1.10. Thus by Lemma 1.9 $\alpha \pm \beta, \alpha\beta \in \mathbb{A}$.

(2) By Lemma 1.9, $\beta^{-1} \in \mathbb{Q}[\beta]$, so $\mathbb{Q}[\beta^{-1}] \subseteq \mathbb{Q}[\beta]$ which is finite-dimensional over $\mathbb{Q}$. Hence, $\dim \mathbb{Q}[\beta^{-1}] < \infty$ and thus $\beta^{-1} \in \mathbb{A}$. □

Theorem 1.13. *The field $\mathbb{A}$ is algebraically closed.*

Proof. Suppose $\alpha_0, \ldots, \alpha_n \in \mathbb{A}$, $n \geqslant 1$, $\alpha_n \neq 0$, $\varphi(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in \mathbb{A}[x]$. It is enough to show that $\varphi(x)$ has a root in $\mathbb{A}$.

Without loss of generality, assume $\alpha_n = 1$. Indeed, by Theorem 1.12 we may divide $\varphi(x)$ by α_n, and the result is still in $\mathbb{A}[x]$.

By the Fundamental Theorem of Algebra, $\varphi(x)$ has a root $\beta \in \mathbb{C}$. Note that

$$\mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha_0, \ldots, \alpha_{n-1}, \beta].$$

Since β^n can be expressed as a linear combination of β^k, $k = 0, \dots, n-1$, with coefficients depending on α_i, $i = 0, \dots, n-1$, as

$$\beta^n = -\alpha_0 - \alpha_1\beta - \dots - \alpha_{n-1}\beta^{n-1},$$

we have

$$\dim \mathbb{Q}[\alpha_0, \dots, \alpha_{n-1}, \beta] \leqslant n \dim \mathbb{Q}[\alpha_0, \dots, \alpha_{n-1}] < \infty.$$

Hence, $\mathbb{Q}[\beta]$ is a finite-dimensional vector space over $\mathbb{Q}$, and by Lemma 1.9 $\beta \in \mathbb{A}$ □

Theorems 1.12 and 1.13 imply that $\mathbb{A}$ is the *algebraic closure* of $\mathbb{Q}$, which is often denoted by $\overline{\mathbb{Q}}$.

4. Algebraic integers. Suppose $K[x_1, \dots, x_n]$ is the ring of polynomials in several variables over a ring K. For $f \in K[x_1, \dots, x_n]$ denote by $\deg f$ the maximal sum of the degrees of the variables that appear in a term of f with a nonzero coefficient. Namely, f may be uniquely written as $f = f_0 + f_1 x_n + \dots + f_m x_n^m$, where $f_i \in K[x_1, \dots, x_{n-1}]$. Assuming $\deg f_i$ are defined by induction, set $\deg f = \max\limits_{i=0,\dots,m} (i + \deg f_i)$.

Theorem 1.14. *The set of all algebraic integers is a subring of the field* $\mathbb{C}$.

Proof. Ii is enough to show that if α, β are algebraic integers then $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers as well. We will prove a more general fact: Every number of the form

$$\gamma = \sum_{k,l} c_{kl} \alpha^k \beta^l, \quad c_{kl} \in \mathbb{Z},$$

is an algebraic integer.

Let

$$h_\alpha(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1} + x^n,$$
$$h_\beta(x) = b_0 + b_1 x + \dots + b_{m-1}x^{m-1} + x^m.$$

By Proposition 1.8, $a_i, b_j \in \mathbb{Z}$. Lemma 1.5 implies that h_α and h_β are irreducible polynomials over $\mathbb{Q}$, thus they have no multiple roots.

Denote by $\alpha_1, \dots, \alpha_n$ all complex roots of $h_\alpha(x)$, and let $\beta_1, \dots, \beta_m$ stand for all complex roots of $h_\beta(x)$. To be more precise, set $\alpha_1 = \alpha$, $\beta_1 = \beta$. Consider the polynomial

$$p(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} \left(x - \sum_{k,l} c_{kl} \alpha_i^k \beta_j^l \right) \in \mathbb{C}[x].$$

It is clear that $p(\gamma) = 0$ and the leading coefficient of $p(x)$ is equal to the identity. It remains to show that $p(x) \in \mathbb{Z}[x]$.

It follows from the definition of $p(x)$ that

$$p(x) = f(x, \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m),$$

where $f \in \mathbb{Z}[x, y_1, \dots, y_n, z_1, \dots, z_m]$. Namely,

$$f(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} \left(x - \sum_{k,l} c_{kl} y_i^k z_j^l \right) \in \mathbb{Z}[x, y_1, \dots, y_n, z_1, \dots, z_m].$$

Moreover, every permutation of the variables $y_1, \dots, y_n$ or $z_1, \dots, z_m$ does not change the polynomial f, i.e., it is symmetric with respect to y_i and with respect to z_i. Hence,

$$f(x, y_1, \dots, y_n, z_1, \dots, z_m) = \sum_{a=0}^{nm} g_a(y_1, \dots, y_n, z_1, \dots, z_m) x^a,$$

where every polynomial g_a is symmetric with respect to y_i and with respect to z_i. On the other hand, for every a we have

$$g_a(y_1, \dots, y_n, z_1, \dots, z_m) = \sum_{d_1, \dots, d_m \geqslant 1} g_{a, d_1, \dots, d_m}(y_1, \dots, y_n) z_1^{d_1} \dots z_m^{d_m},$$

where every polynomial $g_{a,d_1,\dots,d_m}(y_1, \dots, y_n)$ is symmetric (with respect to y_i) and has integral coefficients.

Lemma 1.15. *Let $\Psi(y_1, \dots, y_n) \in \mathbb{Z}[y_1, \dots, y_n]$ be a symmetric polynomial on $y_1, \dots, y_n$, $\deg \Psi = N$, and let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ be the roots of a polynomial $h(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$, $a_n \neq 0$. Then $a_n^N \Psi(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.*

Proof. By the Fundamental Theorem of Symmetric Polynomials, there exists a polynomial $G(t_1, \dots, t_n) \in \mathbb{Z}[t_1, \dots, t_n]$ such that

$$\Psi(y_1, \dots, y_n) = G(\sigma_1, \dots, \sigma_n), \quad \deg G \leqslant N.$$

where $\sigma_i(y_1, \dots, y_n)$ are the elementary symmetric polynomials on $y_1, \dots, y_n$. The Viet formulae imply $\sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k \dfrac{a_{n-k}}{a_n}$, $k = 1, \dots, n$. Since $\deg G \leqslant N$, we obtain

$$a_n^N \Psi(\alpha_1, \dots, \alpha_n) = a_n^N G\left(-\frac{a_{n-1}}{a_n}, \dots, (-1)^n \frac{a_0}{a_n} \right).$$

The latter is an integer number. □

Now we can use Lemma 1.15 for polynomials $g_{a,d_1,\dots,d_m}(y_1,\dots,y_n)$ to obtain $g_{a,d_1,\dots,d_m}(\alpha_1,\dots,\alpha_n) \in \mathbb{Z}$ (in this case, $a_n = 1$ since α_i are algebraic integers). Hence,

$$g_a(\alpha_1,\dots,\alpha_n,z_1,\dots,z_m) \in \mathbb{Z}[z_1,\dots,z_m]$$

are symmetric polynomials on $z_1,\dots,z_m$, and by Lemma 1.15 we have

$$g_a(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_m) \in \mathbb{Z}.$$

Therefore, $p(x) \in \mathbb{Z}[x]$. □

§ 1.2. Diophantine approximations of algebraic numbers

It is well-known from the course of Analysis that the set of rational numbers $\mathbb{Q}$ is a dense subset of the set of real numbers $\mathbb{R}$, i. e., for every $\alpha \in \mathbb{R}$ and for every $\varepsilon > 0$ there exists $\dfrac{p}{q} \in \mathbb{Q}$ such that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon. \tag{1.3}$$

Given a natural number N, the set $\mathbb{Q}_N = \{p/q \mid p \in \mathbb{Z},\ 0 < q \leqslant N\}$, has the following obvious property: $|a-b| \geqslant \dfrac{1}{N^2}$ for all $a, b \in \mathbb{Q}_N$. Hence, for every $\alpha \notin \mathbb{Q}_N$ (in particular, for an irrational one), we have

$$\min_{a\in\mathbb{Q}_N} |a-\alpha| > 0.$$

Therefore, in order to satisfy (1.3) for small ε, the number $\dfrac{p}{q}$ should have a an unboundedly large denominator q. This observation raises the following natural question: How to measure the accuracy of a rational approximation relative to the growing denominator values?

1. Diophantine approximation of degree ν. To estimate the accuracy of an approximation by rationals, we will compare the difference $|\alpha - p/q|$ with a decreasing function $q^{-\nu}$, $\nu > 0$. Namely, let us consider the following quantity:

$$\varepsilon_{\alpha,\nu}(q) = \min_{p\in\mathbb{Z},p/q\neq\alpha} \left\{ q^{\nu} \left|\alpha - \frac{p}{q}\right| \right\}, \quad \nu > 0. \tag{1.4}$$

It turns out that the study of the behavior of $\varepsilon_{\alpha,\nu}(q)$ as q approaches infinity leads to a necessary condition for α to be algebraic.

DEFINITION 1.1. A real number $\alpha \in \mathbb{R}$ *possesses a Diophantine approximation of degree* $\nu > 0$ if

$$\varliminf_{q\to\infty} \varepsilon_{\alpha,\nu}(q) < \infty. \tag{1.5}$$

Let us state a useful criterion that allows to determine whether a given number possesses a Diophantine approximation of a given degree.

Lemma 1.16. *A real number* α *possesses a Diophantine approximation of degree* $\nu > 0$ *if and only if there exists a constant* $c > 0$ *such that the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^\nu} \tag{1.6}$$

holds for infinitely many rationals $\dfrac{p}{q} \in \mathbb{Q}$.

PROOF. Denote by $M = M(\alpha, c, \nu)$ the set of all pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that (1.6) holds.

Suppose α possesses a Diophantine approximation of degree $\nu > 0$. By Definition 1.1, there exists $c > 0$ such that

$$\varepsilon_{\alpha,\nu}(q) < c$$

for infinitely many $q \in \mathbb{N}$. Let us fix this c and note that for every such $q \in \mathbb{N}$ there exists $p \in \mathbb{Z}$ satisfying the inequality (1.6).

Therefore, the set M is infinite, and there is no upper bound for the set $\{q \mid (p, q) \in M \text{ for some } p\}$. It remains to show that the set $\{p/q \mid (p, q) \in M\}$ is also infinite. Indeed, if it were finite then the left-hand side of (1.6) has a positive lower bound, but the right-hand side of (1.6) approaches zero since $\nu > 0$ and q may be chosen to be as large as we need.

Conversely, suppose there exists c such that (1.6) holds for infinitely many rationals p/q. Then the set M defined in the first part of the proof is infinite.

Assume the set $\{q \mid (p, q) \in M \text{ for some } p\}$ has an upper bound N, i.e.,

$$\{p/q \mid (p, q) \in M\} \subseteq \mathbb{Q}_N,$$

where

$$\mathbb{Q}_N = \{p/q \in \mathbb{Q} \mid p \in \mathbb{Z},\ 0 < q \leqslant N\}.$$

As we have already mentioned above, for every distinct $a_1, a_2 \in \mathbb{A}$ the inequality $|a_1 - a_2| > 1/N^2$ holds. Hence, any infinite subset S of $\mathbb{Q}_N$ has infinite diameter, i.e., for any $d > 0$ one may find p_1/q_1 and p_2/q_2 in S such that $|p_1/q_1 - p_2/q_2| > d$.

In particular, the set $S = \{p/q \mid (p,q) \in M\} \subseteq \mathbb{Q}_N$ contains p_1/q_1 and p_2/q_2 such that $|p_1/q_1 - p_2/q_2| > 2c$. Since (1.6) holds for p_i/q_i, $i = 1, 2$, we have

$$\left|\alpha - \frac{p_1}{q_1}\right| < \frac{c}{q_1^\nu}, \quad \left|\alpha - \frac{p_2}{q_2}\right| < \frac{c}{q_2^\nu}$$

which implies

$$2c < \left|\frac{p_1}{q_1} - \frac{p_2}{q_2}\right| < c\left(\frac{1}{q_1^\nu} + \frac{1}{q_2^\nu}\right) < 2c,$$

a contradiction.

Therefore, the set of denominators $\{q \mid (p,q) \in M \text{ for some } p\}$ is infinite, so there exist infinitely many q such that $\varepsilon_{\alpha,\nu}(q) < c$. Hence, the sequence $\{\varepsilon_{\alpha,\nu}(q)\}_{q\in\mathbb{N}}$ has a finite accumulation point, and (1.5) holds. □

Exercise 1.17. Whether a rational number possesses a Diophantine approximation of degree 1?

2. Dirichlet approximation theorem.

Theorem 1.18 (Dirichlet Approximation Theorem)**.** *For every $\alpha \in \mathbb{R}$ and for every $N \in \mathbb{N}$ there exist $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}, \quad q \leqslant N.$$

Proof. Consider the fractional parts of the numbers $k\alpha$, $k = 0, \dots, N$:

$$\xi_k = \{k\alpha\} = k\alpha - [k\alpha] \in [0, 1).$$

Divide the interval $[0, 1)$ into N intervals of length $1/N$ as follows:

$$[k/N, (k+1)/N), \quad k = 0, \dots, N-1.$$

According to the combinatorial Dirichlet's Principle, when $N+1$ numbers $\xi_0, \dots, \xi_N$ are set into N intervals, there exists at least one interval which contains at least two of these numbers, i.e.,

$$|\xi_{k_1} - \xi_{k_2}| < 1/N$$

for some k_1, k_2, $0 \leqslant k_1 < k_2 \leqslant N$.

Let

$$p = [k_2\alpha] - [k_1\alpha], \quad q = k_2 - k_1.$$

Then

$$\left|\alpha - \frac{p}{q}\right| = \frac{1}{q}|\alpha(k_2 - k_1) - [k_2\alpha] + [k_1\alpha]| = \frac{1}{q}|\xi_{k_2} - \xi_{k_1}| < \frac{1}{Nq}.$$

□

Corollary 1.19. *If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ then α possesses a Diophantine approximation of degree $\nu = 2$.*

Proof. Theorem 1.18 implies that for every natural number N there exist $p_N \in \mathbb{Z}$ and $q_N \in \mathbb{N}$, $q_N \leqslant N$, such that

$$\left|\alpha - \frac{p_N}{q_N}\right| < \frac{1}{Nq_N}. \tag{1.7}$$

Let us show that the sequence $\{q_N\}_{N\geqslant 1}$ is not bounded. Assume the converse, i.e., suppose there exists a constant M such that $q_N \leqslant M$ for all N. Then (1.7) implies

$$\min_{p/q\in\mathbb{Q}_M} \left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq_N} \leqslant \frac{1}{N} \underset{N\to\infty}{\to} 0,$$

which is impossible.

Therefore, (1.7) holds for infinitely many numbers q_N. Since $q_N \leqslant N$, we have

$$q_N^2 \left|\alpha - \frac{p_N}{q_N}\right| < 1$$

for infinitely many q_N. □

Proposition 1.20. *Let $\alpha \in \mathbb{Q}$. Then for every function $\varphi : \mathbb{N} \to \mathbb{R}_+$ satisfying $\lim\limits_{q\to\infty} q\varphi(q) = 0$ there exist only a finite number of rationals $\dfrac{p}{q}$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \varphi(q). \tag{1.8}$$

Proof. Denote by S the set of all rationals p/q, $\gcd(p, q) = 1$, satisfying (1.8). Assume S is infinite. It is easy to see that the distance between any two numbers from S does not exceed $2\max\limits_{q\geqslant 1} \varphi(q)$ which is finite. Note that the set of denominators of all fractions from S has no upper bound: Otherwise, if $S \subseteq \mathbb{Q}_N$, where $\mathbb{Q}_N$ introduced in the proof of Lemma 1.16, then S has an infinite diameter.

Let $\alpha = \dfrac{a}{b}$. Then for all rationals $\dfrac{p}{q}$ except α itself the following inequality holds:

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \left|\frac{aq - pb}{bq}\right| \geqslant \frac{1}{bq}.$$

Since b is fixed, we have

$$\frac{1}{bq} > \varphi(q),$$

which is impossible for sufficiently large q. The contradiction obtained proves that S is finite. □

Corollary 1.21. *A rational number α does not have a Diophantine approximation of degree $\nu > 1$.* □

The result obtained is in some sence paradoxical: All irrational numbers possess Diophantine approximations of degree 2, but neither of rationals has a Diophantine approximation of degree $\nu > 1$. Therefore, the existence of a Diophantine approximation of degree $\nu \geqslant 2$ is a criterion of irrationality.

Let us apply the criterion above to the base of the natural logarithm

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \ldots, \tag{1.9}$$

also called the *Euler's number*.

Proposition 1.22. *The Euler's number is irrational.*

Proof. Consider the sum of the first $n+1$ summands in (1.9) and reduce to the common denominator:

$$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} = \frac{p_n}{n!}.$$

Then

$$\left|e - \frac{p_n}{n!}\right| = \frac{1}{(n+1)!}\left(\frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \ldots\right) < \frac{1}{(n+1)!}\left(\frac{1}{2} + \frac{1}{2^2} + \ldots\right) = \frac{2}{(n+1)!}.$$

Define a function $\varphi : \mathbb{N} \to \mathbb{R}$ as follows:

$$\varphi(1) = 1,$$

$$\varphi(q) = \frac{2}{(n+1)!} \text{ for } (n-1)! < q \leqslant n!,\ n \geqslant 2.$$

If $q \in ((n-1)!, n!]$ then

$$q\varphi(q) \leqslant n!\frac{2}{(n+1)!} = \frac{2}{n+1},$$

so $\lim\limits_{q\to\infty} q\varphi(q) = 0$. However,

$$\left|e - \frac{p}{q}\right| < \varphi(q)$$

for infinitely many $p/q = p_n/n!$, $n \geqslant 2$. Hence, e is irrational by Proposition 1.20. □

3. Liouville theorem on Diophantine approximation of algebraic numbers.

Theorem 1.23 (Liouville Theorem)**.** *Let α be an algebraic number of degree $n \geqslant 2$. Then α has no Diophantine approximation of degree $\nu > n$.*

Proof. First, let us find a constant $M > 0$ such that

$$\left|\alpha - \frac{p}{q}\right| > \frac{M}{q^n} \tag{1.10}$$

for all $p \in \mathbb{Z}$ and $q \in \mathbb{N}$.

Set $h(x)$ to be a multiple of the minmal polynomial for α with integer coefficients, e.g., $h(x) = q(h_\alpha)h_\alpha(x)$. Suppose $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ are the complex roots of this polynomial, and assume $\alpha_1 = \alpha$. Then

$$h(x) = a_n \prod_{k=1}^{n}(x - \alpha_k) = a_n(x - \alpha)\prod_{k=2}^{n}(x - \alpha_k),$$

where a_n is the leading coefficient of $h(x)$. Denote by M the following quantity:

$$M = \left(|a_n| \prod_{k=2}^{n}(|\alpha| + |\alpha_k| + 1)\right)^{-1},$$

and let us show that (1.10) holds.

If p and q meet the inequality $|\alpha - p/q| \geqslant 1$ then (1.10) is valid since $M < 1$ ($|\alpha| > 0$, $n \geqslant 2$).

Assume p and q satisfy the condition $|\alpha - p/q| < 1$. In this case,

$$\left|\frac{p}{q}\right| < 1 + |\alpha|$$

and thus

$$|h(p/q)| = |a_n| \left|\alpha - \frac{p}{q}\right| \prod_{k=2}^{n}\left|\alpha_k - \frac{p}{q}\right|$$
$$\leqslant \left|\alpha - \frac{p}{q}\right| |a_n| \prod_{k=2}^{n}\left(|\alpha_k| + \left|\frac{p}{q}\right|\right) < \left|\alpha - \frac{p}{q}\right| \frac{1}{M}.$$

Lemma 1.5 implies $h(x)$ to be irreducible over $\mathbb{Q}$, hence, it has no rational roots. Therefore,

$$|h(p/q)| = \left|a_0 + a_1\frac{p}{q} + \cdots + a_n\frac{p^n}{q^n}\right| \geqslant \frac{1}{q^n},$$

and (1.10) follows.

Finally, apply (1.10) to show that α has no Diophantine approximation of degree $\nu > n$. Assume the converse: Let there exist $\nu > n$ and $c > 0$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^\nu}$$

holds for infinitely many $p/q \in \mathbb{Q}$. Then, as it was shown in the proof of Lemma 1.16, the last inequality holds for infinitely many denominators $q \in \mathbb{N}$. Then for sufficiently large q we have

$$\frac{c}{q^\nu} < \frac{M}{q^n},$$

in contradiction to (1.10). □

The Liouville Theorem is a powerful tool that allows constructing explicit examples of transcendental numbers. Namely, we obtain the following sufficient condition of transcendentality.

Corollary 1.24. *Let α be a real number. If for every $N \in \mathbb{N}$ it possesses a Diophantine approximation of degree $\nu \geqslant N$ then α is transcendental.*

Example 1.2. The following number is transcendental:

$$\alpha = \sum_{n=1}^{\infty} 10^{-n!}.$$

Proof. Given $N \in \mathbb{N}$, consider

$$\frac{p_N}{q_N} = \sum_{n=1}^{N} 10^{-n!} = \frac{p_N}{10^{N!}}.$$

Note that

$$\left|\alpha - \frac{p_N}{q_N}\right| = \sum_{n=N+1}^{\infty} 10^{-n!} < 2 \cdot 10^{-(N+1)!} = \frac{2}{q_N^{N+1}}.$$

Therefore, for every $\nu > 0$ there exist infinitely many rationals $\dfrac{p_N}{q_N}$, $N \geqslant \nu$, satisfying

$$\left|\alpha - \frac{p_N}{q_N}\right| < \frac{2}{q_N^{N+1}} < \frac{2}{q_N^{\nu}}.$$

Hence, α possesses a Diophantine approximation of any degree. Theorem 1.23 implies α is not algebraic. □

§ 1.3. Transcendentality of e and π

The Liouville Theorem provides a sufficient condition for a real number to be transcendental. However, this condition is not necessary. There exist different methods to prove transcendentality of a series of important constants, e.g., e and π. In this section, we are going to study one of these methods known as the *Hermite Method*.

Given an analytic function $f(z)$ on the complex plane, denote by

$$\int_{x_0}^{x} f(z)\,dz$$

the Riemann integral of $f(z)$ along the straight segment starting at $x_0 \in \mathbb{C}$ and ending at $x \in \mathbb{C}$ (the Cauchy Integral Theorem implies that this integral does not depend on the choice of a path with the same endpoints x_0 and x, we choose the straight segment for convenience).

1. Hermite identity.

Lemma 1.25 (Hermite Identity)**.** *Let $\alpha \in \mathbb{C}$, $\alpha \neq 0$, and let $f(x) \in \mathbb{C}[x]$, $\deg f \geqslant 1$. Then for every $x \in \mathbb{C}$ we have*

$$\int_0^x f(t)e^{-\alpha t}\,dt = F(0) - F(x)e^{-\alpha x}, \tag{1.11}$$

where

$$F(x) = \frac{f(x)}{\alpha} + \frac{f'(x)}{\alpha^2} + \cdots + \frac{f^{(n)}(x)}{\alpha^{n+1}}.$$

Proof. According to the Fundamental Theorem of Calculus (the Newton—Leibniz Formula),

$$\frac{d}{dx}\int_0^x f(t)e^{-\alpha t}\,dt = f(x)e^{-\alpha x}.$$

On the other hand,

$$\frac{d}{dx}F(x)e^{-\alpha x} = (F'(x) - \alpha F(x))e^{-\alpha x} = -f(x)e^{-\alpha x}.$$

Hence, the derivatives with respect to x of the both sides of (1.11) coincide. It remains to compare the values at $x = 0$ to obtain the desired equality. □

The main idea of the Hermite's method is to apply the Hermite identity (1.11) to a polynomial of the form

$$H(h(x)) = \frac{1}{(p-1)!}a_n^{(n-1)p}x^{p-1}h(x)^p, \tag{1.12}$$

$h(x) \in \mathbb{Z}[x]$, $n = \deg h$, $p \in \mathbb{N}$. Let us establish the properties of $H(h(x))$.

