

**From p -adic numbers to zeta-functions
(Review with some proofs)**

Marc Levine, Mikhail Shubin

Preprint, May 1997

1. p -adic integers.

Let p be a prime. Consider the p -adic presentation of an integer $n > 0$:

$$(1.1) \quad n = a_0 + a_1p + a_2p^2 + \dots + a_Np^N,$$

where $a_i \in \mathbf{Z}$ are “digits”, $0 \leq a_i \leq p - 1$. For $n = a_kp^k + a_{k+1}p^{k+1} + \dots + a_Np^N$ with $a_k \neq 0$ define $|n|_p = p^{-k}$ and $|0|_p = 0$. Let us extend this norm to \mathbf{Z} by taking $|-x|_p = |x|_p$.

Proposition 1.1. $|\cdot|_p$ is a norm on \mathbf{Z} . Moreover, for any $x, y \in \mathbf{Z}$

$$(1.2) \quad |x + y|_p \leq \max\{|x|_p, |y|_p\}$$

(*non-archimedean triangle inequality*),

$$(1.3) \quad |x \cdot y|_p = |x|_p |y|_p.$$

Proof. The proof is straightforward. \square

Remark. By a norm on \mathbf{Z} we mean a function $|\cdot| : \mathbf{Z} \rightarrow \mathbf{R}$ such that

- 1) $|x| \geq 0$ for all $x \in \mathbf{Z}$; $|x| = 0$ if and only if $x = 0$;
- 2) $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbf{Z}$ (the *triangle inequality*).

The norm is called *non-archimedean* if it satisfies (1.2). Note that (1.2) implies the triangle inequality.

Any norm $|\cdot|$ induces a metric defined by

$$d(x, y) = |x - y|.$$

In particular, the metric induced by $|\cdot|_p$ will be denoted $d_p(\cdot, \cdot)$.

The completion of \mathbf{Z} by the norm $|\cdot|_p$ (or by the metric d_p) is denoted \mathbf{Z}_p . Let us extend the operations from \mathbf{Z} to \mathbf{Z}_p by continuity. Then \mathbf{Z}_p becomes a ring. Its elements are called *p -adic integers*. The norm $|\cdot|_p$ and the metric d_p also can be extended to \mathbf{Z}_p by continuity, and the properties (1.2), (1.3) hold for all $x, y \in \mathbf{Z}_p$. The metric d_p defines topology on \mathbf{Z}_p .

Remark. $|x|_p \leq 1$ for all $x \in \mathbf{Z}_p$ and $|\cdot|_p$ takes only values p^{-k} , $k = 0, 1, 2, \dots$

Proposition 1.2. \mathbf{Z}_p is compact.

Proof. It is sufficient to prove that a sequence $\{x_n | n = 1, 2, \dots\}$ in \mathbf{Z} has a subsequence which is a Cauchy sequence in $|\cdot|_p$.

First note that taking a subsequence we can assume that all x_n have the same sign. Assume for example that $x_n > 0$ for all n . From this sequence we can take a subsequence such that all its members have the same first digit a_0 in the p -adic presentation (1.1). Then we can take a smaller subsequence with the same a_0, a_1 etc. In this way we obtain a series of sequences of integers (each one is a subsequence of the previous one):

$$\begin{aligned} & x_{00}, x_{01}, x_{02}, \dots \\ & x_{10}, x_{11}, x_{12}, \dots \\ & \dots \end{aligned}$$

Applying the Cantor diagonal process we obtain a sequence $x_{00}, x_{11}, x_{22}, \dots$ which is a Cauchy sequence, because all its “digits” stabilize. \square

Proposition 1.3. *Any p -adic integer $a \in \mathbf{Z}_p$ has a unique presentation*

$$(1.4) \quad a = \sum_{i=0}^{\infty} a_i p^i, \quad a_i \in \{0, 1, \dots, p-1\}.$$

Vice versa, any series of the form (1.4) is always convergent and represents an element $a \in \mathbf{Z}_p$.

Proof. Clearly the series in (1.4) is convergent, so its sum is in \mathbf{Z}_p . Vice versa, let us consider an arbitrary $a \in \mathbf{Z}_p$. It is the limit of a Cauchy sequence $a^{(N)} \in \mathbf{Z}$, $N = 1, 2, \dots$. Note first that we can assume that $a^{(N)} > 0$ for all N . Indeed, we can always replace $a^{(N)}$ by $p^{R(N)} + a^{(N)}$ where $R(N) \in \mathbf{Z}$, $R(N) \rightarrow \infty$ as $N \rightarrow \infty$, and we can choose $R(N)$ so that $p^{R(N)} + a^{(N)} > 0$ for all N .

Now assuming that $a^{(N)} > 0$ for all N , we can write

$$a^{(N)} = a_0^{(N)} + a_1^{(N)} p + \dots + a_{M(N)}^{(N)} p^{M(N)}, \quad a_j^{(N)} \in \{0, 1, \dots, p-1\}.$$

Since $a^{(N)}$ is a Cauchy sequence, $a_j^{(N)}$ stabilize as $N \rightarrow \infty$. So this sequence has a limit

$$\sum_{i=0}^{\infty} a_i p^i, \quad \text{where } a_i = \lim_{N \rightarrow \infty} a_i^{(N)}.$$

This limit should coincide with a .

To prove the uniqueness of the presentation (1.4) for any $a \in \mathbf{Z}_p$, note that if there are two different presentations of a in this form, then subtracting one from another, we can easily construct a nontrivial representation of the form (1.4) for $0 \in \mathbf{Z}_p$. This is impossible because the sum of any non-trivial series of the form (1.4) has a non-zero norm. \square

Example. For any prime p we have in \mathbf{Z}_p

$$-1 = \lim_{n \rightarrow \infty} (p^n - 1) = \lim_{n \rightarrow \infty} (p-1)(1 + p + p^2 + \dots + p^{n-1}) = \sum_{n=0}^{\infty} (p-1)p^n.$$

Later on we will use presentations of p -adic integers in the form (1.4) without specifying each time that the “digits” a_i are from $\{0, 1, \dots, p-1\}$.

Denote the set of all invertible elements of the ring \mathbf{Z}_p by \mathbf{Z}_p^\times .

Proposition 1.4.

$$(1.5) \quad \mathbf{Z}_p^\times = \left\{ \sum_{i=0}^{\infty} a_i p^i, a_0 \neq 0 \right\}.$$

Proof.

1) If $a_0 = 0$ then $|a|_p < 1$, hence a is not invertible because $|1| = 1$ but for any $b \in \mathbf{Z}_p$ we will have $|ab|_p = |a|_p |b|_p \leq |a|_p < 1$.

2) Now assume that $a_0 \neq 0$. Then we can find $b_0 \in \{1, 2, \dots, p-1\}$, such that $a_0 b_0 = 1 \pmod p$. Then $ab_0 = 1+r$, $|r|_p < 1$. Therefore $(1+r)^{-1} = 1-r+r^2-r^3+\dots$ and $a^{-1} = b_0(1+r)^{-1}$. \square

Remark. In Proposition 1.4 we assumed that $a_i \in \{0, 1, \dots, p-1\}$. However a more general sufficient condition of invertibility obviously holds: if we consider an arbitrary series of the form (4) with $a_i \in \mathbf{Z}$ (such a series obviously converges in \mathbf{Z}_p), and $a_0 \neq 0 \pmod p$, then $a \in \mathbf{Z}_p^\times$.

Example. Let us calculate $1/2$ in \mathbf{Z}_3 . Since $2 \cdot 2 = 1 + 3$ we have

$$1/2 = 2(1+3)^{-1} = 2 - 2 \cdot 3 + 2 \cdot 3^2 - 2 \cdot 3^3 + \dots = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \dots$$

This is easy to check independently. Indeed, using the summation formula for the geometric series we see that the sum in the right hand side equals $2 + 3 \cdot \frac{1}{1-3} = \frac{1}{2}$.

2. Topological structure and Haar measure for \mathbf{Z}_p .

For any metric space X with the distance d let $B(x, r)$ denote the open ball with the radius $r > 0$ centered at x :

$$B(x, r) = \{y \mid y \in X, d(y, x) < r\}.$$

We will denote by $\bar{B}(x, r)$ the corresponding closed ball:

$$\bar{B}(x, r) = \{y \mid y \in X, d(y, x) \leq r\}.$$

Note that $\bar{B}(x, r)$ does not necessarily coincide with the closure of $B(x, r)$.

Proposition 2.1. *Every ball with the radius $r > 0$ in \mathbf{Z}_p is open and closed.*

Proof. Since the only positive values of the metric $d_p(\cdot, \cdot)$ are p^{-k} , $k = 1, 2, \dots$, the closed ball $\bar{B}(x, r)$ always coincides with an open ball $B(x, r + \varepsilon)$ where $\varepsilon > 0$ is sufficiently small. Similarly any open ball $B(x, r)$ coincides with a closed ball $\bar{B}(x, r - \varepsilon)$ provided $\varepsilon > 0$ is sufficiently small. \square

Remark. It is interesting to notice that all there are only finitely many balls of any given radius in \mathbf{Z}_p . More precisely, all balls of the radius p^{-k} are listed in the right hand side of (2.3), i.e. there are only 2^k of such balls. Indeed, any ball should intersect with one of the balls listed in (2.3), but if two balls of the same radius have a non-empty intersection, then they should coincide due to the non-archimedean triangle inequality (1.2).

Now let us describe the topological structure of \mathbf{Z}_p .

We have

$$(2.1) \quad \mathbf{Z}_p = \bigsqcup_{a_0=0}^{p-1} (a_0 + B_{p^{-1}}(0))$$

(disjoint union). Furthermore,

$$(2.2) \quad a_0 + B_{p^{-1}} = \bigsqcup_{a_1=0}^{p-1} [(a_0 + a_1p) + B_{p^{-2}}(0)].$$

Generally,

$$(2.3) \quad \mathbf{Z}_p = \bigsqcup_{q=0}^{p^k-1} [q + B_{p^{-k}}(0)], \quad k = 1, 2, \dots$$

Proposition 2.2. \mathbf{Z}_p is homeomorphic to a Cantor set.

Proof. For simplicity consider first the case $p = 2$. Consider the standard Cantor set C which is obtained as the set of all numbers $x \in [0, 1]$ which can be presented in the 3-adic system with the use of the “digits” 0 and 2 (i.e. without using the “digit” 1). This means that

$$(2.4) \quad x = \sum_{k=1}^{\infty} x_k 3^{-k}; \quad x_k = 0 \text{ or } 2.$$

(For example $1 = 2 \cdot 3^{-1} + 2 \cdot 3^{-2} + \dots$.) In other words C is obtained by removing from $[0, 1]$ the “middle” open interval $(1/3, 2/3)$, then removing the middle open intervals $(1/9, 2/9)$ and $(7/9, 8/9)$ from the remaining closed intervals $[0, 1/3]$ and $[2/3, 1]$ respectively, etc.

Now let us put two closed and open disjoint subsets $C_0 = C \cap [0, 1/3]$ and $C_1 = C \cap [2/3, 1]$ covering C into a correspondence with the closed balls $B_0 = \bar{B}(0, 1/2)$ and $B_1 = \bar{B}(1, 1/2) = 1 + \bar{B}(0, 1/2)$ which are also disjoint, open and closed in \mathbf{Z}_2 and form a covering of \mathbf{Z}_2 . Then continue in the same way, covering both C_0, C_1 and B_0, B_1 by pairs of similar smaller disjoint open and closed subsets: C_{00}, C_{01} for C_0, C_{10} and C_{11} for C_1, B_{00} and B_{01} for B_0, B_{10} and B_{11} for B_1 . (The subsets C_{ij} are intersections of C with appropriate closed intervals of the length $1/9$ and B_{ij} are closed balls of the radius $1/4$.) Continuing in this way, we will obtain families of closed and open sets $C_{i_1 i_2 \dots i_k}$ and $B_{i_1 i_2 \dots i_k}$

(here $i_j = 0$ or 1) with the diameter 3^{-k} and 2^{-k} respectively, so that every set $C_{i_1 i_2 \dots i_k}$ (resp. $B_{i_1 i_2 \dots i_k}$) is covered by the disjoint sets $C_{i_1 i_2 \dots i_k 0}$ and $C_{i_1 i_2 \dots i_k 1}$ (resp. $B_{i_1 i_2 \dots i_k 0}$ and $B_{i_1 i_2 \dots i_k 1}$). For any sequence i_1, i_2, \dots , of 0's and 1's the intersection $C_{i_0} \cap C_{i_0 i_1} \cap \dots$, (resp. $B_{i_0} \cap B_{i_0 i_1} \cap \dots$) consists of exactly one point $x_{i_1 i_2 \dots}$ in C (resp. $y_{i_1 i_2 \dots}$ in \mathbf{Z}_2) and mapping $x_{i_1 i_2 \dots}$ to $y_{i_1 i_2 \dots}$ gives the desired homeomorphism of C and \mathbf{Z}_2 . \square

Remark. More explicitly the corresponding points in C and \mathbf{Z}_2 constructed above are

$$x_{i_1 i_2 \dots} = 2i_1 \cdot 3^{-1} + 2i_2 \cdot 3^{-2} + \dots \in C \subset [0, 1]$$

and

$$y_{i_1 i_2 \dots} = i_1 + i_2 \cdot 2 + i_3 \cdot 2^2 + \dots \in \mathbf{Z}_2 .$$

Now let us consider the Haar measure μ on \mathbf{Z}_p i.e. the unique Borel measure on \mathbf{Z}_p which is invariant under the translations and normalized by the natural requirement $\mu(\mathbf{Z}_p) = 1$. Then the decomposition (2.1) immediately implies that $\mu(\bar{B}(x, 1/p)) = 1/p$ for every $x \in \mathbf{Z}_p$, because every ball $\bar{B}(x, r)$ is a translation of the ball $\bar{B}(0, r)$ by x . Similarly (2.2) implies that $\mu(\bar{B}(x, p^{-2})) = p^{-2}$ for any $x \in \mathbf{Z}_p$, and generally it follows from (2.3) that

$$(2.5) \quad \mu(B(x, p^{-k})) = p^{-k} \quad \text{for all } x \in \mathbf{Z}_p \quad \text{and } k = 0, 1, 2, \dots .$$

Now we obtain

Proposition 2.3. *The Haar measure on \mathbf{Z}_p is the unique Borel measure on \mathbf{Z}_p which satisfies (2.5).*

Proof. We already proved that the Haar measure should satisfy (2.5). Uniqueness follows from the fact that any open set $U \subset \mathbf{Z}_p$ can be covered by countably many disjoint balls. Indeed, acting by induction, define $F_0 = \emptyset$ and for any $k = 1, 2, \dots$, denote by F_k the union of the balls of the radius p^{-k} which are subsets in $U \setminus F_{k-1}$. Since there are only finitely many balls of any given radius and any two different balls of the same radius are disjoint, we see that

$$U = \bigsqcup_{k=1}^{\infty} F_k$$

and each F_k is a disjoint union of a finite number of balls. \square

3. p -adic numbers .

Note that \mathbf{Z}_p is a ring without divisors of 0. Therefore we can take its field of fractions which is denoted \mathbf{Q}_p . Elements of \mathbf{Q}_p are called p -adic numbers.

We will now give an explicit description of \mathbf{Q}_p .

Proposition 3.1. \mathbf{Q}_p can be described as the set of all formal series

$$(3.1) \quad \mathbf{Q}_p = \left\{ a = \sum_{k=N}^{\infty} a_k p^k, 0 \leq a_k \leq p-1 \right\},$$

where N is an arbitrary integer (possibly negative). Here \mathbf{Z}_p is a subset of \mathbf{Q}_p which is obtained if we take the series with $N \geq 0$ in (3.1). The addition and multiplication are defined naturally. The norm on \mathbf{Q}_p

$$(3.2) \quad \left| \sum_{k=N}^{\infty} a_k p^k \right|_p = p^{-N} \quad \text{if } a_N \neq 0,$$

is a non-archimedean norm on \mathbf{Q}_p and it makes \mathbf{Q}_p a locally compact field (in particular, locally compact abelian group).

Proof. Any element $a \in \mathbf{Z}_p \setminus \{0\}$ can be uniquely represented as $a = p^k \tilde{a}$, where $|\tilde{a}|_p = 1$, i.e. $\tilde{a} \in \mathbf{Z}_p^\times$. Taking another element $b \in \mathbf{Z}_p \setminus \{0\}$, $b = p^l \tilde{b}$, $\tilde{b} \in \mathbf{Z}_p^\times$, we see that naturally $a/b = p^{k-l}(\tilde{a}/\tilde{b})$, and $\tilde{a}/\tilde{b} \in \mathbf{Z}_p$. So we see that the non-zero elements of the field of fractions are in a natural one-one correspondence with the expressions $p^N \tilde{a}$ where $\tilde{a} \in \mathbf{Z}_p^\times$, $N \in \mathbf{Z}$. Such expressions are naturally identified with the series of the form (3.1).

It is easy to see that the expression (3.2) indeed defines a non-archimedean norm on \mathbf{Q}_p . It coincides with the old norm $|\cdot|_p$ on \mathbf{Z}_p . Now the closed unit ball $\bar{B}(0, 1)$ equals \mathbf{Z}_p , therefore \mathbf{Q}_p is locally compact. \square

Remark. Each ball in \mathbf{Q}_p is open and closed, and it is compact. For example, $B_{p^l}(0) = p^{-l} \mathbf{Z}_p$.

Since $\mathbf{Z} \subset \mathbf{Z}_p$, we have $\mathbf{Q} \subset \mathbf{Q}_p$.

Proposition 3.2. \mathbf{Q} is dense in \mathbf{Q}_p .

Proof. The sum in (3.1) is the limit of the finite sums which are obtained by cutting the tails. But any finite sum of this form is in \mathbf{Q} . \square

Proposition 3.3. \mathbf{Q}_p is a disjoint union of countably many closed unit balls.

Proof. Since any two unit balls are either disjoint or coincide, it is sufficient to take all the unit balls centered at the points from \mathbf{Q} . \square

Let us define by μ the Haar measure on \mathbf{Q}_p normalized by the condition $\mu(\mathbf{Z}_p) = 1$, i.e. inducing the normalized Haar measure on \mathbf{Z}_p . Any closed unit ball is a translation of \mathbf{Z}_p , which is sufficient to make the Haar measure explicit.

Proposition 3.4. Let $M_x : \mathbf{Q}_p \rightarrow \mathbf{Q}_p$, $M_x y = xy$, $x \in \mathbf{Q}_p$, $x \neq 0$. Then for any measurable $A \subset \mathbf{Q}_p$ we have

$$(3.3) \quad \mu(M_x A) = |x|_p \mu(A).$$

Proof. Let us represent x in the form $x = p^k \tilde{x}$, where $\tilde{x} \in \mathbf{Z}_p^\times$ or $|\tilde{x}|_p = 1$. The multiplication by \tilde{x} preserves the Haar measure on \mathbf{Z}_p because it is an automorphism of \mathbf{Z}_p as a compact abelian group. Therefore it preserves the Haar measure on \mathbf{Q}_p due to Proposition 3.3. Now it is sufficient to check (3.3) for $x = p^k$ with $k \in \mathbf{Z}$ which is straightforward due to the geometry of balls in \mathbf{Q}_p . \square

4. Adeles (over \mathbf{Q}).

Denote by \mathcal{P} the set of all primes, $\overline{\mathcal{P}} = \mathcal{P} \cup \infty$. Denote $\mathbf{Q}_\infty = \mathbf{R}$. We will also use notation $|x|_\infty = |x|$ for the usual absolute value on \mathbf{R} .

The set of *adeles* \mathbf{Q}_A is a subset

$$(4.1) \quad \mathbf{Q}_A \subset \prod_{p \in \overline{\mathcal{P}}} \mathbf{Q}_p = \mathbf{R} \times \prod_{p \in \mathcal{P}} \mathbf{Q}_p,$$

which consists of all sequences $\{\alpha_p \mid p \in \overline{\mathcal{P}}\}$ such that $\alpha_p \in \mathbf{Z}_p$ except for a finite set of p 's. Clearly \mathbf{Q}_A is a ring. There is a natural imbedding of rings

$$(4.2) \quad \mathbf{Q} \subset \mathbf{Q}_A, \quad r \mapsto (r, r, \dots)$$

(the diagonal imbedding). Indeed, for any $r \in \mathbf{Q}$ we have $r \in \mathbf{Z}_p$ for all p except for a finite number of primes which divide the denominator of r .

We will introduce a topology in \mathbf{Q}_A which will make it a locally compact ring. This will *not* be the topology which is induced by the product topology in the right hand side of (4.1) (such a product topology will not be locally compact).

Let us take a finite set $S \subset \overline{\mathcal{P}}$, such that $S \ni \infty$, and define

$$\mathbf{Q}_A(S) = \prod_{p \in S} \mathbf{Q}_p \times \prod_{p \notin S} \mathbf{Z}_p.$$

Since \mathbf{Z}_p is compact, we easily see that $\mathbf{Q}_A(S)$ is locally compact in the product topology. It is also a topological ring. Now note that $S \subset S'$ implies $\mathbf{Q}_A(S) \subset \mathbf{Q}_A(S')$ and

$$\mathbf{Q}_A = \bigcup_S \mathbf{Q}_A(S) = \varinjlim \mathbf{Q}_A(S),$$

where the direct limit is taken over all finite $S \subset \overline{\mathcal{P}}$, $S \ni \infty$, which are ordered by inclusion.

Let us recall that the direct limit topology means that all imbeddings $\mathbf{Q}_A(S) \rightarrow \mathbf{Q}_A$ are continuous and the topology in \mathbf{Q}_A is the *strongest* topology such that this is true.

Proposition 4.1. *$U \subset \mathbf{Q}_A$ is open if and only if $U \cap \mathbf{Q}_A(S)$ is open for all S .*

Proof. (a) If $U \subset \mathbf{Q}_A$ is open, then $U \cap \mathbf{Q}_A(S)$ is open because the imbedding $\mathbf{Q}_A(S) \subset \mathbf{Q}_A$ is continuous.