Lemma 1.26. *Let $h(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_0, a_n \neq 0$, $n \geqslant 1$, and let $\beta_1, \ldots, \beta_n \in \mathbb{C}$ be the entire collection of roots of $h(x)$ in which every root of multiplicity k appears k times. Then for every $p \in \mathbb{N}$, $p \geqslant 2$, the polynomial $f(x) = H(h(x))$ defined by (1.12) has the following properties:*

(1) $f^{(j)}(0) = 0$, $0 \leqslant j \leqslant p-2$;
(2) $f^{(j)}(\beta_i) = 0$, $0 \leqslant j \leqslant p-1$, $i = 1, \ldots, n$;
(3) $f^{(p-1)}(0) = a_n^{(n-1)p}a_0^p$;
(4) $f^{(j)}(0) \in p\mathbb{Z}$, $j \geqslant p$;
(5) $\sum\limits_{i=1}^{n} f^{(j)}(\beta_i) \in p\mathbb{Z}$, $j \geqslant p$.

Proof. It is easy to see from the construction of $f(x)$ that 0 is its root of multiplicity $p-1$ and every β_i is a root of $f(x)$ of multiplicity at least p. As we know from the Abstract Algebra course, a root of multiplicity k of a polynomial $f(x)$ is also a root of $f'(x), f''(x), \ldots, f^{(k-1)}(x)$. This implies (1) and (2).

To prove (3), let us distribute all brackets in the definition of $f(x)$ and find the term of lowest degree in x, namely, the term is

$$\frac{1}{(p-1)!}a_n^{(n-1)p}a_0^p x^{p-1}.$$

Its $(p-1)$th derivative is equal to $a_n^{(n-1)p}a_0^p$. For all other terms in $f(x)$, their $(p-1)$th derivatives contain x and thus turn into zero at $x = 0$.

Before we proceed with the proof of the remaining statements, note the following general fact. Given a polynomial $\Phi(x) \in \mathbb{Z}[x]$, its jth derivative

$\Phi^{(j)}(x)$, $j \in \mathbb{N}$, belongs to $j!\mathbb{Z}[x]$, i.e., all nonzero coefficients of $\Phi^{(j)}(x)$ contain the factor $j!$. Indeed, for all $m \geqslant j$ we have

$$(x^m)^{(j)} = j!\binom{m}{j}x^{m-j} \in \mathbb{Z}[x],$$

and the jth derivatives of x^m, $m < j$, turn into zero.

To prove (4), consider

$$\Phi(x) = \frac{(p-1)!}{a_n^{(n-1)p}}f(x) = x^{p-1}h(x)^p \in \mathbb{Z}[x].$$

According to the remark stated above, $\Phi^{(j)}(x) \in j!\mathbb{Z}[x]$ and thus

$$f(0) \in \frac{j!}{(p-1)!}\mathbb{Z} \subseteq j\mathbb{Z}$$

for $j \geqslant p$,

Finally, note that

$$h(x) = a_n\prod_{i=1}^{n}(x-\beta_i).$$

Hence,

$$f(x) = \frac{a_n^{np}}{(p-1)!}\prod_{i=1}^{n}(x-\beta_i)^p x^{p-1} = \frac{a_n^{np}}{(p-1)!}\Theta(x,\beta_1,\ldots,\beta_n),$$

where

$$\Theta = x^{p-1}\prod_{i=1}^{n}(x-y_i)^p \in \mathbb{Z}[x,y_1,\ldots,y_n].$$

The polynomial

$$\Psi(y_1,\ldots,y_n) = \sum_{i=1}^{n}\frac{\partial^j\Theta}{\partial x^j}(y_i,y_1,\ldots,y_n) \in \mathbb{Z}[y_1,\ldots,y_n]$$

is symmetric with respect to $y_1,\ldots,y_n$, $\deg\Psi = \deg\Phi - j = np+p-1-j < np$ for $j \geqslant p$, and all coefficients of Ψ are divisible by $j!$. By Lemma 1.15 applied to $\dfrac{1}{j!}\Psi(y_1,\ldots,y_n)$, we obtain

$$\frac{a_n^{np}}{j!}\Psi(\beta_1,\ldots,\beta_n) \in \mathbb{Z}.$$

Since $j \geqslant p$,

$$\frac{a_n^{np}}{(p-1)!}\Psi(\beta_1,\ldots,\beta_n) \in p\mathbb{Z},$$

and it remains to note

$$\sum_{i=1}^{n} f^{(j)}(\beta_i) = \frac{a_n^{np}}{(p-1)!}\Psi(\beta_1, \dots, \beta_n),$$

which proves (5). □

Remark 1.3. Upon the conditions of Lemma 1.26, assume that $\beta_i \in \mathbb{Z}$, $i = 1, \dots, n$. Then the statement (5) of Lemma 1.26 may be enhanced in the obvious way as

$$f^j(\beta_i) \in p\mathbb{Z}, \quad i = 1, \dots, n, \ j \geqslant p.$$

2. Transcendentality of e.

Theorem 1.27. *If $\alpha \in \mathbb{Q} \setminus \{0\}$ then e^α is a transcendental number.*

Proof. Suppose $\beta = e^{a/b}$ is an algebraic number for some $a/b \in \mathbb{Q}$, $a \neq 0$. Then e is a root of the equation $x^a - \beta^b = 0$ with algebraic coefficients. By Theorem 1.13, all roots of such equation (in particular, e) are algebraic numbers. Hence, it is enough to show that e itself is transcendental.

Assume e is algebraic, and let $h_e(x) \in \mathbb{Q}[x]$ be its minimal polynomial. Then there exists $b_n \in \mathbb{Z}$ such that

$$b_n h_e(x) = b_0 + b_1 x + \dots + b_n x^n \in \mathbb{Z}[x].$$

It is clear that $b_0 \neq 0$.

Choose a prime number $p \in \mathbb{Z}$ such that $p > n$ and $p > |b_0|$ (it is possible to make such a choice since the set of primes is infinite).

Consider the polynomial

$$h(x) = (x-1)(x-2)\dots(x-n)$$

and construct

$$f(x) = H(h(x)) = \frac{1}{(p-1)!}x^{p-1}h(x)^p$$

as in (1.12), where $\beta_i = i$, $i = 1, \dots, n$. For every $k = 0, 1, \dots, n$ write the Hermite identity from Lemma 1.25:

$$\int_0^k f(t)e^{-t}\,dt = F(0) - F(k)e^{-k}.$$

Multiply each of these equations by $b_k e^k$ and add the results:

$$\sum_{k=0}^{n} b_k \int_0^k f(t)e^{k-t}\,dt = \sum_{k=0}^{n} b_k e^k (F(0) - F(k)e^{-k})$$
$$= F(0)\sum_{k=0}^{n} b_k e^k - \sum_{k=0}^{n} b_k F(k) = F(0)b_n h_e(e) - \sum_{k=0}^{n} b_k F(k).$$

Therefore,

$$\sum_{k=0}^{n} \int_0^k b_k f(t)e^{k-t}\,dt = -\sum_{k=0}^{n} b_k F(k). \tag{1.13}$$

Recall that

$$F(x) = \sum_{j\geqslant 0} f^{(j)}(x).$$

Consider the right-hand side of (1.13). Lemma 1.12 and Remark 1.3 imply

$$\sum_{k=0}^{n} b_k F(k) = b_0 f^{(p-1)}(0) + b_0 \sum_{j\geqslant p} f^{(j)}(0) + \sum_{k=1}^{n} b_k \sum_{j\geqslant p} f^{(j)}(k).$$

In the last expression, $b_0 f^{(p-1)}(0) = (-1)^{np} b_0 (n!)^p \not\equiv 0 \,(\mathrm{mod}\, p)$ by the choice of p, all other summands are integer multiples of p. Hence, for every sufficiently large prime p the right-hand side of (1.13) is a nonzero integer number.

Now, let us estimate the absolute value of the left-hand side of (1.13):

$$\left|\sum_{k=0}^{n} b_k \int_0^k f(t)e^{k-t}\,dt\right| \leqslant \sum_{k=0}^{n} |b_k| k \max_{t\in[0,k]}\{|f(t)e^{k-t}|\}$$
$$\leqslant (n+1)\max_{k=0,\dots,n}|b_k| n \max_{t\in[0,n]}\{|f(t)|\}e^n \leqslant C\frac{1}{(p-1)!}n^{p-1}(n-1)^{np} \leqslant C\frac{C_1^p}{(p-1)!},$$

where C and C_1 do not depend on the choice of p. Since $\lim\limits_{p\to\infty} \dfrac{C_1^p}{(p-1)!} = 0$,

$$\left|\sum_{k=0}^{n} b_k \int_0^k f(t)e^{k-t}\,dt\right| < 1$$

when p is sufficiently large, but the right-hand side of (1.13) is a nonzero integer and thus its absolute value is greater or equal to 1. The contradiction obtained proves the theorem. □

3. Symmetrized n-tuples.

DEFINITION 1.4. An N-tuple $(\beta_1, \dots, \beta_N) \in \mathbb{C}^N$ is called *symmetrized* if

$$\prod_{j=1}^{N} (x - \beta_j) \in \mathbb{Q}[x].$$

It is clear that a symmetrized tuple remains symmetrized after every permutation of its components. If we add (or remove) a rational number to (or from) a symmetrized tuple then the tuple obtained is symmetrized. Also, the concatenation of two or more symmetrized tuples is again a symmetrized tuple.

To prove the transcendence of π we need the following properties of symmetrized tuples.

Lemma 1.28. *Let $(\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n$ be a symmetrized tuple, and let $\sigma = \sigma_k \in \mathbb{Z}[x_1, \dots, x_n]$, $k \in \{1, \dots, n\}$, be an elementary symmetric polynomial in $x_1, \dots, x_n$. Then*

$$\sigma\big(e^{\alpha_1}, \dots, e^{\alpha_n}\big) = \sum_{j=1}^{N} e^{\beta_j}, \quad N = \binom{n}{k},$$

where $(\beta_1, \dots, \beta_N)$ is a symmetrized tuple.

PROOF. Recall that

$$\sigma = \sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} x_{i_1} \dots x_{i_k}$$

contains $N = \binom{n}{k}$ summands. For every collection of indexes $1 \leqslant i_1 < \dots < i_k \leqslant n$, consider the following polynomial:

$$\eta_{i_1,\dots,i_k}(t_1, \dots, t_n) = t_{i_1} + \dots + t_{i_k} \in \mathbb{Z}[t_1, \dots, t_n].$$

Then

$$\sigma\big(e^{\alpha_1}, \dots, e^{\alpha_n}\big) = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} e^{\eta_{i_1,\dots,i_k}(\alpha_1,\dots,\alpha_n)}.$$

It remains to show that complex numbers

$$\eta_{i_1,\dots,i_k}(\alpha_1, \dots, \alpha_n), \quad 1 \leqslant i_1 < \dots < i_k \leqslant n,$$

form a symmetrized tuple.

Let us enumerate all k-tuples $(i_1, \dots, i_k)$, $1 \leqslant i_1 < \dots < i_k \leqslant n$, by integer numbers $j = 1, \dots, N$. We will use the same enumeration for polynomials $\eta_{i_1,\dots,i_k}$: If $(i_1, \dots, i_k)$ has number j then $\eta_j = \eta_{i_1,\dots,i_k}$.

If $\Phi(y_1, \dots, y_N)$ is a symmetric polynomial in $y_1, \dots, y_N$ with integer coefficients then

$$\Psi = \Phi(\eta_1(t_1, \dots, t_n), \dots, \eta_N(t_1, \dots, t_n)) \in \mathbb{Z}[t_1, \dots, t_n]$$

is a symmetric polynomial in $t_1, \dots, t_n$. Indeed, let us transpose in Ψ two variables t_l and t_i. The set of all polynomials $\eta_1, \dots, \eta_N$ may be divided into three groups: The first group contains all those polynomials that either do not depend in both t_i and t_l, or containt both these variables; The second group consists of all η_js that depend in t_i, but do not depend in t_l; The third group includes all remaining polynomials η_j. When exchanging t_i and t_l, the polynomials of the first group do not change, the polynomials of the second group turn into polynomials of the third group, and, conversely, all polynomials of the third group move into the second group. Finally, we obtain a permutation of $\eta_1, \dots, \eta_N$. Since Φ is symmetric, Ψ is invariant under the transposition of t_l and t_i. It is well-known that every permutation can be obtained by a series of transpositions (all transpositions generate the symmetric group S_n). Hence, Ψ is also symmetric.

Therefore, for every symmetric $\Phi \in \mathbb{Z}[y_1, \dots, y_N]$ we have

$$\Phi(\beta_1, \dots, \beta_N) = \Psi(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}.$$

In particular, all elementary symmetric polynomials in $y_1, \dots, y_N$ take rational values at $\beta_1, \dots, \beta_N$, i.e., $(\beta_1, \dots, \beta_N)$ is a symmetrized N-tuple. □

4. Transcendentality of π.

Lemma 1.29. *Let $(\beta_1, \dots, \beta_N)$ be a symmetrized N-tuple of nonzero complex numbers. If, in addition,*

$$A := \sum_{k=1}^{N} e^{\beta_k} \neq 0,$$

then $A \notin \mathbb{Q}$.

Proof. Assume $A \in \mathbb{Q} \setminus \{0\}$. Without loss of generality, we can suppose $A \in \mathbb{Z}$: If $A = a/b$ then one may just repeat the symmetrized N-tuple b times to get a new symmetrized Nb-tuple with integer sum of exponents.

Consider a polynomial

$$h(x) = b_N \prod_{k=1}^{N} (x - \beta_k) = b_0 + b_1 x + \cdots + b_N x^N \in \mathbb{Z}[x].$$

Here $b_0 = (-1)^N b_N \cdot \beta_1 \cdot \ldots \cdot \beta_N \neq 0$.

Choose a prime number $p \in \mathbb{Z}$ such that $p > |b_N|$, $p > |b_0|$, $p > |A|$, and construct a polynomial

$$f(x) = \frac{1}{(p-1)!} b_N^{(N-1)p} x^{p-1} h(x)^p$$

as in Lemma 1.26. The Hermite identity for $f(x)$ has the following form:

$$\int_0^{\beta_k} f(t) e^{-t}\, dt = F(0) - F(\beta_k) e^{-\beta_k}, \quad k = 1, \ldots, N.$$

Let us multiply each of these expressions by e^{β_k} for the corresponding k, and compute the sum of all values obtained for $k = 1, \ldots, N$. Then

$$\sum_{k=1}^{N} \int_0^{\beta_k} f(t) e^{\beta_k - t}\, dt = AF(0) - \sum_{k=1}^{N} F(\beta_k). \tag{1.14}$$

Consider the right-hand side of equation (1.14):

$$AF(0) - \sum_{k=1}^{N} F(\beta_k) = Af^{(p-1)}(0) + A \sum_{j \geqslant p} f^{(j)}(0) - \sum_{k=1}^{N} \left(\sum_{j \geqslant 0} f^{(j)}(\beta_k) \right).$$

By Lemma 1.26, the first summand $Af^{(p-1)}(0) = Ab_N^{(N-1)p} b_0^p$ is an integer number that cannot be divided by p, but all other summands are integers divisible by p. Hence, the right-hand side of (1.14) is a nonzero integer.

The absolute value of the left-hand side of (1.14) may be estimated from above as $C \dfrac{C_1^p}{(p-1)!}$ in the very same way as it was done in the proof of Theorem 1.27.

Therefore, if p is sufficiently large then (1.14) does not hold. □

Theorem 1.30 (Lindemann Theorem)**.** *If α is a nonzero algebraic number then e^α may not be a negative rational number.*

PROOF. Let α be a root of a polynomial $h(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ which is irreducible over $\mathbb{Q}$, and let $(\alpha_1, \ldots, \alpha_n)$ be all roots of $h(x)$, i.e., all numbers conjugate to α, where $\alpha_1 = \alpha$.

Recall that $e^\alpha \neq 0$ for all $\alpha \in \mathbb{C}$. Assume $e^\alpha = -\dfrac{a}{b}$, $a, b \in \mathbb{N}$, where $\gcd(a, b) = 1$. Consider

$$0 = \prod_{k=1}^{n} \left(e^{\alpha_k} + \frac{a}{b} \right).$$

Distribute the brackets and and multiply by b^n to obtain

$$0 = a^n + \sum_{k=1}^{n-1} a^k b^{n-k} \sigma_{n-k}(e^{\alpha_1}, \ldots, e^{\alpha_n}). \tag{1.15}$$

By Lemma 1.28, for each $k = 1, \ldots, n-1$ there exist a number N_k and a symmetrized N_k-tuple $(\beta_{k1}, \ldots, \beta_{kN_k})$ such that

$$\sigma_{n-k}(e^{\alpha_1}, \ldots, e^{\alpha_n}) = \sum_{j=1}^{N_k} e^{\beta_{kj}}.$$

It may happen that some of β_{kj} are zero. Denote by $m_k \geqslant 0$ the number of zeros among β_{kj}, $j = 1, \ldots, N_k$. Let $(\gamma_1, \ldots, \gamma_N)$ stand for the collection of all nonzero β_{kj} in which every β_{kj} appears $a^k b^{n-k}$ times. This is a symmetrized N-tuple. Now, we may rewrite (1.15) as

$$a^n + \sum_{k=1}^{n-1} a^k b^{n-k} m_k = -\sum_{j=1}^{N} c_j e^{\gamma_j}, \quad c_j \in \mathbb{Z}.$$

The left-hand side is an integer A which is not divisible by b, hence, $A \neq 0$. Thus,

$$-\sum_{j=1}^{N} c_j e^{\gamma_j} = A \neq 0,$$

which is a contradiction to Lemma 1.29. □

Corollary 1.31. *The number π is transcendental.*

PROOF. If π were algebraic then $\alpha = \iota\pi$, where ι is the imaginary identity, is also algebraic as a product of two algebraic numbers. The Euler identity $e^{\iota\pi} = -1 \in \mathbb{Q}$ implies a contradiction to Theorem 1.30. □

As an immediate corollary, we conclude that the famous ancient problem of squaring the circle may not be solved with a straightedge and compass. Indeed, given a segment of unit length in the plane (the radius of

a given circle), every segment one may construct with a straightedge and compass must have algebraic length. Hence, a segment of length $\pi^{1/2}$ (the side of a desired square) cannot be constructed. A finer statement, which is a good exercise for a reader, says that if a segment of length a may be constructed with a straightedge and compass then a is an algebraic number of degree 2^k (a Pythagorean number). In this way, one may prove that an arbitrary angle in the plane may not be divided into three equal parts, and a right heptagon may not be constructed with a straightedge and compass (for more details, see Exercise 2 below).

§ 1.4. Problems

(1) Suppose α is a root of a monic polynomial with algebraic integer coefficients. Show that α is an algebraic integer.
(2) Find the degree of the algebraic number $e^{2\pi\iota/n}$, where ι is the imaginary identity and n is a natural number.
(3) Show that if α is a nonzero algebraic number then e^{α} is transcendental.
(4) Prove the Weierstrass—Lindemann Theorem: If $\alpha_1, \ldots, \alpha_n$ are pairwise different algebraic numbers then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are linearly independent over the field of algebraic numbers.

CHAPTER 2

Asymptotic law of distribution of prime numbers

Prime integers are "atoms" of the numeric Universe and thus they have been attracting attention of researchers for more than two thousand years. Ancient Greek mathematicians obtained a lot of nice results, e.g., Euclid (III BC) proved that there exist infinitely many primes, Eratosthenes (II BC) invented an algorithm to find all primes smaller than a given natural N (the Sieve of Eratosthenes). These results are now considered as "elementary".

The aim of this section is to present a precise answer to the following question: How often prime numbers occur in the series of all natural numbers?

This question was raised by Hauss and Legendre at the end of XVIII, and the Hauss conjecture was proved by Jacques Hadamard and Charles Jean de la Vallée-Poussin in 1896. The result is known as the Prime Number Theorem. To explain the statement, recall the notion of asymptotic equivalence.

Suppose $f(x)$ and $g(x)$ are two real-valued functions defined on a ray $[a, \infty) \subset \mathbb{R}$ such that $f(x), g(x) \neq 0$ for all sufficiently large x. These functions are said to be *asymptotically equivalent* if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

In this case, we write

$$f(x) \sim g(x).$$

Recall that $\mathbb{P} \subset \mathbb{N}$ stands for the set of all primes, $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$.

The main object of study in this chapter is the *prime-counting function* $\pi(x)$, $x > 0$, describing the distribution of prime numbers. Namely, $\pi(x)$ is the cardinality of the set of all primes $p \in \mathbb{P}$ such that $p \leqslant x$, $x \in \mathbb{R}$, $x > 0$.

The main purpose of this section is to prove the following equivalence:

$$\pi(x) \sim \frac{x}{\ln(x)}.$$

EXERCISE 2.1. Prove that $\dfrac{x}{\ln x} \sim \mathrm{li}(x)$, where

$$\mathrm{li}(x) = \int\limits_2^x \frac{dt}{\ln t}.$$

§ 2.1. Chebyshev functions

1. Definition and estimates. Here we will establish important relations between the function $\pi(x)$ and the following functions defined on all positive real numbers:

- $\psi(x) = \sum\limits_{(p,m)\in Q_x} \ln p$, where $Q_x = \{(p,m) \mid p \in \mathbb{P}, m \in \mathbb{N}, p^m \leqslant x\}$. The function ψ is called the *Chebyshev function*;
- $\tilde{\psi}(x) = \int\limits_1^x \dfrac{\psi(t)}{t}\, dt$ is known as the *integral Chebyshev function.*

Note that $\pi(x)$ may be presented in a similar way as

$$\sum_{p\in\mathbb{P}, p\leqslant x} 1.$$

Note that $(p,m) \in Q_x$ if and only if $p \leqslant x$ and $\ln(p^m) = m \ln p \leqslant \ln x$. Therefore, the sum

$$\sum_{(p,m)\in Q_x} \ln p = \psi(x)$$

contains each $\ln p$ as many times as the count of all $m \in \mathbb{N}$ such that $m \ln p \leqslant \ln x$. If $x > 1$ (i.e., $\ln x > 0$) there exist $[\ln x / \ln p]$ of such ms (here $[\cdot]$ stands for the integral part of a real number). Hence,

$$\psi(x) = \sum_{p\in\mathbb{P}, p\leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p, \quad x > 1. \tag{2.1}$$

Proposition 2.2. *The following statements hold:*

(1) $\psi(x) \leqslant \pi(x) \ln x$, $\tilde{\psi}(x) \leqslant \pi(x) \ln^2 x$ *for every* $x > 1$;
(2) $\lim\limits_{x\to\infty} \psi(x)/x^z = \lim\limits_{x\to\infty} \tilde{\psi}(x)/x^z = 0$ *for every* $z \in \mathbb{C}$ *such that* $\operatorname{Re} z > 1$.

PROOF. (1) If we omit $[\cdot]$ in (2.1) then the value of this sum may just increase since $[x] \leqslant x$, i.e.,

$$\psi(x) = \sum_{p \leqslant x} [\ln x / \ln p] \ln p \leqslant \sum_{p \leqslant x} \ln p \leqslant \sum_{p \leqslant x} \ln x = \pi(x) \ln x$$

(hereinafter, when we use "p" for summation index, we assume p ranges over prime numbers, as in (2.1)).