(b) Now we should check that the sets

$$\{U \subset \mathbf{Q}_A \mid U \cap \mathbf{Q}_A(S) \text{ is open for every } S\}$$

form a topology. This is clear, because $(\cup_\alpha U_\alpha) \cap B = \cup_\alpha (U_\alpha \cap B)$. \square

Let us try to make the topology on \mathbf{Q}_A even more explicit.

Proposition 4.2. $\mathbf{Q}_A(S)$ is open and closed in \mathbf{Q}_A .

Proof. (a) The intersection of $\mathbf{Q}_A(S)$ with any $\mathbf{Q}_A(S')$ is $\mathbf{Q}_A(S \cap S')$, which is open in $\mathbf{Q}_A(S')$. It follows that $\mathbf{Q}_A(S)$ is open in \mathbf{Q}_A .

(b) Let us prove that $\mathbf{Q}_A(S)$ is closed in \mathbf{Q}_A . Note first that generally $F \subset \mathbf{Q}_A$ is closed if and only if $F \cap \mathbf{Q}_A(S')$ is closed in $\mathbf{Q}_A(S')$ for any S' , because if $CF = \mathbf{Q}_A \setminus F$, then $CF \cap \mathbf{Q}_A(S') = \mathbf{Q}_A(S') \setminus (F \cap \mathbf{Q}_A(S'))$ which will be always open if and only if all $F \cap \mathbf{Q}_A(S')$ are closed.

It remains to notice that $\mathbf{Q}_A(S) \cap \mathbf{Q}_A(S') = \mathbf{Q}_A(S \cap S')$ is closed in $\mathbf{Q}_A(S')$ because \mathbf{Z}_p is closed in \mathbf{Q}_p for all p . \square

Corollary. \mathbf{Q}_A is a locally compact topological ring.

Proof. Any $\mathbf{Q}_A(S)$ is a neighborhood of 0 and locally compact. \square

Remark. The topology in $\mathbf{Q}_A(S)$ can be defined by a metric

$$(4.3) \quad d(\{\alpha_p\}, \{\beta_p\}) = |\alpha_\infty - \beta_\infty| + \sum_{p \in \mathcal{P}} \frac{1}{2^p} \cdot \frac{|\alpha_p - \beta_p|_p}{1 + |\alpha_p - \beta_p|_p},$$

because both the product topology and the metric (4.3) induce the same (componentwise) convergence.

Let us discuss the Haar measure on \mathbf{Q}_A .

The Haar measure on $\mathbf{Q}_A(S)$ is clearly the product measure (we will take the Haar measures μ_p on \mathbf{Z}_p and \mathbf{Q}_p normalized as discussed above).

The Haar measures on $\mathbf{Q}_A(S)$ and $\mathbf{Q}_A(S')$ agree (i.e. induce the Haar measure on $\mathbf{Q}_A(S) \cap \mathbf{Q}_A(S') = \mathbf{Q}_A(S \cap S')$) because $\mu_p(\mathbf{Z}_p) = 1$. Therefore the Haar measure on \mathbf{Q}_A can be defined as the measure which is induced by the Haar measures on $\mathbf{Q}_A(S)$.

Proposition 4.4. \mathbf{Q} is discrete in \mathbf{Q}_A .

Proof. Clearly

$$\mathbf{Q} \cap \mathbf{Q}_A(\{\infty\}) = \mathbf{Q} \cap (\mathbf{R} \times \prod_{p \neq \infty} \mathbf{Z}_p) = \mathbf{Z},$$

because if $r \in \mathbf{Q} \cap \mathbf{Z}_p$ for all $p \in \mathcal{P}$, then no prime divides the denominator of r .

Define

$$U = \left(-\frac{1}{2}, \frac{1}{2}\right) \times \prod_{p \neq \infty} \mathbf{Z}_p.$$

Then U is an open neighborhood of 0 in \mathbf{Q}_A because $\mathbf{Z}_p \subset \mathbf{Q}_p$ is open, so $U \cap \mathbf{Q}_A(S)$ is open for every S .

Now $U \cap \mathbf{Q} = U \cap \mathbf{Z} = \{0\}$, hence \mathbf{Q} is discrete. \square

Proposition 4.5. \mathbf{Q}_A/\mathbf{Q} is compact.

Proof. We want to find a *compact set of representatives* i.e. a compact set $K \subset \mathbf{Q}_A$ such that the map $K \rightarrow \mathbf{Q}_A/\mathbf{Q}$ (the composition of the injection $K \rightarrow \mathbf{Q}_A$ and the canonical projection $\mathbf{Q}_A \rightarrow \mathbf{Q}_A/\mathbf{Q}$) is surjective.

It will be proved that we can take

$$K = \left[-\frac{1}{2}, \frac{1}{2}\right] \times \prod_{p \neq \infty} \mathbf{Z}_p.$$

We want to prove that for any $\alpha \in \mathbf{Q}_A$ there exists $r \in \mathbf{Q}$ such that $\alpha - r \in K$. Indeed, there exists a finite $S \subset \mathcal{P}$ such that

$$\alpha \in \mathbf{R} \times \prod_{p \in S} \mathbf{Q}_p \times \prod_{p \notin S} \mathbf{Z}_p.$$

For $p \in S$ write

$$\alpha_p = \sum_{i=N_p}^{-1} a_i p^i + \beta_p = r_p + \beta_p,$$

where $r_p \in \mathbf{Q}$ and $\beta_p \in \mathbf{Z}_p$. Moreover, $r_p \in \mathbf{Z}_q$ for all $q \neq p, q \in \mathcal{P}$. Now take $r = \sum_{p \in S} r_p$. Then $r - r_p \in \mathbf{Z}_p$ for every $p \in S$, therefore

$$\alpha - r \in \mathbf{R} \times \prod_{p \neq \infty} \mathbf{Z}_p.$$

But we also have action of \mathbf{Z} by translations in $\mathbf{R} \times \prod_{p \neq \infty} \mathbf{Z}_p$, so $K \rightarrow \mathbf{Q}_A/\mathbf{Q}$ is also surjective. \square

Proposition 4.6. $\text{vol}(\mathbf{Q}_A/\mathbf{Q}) = 1$.

Proof: The fundamental domain is

$$F = \left(-\frac{1}{2}, \frac{1}{2}\right] \times \prod_p \mathbf{Z}_p.$$

Indeed, we have already proved that F has at least one representative in any class of \mathbf{Q}_A/\mathbf{Q} . In fact, it is *exactly* one, because if the translation by $r \in \mathbf{Q}$ leaves $f \in F$ in F (i.e. $r + f \in F$), then $r + f_p \in \mathbf{Z}_p$, so $r \in \mathbf{Z}_p$ for all p , hence $r \in \mathbf{Z}$. Now $r + s \in \left(-\frac{1}{2}, \frac{1}{2}\right]$ for some $s \in \left(-\frac{1}{2}, \frac{1}{2}\right]$ implies $r = 0$.

Since the Haar measure is the product measure, we obtain $\mu(F) = 1$. \square

5. Ideles (over \mathbf{Q}).

Definition 5.1. Let \mathbf{Q}_A^\times be the group of all invertible elements of the ring \mathbf{Q}_A of adèles. Elements of \mathbf{Q}_A^\times are called *ideles*, so \mathbf{Q}_A^\times is also called the *group of ideles* (over \mathbf{Q}).

More explicitly, take $\alpha = \{\alpha_p\}_{p \in \bar{\mathcal{P}}} \in \mathbf{Q}_A$. It is invertible in \mathbf{Q}_A if and only if the following two conditions are satisfied:

- 1) $\alpha_p \neq 0$ for all $p \in \bar{\mathcal{P}}$;
- 2) $\alpha_p \in \mathbf{Z}_p^\times$ for almost all p (i.e. for all $p \in \bar{\mathcal{P}} \setminus S$ where $S = S(\alpha) \subset \bar{\mathcal{P}}$ is finite).

The condition 2) can be also rewritten as follows:

- 2') $|\alpha_p|_p = 1$ for almost all $p \in \bar{\mathcal{P}}$.

Let $S \subset \bar{\mathcal{P}}$ be finite. We will usually assume for simplicity of notations that $S \ni \infty$. Denote $\mathbf{Q}_A^\times(S)$ the group of all invertible elements in $\mathbf{Q}_A(S)$. Clearly $\mathbf{Q}_A^\times(S)$ consists of adèles $\{\alpha_p\}$ such that $\alpha_p \neq 0$ for all $p \in \bar{\mathcal{P}}$ and $\alpha_p \in \mathbf{Z}_p^\times$ for all $p \in \bar{\mathcal{P}} \setminus S$. This means that

$$(5.1) \quad \mathbf{Q}_A^\times(S) = \prod_{p \in S} \mathbf{Q}_p^\times \times \prod_{p \notin S} \mathbf{Z}_p^\times .$$

Obviously, $\mathbf{Q}_A^\times(S) \subset \mathbf{Q}_A^\times(S')$ if $S \subset S'$, and

$$(5.2) \quad \mathbf{Q}_A^\times = \bigcup_S \mathbf{Q}_A^\times(S) = \varinjlim_S \mathbf{Q}_A^\times(S) ,$$

where S runs over all finite subsets $S \subset \bar{\mathcal{P}}$.

TOPOLOGY ON \mathbf{Q}_A^\times .

Topology on \mathbf{Q}_A^\times can be introduced exactly as for adèles in Sect. 4. First introduce the product topology on $\mathbf{Q}_A^\times(S)$ according to (5.1). Here \mathbf{Q}_p^\times and \mathbf{Z}_p^\times are considered with the topologies induced by the inclusions $\mathbf{Q}_p^\times \subset \mathbf{Q}_p$, $\mathbf{Z}_p^\times \subset \mathbf{Z}_p$. Clearly \mathbf{Z}_p^\times is a compact abelian group, and \mathbf{Q}_p^\times is a locally compact abelian group. Therefore with the product topology $\mathbf{Q}_A^\times(S)$ becomes a locally compact abelian group, so that $\mathbf{Q}_A^\times(S)$ is an open and closed subset in $\mathbf{Q}_A^\times(S')$ if $S \subset S'$.

Now let us introduce the direct limit topology in \mathbf{Q}_A^\times using (5.2). As in Sect. 4 we see that a subset $M \subset \mathbf{Q}_A^\times$ is open (resp. closed) if and only if the intersection $M \cap \mathbf{Q}_A^\times(S)$ is open (resp. closed) for all finite $S \subset \bar{\mathcal{P}}$. In particular, $\mathbf{Q}_A^\times(S)$ is open and closed in \mathbf{Q}_A^\times for any finite $S \subset \bar{\mathcal{P}}$. It follows that with this topology $\mathbf{Q}_A^\times(S)$ is a locally compact abelian group.