For the integral Chebyshev function, note that

$$\tilde{\psi}(x) \leqslant \psi(x) \int_1^x \frac{dt}{t} = \psi(x) \ln x.$$

The statement (2) immediately follows from (1): If $z = 1 + a + \imath b$, $a > 0$, then

$$|\psi(x)/x^z| = \psi(x)/x^{1+a} \leqslant \pi(x) \ln x / x^{1+a} \leqslant x \ln x / x^{1+a} = \ln x / x^a \to 0$$

as $x \to \infty$. For $\tilde{\psi}(x)$, the proof is completely similar. □

EXERCISE 2.3. Prove that $\lim\limits_{x \to \infty} \tilde{\psi}(x)/x^z = 0$ for $\operatorname{Re} z > 1$.

2. Equivalence of the asymptotic behavior of Chebyshev functions and of the prime-counting function.

Theorem 2.4. *The following statements are equivalent:*

(A1) $\pi(x) \sim x/lnx$;
(A2) $\psi(x) \sim x$;
(A3) $\tilde{\psi}(x) \sim x$.

PROOF. (A1)⇔(A2) By Proposition 2.2, $\psi(x) \leqslant \pi(x) \ln x$ for $x > 1$. Hence,

$$\frac{\psi(x)}{x} \leqslant \frac{\pi(x)}{x/\ln x},$$

and the same inequality holds for upper and lower limits of these functions as $x \to \infty$. Namely,

$$\text{(A1)} \Rightarrow \varliminf_{x \to \infty} \frac{\psi(x)}{x} \leqslant \varlimsup_{x \to \infty} \frac{\psi(x)}{x} \leqslant 1,$$

$$\text{(A2)} \Rightarrow \varlimsup_{x \to \infty} \frac{\pi(x)}{x/\ln x} \geqslant \varliminf_{x \to \infty} \frac{\pi(x)}{x/\ln x} \geqslant 1.$$

On the other hand, choose a parameter $0 < a < 1$ and consider

$$S(x,a) = \sum_{x^a < p \leqslant x} \ln p, \quad x > 1.$$

Then $\psi(x) \geqslant S(x,a)$, but

$$S(x,a) \geqslant \sum_{x^a < p \leqslant x} \ln(x^a) = \ln(x^a) \sum_{x^a < p \leqslant x} 1 = a \ln x (\pi(x) - \pi(x^a)).$$

Therefore,

$$\frac{\psi(x)}{x} \geqslant a\frac{\pi(x)\ln x}{x} - a\frac{\pi(x^a)\ln x}{x}. \tag{2.2}$$

Note that the second summand in the right-hand side of (2.2) approaches zero as $x \to \infty$ since $\pi(x^a) \leqslant x^a$.

Assume (A1) holds and $B = \varliminf\limits_{x\to\infty} \psi(x)/x$. Then (2.2) implies that $B \geqslant a$ for every positive $a < 1$, i.e., $B \geqslant 1$. But we have already shown that (A1) implies $B \leqslant 1$. Thus, $B = 1$ and (A2) holds.

In a completely similar way, (A2) implies (A1).

(A2)⇒(A3) Suppose $\psi(x) = x + r(x)$, where $r = o(x)$. Then

$$\tilde{\psi}(x) = \int_1^x \frac{\psi(t)}{t}\,dt = x - 1 + \int_1^x \frac{r(t)}{t}\,dt = x + R(x) - 1,$$

where $R'(x) = r(x)/x$. It is enough to check that $R = o(x)$, which is indeed the case by the L'Hopital's Rule.

(A3)⇒(A2) Let $\tilde{\psi}(x) = x + R(x)$, $R = o(x)$. Fix a parameter ε, $0 < \varepsilon < 1$, and consider

$$I_\varepsilon^+(x) = \int_x^{x+\varepsilon x} \frac{\psi(t)}{t}\,dt = \tilde{\psi}(x+\varepsilon x) - \tilde{\psi}(x) = \varepsilon x + o(x).$$

Since ψ is an increasing function, the integral $I_\varepsilon^+(x)$ may be estimated from below as

$$I_\varepsilon^+(x) \geqslant \psi(x) \int_x^{x+\varepsilon x} \frac{dt}{t} = \psi(x)\ln(1+\varepsilon).$$

Similarly, the integral

$$I_\varepsilon^-(x) = \int_{x-\varepsilon x}^x \frac{\psi(t)}{t}\,dt = \tilde{\psi}(x) - \tilde{\psi}(x-\varepsilon x) = \varepsilon x + o(x)$$

may be estimated as

$$I_\varepsilon^-(x) \leqslant \int\limits_{x-\varepsilon x}^{x} \frac{dt}{t} = \psi(x) \ln \frac{1}{1-\varepsilon}.$$

Hence,

$$\frac{\psi(x)}{x} \leqslant \frac{I_\varepsilon^+(x)}{x \ln(1+\varepsilon)} = \frac{\varepsilon}{\ln(1+\varepsilon)} + o(1),$$
$$\frac{\psi(x)}{x} \geqslant \frac{I_\varepsilon^-(x)}{-x \ln(1-\varepsilon)} = \frac{\varepsilon}{-\ln(1-\varepsilon)} + o(1).$$

The upper and lower limits of $\psi(x)/x$ as $x \to \infty$ also satisfy these inequalities for all $\varepsilon \in (0,1)$. It remains evaluate the limit as $\varepsilon \to +0$ to obtain $\psi(x) \sim x$. □

Exercise 2.5. Prove the implication (A2)⇒(A1) in Theorem 2.4.

3. Von Mangoldt function. Yet another form of the Chebyshev function comes directly from the definition:

$$\psi(x) = \sum_{n \in \mathbb{N}, n \leqslant x} \Lambda(n), \tag{2.3}$$

where

$$\Lambda(n) = \begin{cases} \ln p, & n = p^m,\ p \in \mathbb{P},\ m \in \mathbb{N}, \\ 0, & \text{otherwise} \end{cases}$$

is called the *von Mangoldt function*.

It is also possible to express the integral Chebyshev function $\tilde{\psi}(x)$ via $\Lambda(n)$.

Proposition 2.6. *For every $x > 1$ we have*

$$\tilde{\psi}(x) = \sum_{n \in \mathbb{N}, n \leqslant x} \Lambda(n) \ln(x/n).$$

Proof. Denote by $\delta^+(y)$ the step function given by

$$\delta^+(y) = \begin{cases} 0, & y < 0, \\ 1, & y \geqslant 0. \end{cases}$$

Then

$$\tilde{\psi}(x) = \int_1^x \frac{\psi(t)}{t}\,dt = \int_1^x \frac{1}{t}\sum_{n\leqslant t}\Lambda(n)\,dt$$
$$= \int_1^x \frac{1}{t}\sum_{n\leqslant x}\Lambda(n)\delta^+(t-n)\,dt = \sum_{n\leqslant x}\Lambda(n)\int_1^x \frac{\delta^+(t-n)}{t}\,dt$$
$$= \sum_{n\leqslant x}\Lambda(n)\int_n^x \frac{dt}{t} = \sum_{n\leqslant x}\Lambda(n)\ln(x/n),$$

and the Proposition is proved. □

§ 2.2. Riemann function: Elementary properties

1. Riemann function in $\operatorname{Re} z > 1$**.** We have already seen that the asymptotic behaviors of the functions $\pi(x)$ and $\psi(x)$ are equivalent. The latter is asymptotically equivalent to the integral Chebyshev function $\tilde{\psi}(x)$. It follows from the relation (2.3) and from Proposition 2.6 that these functions are of the form

$$f(x) = \sum_{n\leqslant x} f_n,$$

where f_n are some real coefficients, and the summation is made over natural numbers.

One of the most fruitful ideas that lie in the foundation of the analytic number theory is to study a function $f(x)$ as above via the following complex-valued function called *Dirichlet series*:

$$\varphi(z) = \sum_{n=1}^{\infty} \frac{f_n}{n^z}.$$

The new variable z takes its values in an appropriate domain in $\mathbb{C}$.

If $f = \psi$ then $f_n = \Lambda(n)$, and the corresponding function φ turns to be closely related with *Riemann zeta-function* given by

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}, \quad \operatorname{Re} z > 1. \tag{2.4}$$

It is easy to see that the series (2.4) is absolutely converging for $\operatorname{Re} z > 1$. In the semiplane $\operatorname{Re} z \geqslant s$, $s > 1$, the series (2.4) converges uniformly with respect to z. Hence, (2.4) is uniformly converging on every compact subset

in $\operatorname{Re} z > 1$. By the well-known Weierstrass Theorem, the limit of a sequence of analytic functions which is uniformly converging on every compact subset in a given domain is again an analytic function. Therefore, (2.4) defines an analytic function in the semiplane $\operatorname{Re} z > 1$. Later we will see how to extend ζ analytically into the semiplane $\operatorname{Re} z > 0$.

2. Distribution of the Dirichlet series of a multiplicative function. Recall some notions from the elementary number theory. An arbitrary map $f : \mathbb{N} \to \mathbb{C}$ is called an *arithmetic function*. An arithmetic function is called *multiplicative* if $f(1) = 1$ and $f(nm) = f(n)f(m)$ provided that $n, m \in \mathbb{N}$ are relatively prime. The Fundamental Theorem of Arithmetic implies any multiplicative function f to be uniquely determined by its values $f(p^m)$, $p \in \mathbb{P}$, $m \in \mathbb{N}$.

Examples of multiplicative functions are given by:

- the function $I(n)$, $I(p^m) = 1$;
- the *identity function* $e(n)$, $e(p^m) = 0$ (while $e(1) = 1$);
- the *Möbius function* $\mu(n)$, $\mu(p) = -1$, $\mu(p^m) = 0$ for $m > 1$.

Lemma 2.7. *Let f be a multiplicative function and let $z \in \mathbb{C}$. Suppose the series $\sum\limits_{n=1}^{\infty} f(n)n^{-z}$ is absolutely converging. Then*

$$\sum_{n=1}^{\infty} f(n)n^{-z} = \prod_{p\in\mathbb{P}} \left(\sum_{d=0}^{\infty} f(p^d)p^{-dz} \right).$$

Proof. It is easy to see that for every $p \in \mathbb{P}$ the series $\sum\limits_{d=0}^{\infty} f(p^d)p^{-dz}$ contains a part of the initial series and thus converges absolutely. Enumerate prime numbers in the increasing order:

$$\mathbb{P} = \{p_n \mid n \in \mathbb{N}\}, \quad p_1 = 2, p_2 = 3, \ldots,$$

and consider the partial product

$$P_N = \prod_{n=1}^{N} \left(\sum_{d=0}^{\infty} f(p_n^d)p_n^{-dz} \right).$$

Since a product of absolutely converging series is distributive, we may distribute the brackets in the last expression to obtain

$$P_N = \sum_{d_1,\ldots,d_N=0}^{\infty} f(p_1^{d_1}) \ldots f(p_N^{d_N})p_1^{-d_1 z} \ldots p_N^{-d_N z} = \sum_{n\in M_N} f(n)n^{-z},$$

where $M_N \subset \mathbb{N}$ consists of all natural numbers of the form $p_1^{d_1} \dots p_N^{d_N}$, $d_i \geqslant 0$. The least natural number that is not in M_N is equal to p_{N+1}, hence,

$$\left| \sum_{n=1}^{\infty} f(n) n^{-z} - P_N \right| \leqslant \sum_{n=p_{N+1}}^{\infty} |f(n) n^{-z}| \to 0$$

as $N \to \infty$ (since $p_{N+1} \to \infty$). □

3. Convolution product and the Möbius inversion formula. Given two functions $f, g : \mathbb{N} \to \mathbb{C}$, their *convolution product* is an arithmetic function defined by

$$(f \circ g)(n) = \sum_{d|n} f(d) g(n/d), \quad n \in \mathbb{N}. \tag{2.5}$$

where the summation index d ranges over the set of all divisors of n.

Exercise 2.8. Prove that the convolution product is associative and commutative.

Exercise 2.9. For every arithmetic function f, show $f \circ e = e \circ f = f$. (This is the reason why e is called the identity function.)

The following statement shows a nice relation between Dirichlet series and the convolution product.

Lemma 2.10. *Let f and g be arithmetic functions such that their Dirichlet series*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^z}, \quad \sum_{n=1}^{\infty} \frac{g(n)}{n^z}$$

are absolutely converging for some $z \in \mathbb{C}$. Then

$$\left(\sum_{n=1}^{\infty} \frac{f(n)}{n^z} \right) \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^z} \right) = \sum_{n=1}^{\infty} \frac{(f \circ g)(n)}{n^z}. \tag{2.6}$$

Proof. Since the product of absolutely converging series is distributive, we may write

$$\left(\sum_{n=1}^{\infty} \frac{f(n)}{n^z} \right) \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^z} \right) = \sum_{n,m=1}^{\infty} \frac{f(n) g(m)}{n^z m^z}.$$

Introduce new indexes $d = n$, $N = nm$ and change the order of summation (it is possible due to absolute convergence of the product series):

$$\sum_{n,m=1}^{\infty} \frac{f(n)g(m)}{n^z m^z} = \sum_{N=1}^{\infty} \frac{1}{N^z} \sum_{d|N} f(d)g(N/d) = \sum_{N=1}^{\infty} \frac{1}{N^z} (f \circ g)(N).$$

Therefore, (2.6) is proved. □

Moreover, it is known that the set of all multiplicative functions forms a group with respect to the convolution product, i.e., if f and g are multiplicative functions then so is $f \circ g$, and for every multiplicative function f there exists a multiplicative function f^{-1} such that $f \circ f^{-1} = f^{-1} \circ f = e$.

Lemma 2.11 (Möbius inversion formula)**.** *If $f : \mathbb{N} \to \mathbb{C}$ is an arithmetic function and $f \circ I = g$ then $g \circ \mu = f$.*

Proof. Note that $I \circ \mu = e$. Indeed, if the canonical form of n is $q_1^{m_1} \dots q_r^{m_r}$, $q_1, \dots, q_r \in \mathbb{P}$, $r \geqslant 1$, then

$$(I \circ \mu)(n) = \sum_{d|n} \mu(d) = \mu(1) - \sum_{j} \mu(q_j) + \sum_{j_1<j_2} \mu(q_{j_1} q_{j_2} - \dots$$
$$= 1 - r + \binom{r}{2} - \binom{r}{3} + \dots + (-1)^r = (1-1)^r = 0$$

by the Newton binomial formula.

Therefore, $g \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ e = f$. □

Exercise 2.12. The *Euler function* φ is defined by

$$\varphi(n) = |\{m \in \mathbb{N} \mid m \leqslant n, \gcd(m,n) = 1\}|, \quad n \in \mathbb{N}.$$

Prove that $\varphi \circ I = E$, where $E(n) = n$ for all $n \in \mathbb{N}$. Deduce the explicit formula for $\varphi(n)$.

4. Euler identity.

Theorem 2.13. *If $\operatorname{Re} z > 1$ then*

$$\zeta(z) = \prod_{p \in \mathbb{P}} (1 - p^{-z})^{-1} \quad \textit{(the Euler identity)}, \tag{2.7}$$

$$\frac{1}{\zeta(z)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^z}, \tag{2.8}$$

where $\mu(n)$ is the Möbius function. In particular, ζ has no zeros in the semiplane $\operatorname{Re} z > 1$.

PROOF. Apply Lemma 2.7 for $f = I$ to obtain

$$\zeta(z) = \prod_{p\in\mathbb{P}}(1 + p^{-z} + p^{-2z} + \dots) = \prod_{p\in\mathbb{P}}(1 - p^{-z})^{-1},$$

when $\operatorname{Re} z > 1$. This proves (2.7).

To prove (2.8), apply Lemma 2.7 to $f = \mu$. It is possible to do so since $|\mu(n)| \leqslant 1$ and thus the series $\sum\limits_{n=1}^{\infty} \mu(n)n^{-z}$ is absolutely converging for $\operatorname{Re} z > 1$. Hence,

$$\sum_{n=1}^{\infty} \mu(n)n^{-z} = \prod_{p\in\mathbb{P}} \left(\sum_{d=0}^{\infty} \mu(p^d)p^{-dz} \right) = \prod_{p\in\mathbb{P}}(1 - p^{-z}).$$

Thus (2.7) implies (2.8). □

5. Logarithmic derivative of the Riemann function.

Lemma 2.14. *For all $n \in \mathbb{N}$ we have $(\Lambda \circ I)(n) = \ln n$.*

PROOF. For $n = 1$ the statement is obvious. If $n > 1$ then consider the canonical distribution of n, $n = q_1^{a_1} \dots q_r^{a_r}$. By the definitions of the convolution product and of the von Mangoldt function, we have

$$(\Lambda \circ I)(n) = 0 + \sum_{j=1}^{r} \sum_{a=1}^{a_j} \Lambda(q_j^a) \cdot 1 = \sum_{j=1}^{r} a_j \ln q_j.$$

On the other hand, $\ln n = \ln(q_1^{a_1} \dots q_r^{a_r}) = a_1 \ln q_1 + \dots + a_r \ln q_r$. □

Theorem 2.15. *In the semiplane $\operatorname{Re} z > 1$, the following identity holds:*

$$\frac{\zeta'(z)}{\zeta(z)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^z}. \tag{2.9}$$

PROOF. As we have already noted, (2.4) converges uniformly with respect to z in the domain $\operatorname{Re} z \geqslant s$ for every $s > 1$. Hence (as we know from complex analysis) the series (2.4) allows term-by-term derivation at every point of the semiplane $\operatorname{Re} z > 1$:

$$\zeta'(z) = -\sum_{n=1}^{\infty} \frac{\ln n}{n^z}.$$

Multiply the expression obtained by (2.8) for $1/\zeta(z)$:

$$\frac{\zeta'(z)}{\zeta(z)} = -\left(\sum_{n=1}^{\infty} \frac{\ln n}{n^z} \right) \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^z} \right).$$

Since both series in the right-hand side are absolutely converging, we may distribute the brackets and collect similar terms with n^z to obtain

$$\frac{\zeta'(z)}{\zeta(z)} = \sum_{d_1,d_2=1}^{\infty} \frac{\mu(d_2)\ln d_1}{(d_1 d_2)^z} = \sum_{n=1}^{\infty} \left(\sum_{d|n} \mu(d)\ln(n/d) \right) \frac{1}{n^z} = \sum_{n=1}^{\infty} \frac{(\ln\circ\mu)(n)}{n^z}. \quad (2.10)$$

By Lemma 2.14, $(\Lambda \circ I)(n) = \ln n$. Lemma 2.11 implies $\ln\circ\mu = \Lambda$, and it remains to apply (2.10) to complete the proof. □

6. Expression of the integral Chebyshev function via the Riemann function. Denote by L_a ($a \in \mathbb{R}$) the vertical line $\{z \mid \operatorname{Re} z = a\}$ in the complex plane, and consider L_a as a path of integration in the upward direction, i.e., from $a - i\infty$ to $a + i\infty$.

Theorem 2.16. *For every $a > 1$ the following identity holds:*

$$\tilde{\psi}(x) = \frac{1}{2\pi\iota} \int_{L_a} \left(-\frac{\zeta'(z)}{\zeta(z)} \right) \frac{x^z}{z^2}\, dz \quad \text{for} \quad x \geqslant 1. \quad (2.11)$$

Proof. Let $\mathcal{I}_a(x)$ stand for the improper integral in the right-hand side of (2.11).

It follows from (2.9) that

$$\left| -\frac{\zeta'(z)}{\zeta(z)} \frac{x^z}{z^2} \right| \leqslant C \frac{1}{|z|^2},$$

for $z \in L_a$ ($\operatorname{Re} z = a > 1$), where C is a constant which does not depend on z.

Since the integral

$$\left| \int_{L_a} \frac{dz}{z^2} \right| \leqslant \int_{-\infty}^{\infty} \frac{dy}{a^2 + y^2}$$

converges, $\mathcal{I}_a(x)$ is absolutely converging. Therefore, it can be adequately evaluated via the Cauchy principal value. By (2.9),

$$\mathcal{I}_a(x) = \lim_{B\to\infty} \int_{L_a^B} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^z} \frac{x^z}{z^2}\, dz, \quad (2.12)$$

where $L_a^B = \{z \mid \operatorname{Re} z = a, -B \leqslant \operatorname{Im} z \leqslant B\}$. In this expression, the integrand series is uniformly converging with respect to $z \in L_a$ since

$$\left|\frac{\Lambda(n)}{n^z}\frac{x^z}{z^2}\right| \leqslant \frac{x^a}{a^2}\frac{\ln n}{n^a}$$

for every $z \in L_a$ (recall that the series $\sum\limits_{n=1}^{\infty} \ln n/n^a$ converges for $a > 1$). Hence, the integral in the right-hand side of (2.12) can be evaluated in the termwise way:

$$\mathcal{I}_a(x) = \lim_{B\to\infty} \sum_{n=1}^{\infty} \int\limits_{L_a^B} \frac{\Lambda(n)}{n^z}\frac{x^z}{z^2}\,dz. \tag{2.13}$$

On the other hand, $z = a + \imath y$, and thus partial integrals over the segments L_a^B may be estimated as follows:

$$\left|\int\limits_{L_a^B} \frac{\Lambda(n)}{n^z}\frac{x^z}{z^2}\,dz\right| \leqslant \int\limits_{-\infty}^{\infty} \Lambda(n)\left(\frac{x}{n}\right)^a \frac{1}{a^2+y^2}\,dy \leqslant Cx^a\frac{\Lambda(n)}{n^a},$$

where C is a constant not depending on n and B. Since $\Lambda(n) \leqslant \ln n$, the series in the right-hand side of (2.13) converges uniformly with respect to B, hence, the limit as $B \to \infty$ may be evaluated in the termwise way:

$$\mathcal{I}_a(x) = \sum_{n=1}^{\infty} \Lambda(n) \int\limits_{L_a} (x/n)^z \frac{1}{z^2}\,dz. \tag{2.14}$$

The integrand $g_{n,x}(z) = (x/n)^z\dfrac{1}{z^2}$ has the only singular point at $z = 0$. The Laurent series for $g_{n,x}(z)$ at $z = 0$ has the form

$$\begin{aligned}(x/n)^z\frac{1}{z^2} &= \left(1 + \sum_{k=1}^{\infty}\frac{1}{k!}\ln^k(x/n)z^k\right)z^{-2}\\ &= z^{-2} + \ln(x/n)z^{-1} + \frac{1}{2!}\ln^2(x/n) + \ldots,\end{aligned}$$

and thus the residue at $z = 0$ (the coefficient at z^{-1}) is equal to $\ln(x/n)$.

Let us now evaluate the integrals in the right-hand side of (2.14) by means of the Cauchy integral theorem.

Case 1: $x \geqslant n$, $x/n \geqslant 1$. Consider the circle in the complex plane of radius $R = \sqrt{B^2 + a^2}$ centered at the origin and denote by C_a^B the arc of this that lies leftward to the line $\operatorname{Re} z = a$. Being combined with an appropriate

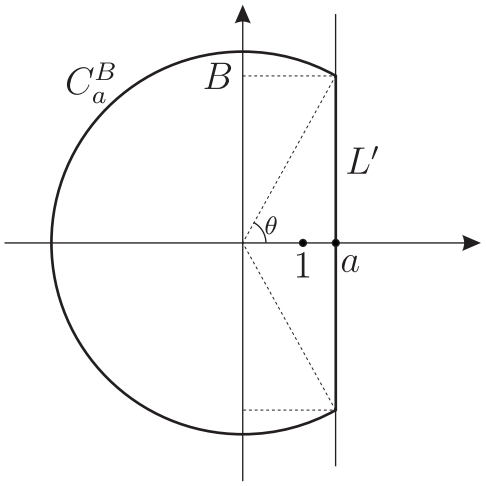

FIGURE 1. Integration path in Case 1

segment $L' = L_a^B$, this arc forms a closed integration path which includes the origin for sufficiently large B (see Fig. 1). Then

$$\left| \int\limits_{C_a^B} (x/n)^z \frac{1}{z^2}\, dz \right| \leqslant \left| \int\limits_{\theta}^{2\pi-\theta} (x/n)^z \frac{1}{R^2 e^{2\iota\varphi}} \iota R e^{\iota\varphi}\, d\varphi \right|$$

$$\leqslant (x/n)^a \int\limits_0^{2\pi} \frac{1}{R}\, d\varphi = O(1/R) = O(1/B).$$

By the Cauchy integral theorem,

$$\frac{1}{2\pi\iota} \left(\int\limits_{L_a^B} (x/n)^z \frac{1}{z^2}\, dz + \int\limits_{C_a^B} (x/n)^z \frac{1}{z^2}\, dz \right) = \ln(x/n).$$

The second summand in the left-hand side approaches zero as $B \to \infty$, and the limit of the first summand is the desired integral over L_a.

CASE 2: $x < n$, $x/n < 1$. Consider the integration path shown in Fig. 2: It consists of the segment L_a^B (as in the previous case) and of the arc $|z| = R = \sqrt{B^2 + a^2}$ which is located to the right of L_a. This is a closed

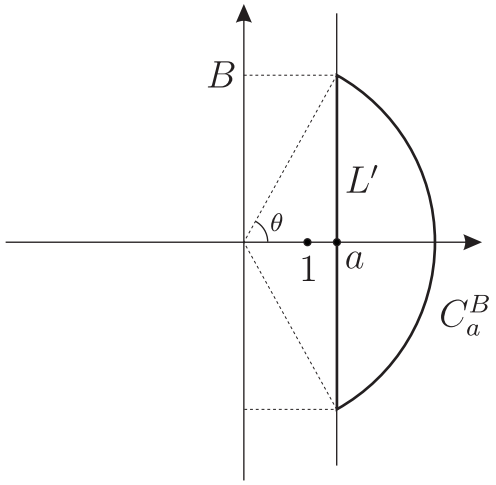

FIGURE 2. Integration path in Case 2

path which contains no singularities of the integrand $(x/n)^z \frac{1}{z^2}$. By the same reasons as those used in Case 1, the integral in the right-hand side of (2.14) is equal to zero for $x < n$.

Summarizing Case 1 and Case 2, conclude that

$$\frac{1}{2\pi\iota}\int\limits_{L_a}(x/n)^z\frac{1}{z^2}\,dz=\begin{cases}\ln(x/n), & n\leqslant x,\\ 0, & n>x.\end{cases}$$

Plug in these expressions into (2.14) to obtain

$$\frac{1}{2\pi\iota}\int\limits_{L_a}\left(-\frac{\zeta'(z)}{\zeta(z)}\right)\frac{x^z}{z^2}\,dz=\sum_{n\leqslant x}\Lambda(n)\ln(x/n).$$

By Proposition 2.6, the last expression is equal to $\tilde{\psi}(x)$. □

§ 2.3. Riemann function: Analytic properties

1. Analytic extension of the Riemann function. Let us first state a general observation that will be useful later. Suppose $f(u,z)$ is a function depending on a real variable $u \in [a,b]$ and on a complex variable $z \in D$, where $[a,b]$ is an interval and D is a domain in $\mathbb{C}$. Assume that for every

$u \in [a,b]$ the function $f(u,z)$ is analytic in $z \in D$. In addition, suppose that for every $\varepsilon > 0$ there exists $\delta > 0$ such that

$$|\Delta u| < \delta, u + \Delta u \in [a,b] \Rightarrow |f(u+\Delta u, z) - f(u,z)| < \varepsilon \tag{2.15}$$

for all $z \in D$, $u \in [a,b]$. Then

$$F(z) = \int_a^b f(u,z)\,du$$

is an analytic function in $z \in D$ such that

$$F'(z) = \int_a^b \frac{\partial f(u,z)}{\partial z}\,du.$$

Indeed, the integral over $[a,b]$ is a limit of a sequence of Riemann sums

$$\Sigma_N = \sum_{j=1}^{N} f(u_j, z)\Delta u, \quad \Delta u = |b-a|/N.$$

Each of Σ_N is an analytic function in $z \in D$. Condition (2.15) guarantees uniform convergence (with respect to $z \in D$)

$$\Sigma_N \underset{N\to\infty}{\to} F(z) = \int_a^b f(u,z)\,du.$$

The Weierstrass theorem implies $F(z)$ to be an analytic function such that the derivative of $F(z)$ is the limit of Σ'_N with respect to z. Every Σ'_N is equal to a Riemann sum for the function $\partial f/\partial z$, and thus

$$\lim_{N\to\infty} S'_N = \int_a^b \frac{\partial f(u,z)}{\partial z}\,du.$$

The following important statement says that the Riemann function defined by (2.4) in the semiplane $\operatorname{Re} z > 1$ may be analytically extended into a wider region in which the series (2.4) is diverging.

Theorem 2.17. *There exists a function $\tilde\zeta(z)$ defined in the semiplane $\operatorname{Re} z > 0$, $z \neq 1$, such that $\tilde\zeta(z) = \zeta(z)$ for $\operatorname{Re} z > 1$. Moreover, $\tilde\zeta(z)$ is analytic at all points of $\operatorname{Re} z > 0$ except for a simple pole at $z = 1$, in which $\operatorname{Res}_{z=1}\tilde\zeta(z) = 1$.*

PROOF. Denote $\rho(u) = 1/2 - \{u\}$, $u > 0$, where $\{u\} = u - [u]$ is the fractional part of a real number u, $[u]$ is the largest integer not greater than u.

Let us fix two natural numbers $N < M$ and consider the following expression:

$$I(N,M,z) := \int\limits_{N+1/2}^{M+1/2} \frac{1}{u^z} + z\frac{\rho(u)}{u^{z+1}}\,du = \int\limits_{N+1/2}^{M+1/2} \frac{1}{u^z} + z\frac{1/2 - u + [u]}{u^{z+1}}\,du$$

$$= \int\limits_{N+1/2}^{M+1/2} \frac{1-z}{u^z}\,du + \frac{1}{2}\int\limits_{N+1/2}^{M+1/2} \frac{z}{u^{z+1}}\,du + \int\limits_{N+1/2}^{M+1/2} \frac{z[u]}{u^{z+1}}\,du$$

$$= \frac{1}{u^{z-1}}\Big|_{N+1/2}^{M+1/2} - \frac{1}{2}\frac{1}{u^z}\Big|_{N+1/2}^{M+1/2} + \int\limits_{N+1/2}^{N+1} \frac{z[u]}{u^{z+1}}\,du$$

$$+ \sum_{k=N+1}^{M-1} \int\limits_{k}^{k+1} \frac{z[u]}{u^{z+1}}\,du + \int\limits_{M}^{M+1/2} \frac{z[u]}{u^{z+1}}\,du$$

$$= \frac{1}{(M+1/2)^{z-1}} - \frac{1}{(N+1/2)^{z-1}} - \frac{1/2}{(M+1/2)^z} + \frac{1/2}{(N+1/2)^z}$$

$$-\frac{N}{(N+1)^z} + \frac{N}{(N+1/2)^z} + \sum_{k=N+1}^{M-1}\left(-\frac{k}{(k+1)^z} + \frac{k}{k^z}\right) - \frac{M}{(M+1/2)^z} + \frac{M}{M^z}.$$

Reduce similar terms to obtain

$$I(N,M,z) = -\frac{N}{(N+1)^z} + \sum_{k=N+1}^{M-1}\left(-\frac{k}{(k+1)^z} + \frac{1}{k^{z-1}}\right) + \frac{1}{M^{z-1}}$$

$$= -\frac{N+1-1}{(N+1)^z} + \sum_{k=N+1}^{M-1}\left(-\frac{k+1-1}{(k+1)^z} + \frac{1}{k^{z-1}}\right) + \frac{1}{M^{z-1}}$$

$$= -\frac{1}{(N+1)^{z-1}} + \frac{1}{(N+1)^z} + \sum_{k=N+1}^{M-1}\left(\frac{1}{k^{z-1}} - \frac{1}{(k+1)^{z-1}}\right)$$

$$+ \sum_{k=N+1}^{M-1} \frac{1}{(k+1)^z} + \frac{1}{M^{z-1}}.$$

Finally,

$$I(N,M,z)=\sum_{k=N+1}^{M}\frac{1}{k^z}$$

Hence, if $\operatorname{Re} z>1$ then

$$\zeta(z)=\sum_{n=1}^{N}\frac{1}{n^z}+\lim_{M\to\infty}I(N,M,z).$$

On the other hand, for $\operatorname{Re} z>1$

$$\lim_{M\to\infty}I(N,M,z)=\frac{(N+1/2)^{-z+1}}{z-1}+z\int\limits_{N+1/2}^{\infty}\frac{\rho(u)}{u^{z+1}}\,du.$$

Therefore,

$$\zeta(z)=\sum_{n=1}^{N}\frac{1}{n^z}+\frac{(N+1/2)^{-z+1}}{z-1}+z\int\limits_{N+1/2}^{\infty}\frac{\rho(u)}{u^{z+1}}\,du,\quad \operatorname{Re} z>1,\qquad (2.16)$$

for every natural N.

In (2.16), the first summand is an analytic function in the entire $\mathbb{C}$, the second one has a unique simple pole $z=1$ (in which the residue is equal to 1), and it remains to analyze the third summand.

The integral in the last summand of the right-hand side of (2.16) may be considered as a series:

$$\int\limits_{N+1/2}^{\infty}\frac{\rho(u)}{u^{z+1}}\,du=\int\limits_{N+1/2}^{N+1}\frac{\rho(u)}{u^{z+1}}\,du+\int\limits_{N+1}^{N+2}\frac{\rho(u)}{u^{z+1}}\,du+\dots.$$

On every interval of integration ($[N+1/2,N+1)$, $[N+1,N+2)$, and so on), $\rho(u)/u^{z+1}$ is a continuous function. Moreover, for every $s>0$, the last series converges uniformly with respect to z in $\operatorname{Re} z\geqslant s$, and the integrand satisfies the condition (2.15). Hence, the third summand in the right-hand side of (2.16) is an analytic function in $\operatorname{Re} z>0$ and

$$\frac{d}{dz}\int\limits_{N+1/2}^{\infty}\frac{\rho(u)}{u^{z+1}}du=\int\limits_{N+1/2}^{\infty}\frac{d}{dz}\frac{\rho(u)}{u^{z+1}}du.$$

Thus, the right-hand side of (2.16) is the desired function $\tilde\zeta(z)$. □

In what follows, we will identify ζ and $\tilde\zeta$.

2. Zeros of the Riemann function.

Lemma 2.18. *For every $s > 1$ and for every $t \in \mathbb{R}$ we have*

$$|\zeta^3(s)\zeta^4(s+\imath t)\zeta(s+2\imath t)| \geqslant 1. \tag{2.17}$$

Proof. Denote $A = |\zeta^3(s)\zeta^4(s+\imath t)\zeta(s+2\imath t)|$. The Euler identity (2.7) implies

$$A = \prod_{p\in\mathbb{P}} \left(|1-p^{-s}|^3|1-p^{-s-\imath t}|^4|1-p^{-s-2\imath t}|\right)^{-1}.$$

Let us evaluate the natural log of the both sides of the last expression using the well-known relation $\ln|w| = \operatorname{Re}\ln w$, $w \in \mathbb{C}\setminus\{0\}$. Then

$$\ln A = -\operatorname{Re}\sum_{p\in\P} \left(3\ln(1-p^{-s}) + 4\ln(1-p^{-s-\imath t}) + \ln(1-p^{-s-2\imath t})\right).$$

Recall that the Taylor series for $\ln(1-z)$ in a neighborhood of $z = 0$ is given by

$$\ln(1-z) = -z - \frac{z^2}{2} - \frac{z^3}{3} - \dots.$$

This series is absolutely converging when $|z| < 1$. Apply this distribution for $z = p^{-s}$, $z = p^{-s-\imath t}$, and $z = p^{-s-2\imath t}$:

$$\begin{aligned}
\ln A &= \sum_{p\in\mathbb{P}} \operatorname{Re}\sum_{n=1}^{\infty}\left(3\frac{p^{-ns}}{n} + 4\frac{p^{-n(s+\imath t)}}{n} + \frac{p^{-n(s+2\imath t)}}{n}\right)\\
&= \sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty}\frac{p^{-ns}}{n}\left(3 + 4\operatorname{Re}p^{-\imath nt} + \operatorname{Re}p^{-2\imath nt}\right)\\
&= \sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty}\frac{p^{-ns}}{n}\left(3 + 4\cos(nt\ln p) + \cos(2nt\ln p)\right). \qquad (2.18)
\end{aligned}$$

Note that

$$3 + 4\cos\theta + \cos(2\theta) = 2(1+\cos\theta)^2 \geqslant 0,$$

and thus all summands in the right-hand side of (2.18) are non-negative. Hence, $\ln A \geqslant 0$, i.e., $A \geqslant 1$. □

Theorem 2.19. *Riemann function $\zeta(z)$ has no zeros in the line* $\operatorname{Re} z = 1$.

PROOF. Let us estimate $\zeta(s)$ in a neighborhood of the pole $z = 1$, namely, in the interval $1 < s < 2$. It is easy to see that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leqslant 1 + \int_1^{\infty} \frac{1}{x^s}\, dx = 1 + \frac{1}{s-1} \leqslant \frac{2}{s-1}$$

(since a right Riemann sum for a decreasing function is no greater that its integral).

Assume $\zeta(1 + \imath t) = 0$ for some $t \neq 0$. Since ζ is analytic at $1 + \imath t$, its derivative is bounded in a neighborhood of this point. In particular,

$$\left| \frac{\zeta(s + \imath t) - \zeta(1 + \imath t)}{s - 1} \right| \leqslant C, \quad 1 < s < 2.$$

Hence, $|\zeta(s + \imath t)| \leqslant C|s - 1|$.

Moreover, since $\zeta(z)$ is analytic, it is in particular continuous on the interval $z = s + 2\imath t$, $1 \leqslant s \leqslant 2$, and thus there exists a constant M, such that $|\zeta(s + 2\imath t)| \leqslant M$ for $1 < s < 2$.

Therefore, we have obtained the following estimates of the factors in (2.17) for $1 < s < 2$:

$$|\zeta(s + \imath t)| \leqslant C|s - 1|,$$
$$|\zeta(s)| \leqslant \frac{2}{s-1},$$
$$|\zeta(s + 2\imath t)| \leqslant M.$$

Then

$$A := |\zeta(s)^3 \zeta(s + \imath t)^4 \zeta(s + 2\imath t)| \leqslant C_1|s - 1| \to 0 \quad \text{as} \quad s \to 1 + 0,$$

where C_1 is a constant, but Lemma 2.18 implies $A \geqslant 1$ for all $s > 1$. The contradiction obtained proves the theorem. □

3. Estimates of the logarithmic derivative. To prove the asymptotic law of distribution of prime numbers, we need an upper estimate of the logarithmic derivative of Riemann function far off the pole $z = 1$. Let us start with estimates of $\zeta(z)$ itself and its derivative. We have already seen that $|\zeta(s)| \leqslant 2/(s - 1)$ for $1 < s < 2$.

Proposition 2.20. *There exist constants $C_1, C_2 > 0$ such that*

(1) $|\zeta(s + \imath t)| \leqslant C_1 \ln |t|$,
(2) $|\zeta'(s + \imath t)| \leqslant C_2 \ln^2 |t|$

for $1 \leqslant s \leqslant 2$, $|t| \geqslant 3$.

PROOF. (1) The explicit expression for $\zeta(s+\iota t)$ is given by Theorem 2.17:

$$\zeta(s+\iota t)=\sum_{k=1}^{N}\frac{1}{k^{s+\iota t}}+\frac{(N+1/2)^{1-s-\iota t}}{s-1+\iota t}+\int\limits_{N+1/2}^{\infty}\frac{(s+\iota t)\rho(u)}{u^{s+1+\iota t}}\,du. \quad (2.19)$$

Suppose $N=[|t|]$, and estimate the absolute values of all summands.

First,

$$\left|\sum_{k=1}^{N}\frac{1}{k^{s+\iota t}}\right|\leqslant\sum_{k=1}^{N}\frac{1}{k}\leqslant 1+\int\limits_{1}^{N}\frac{dx}{x}=1+\ln N\leqslant 1+\ln|t|.$$

Next,

$$\left|\frac{(N+1/2)^{1-s-\iota t}}{s-1+\iota t}\right|\leqslant\frac{1}{3},$$

since $s\geqslant 1$ and $|s+\iota t-1|\geqslant 3$.

Finally,

$$\left|\int\limits_{N+1/2}^{\infty}\frac{(s+\iota t)\rho(u)}{u^{s+1+\iota t}}\,du\right|\leqslant(s+|t|)\int\limits_{|t|-1}^{\infty}\frac{du}{u^{s+1}}=\frac{s+|t|}{s(|t|-1)^{s}}\leqslant\frac{2+|t|}{|t|-1}\leqslant C$$

since $N+1/2\geqslant|t|-1$, $|s+\iota t|\leqslant s+|t|$, and $s\leqslant 2$.

Therefore, the absolute value of the right-hand side of (2.19) does not exceed $B+\ln|t|$ for some constant B (B does not depend on s and t). But $B+\ln|t|<(B+1)\ln|t|$ since $\ln|t|>1$ for $|t|\geqslant 3$.

(2) The derivative of (2.19) may be evaluated in the termwise way since the improper integral in the third summand is uniformly converging. Thus,

$$\zeta'(z)=-\sum_{k=1}^{N}\frac{\ln k}{k^{z}}+\frac{d}{dz}\frac{(N+1/2)^{1-z}}{z-1}+\frac{d}{dz}\int\limits_{N+1/2}^{\infty}\frac{z\rho(u)}{u^{z+1}}\,du.$$

As above, let $z=s+\iota t$, $N=[|t|]$. The second and third summands in the right-hand side of the last expression are bounded (as it was shown in the proof of (1)). To estimate the first summand, consider the integral over $[3,\infty)$ of the function $\dfrac{\ln x}{x}$, which is decreasing on $x\geqslant 3$:

$$\sum_{k=1}^{N}\frac{\ln k}{k^{s}}\leqslant\frac{\ln 2}{2}+\sum_{k=3}^{N}\frac{\ln k}{k}\leqslant C\ln^{2}N.$$

Hence, there exists a constant $C_2 > 0$ such that (2) holds. □

Proposition 2.21. *There exist constants $T_0 \geqslant 3$, $C_3, C_4 > 0$ such that*

(1) $|\zeta(s+\iota t)| \geqslant C_3 \ln^{-31/4}|t| > C_3 \ln^{-8}|t|$,

(2) $\left|\dfrac{\zeta'(s+\iota t)}{\zeta(s+\iota t)}\right| \leqslant C_4 \ln^{10}|t|$

for $1 \leqslant s \leqslant 2$, $|t| \geqslant T_0$.

Proof. (1) Recall the inequality deduced in the proof of Theorem 2.19:

$$|\zeta(s)^3\zeta(s+\iota t)^4\zeta(s+2\iota t)| \geqslant 1.$$

It holds for $s > 1$ and for all real t, in particular, for $|t| \geqslant 3$. Moreover, $\zeta(s) \leqslant 2/(s-1)$ when $1 < s \leqslant 2$.

By Proposition 2.20(1), $|\zeta(s+2\iota t)| \leqslant C_1 \ln(2|t|) \leqslant 2C_1 \ln|t|$ for $s \geqslant 1$, $|t| \geqslant 3$. Hence,

$$|\zeta(s+\iota t)| \geqslant |\zeta(s)|^{-3/4}|\zeta(s+2\iota t)|^{-1/4} \geqslant C\left(\frac{2}{s-1}\right)^{-3/4} \ln^{-1/4}|t|$$

for $1 < s \leqslant 2$, $|t| \geqslant 3$, where C is a constant which does not depend on s and t. Let us fix t, $|t| \geqslant 3$, and consider the interval $1+\delta \leqslant s \leqslant 2$, where

$$\delta = \frac{2}{\ln^{10}|t|}$$

In this interval,

$$|\zeta(s+\iota t)| \geqslant C \ln^{-31/4}|t|.$$

It remains to estimate from below the quantity $|\zeta(s+\iota t)|$ in the interval $1 \leqslant s \leqslant 1+\delta$. Proposition 2.20(2) allows to estimate an increment of $\zeta(z)$ in this interval:

$$|\zeta(1+\delta+\iota t) - \zeta(s+\iota t)| = \left|\int_s^{1+\delta} \zeta'(z)\,dz\right| \leqslant \delta \max_{\operatorname{Im} z = t,\, s \leqslant \operatorname{Re} z \leqslant 1+\delta} |\zeta'(z)|$$
$$\leqslant 2\ln^{-10}|t| C_2 \ln^2|t| = 2C_2 \ln^{-8}|t|.$$

Therefore,

$$|\zeta(s+\iota t)| \geqslant |\zeta(1+\delta+\iota t)| - 2C_2 \ln^{-8}|t| \geqslant C \ln^{-31/4}|t| - 2C_2 \ln^{-8}|t|.$$

Since $-31/4 < -8$, for any constants C and C_2 the second summand in the right-hand side becomes negligible for sufficiently large $|t|$. Hence, there exists $T_0 \geqslant 3$ such that

$$|\zeta(s+\iota t)| \geqslant (C/2) \ln^{-31/4}|t|,$$

for $|t| \geqslant T_0$.

(2) This estimate immediately follows from (1) and Proposition 2.20(2). □

4. Proof of the Prime Number Theorem. Now we are ready to complete the proof of the main statement of this chapter.

Theorem 2.22. *The function $\pi(x)$ is asymptotically equivalent to $x/\ln x$.*

Proof. By Theorem 2.4, it is enough to show that $\lim\limits_{x\to\infty} \dfrac{\tilde{\psi}(x)}{x} = 1$.

Theorem 2.16 implies

$$\frac{\tilde{\psi}(x)}{x} = \frac{1}{2\pi\iota} \int\limits_{L_a} \left(-\frac{\zeta'(z)}{\zeta(z)}\right) \frac{x^{z-1}}{z^2}\, dz$$

for every $x > 1$, $a > 1$. Here L_a stands for the line $\operatorname{Re} z = a$, integration is made from $a - \iota\infty$ to $a + \iota\infty$.

Choose real numbers $U > T > T_0$, where T_0 is the constant from Proposition 2.21.

Since $z = 1$ is a simple pole, there exists a neighborhood U_δ (a circle $|z - 1| < \delta$) in which $|\zeta(z)| > 0$.

Note that the region

$$W = \{z \in \mathbb{C} \mid 1/2 \leqslant \operatorname{Re} z \leqslant 1,\ |\operatorname{Im} z| \leqslant T,\ |z - 1| \geqslant \delta\} \subset \mathbb{C}$$

may contain only a finite number of zeros of the Riemann function. Otherwise, if there are infinitely many zeros in a closed bounded region W, the set of zeros has a condensation point in the same region W. Then the well-known uniqueness theorem of an analytic function implies ζ to be zero on W, which is not the case.

Therefore, for every $T > 0$ there exists $\eta > 0$ such that

$$S(T, \eta) = \{z \in \mathbb{C} \mid 1 - \eta \leqslant \operatorname{Re} z \leqslant 1,\ |\operatorname{Im} z| \leqslant T\}$$

contains no zeros of the Riemann function.

Consider the integration path Γ shown at Fig. 3. It depends on three parameters a, U, and T, where $1 < a < 2$, $U > T > T_0$, and on the quantity $\eta > 0$ which is chosen in such a way that the interior of Γ (and Γ itself) does not contain zeros of the Riemann function.