Remark. Clearly the topology in \mathbf{Q}_A^\times is stronger than the topology induced by the inclusion $\mathbf{Q}_A^\times \subset \mathbf{Q}_A$ and the topology of \mathbf{Q}_A . It is in fact strictly stronger i.e. these two topologies on \mathbf{Q}_A^\times do not coincide. Indeed, let p_n be the n th prime in increasing order, so $p_1 = 2$, $p_2 = 3$ etc. Define a sequence of ideles $\{\alpha^{(n)} | n = 1, 2, \dots\} \subset \mathbf{Q}_A^\times$ as follows: $\alpha_{p_n}^{(n)} = p_n$, $\alpha_p^{(n)} = 1$ if $p \neq p_n$. Clearly, $\alpha^{(n)} \rightarrow 1$ in \mathbf{Q}_A in the topology of \mathbf{Q}_A as $n \rightarrow \infty$.

However, $\alpha^{(n)} \not\rightarrow 1$ in the topology of \mathbf{Q}_A^\times , because if $\alpha^{(n)} \rightarrow 1$ in the topology of \mathbf{Q}_A^\times , then there exists finite $S \subset \bar{\mathcal{P}}$ such that $\alpha^{(n)} \in \mathbf{Q}_A^\times(S)$ for large n , and this is obviously not the case.

Let us indicate another way to see that $\alpha^{(n)} \not\rightarrow 1$ in the topology of \mathbf{Q}_A^\times . If $\alpha^{(n)} \rightarrow 1$ in \mathbf{Q}_A^\times , then $(\alpha^{(n)})^{-1} \rightarrow 1$ in \mathbf{Q}_A^\times because \mathbf{Q}_A^\times is a topological group. However in our example it is not true because there is no finite set $S \subset \bar{\mathcal{P}}$ such that $(\alpha^{(n)})^{-1} \in \mathbf{Q}_A(S)$ for large n . Therefore $(\alpha^{(n)})^{-1}$ does not converge in \mathbf{Q}_A , hence it does not converge in \mathbf{Q}_A^\times . The following proposition shows that this is in fact the only obstruction.

Proposition 5.2. *The topology on \mathbf{Q}_A^\times is induced by the imbedding*

$$\begin{aligned} \mathbf{Q}_A^\times &\longrightarrow \mathbf{Q}_A \times \mathbf{Q}_A \\ \alpha &\mapsto \{\alpha, \alpha^{-1}\} \end{aligned}$$

and the product topology in $\mathbf{Q}_A \times \mathbf{Q}_A$.

Proof. For simplicity of notations let us argue about convergence of sequences, though using nets instead of sequences does not cause any complications. Consider a sequence of ideles $\{\alpha^{(n)} | n = 1, 2, \dots\}$. As we have seen above, convergence of this sequence in \mathbf{Q}_A^\times implies the convergence of both sequences $\{\alpha^{(n)}\}$ and $\{(\alpha^{(n)})^{-1}\}$ in \mathbf{Q}_A .

Vice versa, assume that both sequences $\{\alpha^{(n)}\}$ and $\{(\alpha^{(n)})^{-1}\}$ converge in \mathbf{Q}_A . Then there exists a finite $S \subset \bar{\mathcal{P}}$ such that both $\{\alpha^{(n)}\}$ and $\{(\alpha^{(n)})^{-1}\}$ are in $\mathbf{Q}_A(S)$ for large n . This means that in fact $\alpha^{(n)} \in \mathbf{Q}_A^\times(S)$ for large n . But the topology on $\mathbf{Q}_A^\times(S)$ is already the product topology, so it is induced by the topology of $\mathbf{Q}_A(S)$. Therefore the convergence of $\alpha^{(n)}$ in \mathbf{Q}_A with the extra condition $\{\alpha^{(n)}\} \subset \mathbf{Q}_A^\times(S)$ implies the convergence of $\{\alpha^{(n)}\}$ in $\mathbf{Q}_A^\times(S)$. \square

HAAR MEASURE ON \mathbf{Q}_A^\times .

Since \mathbf{Q}_A^\times is a locally compact abelian group, there exists a Haar measure on it. Denote this measure by μ^\times . Let us choose it properly normalized. To do this note that μ^\times restricts to a Haar measure μ_S^\times on $\mathbf{Q}_A^\times(S)$ for each finite $S \subset \bar{\mathcal{P}}$, so that these measures are compatible: $S \subset S'$ implies that $\mu_{S'}^\times$ restricts to μ_S^\times . Vice versa, if we have chosen Haar measures μ_S^\times for each finite $S \subset \bar{\mathcal{P}}$, so that the above compatibility condition is satisfied, then they define a Haar measure μ on \mathbf{Q}_A .

Now a Haar measure on $\mathbf{Q}_A^\times(S)$ should be a product of Haar measures μ_p^\times on the factors $\mathbf{Z}_p^\times, \mathbf{Q}_p^\times$ in (5.1). Since \mathbf{Z}_p^\times is compact, we naturally choose the Haar measure μ_p^\times so that $\mu_p^\times(\mathbf{Z}_p^\times) = 1$. Note that \mathbf{Z}_p^\times is open and closed subset in \mathbf{Z}_p , hence in \mathbf{Q}_p , hence in \mathbf{Q}_p^\times . Therefore we can define the Haar measure μ_p^\times on \mathbf{Q}_p^\times by requiring that $\mu_p^\times(\mathbf{Z}_p^\times) = 1$. It is easy to see that the corresponding product measures satisfy the compatibility conditions, therefore define a natural Haar measure on \mathbf{Q}_A^\times . We will always use the Haar measure μ^\times on \mathbf{Q}_A^\times which is normalized in this way.

NORM AND THE PRODUCT FORMULA.

Definition 5.3. The *norm* on \mathbf{Q}_A^\times is defined by the formula

$$(5.3) \quad |\alpha| = \prod_{p \in \bar{\mathcal{P}}} |\alpha_p|_p, \quad \alpha = \{\alpha_p\}_{p \in \bar{\mathcal{P}}} \in \mathbf{Q}_A^\times.$$

Here the product in the right hand side makes sense because $|\alpha_p|_p = 1$ for almost all $p \in \bar{\mathcal{P}}$.

Clearly

$$(5.4) \quad |\alpha\beta| = |\alpha| \cdot |\beta|, \quad \alpha, \beta \in \mathbf{Q}_A^\times.$$

The norm $|\cdot|$ is a continuous function on \mathbf{Q}_A^\times (with values in \mathbf{R}). Indeed, it is sufficient to show that its restriction to $\mathbf{Q}_A^\times(S)$ is continuous for each S , and this is obvious because each norm $|\cdot|_p$ is continuous on \mathbf{Q}_p^\times (in the topology of \mathbf{Q}_p^\times which is induced from \mathbf{Q}_p).

We have a natural (diagonal) imbedding

$$(5.5) \quad \mathbf{Q}^\times \subset \mathbf{Q}_A^\times, \quad r \mapsto (\dots, r, r, r, \dots).$$

Indeed, $r \in \mathbf{Z}_p^\times$ for all primes $p \in \mathcal{P}$ except the ones which divide the numerator or the denominator of a fraction which represents r .

Proposition 5.4. (Product formula.) *For any $r \in \mathbf{Q}^\times$ we have $|r| = 1$, i.e.*

$$(5.6) \quad \prod_{p \in \bar{\mathcal{P}}} |r|_p = 1, \quad r \in \mathbf{Q}^\times.$$

We will give two proofs of the product formula.

First proof (by direct computation). We can assume that $r > 0$. If $r = \frac{a}{b}$ where $a, b \in \mathbf{Z}$, $a, b > 0$, and the prime decompositions of a and b are

$$a = \prod_{i=1}^l p_i^{n_i}, \quad b = \prod_{j=1}^s q_j^{m_j},$$

then we clearly have $|r|_p = 1$ if $p \notin \{p_1, \dots, p_l, q_1, \dots, q_s\}$, $|r|_{p_i} = p_i^{-n_i}$, $|r|_{q_j} = q_j^{m_j}$. It follows that

$$\prod_{p \in \mathcal{P}} |r|_p = \frac{1}{r}.$$

Taking into account that $|r|_\infty = r$, we arrive to (5.6). \square

Second proof (with the help of the Haar measure on \mathbf{Q}_A). Let μ denotes the Haar measure on \mathbf{Q}_A , M_x is the multiplication operator by $x \in \mathbf{Q}_A^\times$ in \mathbf{Q}_A . Then using Proposition 3.4, we easily conclude that

$$(5.7) \quad \mu(M_x B) = |x| \mu(B)$$

for any measurable $B \subset \mathbf{Q}_A$. Clearly the same formula is true on \mathbf{Q}_A/\mathbf{Q} (with the Haar measure which is induced by the Haar measure of \mathbf{Q}_A), provided $x = r \in \mathbf{Q}$. Taking $B = \mathbf{Q}_A/\mathbf{Q}$ (which has measure 1 according to Proposition 4.6), we immediately arrive to the conclusion that we should have $|r| = 1$. \square

Remark. The advantage of the second proof is that it works for the number fields which are more general than \mathbf{Q} .

SPLITTING OF \mathbf{Q}_A^\times AND ACTION MAPS.

Let us consider the norm map

$$(5.8) \quad |\cdot| : \mathbf{Q}_A^\times \longrightarrow \mathbf{R}_+^\times,$$

where $\mathbf{R}_+^\times = \{x \in \mathbf{R} \mid x > 0\}$. It is a continuous group homomorphism. Denote its kernel by \mathbf{Q}_{A1}^\times , i.e.

$$(5.9) \quad \mathbf{Q}_{A1}^\times = \{\alpha \in \mathbf{Q}_A^\times \mid |\alpha| = 1\}.$$

It follows that \mathbf{Q}_{A1}^\times is a closed subgroup in \mathbf{Q}_A^\times . We will always consider \mathbf{Q}_{A1}^\times with the topology induced by the inclusion $\mathbf{Q}_{A1}^\times \subset \mathbf{Q}_A^\times$ and the topology of \mathbf{Q}_A^\times .

It follows from the product formula that $\mathbf{Q}^\times \subset \mathbf{Q}_{A1}^\times$.

Proposition 5.5.

- (i) *The norm homomorphism (5.8) is surjective.*
- (ii) *The exact sequence of abelian groups*

$$(5.10) \quad 1 \longrightarrow \mathbf{Q}_{A1}^\times \longrightarrow \mathbf{Q}_A^\times \xrightarrow{|\cdot|} \mathbf{R}_+^\times \longrightarrow 1$$

splits. (Here the second arrow is the natural inclusion $\mathbf{Q}_{A1}^\times \subset \mathbf{Q}_A^\times$.)

Proof. For any $x \in \mathbf{R}_+^\times$ take an idele $\hat{x} = \{x, 1, 1, \dots\}$ i.e. $\hat{x}_\infty = x$ and $\hat{x}_p = 1$ for all $p \in \mathcal{P}$. Define a map $j : \mathbf{R}_+^\times \rightarrow \mathbf{Q}_A^\times$, $j(x) = \hat{x}$. Clearly j is a continuous group homomorphism and $|\cdot| \circ j = \text{Id}_{\mathbf{R}_+^\times}$. This immediately implies both statements (i) and (ii). \square

Proposition 5.6.