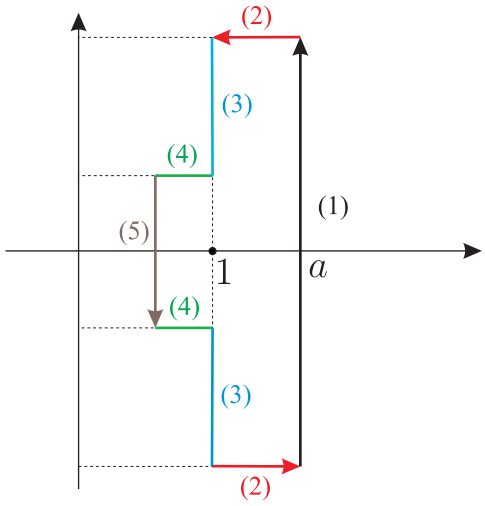

FIGURE 3. Integration path Γ

Consider the integral

$$I = \frac{1}{2\pi\iota} \int\limits_{\Gamma} \left(-\frac{\zeta'(z)}{\zeta(z)} \right) \frac{x^{z-1}}{z^2}\, dz$$

The only singularity of the integrand inside the closed path Γ is at the point $z = 1$, and

$$\operatorname{Res}_{z=1} \left(-\frac{\zeta'(z)}{\zeta(z)} \right) \frac{x^{z-1}}{z^2} = 1. \tag{2.20}$$

By the Cauchy integral theorem, $I = 1$ for all a, U, T.

Let us now present the integral I as a sum of five integrals over straight segments (1)–(5) of the path Γ (see Fig. 3):

$$I = I_1 + I_2 + I_3 + I_4 + I_5 \tag{2.21}$$

(for $k = 2, 3, 4$, I_k contains integrals over both segments (k)). Let us consider these segments separately.

SEGMENT 1. As we have already mentioned,

$$\lim_{U\to\infty} I_1 = \frac{\tilde{\psi}(x)}{x}.$$

SEGMENT 2. By Proposition 2.21(2),

$$|I_2| \leqslant 2\frac{1}{2\pi}\int\limits_1^a C_4 \ln^{10} U \frac{x^{a-1}}{s^2+U^2}\,ds$$

Hence, $|I_2| = O(\ln^{10} U/U^2)$, i.e.,

$$\lim_{U\to\infty} I_2 = 0.$$

SEGMENT 3. By Proposition 2.21(2),

$$|I_3| \leqslant 2\frac{1}{2\pi}\int\limits_T^U \frac{C_4 \ln^{10} t}{1+t^2}\,dt \leqslant C\int\limits_T^\infty \frac{dt}{t^{3/2}} = 2C\frac{1}{T^{1/2}}$$

(since $\ln^{10} t/t^{1/2}$ is a bounded function). Note that the constant C does not depend on x.

SEGMENT 4. Segments (4) and (5) form a compact set, on which $\zeta(z)$ is a nonzero analytic function. Hence, its logarithmic derivative is continuous on these segments. By the Weierstrass theorem on a continuous function, there exists a constant $M = M(T,\eta)$ such that

$$\left|\frac{\zeta'(z)}{\zeta(z)}\right| \leqslant M(T,\eta).$$

Then

$$|I_4| \leqslant 2\frac{1}{2\pi}\int\limits_{1-\eta}^1 M(T,\eta)\frac{x^{s-1}}{s^2+T^2}\,ds \leqslant \frac{M(T,\eta)}{\pi T^2}\int\limits_{1-\eta}^1 x^{s-1}\,ds \leqslant \frac{\bar{C}}{\ln x}.$$

The constant $\bar{C}$ in this expression depends on T and η, since it is proportional to $M(T,\eta)$.

SEGMENT 5. By the same reasons as for the previous segment,

$$|I_5| \leqslant \tilde{C}x^{-\eta},$$

where $\tilde{C}$ depends on T and η.

Now, evaluate the limit of (2.21) as $U \to \infty$:

$$I = 1 = \frac{\tilde{\psi}(x)}{x} + 0 + J_3 + J_4 + J_5,$$

where $J_k = \lim\limits_{U\to\infty} I_k$. As it was shown above,

$$|J_3| \leqslant 2C\frac{1}{T^{1/2}},$$
$$|J_4| \leqslant \frac{\bar{C}(T,\eta)}{\ln x},$$
$$|J_5| \leqslant \tilde{C}(T,\eta)x^{-\eta}.$$

Hence, for every small $\varepsilon > 0$ one may choose T such that $|J_3| \leqslant \varepsilon/2$. For a given T, the quantities $\bar{C}$ and $\tilde{C}$ are fixed, so

$$|J_4| + |J_5| \leqslant \varepsilon/2$$

for a sufficiently large x.

Finally,

$$\left|1 - \frac{\tilde{\psi}(x)}{x}\right| \leqslant |J_3| + |J_4| + |J_5| < \varepsilon$$

for a sufficiently large x. □

Corollary 2.23 (Asymptotic formula for nth prime)**.** *Let p_n, $n = 1, 2, 3, \ldots$, stand for the nth prime number ($p_1 = 2$, $p_2 = 3$ and so on). Then*

$$p_n \sim n \ln n.$$

Proof. By the definition of π, $\pi(p_n) = n$. Moreover, the Euclid theorem implies $p_n \underset{n\to\infty}{\to} \infty$. By Theorem 2.22,

$$n = \pi(p_n) = \frac{p_n}{\ln p_n}(1 + R_n), \quad \lim_{n\to\infty} R_n = 0.$$

Then

$$\ln n = \ln \pi(p_n) = \ln p_n - \ln\ln p_n + \ln(1 + R_n).$$

Multiply these expressions to obtain

$$n \ln n = p_n(1 + R_n)\frac{\ln p_n - \ln\ln p_n + \ln(1 + R_n)}{\ln p_n}.$$

It is easy to see that

$$\frac{n \ln n}{p_n} = (1 + R_n)\left(1 - \frac{\ln\ln p_n}{\ln p_n} + \frac{\ln(1 + R_n)}{\ln p_n}\right) \underset{n\to\infty}{\to} 1.$$

□

§ 2.4. Problems

(1) Prove that

$$\sum_{p\in\mathbb{P},p\leqslant x}\frac{\ln p}{p}=\ln x+O(1).$$

(2) Show that there exists a constant $C>0$ such that

$$\sum_{p\in\mathbb{P},p\leqslant x}\frac{1}{p}=C+\ln(\ln x)+O(1/\ln x).$$

(3) The famous *Riemann hypothesis* states that all zeros of $\zeta(z)$ in the semiplane $\operatorname{Re} z>0$ lie in the line $\operatorname{Re} z=\frac{1}{2}$.

Assuming Riemann hypothesis is true, prove

$$\psi(x)=x+O(x^{\varepsilon+0.5}),\quad \pi(x)=\ln(x)+O(x^{\varepsilon+0.5})$$

for every $\varepsilon>0$.

CHAPTER 3

Dirichlet Theorem

In this chapter we prove the famous Dirichlet theorem on the number of primes in an arithmetic progression with coprime difference and the first member. We start with the structure and properties of finite abelian groups.

§ 3.1. Finite abelian groups and groups of characters

1. Finite abelian groups. Recall that the set G with an algebraic binary operation "$\cdot$" is called a *group* (we often omit "$\cdot$" and write g_1g_2 instead of $g_1 \cdot g_2$), if the following axioms are satisfied:

(a) for every $a, b, c \in G$ the identity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds;
(b) there exists $e \in G$ such that for every $a \in G$ we have $a \cdot e = e \cdot a = a$, such element e is called the *identity* element or the *neutral* element;
(c) for every $a \in G$ there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$, such a^{-1} is called the *inverse* element.

If an additional axiom of commutativity holds:

(d) for every $a, b \in G$ we have $a \cdot b = b \cdot a$,

then the group is called *abelian*. If G is abelian, then the additive notation is used very often, so the operation is denoted by "+", the identity element is denoted by "0", and the inverse element is denoted by "$-a$". By $|G|$ we denote the cardinality of G.

A one-generated group is called *cyclic*, i.e. a group G is called *cyclic* if there exists $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$ (in additive notation, $G = \{na \mid n \in \mathbb{Z}\}$. Notice that for every group G and for every $g \in G$ the set $\{g^n \mid n \in \mathbb{Z}\}$ appears to be a subgroup of G. This subgroup is called the *cyclic subgroup generated by* g and is denoted by $\langle g \rangle$. The cardinality $|\langle g \rangle|$ is called the *order* of g and is denoted by $|g|$. Clearly $\langle \mathbb{Z}, + \rangle$ is an infinite cyclic group and, for every $n \in \mathbb{N}$, $\langle \mathbb{Z}_n, + \rangle$ is a finite cyclic group of order n.

Exercise 3.1. Let G be a group and g be an element of G. Then the following hold.

(1) Either $|g| = \infty$, or $|g|$ is the minimal positive integer k such that $g^k = e$.
(2) If $|g| = \infty$, then $\langle g \rangle \simeq \mathbb{Z}$; if $|g| = n$, then $\langle g \rangle \simeq \mathbb{Z}_n$[1].
(3) If $g^m = e$, then $|g|$ divides m.
(4) If $g_1, g_2 \in G$ are chosen so that $g_1 \cdot g_2 = g_2 \cdot g_1$, and $\langle g_1 \rangle \cap \langle g_2 \rangle = \{e\}$, then $|g_1 \cdot g_2| = \mathrm{lcm}(|g_1|, |g_2|)$. In particular, if $|g_1|, |g_2|$ are coprime then $|g_1 \cdot g_2| = |g_1| \cdot |g_2|$.

If $G_1, \dots G_n$ are groups, then

$$G_1 \times \ldots \times G_n = \{(g_1, \dots, g_n) \mid g_1 \in G_1, \dots, g_n \in G_n\}$$

with coordinate-wise multiplication is called the *direct product* of $G_1, \dots, G_n$. If G is abelian and $G_1, \dots, G_n$ are subgroups of G, then the set $G_1 \cdot \ldots \cdot G_n = \{g_1 \cdot \ldots \cdot g_n \mid g_1 \in G_1, \dots, g_n \in G_n\}$ forms a subgroup of G.

Exercise 3.2. Let G be an abelian group. Assume that subgroups $G_1, \dots, G_n$ of G satisfy to the following

(1) $G = G_1 \cdot \ldots \cdot G_n$.
(2) for every i we have $G_i \cap (G_1 \cdot \ldots \cdot G_{i-1} \cdot G_{i+1} \cdot \ldots \cdot G_n) = \{e\}$.

Then $G \simeq G_1 \times \ldots \times G_n$. In such case G is also called a *direct product of subgroups* $G_1, \dots, G_n$.

Hint: Prove that conditions (1) and (2) are equivalent to the statement "for every $g \in G$ there exist unique $g_1 \in G_1, \dots, g_n \in G_n$ such that $g = g_1 \cdot \ldots \cdot g_n$".

The proof of the following theorem can be found in many algebra textbooks and we do not provide the proof here.

Theorem 3.3. *Let G be a finite abelian group. Then there exist $d_1, \dots, d_n \in \mathbb{N}$ such that $G \simeq \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_n}$. Moreover such $d_1 \dots, d_n$ can be uniquely determined by the following condition: for every $i = 1, \dots, n-1$, d_i divides d_{i+1}.*

Recall that by $\mathbb{Z}_n^*$ we denote the (multiplicative) group of invertible elements in $\mathbb{Z}_n$.

Exercise 3.4. Prove that $|\mathbb{Z}_n^*| = \varphi(n)$, where $\varphi(n)$ is the Euler function. If $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ is the canonical decomposition of n into the product of primes, then $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$ and for every prime p and positive integer k, $\varphi(p^k) = p^k - p^{k-1}$.

[1]Recall that groups G, H are isomorphic if there exists a bijection $\varphi : G \to H$ preserving operation, i.e. $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$.

Hint: Prove that $\varphi \circ I = E$, where $I(n) = 1$, $E(n) = n$ for all natural n. Here "$\circ$" stands for the convolution product of arithmetic functions mentioned in Chapter 2.

2. Characters. Let G be a finite abelian group. A homomorphism[2] $\chi : G \to \mathbb{C}^*$ is called a *character* of G. The set of all characters of G is denoted by $\widehat{G}$. Define a multiplication on $\widehat{G}$ by

for every $\chi_1, \chi_2 \in \widehat{G}$ and $g \in G$ we have $(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$.

Theorem 3.5. *$\widehat{G}$ is an abelian group. Moreover, G and $\widehat{G}$ are isomorphic.*

Proof. The multiplication on $\widehat{G}$ is clearly an algebraic operation, and it is associative and commutative (we leave the proof for the reader). Denote by χ_e the *principal* character, it is defined by $\chi_e(g) = 1$ for all $g \in G$. It is immediate that χ_e is the identity element of $\widehat{G}$. For every $\chi \in \widehat{G}$ define χ^{-1} by $\chi^{-1}(g) = 1/\chi(g)$. Evidently, χ^{-1} is the inverse element for χ. Thus $\widehat{G}$ is an abelian group.

In view of the theorem about the structure of finite abelian groups (Theorem 3.3) we have $G = \langle g_1 \rangle \times \ldots \times \langle g_r \rangle$ for suitable $g_1, \ldots, g_r \in G$. Denote $|g_k|$ by h_k, let $\varepsilon_k = \exp(\frac{2\pi\iota}{h_k})$. For $k = 1, \ldots, r$ define the map $\chi_k : G \to \mathbb{C}^*$ by $\chi_k(g_1^{a_1} \ldots g_r^{a_r}) = \varepsilon_k^{a_k}$. It is straightforward that χ_k is a character of G for $k = 1, \ldots, r$. It is also clear that $\chi_k, \chi_k^2, \ldots, \chi_k^{h_k} = \chi_e$ are distinct characters, since their values on g_k are distinct.

Consider the map $\varphi : G \to \widehat{G}$ defined by $\varphi : g_1^{a_1} \ldots g_r^{a_r} \mapsto \chi_1^{a_1} \ldots \chi_r^{a_r}$. By the definition, φ preserves the multiplication. The map φ is clearly injective: if $e \neq x \in G$, then $x = g_1^{a_1} \ldots g_r^{a_r}$ and there exists a_k such that $g_k^{a_k} \neq e$; therefore

$$\varphi(x)(g_k) = (\chi_1^{a_1} \ldots \chi_r^{a_r})(g_k) = \exp\left(\frac{2a_k\pi\iota}{h_k}\right) \neq 1.$$

In order to prove that φ is surjective note that $g_k^{h_k} = e$ implies $\chi(g_k^{h_k}) = \chi(g_k)^{h_k} = 1$ for every $\chi \in \widehat{G}$. Hence, $\chi(g_k)$ is a complex root of unity of order h_k, and thus $\chi(g_k) = \varepsilon_k^{a_k}$ for appropriate a_k. It is straightforward to check that $\chi(g) = (\chi_1^{a_1} \ldots \chi_r^{a_r})(g)$ for all $g \in G$. Therefore, $\chi = \chi_1^{a_1} \ldots \chi_r^{a_r} =$

[2] *Homomorphism of groups* is a map, preserving the operation. Namely, the map $\varphi : G \to H$ is called a *homomorphism*, if for every $g_1, g_2 \in G$ we have $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$

$\varphi(g_1^{a_1} \dots g_r^{a_r})$, and φ is surjective. This completes the proof of the theorem. □

Exercise 3.6. Check all technical statements in the proof.

Remark 3.1. Theorem 3.5 is a particular case of Pontryagin duality between discrete and continuous abelian groups. The group of characters $\widehat{G}$ can be considered as a dual group for G and $\chi_1, \dots, \chi_r$ is the dual basis for $g_1, \dots, g_r$.

In the proof of the theorem we also derive the following

Corollary 3.7. *For every nonidentity $g \in G$ there exists $\chi_0 \in \widehat{G}$ such that $\chi_0(g) \neq 1$.*

In the theory of characters for finite groups the following proposition plays an important role.

Proposition 3.8. (Orthogonality relations) *The following hold*

(1) *for every $\chi \in \widehat{G}$ we have*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{if } \chi = \chi_e; \\ 0, & \text{if } \chi \neq \chi_e. \end{cases}$$

(2) *for every $g \in G$ we have*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G|, & \text{if } g = e; \\ 0, & \text{if } g \neq e. \end{cases}$$

Proof. Clearly we need to proof the first identity in case $\chi \neq \chi_e$, and the second in case $g \neq e$.

(1) If $\chi \neq \chi_e$, then there exists g_0 such that $\chi(g_0) \neq 1$. Then

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(gg_0) = \left(\sum_{g \in G} \chi(g) \right) \chi(g_0),$$

so $\sum_{g \in G} \chi(g) = 0$.

(2) If $g \neq e$, then Corollary 3.7 implies that the existence χ_0 such that $\chi_0(g) \neq 1$. Then

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\chi_0 \chi)(g) = \left(\sum_{\chi \in \widehat{G}} \chi(g) \right) \chi_0(g),$$

so $\sum_{\chi \in \widehat{G}} \chi(g) = 0$. □

3. Characters modulo m. Consider $G = \mathbb{Z}_m^*$. Denote by $\bar{n}$ the residual of n modulo m. Then each character $\chi \in \widehat{G}$ can be extended to an arithmetic function $\chi : \mathbb{N} \to \mathbb{C}$ by

$$\chi(n) = \begin{cases} \chi(\bar{n}), & \text{if } \gcd(n,m) = 1; \\ 0, & \text{otherwise.} \end{cases} \tag{3.1}$$

This construction lead us to the notion of a character modulo m. More formally, an arithmetic function $\chi : \mathbb{N} \to \mathbb{C}$ is called a *character modulo* m, if the following conditions are satisfied:

(1) $\chi(n) \neq 0$ if $\gcd(n,m) = 1$;
(2) $\chi(n) = 0$ if $\gcd(n,m) > 1$;
(3) $\chi(n_1) = \chi(n_2)$ if $n_1 \equiv n_2 \pmod{m}$;
(4) $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$ for all $n_1 n_2 \in \mathbb{N}$.

Define the set of all characters modulo m by G_m. It follows by definition that each character modulo m is a character of $\mathbb{Z}_m^*$ extended to all positive integers by using (3.1). So the following proposition is an immediate corollary to the properties of characters of finite abelian groups obtained above.

Proposition 3.9. *The following hold*

(1) *There exist exactly $\varphi(m)$ distinct characters modulo m.*
(2) *All characters modulo m forms a group G_m under usual multiplication: $(\chi_1 \cdot \chi_2)(n) = \chi_1(n) \cdot \chi_2(n)$.*
(3) *If Ω_m is a full system of residuals modulo m, then*

$$\sum_{n \in \Omega_m} \chi(n) = \begin{cases} \varphi(m), & \text{if } \chi = \chi_e, \\ 0, & \text{otherwise.} \end{cases}$$

(4) *For every $n \in \mathbb{Z}$ we have*

$$\sum_{\chi \in G_m} \chi(n) = \begin{cases} \varphi(m), & \text{if } n \equiv 1 \pmod{m}, \\ 0, & \text{otherwise.} \end{cases}$$

§ 3.2. Dirichlet series

1. Convergence of L-series. Given $\chi \in G_m$ define an *L-series* $L(z,\chi)$, where $z \in \mathbb{C}$, by

$$L(z,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}. \tag{3.2}$$

The series $L(z,\chi)$ is called an *L-series of character* χ.

Theorem 3.10. *Let χ be a character modulo m. Then the following statements hold.*

(1) *The series $L(z,\chi)$ is absolutely converging for $\operatorname{Re} z > 1$.*
(2) *If $\chi \neq \chi_e$, then $L(z,\chi)$ is uniformly converging in every compact domain of the semiplane $\operatorname{Re} z > 0$.*
(3) *If $\chi = \chi_e$, then $L(z,\chi)$ is uniformly converging in semiplane $\operatorname{Re} z \geqslant s$ for every $s > 1$. Moreover, $L(z,\chi)$ possesses an analytic continuation in domain $\operatorname{Re} z > 0$, $z \neq 1$ with the unique simple pole $z = 1$.*

Proof. (1) is evident, since $|\chi(n)| \leqslant 1$.
(2) Consider the series

$$L(z,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z},$$

set $s(x) := \sum_{n \leqslant x} \chi(n)$. The main idea of the proof comes from the harmonic series. In view of Proposition 3.9(3) we have

$$s(m) = \sum_{k=1}^{m} \chi(k) = \sum_{\bar{k} \in \mathbb{Z}_m^*} \chi(\bar{k}) = 0.$$

Moreover, for every $q \in \mathbb{N}$ we have $\sum_{k=1}^{m} \chi(qm+k) = 0$. Therefore, for each $N \in \mathbb{N}$ the inequality

$$\Big|\sum_{k=1}^{N} \chi(k)\Big| < m \tag{3.3}$$

holds.

Now consider $\chi(n) = s(n) - s(n-1)$. We obtain

$$\sum_{n=1}^{N} \frac{\chi(n)}{n^z} = \sum_{n=1}^{N} \frac{s(n) - s(n-1)}{n^z} = \frac{s(N)}{N^z} - \frac{s(N-1)}{N^z} + \frac{s(N-1)}{(N-1)^z} - \frac{s(N-2)}{(N-1)^z} + \ldots + \frac{s(2)}{2^z} - \frac{s(1)}{2^z} + \frac{s(1)}{1} = \frac{s(N)}{N^z} - \sum_{n=1}^{N-1} s(n) \cdot \left[\frac{1}{(n+1)^z} - \frac{1}{n^z} \right] = \frac{s(N)}{N^z} + \sum_{n=1}^{N-1} s(n) \cdot \int_n^{n+1} \frac{z}{x^{z+1}} \mathrm{d}x = \frac{s(N)}{N^z} + \sum_{n=1}^{N-1} z \cdot \int_n^{n+1} \frac{s(x)}{x^{z+1}} \mathrm{d}x,$$

in the last step we use the identity $s(x) = s(n)$ for $x \in [n, n+1)$. Set

$$I_n(z) := z \cdot \int_n^{n+1} \frac{s(x)}{x^{z+1}} \mathrm{d}x.$$

Now we can bound $|I_n(z)|$. In view of (3.3) we have

$$|I_n(z)| \leqslant |z| \cdot \int_n^{n+1} \frac{m}{x^{s+1}} \mathrm{d}x = \frac{m|z|}{s} \cdot \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right).$$

Therefore

$$\sum_{n=1}^{N-1} |I_n(z)| < \frac{m|z|}{s} \left(1 - \frac{1}{N^s} \right) < \frac{m|z|}{s},$$

so the series $L(z, \chi)$ is uniformly converging.

(3) The series $L(z, \chi_e)$ is absolutely converging for $\operatorname{Re} z > 1$, so

$$L(z, \chi_e) = \sum_{n=1}^{\infty} \frac{\chi_e(n)}{n^z} = \prod_{p \in \mathbb{P}} \left(\sum_{d=0}^{\infty} \chi_e(p^d) \cdot p^{-dz} \right) = \prod_{p \in \mathbb{P}} (1 - \chi_e(p) \cdot p^{-z})^{-1} = \prod_{p \in \mathbb{P}, p \nmid m} (1 - p^{-z})^{-1},$$

whence Euler identity (see Theorem 2.13) implies that the following identity holds

$$L(z, \chi_e) \cdot \prod_{p \in \mathbb{P}, p \mid m} (1 - p^{-z})^{-1} = \zeta(z). \tag{3.4}$$

We can define now $L(z, \chi_e)$ on $\operatorname{Re} z > 0$ by

$$L(z, \chi_e) = \zeta(z) \cdot \left(\prod_{p \in \mathbb{P}, p|m} (1 - p^{-z}) \right),$$

whence item (3) of the theorem. □

Lemma 3.11. *Set*

$$L(z, G_m) = \prod_{\chi \in H} L(z, \chi).$$

Then for $\operatorname{Re} z > 1$ *the series* $L(z, G_m)$ *can be written in the following form*

$$\sum_{n=0}^{\infty} \frac{a_n}{n^z},$$

where every a_n *is a nonnegative integer and, moreover, if* $n = k^{\varphi(m)}$ *and* $(k, m) = 1$, *then* $a_n \geqslant 1$. *Moreover,*

$$L(z, G_m)^{(k)} = (-1)^k \sum_{n=1}^{\infty} \frac{a_n (\ln n)^k}{n^z}, k = 1, 2, \ldots$$

Proof. The statement about derivations follows from the fact that the series

$$\sum_{n=0}^{\infty} \frac{a_n}{n^z}$$

is absolutely converging for $\operatorname{Re} z > 1$ (as a product of a finite number of absolutely converging series). Thus we need to show that

$$L(z, G_m) = \sum_{n=0}^{\infty} \frac{a_n}{n^z}.$$

Since χ is multiplicative for every $\chi \in G_m$, Lemma 2.7 implies that

$$L(z, \chi) = \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^z}\right)^{-1}.$$

Therefore,

$$L(z, G_m) = \prod_{\chi \in H} \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^z}\right)^{-1} = \prod_{p \in \mathbb{P}} \prod_{\chi \in G_m} \left(1 - \frac{\chi(p)}{p^z}\right)^{-1},$$

where we change the order of multiplication, since G_m is finite and

$$\prod_{p\in\mathbb{P}}\left(1-\frac{\chi(p)}{p^z}\right)^{-1}$$

is absolutely converging.

For every $p\in\mathbb{P}$ denote by f_p the multiplicative order of p in $\mathbb{Z}_m^*$, i.e. the minimal positive k with $p^k\equiv q\,(\mathrm{mod}\ m)$. Then

$$1=\chi(1)=\chi(p^{f_p})=\chi(p)^{f_p},$$

so $\chi(p)=\exp(2\pi\iota k/f_p)$ for some $k=0,1,\dots,f_p=1$. It follows that the map

$$\psi: G_m\to\mathbb{C}^*$$

acting by

$$\psi:\chi\mapsto\chi(p)$$

maps G_m into $\{\exp(2\pi\iota k/f_p)\mid k=0,1,\dots,f_p-1\}$. Clearly ψ is a homomorphism. Notice that ψ is surjective. Indeed, we can define a character χ_p on a power of a prime r^s by

$$\chi_p(r^s)=\begin{cases}\exp(2\pi\iota/f_p)^s, & \text{if } r=p\\ 1 & \text{if } r\neq p \text{ and } (r,m)=1\\ 0 & \text{if } r \text{ divides } m,\end{cases}$$

and extend it on all integers by multiplicativity. Then $\langle\chi_p\rangle$ is a subgroup of G_m and $\psi(\langle\chi_p\rangle)=\{\exp(2\pi\iota k/f_p)\mid k=0,1,\dots,f_p-1\}$. So the kernel of ψ has order $|G_m|/f_p=\varphi(m)/f_p=:g_p$. It follows that for every $k=0,1,\dots,f_p-1$ there exists exactly g_p characters $\chi\in G_m$ with $\chi(p)-\exp(2\pi\iota k/f_p)$. Therefore, a polynomial

$$\prod_{\chi\in G_m}(1-\chi(p)t)$$

equals $(1-t^{f_p})^{g_p}$. Thus

$$L(z,G_m)=\prod_{p\in\mathbb{P};(p,m)=1}(1-p^{-f_pz})^{-g_p}.$$

Now the Taylor series for $(1-z)^{-g}$ equals

$$\sum_{k=0}^{\infty}\frac{(g+k-1)!}{(g-1)!k!}z^k,$$

and the series is absolutely converging for $|z| < 1$. Since $|p^{-f_p z}| < 1$, we can apply the Taylor series to the expression of $L(z, G_m)$. We obtain

$$(1 - p^{-f_p z})^{-g_p} = \sum_{k=0}^{\infty} \frac{(g_p + k - 1)!}{(g_p - 1)!k!} p^{-f_p kz} = \sum_{k=0}^{\infty} \frac{u_{p,k}}{p^{kz}},$$

where

$$u_{p,k} = \begin{cases} 0, & \text{if } k \text{ is not divisible by } f_p, \\ \frac{(g_p+r-1)!}{(g_p-1)!r!}, & \text{if } k = r \cdot f_p. \end{cases}$$

Since for every $p \in \mathbb{P}$ the series

$$\sum_{k=0}^{\infty} \frac{u_{p,k}}{p^{kz}}$$

is absolutely converging, we obtain the following identity for every N:

$$\prod_{p \le N; (p,m)=1} (1 - p^{-f_p z})^{-g_p} = \sum_{n=1}^{\infty} \frac{a_n}{n^z},$$

where

$$a_n = \begin{cases} 0, & \text{if } (n, m) > 1, \\ u_{p_1,k_1} \cdot \ldots \cdot u_{p_l,k_l}, & \text{if } (n, m) = 1 \text{ and } n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}. \end{cases}$$

Consider $1 < s \in \mathbb{R}$. Then $L(s, G_m)$ is converging. On the other hand, for every M,

$$\sum_{n=1}^{M} \frac{a_n}{n^s} \le L(s, G_m),$$

so the series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

is converging, and so the series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^z}$$

is absolutely converging for every z with $\operatorname{Re} z > 1$. It follows that

$$L(z, G_m) = \sum_{n=1}^{\infty} \frac{a_n}{n^z},$$

where the coefficients a_n-s are defined above. From the definition we obtain that a_n are nonnegative integers. Since f_p divides $\varphi(m)$, we obtain that $a_n \neq 0$, if $n = k^{\varphi(m)}$ for $(k, m) = 1$. □

2. Landau Theorem. Consider

$$L(z) := L(z, G_m) = L(z, \chi_e) \cdot \prod_{\chi \in G_m \setminus \{\chi_e\}} L(z, \chi).$$

Theorem 3.10 implies that $L(z, \chi_e)$ is analytic in semiplane $\operatorname{Re} z > 0$ with a unique simple pole $z = 1$, while each $L(z, \chi)$ for $\chi \neq \chi_e$ is analytic in the semiplane $\operatorname{Re} z > 0$, i.e. $\prod_{\chi \in G_m \setminus \{\chi_e\}} L(z, \chi)$ is analytic in the semiplane $\operatorname{Re} z > 0$. Thus $L(z)$ is analytic in the semiplane $\operatorname{Re} z > 0$ with one possible simple pole $z = 1$. In order to prove that $z = 1$ is indeed a simple pole for $L(z)$ we need to prove that for every $\chi \in G_m \setminus \{\chi_e\}$ we have $L(1, \chi) \neq 0$. The next theorem helps us to prove the desired statement.

Theorem 3.12. (Landau Theorem) *Assume that a function $F(z)$ is analytic in $\operatorname{Re} z > 0$ and suppose that for $\operatorname{Re} z > 1$ we can write $F(z)$ as a series*

$$F(z) = \sum_{n=1}^{\infty} \frac{a_n}{n^z}, \tag{3.5}$$

where $a_n \geqslant 0$ for every n. Assume also that in the semiplane $\operatorname{Re} z > 1$ we have

$$F^{(k)}(z) = (-1)^k \sum_{n=1}^{\infty} \frac{a_n (\ln n)^k}{n^z},$$

i.e. series (3.5) can be differentiated term by term in the semiplane $\operatorname{Re} z > 1$. Then the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is converging in the interval $s \in (0, 2)$.

Proof. We consider the Taylor series for $F(s)$ about $s = 2$:

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(2)}{k!} (s-2)^k. \tag{3.6}$$

The Taylor series of an analytic function is converging in the circle of radius r centered at s_0, where r is the distance to the nearest singular point, i.e. series (3.6) is converging for every $s \in (0, 2)$. Now

$$F^{(k)}(2) = \sum_{n=1}^{\infty} (-1)^n \frac{a_n (\ln n)^k}{n^2},$$

hence

$$F(s) = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(-1)^k}{k!} \cdot \frac{a_n (\ln n)^k}{n^2} \cdot (s-2)^k.$$

The series is converging, moreover, $(-1)^k$ and $(s-2)^k$ for $s \in (0,2)$ have the same sign, so all terms in the series are nonnegative. Therefore the series is absolutely converging and we can change the order of summation. So we obtain

$$F(s) = \sum_{n=1}^{\infty} \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \cdot \frac{a_n (\ln n)^k}{n^2} \cdot (s-2)^k =$$

$$\sum_{n=1}^{\infty} \frac{a_n}{n^2} \left(\sum_{k=0}^{\infty} \frac{(\ln n)^k (2-s)^k}{k!} \right) =$$

// the inner sum is equal to $\exp((2-s)\ln n) = n^{2-s}$ // =

$$\sum_{n=1}^{\infty} \frac{a_n}{n^2} \cdot n^{2-s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

and the theorem follows. □

Now we can prove that for every $\chi \in G_m \setminus \{\chi_e\}$ we have $L(1,\chi) \neq 0$.

Corollary 3.13. *If $\chi \in G_m \setminus \{\chi_e\}$ then $L(1,\chi) \neq 0$.*

Proof. Assume that $L(1,\chi) = 0$. Then $L(z) = L(z, G_m)$ is analytic in the semiplane $\operatorname{Re} z > 0$. Moreover,

$$L(z) = \sum_{n=1}^{\infty} \frac{a_n}{n^z},$$

where $a_n \geqslant 0$ and further $a_n \geqslant 1$ for $n = k^{\varphi(m)}$ and $\gcd(k,m) = 1$. Every series $L(z,\chi)$ is absolutely converging in the semiplane $\operatorname{Re} z > 1$, so $L(z)$ is absolutely converging for $\operatorname{Re} z > 1$. Therefore the series $L(z)$ can be differentiated term by term any number of times. By the Landau theorem the series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

is converging for $0 < s < 2$. For $n = (km+1)^{\varphi(m)}$ we have $a_n \geqslant 1$, so

$$\sum_{n=1}^{N} \frac{a_n}{n^s} \geqslant \text{//for } s = \frac{1}{\varphi(m)} \text{//} \geqslant \sum_{k=1}^{[\frac{N}{m}-1]} \frac{1}{km+1} \underset{N\to\infty}{\to} \infty,$$

a contradiciton. □

3. Proof of the Dirichlet Theorem. First we recall the statement of the theorem.

Theorem 3.14. (Dirichlet Theorem) *Assume that a, m are natural coprime numbers.*

Then there exist infinitely many primes of the form $a + km$, or, equivalently, there exist infinitely many primes p such that $p \equiv a \pmod m$.

Proof. Consider the series

$$L(z, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z},$$

where $\chi \in G_m$ and $\operatorname{Re} z > 1$. First we prove that

$$\frac{1}{L(z, \chi)} = \sum_{n=1}^{\infty} \frac{\chi(n) \cdot \mu(n)}{n^z}, \tag{3.7}$$

where $\mu(n)$ is the Möbius function. Indeed, the series $\sum_{n=1}^{\infty} \frac{\chi(n)\cdot\mu(n)}{n^z}$ and $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}$ are absolutely converging, therefore by Lemma 2.10 we have

$$\left(\sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}\right) \cdot \left(\sum_{n=1}^{\infty} \frac{\chi(n) \cdot \mu(n)}{n^z}\right) = \sum_{n=1}^{\infty} \frac{(\chi \circ (\chi \cdot \mu))(n)}{n^z}.$$

Now $\chi \circ (\chi \cdot \mu) = (\chi \cdot I) \circ (\chi \cdot \mu) = \chi \cdot (I \circ \mu)$, and the Möbius inversion formulae (Lemma 2.11) implies that $I \circ \mu = e$, so $\chi \cdot (I \circ \mu) = \chi \cdot e = e$, so we get (3.7). For $\operatorname{Re} z > 1$ we have

$$L'(z, \chi) = -\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^z}.$$

Thus,

$$\frac{L'(z, \chi)}{L(z, \chi)} = \left(\sum_{n=1}^{\infty} \frac{\chi(n) \cdot \mu(n)}{n^z}\right) \cdot \left(-\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^z}\right) =$$

$$-\sum_{n=1}^{\infty} \frac{((\chi \cdot \ln) \circ (\chi \cdot \mu))(n)}{n^z} = -\sum_{n=1}^{\infty} \frac{(\chi \cdot (\ln \circ \mu))(n)}{n^z} =$$

$$//\text{Lemmas 2.11 and 2.14}// = -\sum_{n=1}^{\infty} \frac{(\chi \cdot \Lambda)(n)}{n^z},$$

where $\Lambda(n)$ is the von Mangoldt function, i.e. we obtain the identity

$$\frac{L'(z,\chi)}{L(z,\chi)} = -\sum_{n=1}^{\infty} \frac{(\chi\cdot\Lambda)(n)}{n^z}.$$

By definition we have $\chi(p^k) = \chi(p)^k$ and $\chi(p) \neq 0$ if and only if $\gcd(p,m) = 1$. Therefore

$$-\frac{L'(z,\chi)}{L(z,\chi)} = \sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty} \frac{\chi(p)^k\cdot\ln p}{p^{kz}} =$$

$$//\text{the series is absolutely converging for } \operatorname{Re} z > 1,$$
$$\text{so we can change the order of summation}// =$$
$$\sum_{k=1}^{\infty}\sum_{p\in\mathbb{P}} \frac{\chi(p)^k\cdot\ln p}{p^{kz}} = \sum_{p\in\mathbb{P}} \frac{\chi(p)\cdot\ln p}{p^z} + \sum_{k=2}^{\infty}\sum_{p\in\mathbb{P}} \frac{\chi(p)^k\cdot\ln p}{p^{kz}}.$$

Denote the second summand by $R(z,\chi)$. We show that $R(z,\chi)$ is absolutely converging for $\operatorname{Re} z \geqslant \frac{1}{2} + \varepsilon$ for every $\varepsilon > 0$. Indeed, we need to show that the series

$$\sum_{p\in\mathbb{P}} \ln p \sum_{k=2}^{\infty} \left(\frac{\chi(p)}{p^z}\right)^k$$

is absolutely converging, since in this case we can change the order of summation and derive that $R(z,\chi) = \sum_{k=2}^{\infty}\sum_{p\in\mathbb{P}} \frac{\chi(p)^k\cdot\ln p}{p^{kz}}$ is absolutely converging as well. Now we have

$$\sum_{p\in\mathbb{P}} \ln p \sum_{k=2}^{\infty} \left(\frac{\chi(p)}{p^z}\right)^k = \sum_{p\in\mathbb{P}} \ln p\cdot\frac{\chi(p)^2}{p^{2z}}\cdot\frac{1}{1-\frac{\chi(p)}{p^z}}.$$

Since $|1-\frac{\chi(p)}{p^z}| \geqslant |1-\frac{1}{p^{1/2}}|$, we have

$$\left|\ln p\cdot\frac{\chi(p)^2}{p^{2z}}\cdot\frac{1}{1-\frac{\chi(p)}{p^z}}\right| \leqslant \frac{\ln p}{p^{1+2\varepsilon}}\cdot\frac{1}{|1-\frac{1}{\sqrt{p}}|} \leqslant \frac{4\ln p}{p^{1+2\varepsilon}},$$

and thus we obtain that the series $R(z,\chi)$ is absolutely converging. By the condition of the theorem $\gcd(a,m) = 1$, so we can choose b so that

$b \cdot a \equiv 1 \pmod m$. Then we have

$$\sum_{\chi \in G_m} \chi(b) \cdot \left(-\frac{L'(z,\chi)}{L(z,\chi)} \right) =$$

$$\sum_{\chi \in G_m} \sum_{p \in \mathbb{P}} \frac{\chi(b) \cdot \chi(p) \cdot \ln p}{p^z} + \sum_{\chi \in G_m} \chi(b) \cdot R(z,\chi) =$$

$$\sum_{p \in \mathbb{P}} \frac{\ln p}{p^z} \cdot \left(\sum_{\chi \in G_m} \chi(b) \cdot \chi(p) \right) + \sum_{\chi \in G_m} \chi(b) \cdot R(z,\chi) =$$

$$//\text{recall that } \sum_{\chi \in G_m} \chi(bp) \text{ equals } \varphi(m)$$

$$\text{if } bp \equiv 1 \pmod m \text{ and } 0 \text{ otherwise } // =$$

$$\sum_{p \in \mathbb{P}, p \equiv a \pmod m} \frac{\varphi(m) \cdot \ln p}{p^z} + \sum_{\chi \in G_m} \chi(b) \cdot R(z,\chi).$$

The second summand is analytic for $\operatorname{Re} z > \frac{1}{2}$. If the theorem is false, then the first summand is finite and therefore it has a precise value for $z = 1$. On the other hand,

$$\sum_{\chi \in G_m} \chi(b) \cdot \left(\frac{L'(z,\chi)}{L(z,\chi)} \right) = \frac{L'(z,\chi_e)}{L(z,\chi_e)} + \sum_{\chi \in G_m \setminus \{\chi_e\}} \chi(b) \cdot \left(\frac{L'(z,\chi)}{L(z,\chi)} \right).$$

By Theorem 3.10 and Corollary 3.13 we obtain that the second summand is bounded for $z = 1$, while for the first summand we have

$$\frac{L'(z,\chi_e)}{L(z,\chi_e)} = \ln(L(z,\chi_e))',$$

and $\ln(L(z,\chi_e))'$ has a pole at $z = 1$ since $L(z,\chi_e)$ has a pole at $z = 1$. $\square$

CHAPTER 4

p-adic numbers

§ 4.1. Valuation fields

1. Basic properties. Let F be a field and $v : F \to \mathbb{R}$ a map from F to the field of real numbers. Then (F, v) is called a *valuation field*, while v is called a *valuation* of F, if

(1) For every $x \in F$ we have $v(x) \geqslant 0$ and $v(x) = 0$ if and only if $x = 0$.
(2) $v(x + y) \leqslant v(x) + v(y)$ (triangle inequality).
(3) $v(x \cdot y) = v(x) \cdot v(y)$.

We collect evident properties of a valuation in the next proposition.

Proposition 4.1. *Let (F, v) be a valuation field. Then $v(1) = 1$, $v(-1) = 1$, and, for every $x \in F^*$ and every $k \in \mathbb{Z}$ we have $v(x^k) = (v(x))^k$.*

Proof. Since $v(x) = v(x \cdot 1) = v(x) \cdot v(1)$ we obtain that $v(1) = 1$. Now $v(-1)^2 = v((-1)^2) = 1$ and $v(-1) > 0$, whence $v(-1) = 1$. We also have $1 = v(1) = v(x \cdot x^{-1}) = v(x) \cdot v(x^{-1})$, so $v(x^{-1}) = \frac{1}{v(x)}$. The remaining statement follows immediately. □

If F is the field of rationals, then we can define the following valuations:

(1) $v(x) = \begin{cases} 0, & \text{if } x = 0, \\ 1, & \text{otherwise;} \end{cases}$ the *trivial valuation* (it can be defined over arbitrary field).
(2) $v_\alpha(x) = |x|^\alpha$ for $0 < \alpha \leqslant 1$.
(3) $v_{p,\rho}(x) = \rho^{\nu_p(x)}$, where $0 < \rho < 1$, p is a prime, and $\nu_p(x) \in \mathbb{Z}$ is given by the identity $x = p^{\nu_p(x)} \cdot \frac{a}{b}$, where p does not divide $a \cdot b$, and $v_{p,\rho}(0) := 0$; the *p-adic valuation*.

Exercise 4.2. Check, that all defined above valuations satisfy to the definition. Can α be greater than 1 in item (2)? Can α be less, than 0 in item (2)?

Clearly, every valuation defines a topology on F. Namely, we can define an open sphere of radius $\varepsilon \in \mathbb{R}_{>0}$ centered at $a \in F$ by

$$B_\varepsilon(a) = \{x \in F \mid v(a-x) < \varepsilon\}, \tag{4.1}$$

and consider the family of all such spheres as a basis of a topology. It is clear that F with the topology is a Hausdorff space. Moreover, the operations "$+$", "$\cdot$" (considered as maps $F \times F \to F$) and "$-$", $^{-1}$ (considered as maps $F \to F$) are continuous. In particular, F is a topological field.

Exercise 4.3. Prove that all operations are continuous maps. Prove that induced topology is a Hausdorff space.

Let (F, v) be a valuation field, $a \in F$. A sequence $\{a_n\}_{n\geqslant 1}$ is said to converge to a (under the valuation v, we use notation $a_n \underset{(v)}{\to} a$), if

$$\lim_{n\to\infty} v(a_n - a) = 0.$$

The following basic properties of limits hold.

Proposition 4.4. *The following identities hold:*

$$\lim_{n\to\infty}(a_n \pm b_n) = \lim_{n\to\infty} a_n \pm \lim_{n\to\infty} b_n;$$
$$\lim_{n\to\infty}(a_n \cdot b_n) = \lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} b_n;$$
$$\lim_{n\to\infty} a_n^{-1} = \Big(\lim_{n\to\infty} a_n\Big)^{-1},$$

where $\lim\limits_{n\to\infty} a_n$ *and* $\lim\limits_{n\to\infty} b_n$ *are assumed to exist and, in the last identity all* a_n*-s and* $\lim\limits_{n\to\infty} a_n$ *are assumed to be not equal to* 0.

Exercise 4.5. Prove Proposition 4.4.

Let F be a field and v_1, v_2 be its valuations. The valuations v_1, v_2 are called *equivalent* ($v_1 \sim v_2$), if, for every sequence $\{a_n\}_{n\geqslant 1}$, we have

$$\{a_n\}_{n\geqslant 1} \underset{(v_1)}{\to} a \iff \{a_n\}_{n\geqslant 1} \underset{(v_2)}{\to} a.$$

Lemma 4.6. *Valuations* v_1, v_2 *of* F *are equivalent if and only if for every* $x \in F$ *we have* $v_1(x) < 1 \Leftrightarrow v_2(x) < 1$.

Proof. Assume that v_1 and v_2 are equivalent. Then for every $x \in F$ the inequality $v_1(x) < 1$ is equivalent to $x^n \underset{(v_1)}{\to} 0$. Since v_1 and v_2 are equivalent, it follows that $x^n \underset{(v_2)}{\to} 0$, so $v_2(x) < 1$.

Now we prove the converse statement. If v_1 is trivial, then v_2, clearly, is also trivial and the claim is evident. Assume that v_1 is nontrivial. Then there exists $x \in F$ such that $v_1(x) \neq 1$. By Proposition 4.1 we obtain that either $v_1(x) > 1$, or $v_1(x^{-1}) > 1$. Without loss of generality we may assume that $v_1(x) > 1$ (and so $v_2(x) > 1$). Choose a sequence $\{a_n\}_{n\geqslant 1}$ such that $a_n \underset{(v_1)}{\to} a$. Therefore, for every $m \in \mathbb{N}$, we have $x^m \cdot a_n \underset{(v_1)}{\to} x^m \cdot a$, i.e. $v_1(x^m a_n - x^m a) \underset{n\to\infty}{\to} 0$. Now denote $v_2(x)$ by α (recall that $v_2(x) > 1$). Then for every $\varepsilon > 0$ there exists $M \in \mathbb{N}$ such that for every $m > M$ we have $\frac{1}{\alpha^m} < \varepsilon$.

Since $v_1(x^m a_n - x^m a) \underset{n\to\infty}{\to} 0$, it follows that there exists $N \in \mathbb{N}$ such that for every $n > N$ we have $v_1(x^m a_n - x^m a) < 1$. The condition of the lemma implies that for every $n > N$ the inequality $v_2(x^m a_n - x^m a) < 1$ holds. Thus we obtain that for every $n > N$ the inequality $v_2(x)^m \cdot v_2(a_n - a) < 1$ holds. Hence, for every $n > \max\{M, N\}$ we have $v_2(a_n - a) < \varepsilon$, i.e. $a_n \underset{(v_2)}{\to} a$. The implication $a_n \underset{(v_2)}{\to} a \Rightarrow a_n \underset{(v_1)}{\to} a$ follows by the symmetry. □

Corollary 4.7. *Every valuation v_α of $\mathbb{Q}$, where $0 < \alpha \leqslant 1$, is equivalent to $v_1(x) = |x|$. If p is a fixed prime, then for every $0 < \rho < 1$ all valuations $v_{p,\rho}$ are equivalent, the corresponding equivalence class is denoted by v_p. If p, q are distinct primes, then $v_{p,\rho}$ and $v_{q,\rho}$ are not equivalent. Moreover, v_α and $v_{p,\rho}$ are not equivalent.*

Exercise 4.8. Prove Corollary 4.7

The topology induced on $\mathbb{Q}$ by a p-adic valuation is called a *p-adic topology*. The p-adic valuation of a number grows with the power of p in denominator. For example, if $a_n = p^n$, then $a_n \underset{n\to\infty}{\to} 0$. Valuation fields (F_1, v_1) and (F_2, v_2) are *topologically isomorphic*, if there exists an isomorphism of fields $\varphi : F_1 \to F_2$ such that for every sequence $\{a_n\}_{n\geqslant 1}$, $a_n \underset{(v_1)}{\to} a$ if and only if $\varphi(a_n) \underset{(v_2)}{\to} \varphi(a)$. In particular, if $F_1 = F_2 = F$, then $v_1 \sim v_2$ if and only if (F, v_1) is topologically isomorphic to (F, v_2) with isomorphism Id, where Id is the identical map.