- (i) *\mathbf{Q}^\times is a discrete subgroup in \mathbf{Q}_{A1}^\times .*
- (ii) *The group $\mathbf{Q}_{A1}^\times/\mathbf{Q}^\times$ is compact.*

Proof. We should try to find a compact set of representatives for the elements of $\mathbf{Q}_{A1}^\times/\mathbf{Q}^\times$ in \mathbf{Q}_{A1}^\times . Let us take an idele $\alpha = \{\alpha_p \mid p \in \bar{\mathcal{P}}\} \in \mathbf{Q}_{A1}^\times$. For any $p \in \mathcal{P}$ we can write $\alpha_p = p^{n_p} u_p$ where $n_p \in \mathbf{Z}$ and $|u_p|_p = 1$. Since $\alpha_p \in \mathbf{Z}_p^\times$ for almost all p , we have $n_p = 0$ for all $p \in \mathcal{P} \setminus S$ where $S \subset \mathcal{P}$ is finite. Now we can define

$$r = \prod_{p \in S} p^{n_p} \in \mathbf{Q}^\times,$$

and then

$$\frac{\alpha}{r} = \left\{ \frac{\alpha_p}{r} \mid p \in \bar{\mathcal{P}} \right\} \in \mathbf{R}^\times \times \prod_{p \in \mathcal{P}} \mathbf{Z}_p^\times .$$

Now note that $|\alpha| = 1$, and besides $|r| = 1$ by the product formula. Therefore $\left| \frac{\alpha}{r} \right| = 1$ and we should have $\alpha_\infty = \pm r$. Without loss of generality we can assume that $\alpha_\infty = r$ (otherwise replace r by $-r$). We see then that

$$(5.11) \quad \frac{\alpha}{r} \in K_1, \quad K_1 = 1 \times \prod_{p \in \mathcal{P}} \mathbf{Z}_p^\times .$$

So the compact subgroup $K_1 \subset \mathbf{Q}_{A_1}^\times$ can be taken as the set of representatives of elements of $\mathbf{Q}_{A_1}^\times / \mathbf{Q}^\times$ in $\mathbf{Q}_{A_1}^\times$. This proves the statement (ii).

It is easy to see that for any fixed $\alpha \in \mathbf{Q}_{A_1}^\times$ the number $r \in \mathbf{Q}^\times$ satisfying (5.11) is unique. Indeed, for any numbers r_1, r_2 satisfying (5.11) with the same α , we would have

$$r = \frac{r_1}{r_2} \in 1 \times \prod_{p \in \mathcal{P}} \mathbf{Z}_p^\times ,$$

which implies $r = 1$ and $r_1 = r_2$.

Clearly $K_1 \cong \prod_{p \in \mathcal{P}} \mathbf{Z}_p^\times$ is a compact subgroup in $\mathbf{Q}_{A_1}^\times$. The canonical inclusion with the canonical projection

$$(5.12) \quad K_1 \hookrightarrow \mathbf{Q}_{A_1}^\times \longrightarrow \mathbf{Q}_{A_1}^\times / \mathbf{Q}^\times$$

induce a group isomorphism

$$(5.13) \quad \mathbf{Q}_{A_1}^\times / \mathbf{Q}^\times \cong K_1 \cong \prod_{p \in \mathcal{P}} \mathbf{Z}_p^\times .$$

Now let us prove that K_1 is also open in $\mathbf{Q}_{A_1}^\times$. Let us fix a finite $S \subset \mathcal{P}$ and denote $\bar{S} = S \cup \{\infty\}$. We should prove that K_1 is open in $\mathbf{Q}_{A_1}^\times(\bar{S}) = \mathbf{Q}_{A_1}^\times \cap \mathbf{Q}_A^\times(\bar{S})$ with the topology induced by the inclusion $\mathbf{Q}_{A_1}^\times(\bar{S}) \subset \mathbf{Q}_A^\times(\bar{S})$ and the product topology on $\mathbf{Q}_A^\times(\bar{S})$. This amounts to proving that

$$(5.14) \quad K_1(S) = 1 \times \prod_{p \in S} \mathbf{Z}_p^\times \quad \text{is open in} \quad G_1(S) = \left\{ \alpha \in \mathbf{R}_+^\times \times \prod_{p \in S} \mathbf{Q}_p^\times \mid \prod_{p \in \bar{S}} |\alpha_p|_p = 1 \right\} .$$

The canonical projection

$$G_1(S) \longrightarrow \prod_{p \in S} \mathbf{Q}_p^\times$$

(forgetting the component $\alpha_\infty > 0$) is an isomorphism of topological groups because α_∞ can be recovered from the other components due to the product of norms condition. Now

we should only notice that $\prod_{p \in S} \mathbf{Z}_p^\times$ is open in $\prod_{p \in S} \mathbf{Q}_p^\times$. This implies (5.14), hence the fact that \mathbf{Q}^\times is a discrete subgroup in \mathbf{Q}_{A1}^\times . This proves the statement (i). \square

Remark. Arguments given above in the proof of Proposition 5.6 show that (5.13) is an isomorphism of topological groups. In fact we even have an obvious topological splitting

$$\mathbf{Q}_{A1}^\times \cong \mathbf{Q}^\times \times K_1,$$

where $(r, \beta) \in \mathbf{Q}^\times \times K_1$ corresponds to $r\beta \in \mathbf{Q}_{A1}^\times$, $r \in \mathbf{Q}^\times$ being identified with an element from \mathbf{Q}_{A1}^\times by the diagonal inclusion $\mathbf{Q}^\times \subset \mathbf{Q}_{A1}^\times$.

Proposition 5.7. *The left multiplication maps*

$$(5.15) \quad \begin{aligned} \mathbf{Q}_A^\times \times \mathbf{Q}_A &\rightarrow \mathbf{Q}_A, & \mathbf{Q}_{A1}^\times \times \mathbf{Q}_A &\rightarrow \mathbf{Q}_A \\ (\beta, \alpha) &\longrightarrow \beta\alpha \end{aligned}$$

are continuous actions. They induce continuous actions

$$(5.16) \quad \mathbf{Q}_A^\times \times \mathbf{Q}_A^\times \rightarrow \mathbf{Q}_A^\times, \quad \mathbf{Q}_{A1}^\times \times \mathbf{Q}_A^\times \rightarrow \mathbf{Q}_A^\times, \quad \mathbf{Q}_{A1}^\times \times \mathbf{Q}_{A1}^\times \rightarrow \mathbf{Q}_{A1}^\times,$$

$$(5.17) \quad \mathbf{Q}_A^\times \times (\mathbf{Q}_A^\times / \mathbf{Q}^\times) \rightarrow \mathbf{Q}_A^\times / \mathbf{Q}^\times, \quad \mathbf{Q}_{A1}^\times \times (\mathbf{Q}_A^\times / \mathbf{Q}^\times) \rightarrow \mathbf{Q}_A^\times / \mathbf{Q}^\times,$$

and

$$(5.18) \quad \mathbf{Q}_{A1}^\times \times (\mathbf{Q}_{A1}^\times / \mathbf{Q}^\times) \rightarrow \mathbf{Q}_{A1}^\times / \mathbf{Q}^\times.$$

Proof. The proof easily follows from the definition of topologies on all the groups which are involved. The choice of the direct limit topologies reduces checking of the continuity to the product topologies on $\mathbf{Q}_A^\times(S)$, $\mathbf{Q}_A(S)$ etc. In the product topologies the continuity becomes obvious because then it reduces to the continuity of the multiplication on every factor. \square

Remark. The action in (5.18) is most interesting because it is an action of a locally compact group on a *compact* space.

HAAR MEASURE ON \mathbf{Q}_{A1}^\times .

Since \mathbf{Q}_{A1}^\times is a locally compact abelian group, there exists a Haar measure on it. Let us discuss its structure and choose an appropriate normalization.

Denote

$$(\mathbf{Q}_{A1}^\times)^+ = \{\alpha \in \mathbf{Q}_{A1}^\times \mid \alpha_\infty > 0\}.$$

Clearly $(\mathbf{Q}_{A1}^\times)^+$ is an open subgroup of index 2 in \mathbf{Q}_{A1}^\times . Therefore it is also closed. It suffices to introduce the Haar measure on $(\mathbf{Q}_{A1}^\times)^+$.

The advantage of working with $(\mathbf{Q}_{A_1}^\times)^+$ is that its canonical projection

$$(\mathbf{Q}_{A_1}^\times)^+ \longrightarrow \prod_{p \in \mathcal{P}} \mathbf{Q}_p^\times$$

(forgetting α_∞) is an inclusion, and it induces an isomorphism of topological groups

$$(\mathbf{Q}_{A_1}^\times)^+ \cong \bigcup_{S \subset \mathcal{P}} \left(\prod_{p \in S} \mathbf{Q}_p^\times \times \prod_{p \in \mathcal{P} \setminus S} \mathbf{z}_p^\times \right) = \varinjlim \left(\prod_{p \in S} \mathbf{Q}_p^\times \times \prod_{p \in \mathcal{P} \setminus S} \mathbf{z}_p^\times \right),$$

where the right hand side is taken in the direct limit topology. Now the groups under the limit have the product Haar measures with the natural normalizations. These measures are compatible and define the Haar measure on $(\mathbf{Q}_{A_1}^\times)^+$. We will denote the Haar measure on $\mathbf{Q}_{A_1}^\times$ by μ_1^\times .

Proposition 5.8. *In the Haar measure μ_1^\times*

$$(5.19) \quad \text{vol}(\mathbf{Q}_{A_1}^\times / \mathbf{Q}^\times) = 1.$$

Proof. This follows from the structure of the fundamental domain as described in the proof of Proposition 5.6. In fact the isomorphism (5.13) is measure preserving if the product on the right had side is equipped with the product measure, which has the full volume 1. \square

6. Number fields and integral elements.

Definition 6.1. A *number field* is a finite field extension $k \supset \mathbf{Q}$, i.e. k is a field which includes \mathbf{Q} as a subfield, and $\dim_{\mathbf{Q}} k < \infty$. The positive integer $[k : \mathbf{Q}] = \dim_{\mathbf{Q}} k$ is called the *degree* of the extension.

More generally, a field k_1 is called an *extension* of a field k_2 if $k_1 \supset k_2$, and the positive integer $[k_1 : k_2] = \dim_{k_2} k_1$ is called the *degree* of this extension. An extension is called *finite* if its degree is finite.

If $k_1 \supset k_2 \supset k_3$ where both inclusions are finite field extensions, then

$$(6.1) \quad [k_1 : k_3] = [k_1 : k_2][k_2 : k_3].$$

Indeed, if $\alpha_1, \dots, \alpha_r$ is a basis of k_1 as a vector space over k_2 , and β_1, \dots, β_s is a basis of k_2 as a vector space over k_3 (hence $r = [k_1 : k_2]$ and $s = [k_2 : k_3]$), then $\{\alpha_i \beta_j\}$ form a basis of k_1 as a vector space over k_3 .

Definition 6.2. Let $k \supset \mathbf{Q}$ be a number field. An element $\alpha \in k$ is called an *integral element* (over \mathbf{Z}) if α is a root of a monic polynomial with coefficients in \mathbf{Z} , i.e. there exist $n \in \mathbf{Z}$, $n > 0$, and $a_0, \dots, a_{n-1} \in \mathbf{Z}$, such that

$$(6.2) \quad \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0.$$

Denote the set of all integral elements of k by \mathcal{O}_k .

Examples. 1) If $k = \mathbf{Q}$ then $\mathcal{O}_k = \mathbf{Z}$. This means that if $\alpha \in \mathbf{Q}$ is a root of a monic polynomial with integer coefficients, then in fact $\alpha \in \mathbf{Z}$. Indeed, assume that $\alpha = r/s$ with $r, s \in \mathbf{Z}$ mutually prime, $|s| > 1$, and α satisfies (6.2). Then, multiplying (6.2) by s^n we come to a contradiction because all terms on the left will be integers divisible by s , except the first one which will be equal to r^n .

2) Consider $k = \mathbf{Q} + \mathbf{Q}[\sqrt{2}]$. Assume that $\alpha = a + b\sqrt{2} \in \mathcal{O}_k$ i.e. $a, b \in \mathbf{Q}$ and α is a root of a monic polynomial $P(t) \in \mathbf{Z}[t]$. Then $\bar{\alpha} = a - b\sqrt{2}$ also satisfies this equation, therefore $P(t)$ is divisible by the irreducible (over \mathbf{Q}) polynomial

$$(t - \alpha)(t - \bar{\alpha}) = t^2 - 2at + (a^2 - 2b^2).$$

It follows that $2a, a^2 - 2b^2 \in \mathbf{Z}$. Using divisibility arguments, it is easy to deduce that in fact a, b should be integers too. Therefore we can conclude that $\mathcal{O}_k = \mathbf{Z} + \mathbf{Z}\sqrt{2}$.

3) If $k = \mathbf{Q} + \mathbf{Q}[\sqrt{5}]$ then it is easy to see, using the same arguments as in the previous example, that $\mathcal{O}_k = \frac{1}{2}\mathbf{Z} + \frac{1}{2}\mathbf{Z}[\sqrt{5}]$.

4) Consider $k = \mathbf{Q} + \mathbf{Q}[\sqrt{-1}]$. Then arguments similar to the ones in the second example show that $\mathcal{O}_k = \mathbf{Z} + \mathbf{Z}[\sqrt{-1}]$.

Proposition 6.3. *Let $k \supset \mathbf{Q}$ be a number field. For any $\alpha \in k$ there exists $N \in \mathbf{Z}$, $N > 0$, such that $N\alpha \in \mathcal{O}_k$.*

Proof. Note that any $\alpha \in k$ satisfies an equation of the form (6.2) with coefficients $a_j \in \mathbf{Q}$ and with $n = [k : \mathbf{Q}]$, because $1, \alpha, \alpha^2, \dots, \alpha^n$ should be linearly dependent over \mathbf{Q} . Multiplying such an equation by N^n where N is the product of all denominators of the non-zero coefficients a_j , we see that $N\alpha \in \mathcal{O}_k$. \square

Lemma 6.4. *Let $k \supset \mathbf{Q}$ be a number field and $\alpha \in k$. Then α is integral over \mathbf{Z} if and only if there exists a non-zero finitely generated \mathbf{Z} -module (abelian subgroup) $M \subset k$ such that $\alpha M \subset M$.*

Proof. If α is integral and satisfies (6.2) (with coefficients $a_j \in \mathbf{Z}$), then we can take $M = \mathbf{Z} \cdot 1 + \mathbf{Z} \cdot \alpha + \dots + \mathbf{Z} \cdot \alpha^{n-1}$.

Vice versa, assume that $M \subset k$ is generated by $v_1, \dots, v_n \in k$ as an abelian subgroup. Then we should have

$$\alpha v_1 = c_{11}v_1 + \dots + c_{1n}v_n$$

...

$$\alpha v_n = c_{n1}v_1 + \dots + c_{nn}v_n$$

where $c_{ij} \in \mathbf{Z}$. It follows that $(\det(\alpha\delta_{ij} - c_{ij}))v_m = 0$ for all $m = 1, \dots, n$. Since at least one of v_m should be non-zero, we obtain $\det(\alpha\delta_{ij} - c_{ij}) = 0$, therefore α is integral. \square

Proposition 6.5. *\mathcal{O}_k is a subring in k .*

Proof. Let us take $\alpha, \beta \in \mathcal{O}_k$, and find finitely generated abelian subgroups $M, N \subset k$ such that $\alpha M \subset M, \beta N \subset N$. Let MN denote the abelian subgroup in k generated by products $xy, x \in M, y \in N$. Clearly MN is finitely generated. Also $(\alpha \pm \beta)MN \subset MN$ and $(\alpha\beta)MN \subset MN$ which proves that $\alpha \pm \beta, \alpha\beta \in \mathcal{O}_k$ due to Lemma 6.4. \square

Definition 6.6. Let $k \supset \mathbf{Q}$ be a number field. The *trace* on k is a \mathbf{Q} -linear map

$$\mathrm{Tr} = \mathrm{Tr}_{\mathbf{Q}}^k : k \longrightarrow \mathbf{Q}$$

defined by the formula

$$(6.3) \quad \mathrm{Tr}(\alpha) = \mathrm{Tr} M_\alpha ,$$

where $M_\alpha : k \rightarrow k$ is the \mathbf{Q} -linear multiplication by α map, i.e. $M_\alpha x = \alpha x, x \in k$.

The *norm* of $\alpha \in k$ is defined by the formula

$$(6.4) \quad N(\alpha) = N_{\mathbf{Q}}^k(\alpha) = \det M_\alpha .$$

It has the property

$$(6.5) \quad N(\alpha\beta) = N(\alpha)N(\beta), \quad \alpha, \beta \in k ,$$

i.e. the norm defines a group homomorphism $N : k^\times \rightarrow \mathbf{Q}^\times$.

Proposition 6.7. Let $k \supset \mathbf{Q}$ be a number field. Then $\mathrm{Tr}(\alpha) \in \mathbf{Z}$ and $N(\alpha) \in \mathbf{Z}$ for any $\alpha \in \mathcal{O}_k$.

Proof. Let us fix $\alpha \in \mathcal{O}_k$. There exists a monic polynomial $P \in \mathbf{Z}[t]$ such that $P(\alpha) = 0$. We can assume that it has a minimal degree, then we will call it the *minimal polynomial* of α and denote $P_{\min}(t)$. Denote also $d = \deg P_{\min}$. The relation $P(\alpha) = 0$ is equivalent to $P(M_\alpha) = 0$. The Hamilton–Cayley theorem implies that $P_{\min}(t)$ divides the characteristic polynomial of M_α which is $\mathrm{ch}_\alpha(t) = \det(t \cdot \mathrm{Id} - M_\alpha)$. It follows that

$$d = \deg P_{\min} \leq n = \deg \mathrm{ch}_\alpha = [k : \mathbf{Q}] .$$

Note now that $P(M_\alpha) = M_{P(\alpha)}$ for any polynomial $P \in \mathbf{Q}[t]$. This implies the following specific property of the operator M_α : if $P(M_\alpha)x = 0$ for some $x \in k, x \neq 0$, then $P(\alpha) = 0$. It follows that there exists a chain of \mathbf{Q} -linear subspaces

$$\{0\} = E_0 \subset E_1 \subset \dots \subset E_s = k ,$$

such that each subspace E_j is M_α -invariant, and $\dim E_j/E_{j-1} = d, j = 1, \dots, s$. The restriction of M_α on E_j/E_{j-1} has the characteristic polynomial P_{\min} , so $\mathrm{ch}_\alpha = (P_{\min})^s$, and in particular d divides n .

It follows that $\mathrm{ch}_\alpha \in \mathbf{Z}[t]$. The desired statement follows because both $\mathrm{Tr}(\alpha)$ and $N(\alpha)$ are coefficients of ch_α . \square

Proposition 6.8. *The map $x, y \mapsto B(x, y) = \text{Tr}(xy)$ is a symmetric non-degenerate \mathbf{Q} -bilinear form $B : k \times k \rightarrow \mathbf{Q}$.*

Proof. The symmetry of B is obvious, and the non-degeneracy follows from the fact that for any $x \in k$, $x \neq 0$, we can take $y = x^{-1}$, and then $\text{Tr}(xy) = \text{Tr}(1) = n \neq 0$. \square

Proposition 6.9. *Let $k \supset \mathbf{Q}$ be a number field. Then \mathcal{O}_k is finitely generated as an abelian group, namely $\mathcal{O}_k \cong \mathbf{Z}^n$ where $n = [k : \mathbf{Q}]$.*

Proof. Due to Proposition 6.3 we can choose elements $v_1, \dots, v_n \in \mathcal{O}_k$ which are linearly independent over \mathbf{Q} . They generate a free abelian subgroup $\Gamma \subset \mathcal{O}_k$ which is isomorphic to \mathbf{Z}^n .

Now using the form B from Proposition 6.8 define the following characteristic of Γ :

$$(6.6) \quad \text{vol}(\Gamma) = |\det(B(v_i, v_j))| \in \mathbf{Z}.$$

It is easy to see that $\text{vol}(\Gamma) > 0$ and $\text{vol}(\Gamma)$ does not depend on the choice of the basis v_1, \dots, v_n . Now assuming that Γ_1 is another subgroup in \mathcal{O}_k with the same properties, such that $\Gamma_1 \supset \Gamma$, we easily obtain that $\text{vol}(\Gamma_1)$ divides $\text{vol}(\Gamma)$ and $\text{vol}(\Gamma_1) < \text{vol}(\Gamma)$ provided $\Gamma_1 \neq \Gamma$. It follows that there exists a maximal group Γ with the above properties. Then clearly $\Gamma = \mathcal{O}_k$. \square

Corollary 6.10. *The pair $\mathcal{O}_k \subset k$ is isomorphic to the pair $\mathbf{Z}^n \subset \mathbf{Q}^n$ in the category of abelian groups.*

This means that \mathcal{O}_k is a lattice in k , situated exactly as \mathbf{Z}^n in \mathbf{Q}^n .

Proposition 6.11. *\mathcal{O}_k is the largest subring in k which is finitely generated as an abelian group. More precisely, if R is a subring in k which is finitely generated as an abelian group, then $R \subset \mathcal{O}_k$.*

Proof. If $\alpha \in R$, then the abelian subgroup Γ_α generated by $\{1, \alpha, \alpha^2, \dots\}$, should be finitely generated. This implies that in fact Γ_α is generated by $\{1, \alpha, \alpha^2, \dots, \alpha^{N-1}\}$ for a sufficiently large N . It follows that α is a root of a monic polynomial $P \in \mathbf{Z}[t]$ of degree N . Hence $R \subset \mathcal{O}_k$. \square

7. Arithmetic of ideals.

Everywhere in this section a ring will mean a commutative ring with a unit element which will be denoted by 1. Let us recall that an ideal I in a ring R is an abelian subgroup $I \subset R$ such that $ab \in I$ for any $a \in R$ and $b \in I$. In other words I should be a submodule of R which is considered as R -module. An ideal I is called *proper* if $I \neq R$.