Exercise 4.9. Prove that $(\mathbb{Q}, v_p)$ is not topologically isomorphic to $(\mathbb{Q}, v_q)$ for distinct primes p, q.

We say that a valuation field (F_1, v_1) *can be embedded* into a valuation field (F_2, v_2), if there exists an injective homomorphism $\varphi : F_1 \to F_2$ such that the restriction of v_2 on $\varphi(F_1)$ coincides with v_1.

2. Valuations over rationals.

Theorem 4.10. (On valuations over rationals) *Let $(\mathbb{Q}, v)$ be a valuation field. Then either v is the trivial valuation, or $v = v_\alpha$, or $v = v_{p,\rho}$.*

Proof. If v is the trivial valuation, we have nothing to prove. Assume that v is not trivial. Then there exists $n \in \mathbb{N}$ such that $v(n) \neq 1$. Indeed, since v is nontrivial, there exists $\frac{p}{q} \in \mathbb{Q}$ such that $v(\frac{p}{q}) \neq 1$. Hence either $v(p) \neq 1$, or $v(q) = v(\frac{1}{q})^{-1} \neq 1$. Now $p, q \in \mathbb{Z}$, hence for some $p \in \mathbb{Z}$, we obtain $v(p) \neq 1$. By Proposition 4.1 we have $v(p) = v(-p)$, so there exists $n \in \mathbb{N}$ such that $v(n) \neq 1$. Now one of the following two cases holds: either there exists $n \in \mathbb{N}$ such that $v(n) > 1$, or for every $n \in \mathbb{N}$ the inequality $v(n) \leqslant 1$ holds. Consider these cases separately.

Case 1. There exists n such that $v(n) > 1$. We have

$$v(n) = v(\underbrace{1 + \ldots + 1}_{n \text{ times}}) \leqslant \underbrace{1 + \ldots + 1}_{n \text{ times}} = n,$$

so there exists $\alpha \in (0, 1]$ such that $v(n) = n^\alpha$. By Proposition 4.1 we obtain that $v(n^k) = n^{k\alpha}$ for every $k \in \mathbb{Z}$. Assume that $m \in \mathbb{N}$. Then there exists $k \geqslant 0$ such that $n^k \leqslant m < n^{k+1}$. Consider the expansion of m in base n, we obtain:

$$m = a_0 + a_1 n + \ldots + a_k n^k,$$

where $0 \leqslant a_i \leqslant n - 1$ for $i = 0, 1, \ldots, k$; and $a_k \neq 0$. Now we have

$$v(m) \leqslant v(a_0) + v(a_1) \cdot n^\alpha + \ldots + v(a_k) \cdot n^{k\alpha} \leqslant$$
$$//\text{for every } i,\ v(a_i) \leqslant a_i \leqslant n - 1// \leqslant (n-1)(1 + n^\alpha + \ldots + n^{k\alpha}) \leqslant$$
$$\frac{n-1}{n^\alpha - 1}(n^{(k+1)\alpha} - 1) < \left[\frac{n-1}{n^\alpha - 1} n^\alpha\right] \cdot n^{k\alpha} \leqslant C \cdot m^\alpha.$$

Thus there exists a constant C such that for every $m \in \mathbb{N}$ we have $v(m) < C \cdot m^\alpha$. We state that for every m we have

$$v(m) \leqslant m^\alpha. \tag{4.2}$$

Indeed, assume that there exists $k \in \mathbb{N}$ such that $v(k) > k^\alpha$, i.e. $\frac{v(k)}{k^\alpha} = D > 1$. Then for every $s \in \mathbb{N}$ we have

$$\frac{v(k^s)}{k^{s\alpha}} = D^s \underset{s \to \infty}{\to} \infty.$$

On the other hand, $\frac{v(k^s)}{k^{s\alpha}} < C$, a contradiction. Thus (4.2) holds for every $m \in \mathbb{N}$.

Now $n^{k+1} = m + m_1$, where $0 < m_1 \leqslant n^k(n-1)$. Therefore $v(n^{k+1}) \leqslant v(m) + v(m_1)$, so

$$v(m) \geqslant n^{(k+1)\alpha} - v(m_1) \geqslant n^{(k+1)\alpha} - m_1^\alpha \geqslant$$
$$n^{k\alpha}(n^\alpha - (n-1)^\alpha) = n^{(k+1)\alpha}\left(1 - \left(\frac{n-1}{n}\right)^\alpha\right) > C_1 \cdot m^\alpha.$$

It follows that there exists a constant $C_1 > 0$ such that for every $m \in \mathbb{N}$ we have $v(m) > C_1 \cdot m^\alpha$. We state that

$$v(m) \geqslant m^\alpha. \tag{4.3}$$

Indeed, assume that there exists $k \in \mathbb{N}$ such that $v(k) < k^\alpha$, i.e. $\frac{v(k)}{k^\alpha} = D_1 < 1$. So for every $s \in \mathbb{N}$ we have

$$\frac{v(k^s)}{k^{s\alpha}} = D_1^s \underset{s\to\infty}{\to} 0.$$

On the over hand, $\frac{v(k^s)}{k^{s\alpha}} \geqslant C_1$, a contradiction. Combining inequalities (4.2) and (4.3) we obtain that for every $m \in \mathbb{N}$ the identity $v(m) = m^\alpha$ holds. By Proposition 4.1 it follows that $v(-m) = v(m)$ and $v(m^{-1}) = (v(m))^{-1}$, so for every $\frac{p}{q} \in \mathbb{Q}$, the identity $v\left(\frac{p}{q}\right) = \left|\frac{p}{q}\right|^\alpha$ holds.

Case 2. For every $n \in \mathbb{N}$ we have $v(n) \leqslant 1$. Choose n so that $v(n) \neq 1$ (hence $v(n) < 1$). Consider the decomposition of n into the product of primes $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Then $v(n) = v(p_1)^{\alpha_1} \cdot \ldots \cdot v(p_k)^{\alpha_k}$, so there exists a prime p with $v(p) = \rho < 1$. We show first that for every prime $q \neq p$ the identity $v(q) = 1$ holds. Otherwise there would exist $q \neq p$ with $v(q) = \mu < 1$. Since both ρ and μ are less than 1, there exists $k \in \mathbb{N}$ such that both ρ^k, μ^k are less than $\frac{1}{2}$. On the other hand, $\gcd(p^k, q^k) = 1$, so there exist $a, b \in \mathbb{Z}$ such that $a \cdot p^k + b \cdot q^k = 1$. Thus we obtain

$$1 = v(1) = v(a \cdot p^k + b \cdot q^k) \leqslant v(a) \cdot v(p^k) + v(b) \cdot v(q^k) \leqslant$$
$$1 \cdot \rho^k + 1 \cdot \mu^k < \frac{1}{2} + \frac{1}{2} = 1,$$

a contradiction. Now for every $\frac{m}{n} \in \mathbb{Q}$ we have $m = p^{\alpha_1} \cdot m_1$, $n = p^{\alpha_2} \cdot n_1$, where $\gcd(m_1 \cdot n_1, p) = 1$, therefore

$$v\left(\frac{m}{n}\right) = \rho^{\alpha_1 - \alpha_2} \cdot \frac{v(m_1)}{v(n_1)} = \rho^{\alpha_1 - \alpha_2} = \rho^{\nu_p\left(\frac{m}{n}\right)}$$

and the theorem follows. □

3. The replenishment of a valuation field. A classical result claim that every topological space admits a replenishment. Now we construct a replenishment for a valuation field and prove that the replenishment is unique (up to a topological isomorphism).

Let (F, v) be a valuation field. A sequence $\{a_n\}_{n\geqslant 1}$, where $a_n \in F$ is called *fundamental*, if for every $\varepsilon > 0$ there exists N such that for every $n, m > N$ we have $v(a_n - a_m) < \varepsilon$.

Lemma 4.11. *The following hold:*

(1) *Assume that v_1 and v_2 are equivalent valuations of a field F. A sequence $\{a_n\}_{n\geqslant 1}$ is fundamental in v_1 if and only if it is fundamental in v_2.*
(2) *If $\{a_n\}_{n\geqslant 1}$ is a fundamental sequence in (F, v), then $\{v(a_n)\}_{n\geqslant 1}$ is a fundamental sequence in $\mathbb{R}$ under valuation $v(x) = |x|$.*

Proof. We prove item (1) first. If v_1 is the trivial valuation, then v_2 is also trivial and we have nothing to prove. If v_1 is nontrivial, then there exists $x \in F$ such that $v_1(x) = \alpha > 1$. Then for every $\varepsilon > 0$ there exists $m \in \mathbb{N}$ such that $\alpha^{-m} < \varepsilon$. If the sequence $\{a_n\}_{n\geqslant 1}$ is fundamental in v_1, then $\{x^m \cdot a_n\}_{n\geqslant 1}$ is also fundamental in v_1, so there exists $N \in \mathbb{N}$ such that for every $n, k > N$ we have $v_1(x^m a_n - x^m a_k) < 1$. Whence $v_2(x^m a_n - x^m a_k) < 1$, and so $v_2(a_n - a_k) < \alpha^{-m} < \varepsilon$.

Now we turn to (2). Since $v(a_n) = v(a_n - a_m + a_m) \leqslant v(a_m) + v(a_n - a_m)$, and, by symmetry, $v(a_m) \leqslant v(a_n) + v(a_n - a_m)$, it follows that $|v(a_n) - v(a_m)| \leqslant v(a_n - a_m)$. □

A valuation field (F, v) is called *complete* if every fundamental sequence in G is converging, i.e. it has the limit in F. If a valuation field is embedded into a complete valuation field $(\overline{F}, \bar{v})$ so that F is dense in $\overline{F}$ then $(\overline{F}, \bar{v})$ is called a replenishment of (F, v).

Theorem 4.12. *For every valuation field (F, v) there exists a unique up to isomorphism replenishment $(\overline{F}, \bar{v})$.*

Proof. We construct a replenishment using the standard construction for the real numbers. Let

$$\mathcal{F} = \{\{a_n\}_{n\geqslant 1} \mid \{a_n\}_{n\geqslant 1} \text{ is a fundamental sequence of } (F, v)\}$$

be a set of all fundamental sequences consisting of elements from F. Define the addition and multiplication on $\mathcal{F}$ by

$$\{a_n\}_{n\geqslant 1} + \{b_n\}_{n\geqslant 1} = \{a_n + b_n\}_{n\geqslant 1},$$
$$\{a_n\}_{n\geqslant 1} \cdot \{b_n\}_{n\geqslant 1} = \{a_n \cdot b_n\}_{n\geqslant 1},$$

Clearly both $\{a_n + b_n\}_{n\geqslant 1}$ and $\{a_n \cdot b_n\}_{n\geqslant 1}$ are fundamental sequence. We prove, for example, that $\{a_n \cdot b_n\}_{n\geqslant 1}$ is fundamental provided both $\{a_n\}_{n\geqslant 1}$, $\{b_n\}_{n\geqslant 1}$ are fundamental. We have

$$v(a_n \cdot b_n - a_m \cdot b_m) = v(a_n \cdot b_n - a_m \cdot b_n + a_m \cdot b_n - a_m \cdot b_m) \leqslant$$
$$v(a_n \cdot b_n - a_m \cdot b_n) + v(a_m \cdot b_n - a_m \cdot b_m) =$$
$$v(a_n - a_m) \cdot v(b_n) + v(b_n - b_m)v(a_m).$$

Since $\{a_n\}_{n\geqslant 1}$, $\{b_n\}_{n\geqslant 1}$ are fundamental sequences, Lemma 4.11(2) implies that $\{v(a_n)\}_{n\geqslant 1}$, $\{v(b_n)\}_{n\geqslant 1}$ are fundamental sequences as well. Therefore the sequences $\{v(a_n)\}_{n\geqslant 1}$ and $\{v(b_n)\}_{n\geqslant 1}$ are uniformly bounded by an absolute constant C. Since for every ε there exists N such that for every $m, n > N$ we have $v(a_n - a_m) < \frac{\varepsilon}{2C}$ and $v(b_n - b_m) < \frac{\varepsilon}{2C}$. So

$$v(a_n - a_m) \cdot v(b_n) + v(b_n - b_m)v(a_m) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

hence $\{a_n \cdot b_n\}_{n\geqslant 1}$ is fundamental.

Thus $\mathcal{F}$ is a commutative ring with 1. Consider

$$I_0 = \{\{a_n\}_{n\geqslant 1} \mid a_n \underset{n\to\infty}{\to} 0\}.$$

Clearly I_0 is an ideal of $\mathcal{F}$. We show that $\mathcal{F}/I_0$ is a field. Since $\mathcal{F}$ is a commutative ring with 1, we remain to prove that each nonzero element of $\mathcal{F}/I_0$ has inverse. Consider $\{a_n\}_{n\geqslant 1}+I_0 \neq 0+I_0$. Since $\{a_n\}_{n\geqslant 1} \in \mathcal{F}\setminus I_0$, it follows that $a_n \underset{n\to\infty}{\not\to} 0$, i.e. there exists $\varepsilon > 0$ and $N \in \mathbb{N}$ such that for every $n \geqslant N$ we have $v(a_n) > \varepsilon$. Consider the sequence $\{\frac{1}{a_n}\}_{n\geqslant N}$. The sequence is well-defined, since $a_n \neq 0$ for $n \geqslant N$. Moreover, for every $n, m \geqslant N$ we have

$$v\left(\frac{1}{a_n} - \frac{1}{a_m}\right) = \frac{v(a_m - a_n)}{v(a_n \cdot a_m)} \leqslant \frac{v(a_m - a_n)}{\varepsilon^2},$$

so the sequence $\{\frac{1}{a_n}\}_{n\geqslant N}$ is fundamental, i.e. $\{\frac{1}{a_n}\}_{n\geqslant N} \in \mathcal{F}$. Define the sequence $\{b_n\}_{n\geqslant 1}$ by: $b_n = 1$ for $n < N$ and $b_n = \frac{1}{a_n}$ for $n \geqslant N$. Then $\{b_n\}_{n\geqslant 1} \in \mathcal{F}$ and $a_n \cdot b_n - 1 = 0$ for all $n > N$. Hence,

$$(\{a_n\}_{n\geqslant 1} + I_0) \cdot (\{b_n\}_{n\geqslant 1} + I_0) = \{a_n \cdot b_n\}_{n\geqslant 1} + I_0 = \{1\}_{n\geqslant 1} + I_0,$$

i.e. $\{b_n\}_{n\geqslant 1} + I_0 = (\{a_n\}_{n\geqslant 1} + I_0)^{-1}$. Therefore $\overline{F} = \mathcal{F}/I_0$ is a field. The embedding $F \to \overline{F}$ is defined by $a \mapsto \{a_n\}_{n\geqslant 1} + I_0$, where $a_n = a$ for all $n \in \mathbb{N}$ (we use the notation $\{a\}_{n\geqslant 1}$ below). Define a valuation on $\mathcal{F}$ in the following way:

$$\text{if } \alpha = \{a_n\}_{n\geqslant 1} + I_0, \text{ then } \bar{v}(\alpha) = \lim_{n\to\infty} v(a_n).$$

Clearly, $\bar{v}$ does not depend on the representative of a coset $\{a_n\}_{n\geqslant 1} + I_0$, since the identity

$$\lim_{n\to\infty}(v(a_n)+v(b_n)) = \lim_{n\to\infty} v(a_n) + \lim_{n\to\infty} v(b_n)$$

holds. It is also evident that the restriction of $\bar{v}$ on F coincides with v. Now we check the properties of a valuation.

(1) $\bar{v}(\{a_n\}_{n\geqslant 1} + I_0) \geqslant 0$ and $\bar{v}(\{a_n\}_{n\geqslant 1} + I_0) = 0$ if and only if $\{a_n\}_{n\geqslant 1} + I_0 = I_0$, i.e. $a_n \underset{n\to\infty}{\to} 0$. Indeed, since for each n we have $v(a_n) \geqslant 0$, it follows that $\lim_{n\to\infty} v(a_n) = \bar{v}(\{a_n\}_{n\geqslant 1} + I_0) \geqslant 0$. If $\bar{v}(\{a_n\}_{n\geqslant 1} + I_0) = 0$, then $\lim_{n\to\infty} v(a_n) = 0$, so $\{a_n\}_{n\geqslant 1} \in I_0$.

(2)

$$\begin{aligned}\bar{v}(\{a_n\}_{n\geqslant 1} + I_0 + \{b_n\}_{n\geqslant 1} + I_0) = \\ \bar{v}(\{a_n + b_n\}_{n\geqslant 1} + I_0) = \\ \lim_{n\to\infty} v(a_n + b_n) \leqslant \\ \lim_{n\to\infty}(v(a_n) + v(b_n)) = \\ \lim_{n\to\infty} v(a_n) + \lim_{n\to\infty} v(b_n) = \\ \bar{v}(\{a_n\}_{n\geqslant 1} + I_0) + \bar{v}(\{b_n\}_{n\geqslant 1} + I_0).\end{aligned}$$

(3)

$$\begin{aligned}\bar{v}(\{a_n\}_{n\geqslant 1} + I_0) \cdot \bar{v}(\{b_n\}_{n\geqslant 1} + I_0) = \\ \bar{v}(\{a_n \cdot b_n\}_{n\geqslant 1} + I_0) = \\ \lim_{n\to\infty} v(a_n \cdot b_n) = \\ \lim_{n\to\infty} v(a_n) \cdot v(b_n) = \\ \lim_{n\to\infty} v(a_n) \cdot \lim_{n\to\infty} v(b_n) = \\ \bar{v}(\{a_n\}_{n\geqslant 1} + I_0) \cdot \bar{v}(\{b_n\}_{n\geqslant 1} + I_0).\end{aligned}$$

So $\bar{v}$ is a valuation.

Now we show that F is dense in $\overline{F}$. If $\alpha = \{a_n\}_{n\geqslant 1}$ is a fundamental sequence, then the sequence $\{\alpha_n\}_{n\geqslant 1}$, where $\alpha_n = \{a_n\}_{k\geqslant 1} \in F$ (recall that $\{a_n\}_{k\geqslant 1}$ is a sequence such that all its members are equal to a_n), is clearly converging to α. We remain to show that $\overline{F}$ is complete. Assume that $\{\alpha_n\}_{n\geqslant 1}$ is a fundamental sequence in $\overline{F}$. Since F is dense in $\overline{F}$, for every n we can choose $a_n \in F$ such that $\bar{v}(\alpha_n - \{a_n\}_{k\geqslant 1}) < \frac{1}{n}$. Let $\alpha = \{a_n\}_{n\geqslant 1}$.

We claim that $\alpha \in \mathcal{F}$ (so $\alpha + I_0 \in \overline{F}$) and $\alpha_n \underset{(\bar{v})}{\to} \alpha$. Indeed, for every ε there exists M such that $\bar{v}(\alpha_n - \alpha_m) < \frac{\varepsilon}{3}$ for all $m, n > M$. Further, there exists $N \geqslant M$ such that $\frac{1}{N} < \frac{\varepsilon}{3}$. So for $n, m \geqslant N$ we have

$$v(a_n - a_m) = \bar{v}(\{a_n\}_{k\geqslant 1} - \alpha_n + \alpha_n - \alpha_m + \alpha_m - \{a_m\}_{k\geqslant 1}) \leqslant \\ \bar{v}(\{a_n\}_{k\geqslant 1} - \alpha_n) + \bar{v}(\alpha_n - \alpha_m) + \bar{v}(\alpha_m - \{a_m\}_{k\geqslant 1}) < \varepsilon,$$

so α is a fundamental sequence. Now, by construction, we have

$$\bar{v}(\alpha_n - \alpha) \leqslant \bar{v}(\alpha_n - \{a_n\}_{k\geqslant 1}) + \bar{v}(\{a_n\}_{k\geqslant 1} - \alpha) \leqslant \\ \frac{1}{n} + \lim_{m\to\infty} v(a_n - a_m).$$

Since for every $\varepsilon > 0$ there exists N such that $\frac{1}{N} < \frac{\varepsilon}{2}$ and for every $n, m \geqslant N$, $v(a_n - a_m) < \frac{\varepsilon}{2}$, we obtain that for every $n \geqslant N$ the inequality $\bar{v}(\alpha_n - \alpha) < \varepsilon$ holds. Thus $\alpha_n \underset{(\bar{v})}{\to} \alpha$. This completes the proof of existence.

Now we prove the uniqueness. Let (F_1, v_1) and (F_2, v_2) be two replenishments of (F, v). We want to construct a topological isomorphism σ. Define σ in F as the identity map. By definition, F is dense in both F_1 and F_2, so every element of F_1 is a limit of a fundamental sequence $\{a_n\}_{n\geqslant 1}$, where each a_n lies in F. We extend σ to the map $\sigma : F_1 \to F_2$ by assuming that for $\alpha \in F_1$ such that $\alpha = \lim_{n\to\infty} a_n$ that $\sigma(\alpha) = \lim_{n\to\infty} \sigma(a_n)$. Clearly this definition is correct, since $\{\sigma(a_n)\}_{n\geqslant 1}$ is a fundamental sequence in F_2 and since for two fundamental sequences $\{a_n\}_{n\geqslant 1}$, $\{b_n\}_{n\geqslant 1}$ with $\lim_{n\to\infty} a_n = \alpha = \lim_{n\to\infty} b_n$ the sequence $\{c_n\}_{n\geqslant 1}$, where $c_{2n-1} = a_n, c_{2n} = b_n$, is fundamental and $\lim_{n\to\infty} c_n = \alpha$. It is technical to prove that σ is a bijection and that σ preserves the operation, and we leave the detailed proof to the reader. □

Exercise 4.13. Complete the technical details of the proof of Theorem 4.12.

§ 4.2. Construction and properties of p-adic fields

Clearly, if valuations v_1 and v_2 of a field F are equivalent, then the replenishments of (F, v_1) and (F, v_2) are topologically isomorphic. Recall that we denote the class of equivalent valuations $v_{p,\rho}$ of $\mathbb{Q}$ by v_p. A replenishment of $(\mathbb{Q}, v_p)$ is denoted by $\overline{\mathbb{Q}}_p$ and is called a *field of p-adic numbers* or a *p-adic field*. Theorem 4.12 implies that $\overline{\mathbb{Q}}_p$ exists and is unique up to

isomorphism. In this section we construct $\overline{\mathbb{Q}}_p$ explicitly and derive some its properties.