Proposition 7.1. *Let $k \supset \mathbf{Q}$ be a number field, I a non-zero ideal in \mathcal{O}_k . Then $I \cap \mathbf{Z} \neq \{0\}$.*

Proof. Let us take $\alpha \in I$, $\alpha \neq 0$, and consider the multiplication operator $M_\alpha : k \rightarrow k$, $M_\alpha x = \alpha x$. Then $M_\alpha(\mathcal{O}_k) \subset \mathcal{O}_k$ because \mathcal{O}_k is a subring in k . Using Corollary 6.10 we can choose a basis in k (over \mathbf{Q}) such that in this basis M_α is given by a matrix with entries from \mathbf{Z} . Let $\text{ch}_\alpha(t)$ be the characteristic polynomial of M_α . It follows that $\text{ch}_\alpha \in \mathbf{Z}[t]$, so

$$\text{ch}_\alpha(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0, \quad a_0, \dots, a_{n-1} \in \mathbf{Z}.$$

Note that $a_0 = \det(M_\alpha) \neq 0$. By the Hamilton–Cayley theorem we obtain $\text{ch}_\alpha(M_\alpha) = 0$ or, equivalently, $\text{ch}_\alpha(\alpha) = 0$. Therefore,

$$a_0 = -\alpha^n - a_{n-1}\alpha^{n-1} - \dots - a_1\alpha \in I. \quad \square$$

Corollary 7.2. *For any proper non-zero ideal $I \subset \mathcal{O}_k$ the quotient ring \mathcal{O}_k/I is finite.*

Proof. Let us take $a \in I \cap \mathbf{Z}$, $a \neq 0$. We can assume $a > 0$. Then

$$\mathcal{O}_k \supset I \supset a\mathcal{O}_k.$$

Let us use an isomorphism of abelian groups $\mathcal{O}_k \cong \mathbf{Z}^n$ (Proposition 6.9). Then

$$\text{Card}(\mathcal{O}_k/I) \leq \text{Card}(\mathcal{O}_k/a\mathcal{O}_k) = \text{Card}(\mathbf{Z}^n/a\mathbf{Z}^n) = a^n. \quad \square$$

Let us recall that a proper non-zero ideal I in a ring R is called *prime* if $a, b \in R$ and $ab \in I$ imply that either $a \in I$ or $b \in I$. In other words I is prime if $I \neq \{0\}$, I is proper and the ring R/I is an integral domain, i.e. has no zero-divisors. A proper ideal $I \subset R$ is called *maximal* if it is not contained in any larger proper ideal or, equivalently, if R/I is a field.

Lemma 7.3. *Any finite integral domain is a field.*

Proof. If R is a finite integral domain, then for any $a \in R$ the map M_a of multiplication by a in R is injective, hence bijective. \square

Proposition 7.4. *Let $k \supset \mathbf{Q}$ be a number field. Then every prime ideal in \mathcal{O}_k is maximal.*

Proof. The result follows from Corollary 7.2 and Lemma 7.3. \square

Recall that any ideal I in \mathbf{Z} is a principal ideal i.e. there exist $a \in \mathbf{Z}$ such that $I = (a) = a\mathbf{Z}$. The ideal (a) is prime if and only if the integer $|a|$ is prime.

Proposition 7.5. (i) *Let \mathcal{P} be a prime ideal in \mathcal{O}_k . Then $\mathcal{P} \cap \mathbf{Z} = (p)$ for a prime $p \in \mathbf{Z}$.*
(ii) *If p is as above, then $\mathcal{O}_k/\mathcal{P} \supset \mathbf{Z}/(p)$ is a finite field extension.*
(iii) *If \mathcal{P} and p are as above, then $\text{Card}(\mathcal{O}_k/\mathcal{P}) = p^f$, where $f = f(\mathcal{P})$ is a positive integer.*

Proof. (i) follows from the fact that $\mathcal{P} \cap \mathbf{Z}$ is a prime ideal in \mathbf{Z} .

(ii) is obvious due to Corollary 7.2 and Proposition 7.4.

To prove (iii) note that $\mathcal{O}_k/\mathcal{P}$ is a vector space over $\mathbf{Z}/(p)$, therefore it has p^f elements where f is its dimension. \square

Definition 7.6. For any proper non-zero ideal $I \subset \mathcal{O}_k$ its *norm* is

$$(7.1) \quad N(I) = \text{Card}(\mathcal{O}_k/I).$$

In particular, if \mathcal{P} is a prime ideal in \mathcal{O}_k , then

$$N(\mathcal{P}) = p^{f(\mathcal{P})},$$

where $p, f(\mathcal{P})$ are as in Proposition 7.5.

Let us recall definitions of operations on ideals in a ring R . If I_1, I_2 are such ideals, then their sum is another ideal

$$I_1 + I_2 = \{x + y \mid x \in I_1, y \in I_2\} \subset R.$$

The product $I_1 I_2$ is defined as an abelian group generated by all elements $xy \in R$ such that $x \in I_1, y \in I_2$. Clearly $I_1 I_2$ is again an ideal in R . Also the intersection $I_1 \cap I_2$ is an ideal in R , and $I_1 I_2 \subset I_1 \cap I_2$.

The sum, product and intersection of ideals are associative and commutative operations, so the sum, product and intersection of any finite set of ideals is well defined. In particular I^n is a well defined ideal in the ring R for any ideal $I \subset R$ and any positive integer n .

Let us recall that a commutative ring R is called *Noetherian* if every ideal $I \subset R$ is finitely generated as R -module. It is easy to see that R is Noetherian if and only if any increasing sequence of ideals in R

$$(7.2) \quad I_1 \subset I_2 \subset I_3 \subset \dots$$

such that $I_k \neq I_{k+1}$ for all $k = 1, 2, \dots$, is in fact finite. Indeed, if every ideal is finitely generated, then the union of the ideals in (7.2), which is also an ideal, should be finitely generated, hence its generators belong to I_k for some k , therefore the sequence (7.2) is finite. Vice versa, if every sequence (7.2) is finite, we can easily construct finite set of generators of an arbitrary ideal I . Namely, start with $I_1 = (a_1)$ where $a_1 \in I \setminus \{0\}$. If $I_1 \neq I$, pick up $a_2 \in I \setminus I_1$ and consider an ideal $I_2 = (a_1, a_2)$ which is generated by a_1, a_2 etc. At the end we will obtain a set of generators $\{a_1, a_2, \dots, a_N\}$ for I .

Proposition 7.7. *Let $k \supset \mathbf{Q}$ be a number field. Then the ring \mathcal{O}_k is Noetherian.*

Proof. Any ideal $I \subset \mathcal{O}_k$ is in particular an abelian subgroup in $\mathcal{O}_k \cong \mathbf{Z}^n$. It is easy to see that a strictly increasing chain of abelian subgroups in \mathbf{Z}^n should be finite (see e.g. an argument given in the proof of Proposition 6.9.) \square

The following theorem is a generalization of the prime factorization theorem for usual integers.

Theorem 7.8. (i) *Let $k \supset \mathbf{Q}$ be a number field. Then any proper non-zero ideal $I \subset \mathcal{O}_k$ has a prime decomposition*

$$(7.3) \quad I = \prod_{i=1}^s \mathcal{P}_i^{n_i},$$

where $\mathcal{P}_1, \dots, \mathcal{P}_s$ are different prime ideals in \mathcal{O}_k , $n_i \in \mathbf{Z}$, $n_i > 0$. Here the set $\{\mathcal{P}_1, \dots, \mathcal{P}_s\}$ is exactly the set of prime ideals \mathcal{P} in \mathcal{O}_k such that $\mathcal{P} \supset I$.

(ii) *The decomposition (7.3) is unique up to the order of factors.*

For the proof of this non-trivial theorem see e.g. [L2], Ch.1, Sect.6.

Proposition 7.9. (Chinese Remainder Theorem) *Let R be a ring, I_1, \dots, I_m its ideals such that $I_j + I_k = R$ for all $j \neq k$. Then given arbitrary elements $x_1, \dots, x_m \in R$, there exists $x \in R$ such that $x - x_j \in I_j$ for all $j = 1, \dots, m$.*

Proof. We will use induction with respect to m . The statement is obvious for $m = 1$. If $m = 2$, we can write $1 = a_1 + a_2$ for some $a_j \in I_j$, $j = 1, 2$. Then we can take $x = x_2 a_1 + x_1 a_2$. Indeed, taking into account the relations $x_j = x_j a_1 + x_j a_2$, $j = 1, 2$, we immediately obtain that $x - x_j \in I_j$, $j = 1, 2$.

Now for each $j \in \{2, \dots, m\}$ we can find elements $a_j \in I_1$ and $b_j \in I_j$ such that $a_j + b_j = 1$. Then the product $\prod_{j=2}^m (a_j + b_j)$ equals 1 but it is on the other hand in $I_1 + \prod_{j=2}^m I_j$. Using already established particular case $m = 2$, we can find $y_1 \in R$ such that

$$y_1 - 1 \in I_1, \quad y_1 \in \prod_{j=2}^m I_j.$$

In particular, $y_1 \in I_j$ for all $j = 2, \dots, m$.

Similarly we can find elements y_2, \dots, y_m , such that

$$y_j - 1 \in I_j; \quad y_j \in I_k \text{ for all } k \neq j.$$

Now we can take $x = x_1 y_1 + \dots + x_m y_m$. \square

Remark 1. The construction in the proof above can be geometrically interpreted as follows. Let us interpret the ideals I_1, \dots, I_m as “points”, and any element $x \in R$ as a “function” on the set of the “points”, so that the value of x at I_j is $x \bmod I_j = x + I_j \in R/I_j$. Then the elements y_1, \dots, y_m constitute a “partition of unity” on the set of all points.

Remark 2. Let us consider a particular case $R = \mathbf{Z}$, $I_j = (a_j)$ where a_1, \dots, a_m are positive integers. The condition $I_j + I_k = \mathbf{Z}$ is equivalent to saying that a_j and a_k are mutually prime. The result says then that for any $x_1, \dots, x_m \in \mathbf{Z}$ there exists $x \in \mathbf{Z}$ such that $x \equiv x_j \pmod{a_j}$, $j = 1, \dots, m$.

Let us give a more elementary proof for this particular case. It is clear that that the relations $x \equiv x_j \pmod{a_j}$ depend only on $x \bmod a_1 \dots a_m$. Consider a map

$$\begin{aligned} \mathbf{Z}/(a_1 \dots a_m) &\longrightarrow \mathbf{Z}/(a_1) \times \dots \times \mathbf{Z}/(a_m) \\ x \bmod (a_1 \dots a_m) &\longmapsto (x \bmod a_1, \dots, x \bmod a_m) \end{aligned}$$

This map is injective which means that if $x \in \mathbf{Z}$ and $x \in (a_j)$ for all j , then $x \in (a_1 \dots a_m)$, which is true because a_j and a_k are mutually prime for $j \neq k$. Therefore this map is surjective because both groups $\mathbf{Z}/(a_1 \dots a_m)$ and $\mathbf{Z}/(a_1) \times \dots \times \mathbf{Z}/(a_m)$ have $a_1 \dots a_m$ elements.