1. Ring of p-adic integers and its properties. Throughout we fix a prime p. Consider

$$\mathcal{Z}_p = \left\{ \{a_n\}_{n\geqslant 0} \mid a_n \in \mathbb{Z}, a_n \equiv a_{n-1} \,(\mathrm{mod}\ p^n) \text{ for } n \geqslant 1 \right\}.$$

Define addition and multiplication on $\mathcal{Z}_p$ as the addition and the multiplication of sequences, i.e. $\{a_n\}_{n\geqslant 0} + \{b_n\}_{n\geqslant 0} = \{a_n + b_n\}_{n\geqslant 0}$ and $\{a_n\}_{n\geqslant 0} \cdot \{b_n\}_{n\geqslant 0} = \{a_n \cdot b_n\}_{n\geqslant 0}$. Clearly $\mathcal{Z}_p$ is a ring under these operations. Consider

$$\mathcal{I}_p = \left\{ \{a_n\}_{n\geqslant 0} \in \mathcal{Z}_p \mid a_n \equiv 0 \,(\mathrm{mod}\ p^{n+1}) \right\}.$$

It is also evident that $\mathcal{I}_p$ is an ideal of $\mathcal{Z}_p$. Define $\overline{\mathbb{Z}}_p := \mathcal{Z}_p/\mathcal{I}_p$, a *ring of p-adic integers*. The embedding $\mathbb{Z} \to \overline{\mathbb{Z}}_p$ is defined by $m \mapsto \{a_n\}_{n\geqslant 0}$, where $a_0 = a_1 = \ldots = m$. Clearly this embedding preserves the addition and multiplication. Moreover, the unit of $\mathbb{Z}$ coincides with the unit of $\overline{\mathbb{Z}}_p$. Now we choose a canonical representation for every element from $\overline{\mathbb{Z}}_p$. Namely, for every sequence $\{a_n\}_{n\geqslant 0} \in \mathcal{Z}_p$ there exists a unique sequence $\{x_n\}_{n\geqslant 0} \in \mathcal{Z}_p$ such that for every n we have $0 \leqslant x_n < p^{n+1}$ and $a_n \equiv x_n \,(\mathrm{mod}\ p^{n+1})$, in particular $\{a_n\}_{n\geqslant 0} + \mathcal{I}_p = \{x_n\}_{n\geqslant 0} + \mathcal{I}_p$. The sequence $\{x_n\}_{n\geqslant 0}$ with $0 \leqslant x_n < p^{n+1}$ is a canonical representative of the coset $\{a_n\}_{n\geqslant 0} + \mathcal{I}_p$.

Theorem 4.14. *Let $\overline{\mathbb{Z}}_p$ be the ring of p-adic integers. Then the following hold.*

(1) *An element $\{x_n\}_{n\geqslant 0} \in \overline{\mathbb{Z}}_p$ is invertible in $\overline{\mathbb{Z}}_p$ if and only if $x_0 \neq 0$.*
(2) *For every $0 \neq \alpha \in \overline{\mathbb{Z}}_p$ there exist the unique $n \in \mathbb{N}$ and $\xi \in \overline{\mathbb{Z}}_p^*$ such that $\alpha = p^n \cdot \xi$.*
(3) *$\overline{\mathbb{Z}}_p$ is an integral domain.*

Proof. Recall that if $m \in \mathbb{Z}$, then we identify m with its image $(m, m, \ldots) \in \overline{\mathbb{Z}}_p$. In particular, $1 = (1, 1, \ldots)$.

(1) Necessity. If $x_0 = 0$, then for every $n \in \mathbb{Z}$ we have $x_0 \cdot n = 0$, therefore $\{x_n\}_{n\geqslant 0} \notin \overline{\mathbb{Z}}_p^*$.

Sufficiency. Assume that $x_0 \neq 0$. Since $0 < x_0 < p$, it follows that $\gcd(x_0, p) = 1$. Now, by definition, $x_1 \equiv x_0 \,(\mathrm{mod}\ p)$, therefore $\gcd(x_1, p) = 1$. Repeating the argument, by induction, we obtain that $\gcd(x_n, p) = 1$ for every n. Therefore, for every n we have $\gcd(x_n, p^{n+1}) = 1$. Hence, for every $n \geqslant 0$ there exists $0 < y_n < p^{n+1}$ such that $x_n \cdot y_n \equiv 1 \,(\mathrm{mod}\ p^{n+1})$. Since $x_n \equiv x_{n-1} \,(\mathrm{mod}\ p^n)$ and both $x_{n-1} \cdot y_{n-1}$ and $x_n \cdot y_n$ are equivalent

1 modulo p^n, it follows that $y_n \equiv y_{n-1} \pmod{p^n}$, i.e. $\{y_n\}_{n\geqslant 0} \in \mathcal{Z}_p$. Since $x_n \cdot y_n \equiv 1 \pmod{p^{n+1}}$ it follows that there exists z_n such that $x_n \cdot y_n = 1 + z_n \cdot p^{n+1}$. Therefore $\{x_n\}_{n\geqslant 0} \cdot \{y_n\}_{n\geqslant 0} = \{1\}_{n\geqslant 0} + \{z_n \cdot p^{n+1}\}_{n\geqslant 0}$ and the second summand in the right hand side lies in $\mathcal{I}_p$.

(2) If $\alpha = \{x_n\}_{n\geqslant 0} \in \overline{\mathbb{Z}}_p \setminus \{0\}$, then there exists a minimal n such that $x_n \neq 0$. If $n = 0$ then $\alpha = p^0\xi$ and $\xi = \alpha$. Suppose $n > 0$, then, by definition, $x_n \equiv x_{n-1} \pmod{p^n}$ and in view of our choice $x_{n-1} = 0$, so x_n is divisible by p^n and $x_n \not\equiv 0 \pmod{p^{n+1}}$, in particular, $\frac{x_n}{p^n} \not\equiv 0 \pmod{p}$ and $\gcd(x_n/p^n, p) = 1$. Now $x_{n+1} \equiv x_n \pmod{p^{n+1}}$, so $x_{n+1}/p^n \not\equiv 0 \pmod{p}$. Arguing in the same way by induction for every $k \geqslant n$ we obtain that $x_k/p^n \not\equiv 0 \pmod{p}$. Moreover, since $0 \leqslant x_k < p^{k+1}$, we have $0 < x_k/p^n < p^{k-n+1}$. Consider

$$\xi = \left(\frac{x_n}{p^n}, \frac{x_n}{p^n}, \dots, \frac{x_n}{p^n}, \frac{x_{n+1}}{p^n}, \frac{x_{n+2}}{p^n}, \dots\right) \text{ (first } n+1 \text{ terms are equal).}$$

In view of item (1) of the theorem, ξ is invertible in $\overline{\mathbb{Z}}_p$ and, by construction, $\alpha = p^n \cdot \xi$.

Now we show the uniqueness of n and ξ. If $\alpha = p^n \cdot \xi = p^m \cdot \zeta$, then the first nonzero term of $p^n \cdot \xi$ has number n, while the first nonzero term of $p^m \cdot \zeta$ has number m, so $n = m$. Let $\xi = \{x_n\}_{n\geqslant 0}$ and $\zeta = \{y_n\}_{n\geqslant 0}$. Since $p^n \cdot \xi = p^n \cdot \zeta$, we obtain that $x_m = y_m$ for $m \geqslant n$. Moreover

$$x_{n-1} = (x_n \mod p^n) = (y_n \mod p^n) = y_{n-1}.$$

Arguing in the same way we obtain that for all $i < n$ the equality $x_i = y_i$ holds (indeed, if $x_i = y_i$, then $x_{i-1} = (x_i \mod p^i) = (y_i \mod p^i) = y_{i-1}$). Thus $\xi = \zeta$.

(3) Assume that $\alpha, \beta \in \overline{\mathbb{Z}}_p \setminus \{0\}$ and $\alpha \cdot \beta = 0$. In view of item (2) of the theorem, $\alpha = p^n \cdot \xi$, $\beta = p^m \cdot \zeta$, hence $\alpha \cdot \beta = p^{n+m}(\xi \cdot \zeta) = 0$. Multiplying the left hand side of the identity by $\xi^{-1} \cdot \zeta^{-1}$ we obtain $p^n \cdot p^m = 0$. But $(n+m)$-th term of p^{n+m} equals $p^{n+m} \not\equiv 0 \pmod{p^{n+m+1}}$, a contradiction. □

Corollary 4.15. *An integer $a \in \mathbb{Z}$ is invertible in $\overline{\mathbb{Z}}_p$ if and only if* $\gcd(a, p) = 1$.

2. The field of p-adic rationals is the replenishment of rationals in p-adic metric. Corollary 4.15 implies that rational numbers of the form $\frac{a}{b}$ with $\gcd(b, p) = 1$ are naturally embedded into $\overline{\mathbb{Z}}_p$. Since $\overline{\mathbb{Z}}_p$ is an integral domain, it possesses a field of fractions, denote it by $\overline{\mathbb{Q}}_p$. We introduce a valuation v_p on $\overline{\mathbb{Q}}_p$ and show that $\overline{\mathbb{Q}}_p$ is a replenishment of $\mathbb{Q}$ under a p-adic valuation, i.e. we show that $\overline{\mathbb{Q}}_p$ is a field of p-adic numbers.

In view of Theorem 4.14 all elements of $\overline{\mathbb{Z}}_p$ have form $p^n \cdot \xi$, so we need to add the inverses for powers of p, i.e.

$$\overline{\mathbb{Q}}_p = \{p^n \cdot \xi \mid n \in \mathbb{Z}, \xi \in \overline{\mathbb{Z}}_p^*\} \cup \{0\}. \tag{4.4}$$

Given $\alpha = p^n \cdot \xi \in \overline{\mathbb{Q}}_p^*$ set $\nu_p(\alpha) = n$, and let $\nu_p(0) = \infty$. For brevity we use ν instead of ν_p below. Choose $0 < \rho < 1$ and set $v_p(\alpha) = \rho^{\nu_p(\alpha)}$. Every $\frac{a}{b} \in \mathbb{Q}$ can be uniquely written as $p^n \frac{a_1}{b_1}$, where p does not divide $a_1 \cdot b_1$. Then both a_1 and b_1 belong to $\overline{\mathbb{Z}}_p^*$, and thus $\frac{a_1}{b_1} = a_1 b_1^{-1} = \xi$ is an invertible p-adic integer. Therefore, $\frac{a}{b}$ corresponds to $p^n \xi \in \overline{\mathbb{Q}}_p$ and this correspondence gives the canonical embedding of $\mathbb{Q}$ into $\overline{\mathbb{Q}}_p$.

Theorem 4.16. *In the above notations for every $\alpha, \beta \in \overline{\mathbb{Q}}_p$ the following hold.*

(1) $\nu(\alpha \cdot \beta) = \nu(\alpha) \cdot \nu(\beta)$.
(2) $\nu(\alpha+\beta) \geqslant \min(\nu(\alpha), \nu(\beta))$, *moreover for $\nu(\alpha) \neq \nu(\beta)$ the equality holds.*
(3) v_p *is a valuation of $\overline{\mathbb{Q}}_p$ and the restriction of v_p on $\mathbb{Q}$ coincides with the valuation $v_{p,\rho}$ of $\mathbb{Q}$.*

Proof. (1), (2). If $\alpha = p^n \cdot \xi$, $\beta = p^m \cdot \zeta$, then $\alpha \cdot \beta = p^{n+m} \cdot (\xi \cdot \zeta)$, therefore $\nu(\alpha \cdot \beta) = \nu(\alpha) + \nu(\beta)$. Without loss of generality assume that $n \geqslant m$. Then we have

$$\alpha + \beta = p^n \cdot \xi + p^m \cdot \zeta = p^m(p^{n-m} \cdot \xi + \zeta),$$

and $p^{n-m} \cdot \xi + \zeta$ lies in $\overline{\mathbb{Z}}_p$, so $\nu(\alpha + \beta) \geqslant m = \min(\nu(\alpha), \nu(\beta))$. If $n > m$, then the first term of $p^{n-m} \cdot \xi + \zeta$ equals the first term of ζ, so is not equal to 0, therefore $p^{n-m} \cdot \xi + \zeta$ is invertible in $\overline{\mathbb{Z}}_p$ and $\nu(\alpha + \beta) = m$.

(3) First we check that v_p is a valuation. We have

$v_p(\alpha + \beta) \leqslant \rho^{\min(\nu(\alpha),\nu(\beta))} = \max(v_p(\alpha), v_p(\beta)) \leqslant v_p(\alpha) + v_p(\beta)$.
$v_p(\alpha \cdot \beta) = \rho^{\nu(\alpha)+\nu(\beta)} = v_p(\alpha) \cdot v_p(\beta)$.
$v_p(\alpha) \geqslant 0$ and $v_p(\alpha) = 0$ if and only if $\alpha = 0$.

So v_p is a valuation. The restriction of v_p on $\mathbb{Q}$ coincides with $v_{p,\rho}$ and we leave the details of the proof for the reader. □

Exercise 4.17. Prove that the restriction of v_p on $\mathbb{Q}$ coincides with $v_{p,\rho}$.

Theorem 4.18. *The valuation field $(\overline{\mathbb{Q}}_p, v_p)$ is a replenishment of $(\mathbb{Q}, v_{p,\rho})$.*

PROOF. We need to prove that $\overline{\mathbb{Q}}_p$ is complete and that $\mathbb{Q}$ is dense in $\overline{\mathbb{Q}}_p$. Let $\{\alpha_n\}_{n\geqslant 1}$ be a fundamental sequence in $\overline{\mathbb{Q}}_p$ and every α_n has the form $p^{m_n}\cdot\xi_n$, where $m_n\in\mathbb{Z}$ and $\xi_n\in\overline{\mathbb{Z}}_p^*\cup\{0\}$. Since the sequence $\{\alpha_n\}_{n\geqslant 1}$ is fundamental, it follows that $v_p(\alpha_n-\alpha_m)\underset{n,m\to\infty}{\to}0$. Now $v_p(\alpha_n-\alpha_m)=\rho^{\nu(\alpha_n-\alpha_m)}$. If the sequence $\{m_n\}_{n\geqslant}$ is not stabilizing, then for every n there exists $k>n$ such that $m_n\neq m_k$. In view of Theorem 4.16(2) we obtain

$$\rho^{\nu(\alpha_n-\alpha_m)}=\rho^{\min(m_n,m_k)}\underset{n,k\to\infty}{\to}0.$$

Therefore $m_n\underset{n\to\infty}{\to}\infty$, i.e. $\alpha_n\underset{(v_p)}{\to}0$. Assume that the sequence $\{m_n\}_{n\geqslant 1}$ is stabilizing, i.e. there exist $N\in\mathbb{N}, M\in\mathbb{Z}$ such that for every $n\geqslant N$ we have $m_n=M$. Then for every $n,m\geqslant N$ we have

$$v_p(\alpha_n-\alpha_m)=v_p(p^M(\xi_n-\xi_m))=v_p(p^M)\cdot v_p(\xi_n-\xi_m),$$

i.e. the sequence $\{\xi_n\}_{n\geqslant 1}$ is fundamental. Hence for every $m\in\mathbb{N}$ there exists $N_m\in\mathbb{N}$ such that for all $n_1,n_2>N_m$ we have $v_p(\xi_{n_1}-\xi_{n_2})<\rho^m$. So $\xi_{n_1}-\xi_{n_2}=p^{m+1}\cdot\xi$, where $\xi\in\overline{\mathbb{Z}}_p$. Let $\xi_n=\{x_k^{(n)}\}_{k\geqslant 0}$, consider $\xi=\{x_k\}_{k\geqslant 0}$, where $x_m:=x_m^{(N_m)}$. We claim that $\xi\in\overline{\mathbb{Z}}_p$ and that $\xi_n\underset{n\to\infty}{\to}\xi$. Show that $x_{m-1}\equiv x_m\,(\mathrm{mod}\ p^m)$ (and so $\xi\in\overline{\mathbb{Z}}_p$). Indeed, by definition, $x_{m-1}=x_{m-1}^{(N_{m-1})}$, i.e. for each $k>N_{m-1}$ we have $v(\xi_{N_{m-1}}-\xi_k)<\rho^{m-1}$, therefore $\xi_{N_{m-1}}-\xi_k=p^m\cdot\zeta$ for some $\zeta\in\overline{\mathbb{Z}}_p$. In particular, $x_{m-1}^{(N_{m-1})}-x_{m-1}^{(k)}\equiv 0\,(\mathrm{mod}\ p^m)$. Choose $k=N_m$, then, since $\xi_{N_m}\in\overline{\mathbb{Z}}_p$, we have $x_{m-1}^{(N_m)}\equiv x_m^{(N_m)}\,(\mathrm{mod}\ p^m)$, whence $x_{m-1}^{(N_{m-1})}\equiv x_m^{(N_m)}\,(\mathrm{mod}\ p^m)$. Now if $k\geqslant N_m$, then $v_p(\xi_k-\xi)\leqslant\rho^m$, so $\xi_n\underset{(v_p)}{\to}\xi$ and $\alpha_n\underset{(v_p)}{\to}p^M\cdot\xi$.

We remain to show that $\mathbb{Q}$ is dense in $\overline{\mathbb{Q}}_p$. Let $\alpha=p^n\cdot\xi$, where $n\in\mathbb{Z}$ and $\xi=(x_0,x_1,x_2,\ldots)\in\overline{\mathbb{Z}}_p^*$. Set $\alpha_m=p^n\cdot x_m\in\mathbb{Q}$. Then

$$v_p(\alpha_m-\alpha)=\rho^n\cdot v_p(0,\ldots,0,x_m-x_{m+1},x_m-x_{m+2},\ldots)\leqslant\rho^{n+m}\underset{m\to\infty}{\to}0,$$

and the theorem follows. □

EXERCISE 4.19. Prove that for every $\alpha\in\overline{\mathbb{Z}}_p$ there exists a sequence $\{x^{(m)}\}_{m\geqslant 0}$, $x^{(m)}\in\mathbb{Z}$, such that $x^{(m)}-\alpha\in p^{m+1}\overline{\mathbb{Z}}_p$ (in particular, $x^{(m)}\underset{(v_p)}{\to}\alpha$ as $m\to\infty$).

3. Applications. The construction of p-adic numbers shows that they are closely related to residuals modulo powers of p. This connection becomes clear due to the following theorem.

Theorem 4.20. *Assume that $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ is a polynomial with integer coefficients. The congruence*

$$F(x_1, \dots, x_n) \equiv 0 \,(\mathrm{mod}\ p^m) \tag{4.5}$$

has a solution in $\mathbb{Z}$ for every $m \geqslant 0$ if and only if

$$F(x_1, \dots, x_n) = 0 \tag{4.6}$$

has a solution in $\overline{\mathbb{Z}}_p$.

Proof. Assume that the equation (4.6) has a solution $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Z}}_p$. Denote by I_m the ideal $p^m \cdot \overline{\mathbb{Z}}_p$ of $\overline{\mathbb{Z}}_p$. Then for every m there exist $x_1^{(m)}, \dots, x_n^{(m)} \in \mathbb{Z}$ such that $\alpha_i + I_m = x_i^{(m)} + I_m$ (this statement follows from Exercise 4.19). Therefore

$$F(x_1^{(m)}, \dots, x_n^{(m)}) + I_m = F(\alpha_1, \dots, \alpha_n) + I_m = 0.$$

Now $F(x_1^{(m)}, \dots, x_n^{(m)})$ is an integer, so $F(x_1^{(m)}, \dots, x_n^{(m)}) \in I_m \cap \mathbb{Z} = p^m \cdot \mathbb{Z}$, i.e. $x_1^{(m)}, \dots, x_n^{(m)}$ is a solution for the congruence $F(x_1, \dots, x_n) \equiv 0 \,(\mathrm{mod}\ p^m)$.

Now assume that the congruences (4.5) have solution for each $m \geqslant 0$. Consider the sequence $\{(x_1^{(m)}, \dots, x_n^{(m)})\}_{m \geqslant 0}$ of solutions for congruences (4.5). Notice that we may choose a subsequence $\{(x_1^{(m_k)}, \dots, x_n^{(m_k)})\}_{k \geqslant 0}$ such that $x_i^{(m_k)}$ is converging to $\alpha_i \in \overline{\mathbb{Z}}_p$ for $1 \leqslant i \leqslant n$. Indeed, consider zero coordinates of $\{(x_1^{(m)}, \dots, x_n^{(m)})\}_{m \geqslant 0}$. We obtain the set of tuples of the form $(a_1, \dots, a_n)$, where $0 \leqslant a_i < p$ for each $i = 1, \dots, n$. Since $\{(x_1^{(m)}, \dots, x_n^{(m)})\}_{m \geqslant 0}$ is infinite, there exists an n-tuple $(a_1, \dots, a_n)$ such that the zero coordinate of $x_i^{(m)}$ equals a_i for infinitely many m and they form a subsequence $\{(x_1^{(m_0)}, \dots, x_n^{(m_0)})\}_{m_0 \geqslant 0}$ of $\{(x_1^{(m)}, \dots, x_n^{(m)})\}_{m \geqslant 0}$. We repeat the arguments for the first coordinates of $\{(x_1^{(m_0)}, \dots, x_n^{(m_0)})\}_{m_0 \geqslant 0}$ and derive an infinite subsequence $\{(x_1^{(m_1)}, \dots, x_n^{(m_1)})\}_{m_1 \geqslant 0}$. We repeat the arguments for every $k \geqslant 0$. Now we take any element from k-th subsequence and obtain the subsequence $\{(x_1^{(m_k)}, \dots, x_n^{(m_k)})\}_{k \geqslant 0}$ of $\{(x_1^{(m)}, \dots, x_n^{(m)})\}_{m \geqslant 0}$ satisfying the condition: for every $i = 1, \dots, n$ the first k coordinates of $x_i^{(m_t)}$ are equal to the coordinates of $x_i^{(m_k)}$ for every $t \geqslant k$. Therefore $v_p(x_i^{(m_t)} - x_i^{(m_s)}) < \rho^t \underset{t,s \to \infty}{\to} 0$, i.e. for every i the sequence $\{x_i^{(m_k)}\}_{k \geqslant 0}$

is fundamental. So the sequences $\{x_1^{(m_k)}\}_{k\geqslant 0}, \ldots, \{x_n^{(m_k)}\}_{k\geqslant 0}$ have limits $\alpha_1, \ldots, \alpha_n$ respectively and, by construction, each α_i lies in $\overline{\mathbb{Z}}_p$. Again by construction $F(\alpha_1, \ldots, \alpha_n)$ lies in every ideal I_m, so $F(\alpha_1, \ldots, \alpha_n) = 0$. □

§ 4.3. Problems

1. Prove that a valuation defines on a field the structure of Hausdorff space. Find a topological field that is not homeomorphic to a valuation field, i.e. there exist topological fields that do not possess a valuation inducing the same topology.
2. Prove that $(\overline{\mathbb{Z}}_p, v_p)$ is a compact topological space.
3. How many distinct solutions in $\overline{\mathbb{Z}}_5$ has the equation $x^2 + y^2 = 0$?

Bibliography

[1] Apostol T. V. *Introduction to Analytic Number Theory.* Springer, New York, 1976.

[2] Bateman P. D., Diamond H. G. *Analytic Number Theory – An Introductionary Course.* World Scientific Publ., Singapore, 2002.

[3] Bicadze A. V. *Foundations of the Theory of Analytic Functions of a Complex Variable* [Russian]. M.: Nauka, 1969.

[4] Borevich Z. I., Shafarevich I. R. *Number Theory* [Russian]. M.: Nauka, 1985.

[5] Buhshtab A. A. *Number Theory* [Russian]. M.: Prosveschenie, 1966.

[6] Chandrasekharan K. *Introduction to Analytic Number Theory.* Springer, Berlin-Heidelberg, 2012.

[7] Galochkin A. I., Nesterenko Yu. F., Shidlovskii A. B. *Introduction to Number Theory* [Russian]. M.: MSU, 1984.

[8] Gelfond A. O. *Transcendental and Algebraic Numbers* [Russian]. M.: Gostehizdat, 1952.

[9] Ingam A. V. *The Distribution of Prime Numbers* [Russian translation]. M.: Librokom, 2009.

[10] Karatsuba A. L. *Foundations of Analytic Number Theory* [Russian]. M.: URSS, 1983.

[11] Kostrikin A. I. *Introduction to Algebra* (Part 3) [Russian]. M.: Fizmatlit, 2004.

[12] Vinogradov I. M. *Elements of Number Theory* [Russian]. M.: Nauka, 1972.

Glossary

Index