The last argument is generalized in the following

Proposition 7.10. *Let R be a ring, I_1, \dots, I_m its ideals such that $I_j + I_k = R$ for all $j \neq k$. Let*

$$(7.4) \quad f : R \longrightarrow \prod_{j=1}^m R/I_j = (R/I_1) \times \dots \times (R/I_m)$$

be the map which is induced by the canonical surjections of R onto R/I_j for each j . Then

$$(7.5) \quad \text{Ker } f = \bigcap_{j=1}^m I_j = \prod_{j=1}^m I_j ,$$

and f is surjective, so it induces an isomorphism

$$(7.6) \quad R / \left(\prod_{j=1}^m I_j \right) \cong \prod_{j=1}^m R/I_j .$$

Proof. It is obvious that $\text{Ker } f$ is the intersection of all I_j , and the surjectivity follows from the Chinese Remainder Theorem. So it remains to establish that $\bigcap_{j=1}^m I_j = \prod_{j=1}^m I_j$. Let us do it by induction with respect to m .

The claim is obvious for $m = 1$. Let us consider the case $m = 2$. It is easy to see that for any two ideals $I_1, I_2 \subset R$

$$(I_1 + I_2)(I_1 \cap I_2) \subset I_1 I_2 .$$

Therefore $I_1 + I_2 = R$ implies $(I_1 \cap I_2) \subset I_1 I_2$ and the inverse inclusion is obvious, so $(I_1 \cap I_2) = I_1 I_2$.

Now an argument given in the proof of the Chinese Remainder Theorem shows that under the assumptions above

$$I_1 + \prod_{j=2}^m I_j = R .$$

Using the induction assumption we obtain

$$\bigcap_{j=1}^m I_j = I_1 \cap \prod_{j=2}^m I_j = \prod_{j=1}^m I_j . \quad \square$$

Proposition 7.11. *Let R be a ring, I_1, \dots, I_m its ideals such that*

$$(7.7) \quad I_1 + \dots + I_m = R .$$

Then

$$(7.8) \quad I_1^{n_1} + \dots + I_m^{n_m} = R$$

for any positive integers n_1, \dots, n_m .

Proof. The relation (7.7) is equivalent to the existence of elements $a_j \in I_j$, $j = 1, \dots, m$, such that $a_1 + \dots + a_m = 1$. But then $(a_1 + \dots + a_m)^N = 1$ for any positive integer N . Taking $N \geq n_1 + \dots + n_m$ and opening brackets, we see that there exist $b_j \in I_j^{n_j}$, $j = 1, \dots, m$, such that $b_1 + \dots + b_m = 1$. This implies (7.8). \square

Lemma 7.12. *Let $k \supset \mathbf{Q}$ be a number field, I_1, \dots, I_m ideals in \mathcal{O}_k such that $I_j + I_k = \mathcal{O}_k$ for any j, k with $j \neq k$. Then*

$$(7.9) \quad N\left(\prod_{j=1}^m I_j\right) = \prod_{j=1}^m N(I_j).$$

Proof. The result immediately follows from the isomorphism (7.6) in Proposition 7.10. \square

Now let us point out another case of multiplicativity of the norm on ideals.

Lemma 7.13. *Let \mathcal{P} is a prime ideal in \mathcal{O}_k . Then*

$$(7.10) \quad N(\mathcal{P}^k) = (N(\mathcal{P}))^k$$

for any integer $k \geq 1$.

Proof. (i) Let us consider a chain of ideals

$$(7.11) \quad \mathcal{O}_k = \mathcal{P}^0 \supset \mathcal{P} = \mathcal{P}^1 \supset \mathcal{P}^2 \supset \dots \supset \mathcal{P}^k.$$

Let us prove first that there are no intermediate ideals in this chain, i.e. if I is an ideal in \mathcal{O}_k such that $\mathcal{P}^r \supset I \supset \mathcal{P}^{r+1}$, where $r \in \{0, \dots, k-1\}$, then $I = \mathcal{P}^r$ or $I = \mathcal{P}^{r+1}$. Note first that this is obvious for $r = 0$ because the ideal \mathcal{P} is maximal. So we can assume that $r \geq 1$. Let us use Theorem 7.8 to present I as a product

$$I = \prod_{j=1}^m \mathcal{P}_j^{n_j},$$

where $\mathcal{P}_1, \dots, \mathcal{P}_m$ are prime ideals in \mathcal{O}_k , $\mathcal{P}_i \neq \mathcal{P}_j$ if $i \neq j$, and n_j are positive integers. We claim that no ideal $\mathcal{P}_j \neq \mathcal{P}$ can be present in this decomposition. Indeed, if this happens, then we should have

$$\mathcal{P}_j \supset \mathcal{P}_j^{n_j} \supset I \supset \mathcal{P}^r,$$

therefore \mathcal{P}_j should be present in the prime decomposition of \mathcal{P}^r due to Theorem 7.8. This is only possible if $\mathcal{P}_j = \mathcal{P}$ because of the uniqueness of the decomposition into the product of prime ideals.

Denote $F = \mathcal{O}_k/\mathcal{P}$, so F is a finite field. Clearly, $\mathcal{P}^r/\mathcal{P}^{r+1}$ is an F -module i.e. a vector space over F . It is obviously finite-dimensional because $\mathcal{P}^r/\mathcal{P}^{r+1} \subset \mathcal{O}_k/\mathcal{P}^{r+1}$ is finite. There is a canonical bijection between all linear subspaces of $\mathcal{P}^r/\mathcal{P}^{r+1}$ (over F) and all

intermediate ideals $\mathcal{P}^{r+1} \subset I \subset \mathcal{P}^r$. Therefore there are no non-trivial linear subspaces in $\mathcal{P}^r/\mathcal{P}^{r+1}$, hence $\dim_F \mathcal{P}^r/\mathcal{P}^{r+1} = 1$. Considering now the chain (7.11), we see that $\dim_F \mathcal{O}_k/\mathcal{P}^k = k$, hence

$$N(\mathcal{P}^k) = \text{Card}(\mathcal{O}_k/\mathcal{P}^k) = (\text{Card } F)^k = (N(\mathcal{P}))^k. \quad \square$$

Corollary 7.14. *Let I be a non-zero ideal in \mathcal{O}_k which has the prime decomposition (7.3). Then*

$$(7.12) \quad N(I) = \prod_{i=1}^s N(\mathcal{P}_i)^{n_i}.$$

Proof. The result immediately follows from Lemmas 7.12 and 7.13. \square

Corollary 7.15. *Let I_1, I_2 be arbitrary non-zero ideals in \mathcal{O}_k . Then*

$$(7.13) \quad N(I_1 I_2) = N(I_1) N(I_2).$$

Proof. The result immediately follows from Theorem 7.8 and Corollary 7.14. \square

Example 7.16. The proof of the multiplicativity of norms of ideals (Corollary 7.15) uses Theorem 7.8 and other intricate algebraic machinery. It might seem that such a simple statement should have a much simpler proof. For example one might wonder whether the multiplicativity property (7.13) is true for ideals in a ring R provided $\text{Card}(R/I) < \infty$ for every non-zero ideal $I \subset R$. The following example shows that this is not the case.

Define $R = \mathbf{Z}[\sqrt{-3}] = \mathbf{Z} + \mathbf{Z}\sqrt{-3}$. Let I be a non-zero ideal in R , $a + b\sqrt{-3} \in I \setminus \{0\}$, $a, b \in \mathbf{Z}$. Then $(a - b\sqrt{-3})(a + b\sqrt{-3}) = a^2 + 3b^2 \in I$, therefore $I \cap \mathbf{Z} \neq \{0\}$. Taking $m \in (I \cap \mathbf{Z}) \setminus \{0\}$ we see that $I \supset \{m\mathbf{Z} + m\mathbf{Z}\sqrt{-3}\}$, hence $\text{Card}(R/I) \leq m^2 < \infty$.

Now consider an ideal $\mathcal{M} \subset R$, $\mathcal{M} = (2, 1 + \sqrt{-3})$. It is easy to see that

$$\mathcal{M} = \{a + b\sqrt{-3} \mid a - b \equiv 0 \pmod{2}\},$$

so $\text{Card}(R/\mathcal{M}) = 2$ and \mathcal{M} is a maximal ideal. Now

$$\mathcal{M}^2 = (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}),$$

hence

$$\mathcal{M}^2 = \{a + b\sqrt{-3} \in R \mid a, b \text{ even, } a \equiv b \pmod{4}\}$$

and $\text{Card}(R/\mathcal{M}^2) = 8$. So if we use the norm defined on ideals I of R as $|I| = \text{Card}(R/I)$, then $N(\mathcal{M}) = 2$ and $N(\mathcal{M}^2) = 8 \neq (N(\mathcal{M}))^2$.

It follows in particular that the statement of Theorem 7.8 on the prime decomposition of ideals does not hold for the ring R .

Note that $R = \mathbf{Z}[\sqrt{-3}] \neq \mathcal{O}_k$ for $k = \mathbf{Q}[\sqrt{-3}]$. It is easy to see that in this case

$$\mathcal{O}_k = \left\{ \frac{1}{2}(a + b\sqrt{-3}) \mid a, b \in \mathbf{Z}, a \equiv b \pmod{2} \right\},$$

so \mathcal{O}_k includes R as a subring which has index 2 as an abelian subgroup.

The following proposition will be an application of the general prime decomposition of Theorem 7.8 to a special case: the ideal $p\mathcal{O}_k$.

Proposition 7.17. *Let $k \supset \mathbf{Q}$ be a number field. Let us choose a prime $p \in \mathbf{Z}$. Then*

$$(7.14) \quad p\mathcal{O}_k = \prod_{j=1}^g \mathcal{P}_j^{e_j},$$

where e_j are positive integers and the set $\{\mathcal{P}_1, \dots, \mathcal{P}_g\}$ consists of all prime ideals \mathcal{P} in \mathcal{O}_k such that $\mathcal{P} \cap \mathbf{Z} = (p)$. There is only a finite number $g = g(p)$ of prime ideals with this property. Also

$$(7.15) \quad n = \sum_{i=1}^g e_i f_i,$$

where $n = [k : \mathbf{Q}]$, e_i are the same as in (7.14) and $f_i = f(\mathcal{P}_i)$, where $f(\mathcal{P})$ is defined as in Proposition 7.5.

Proof. Theorem 7.8 implies (7.14) with the set $\{\mathcal{P}_1, \dots, \mathcal{P}_g\}$ consisting of prime ideals \mathcal{P} in \mathcal{O}_k such that $\mathcal{P} \supset p\mathcal{O}_k$. Clearly the last inclusion is equivalent to $(p) \subset \mathcal{P} \cap \mathbf{Z}$, which is, in turn, equivalent to $(p) = \mathcal{P} \cap \mathbf{Z}$ because $\mathcal{P} \cap \mathbf{Z}$ is an ideal in \mathbf{Z} and the ideal (p) is maximal.

Note that $N(p\mathcal{O}_k) = p^n$ because $\mathcal{O}_k \cong \mathbf{Z}^n$ as an abelian group. On the other hand, using Corollary 7.14, we obtain

$$N(p\mathcal{O}_k) = \prod_{i=1}^g N(\mathcal{P}_i)^{e_i} = \prod_{i=1}^g (p^{f_i})^{e_i} = p^{\sum_{i=1}^g e_i f_i}.$$

Since this should be equal to p^n , we arrive to (7.15). \square

8. Zeta functions and L -functions.

Definition 8.1. Let $k \supset \mathbf{Q}$ be a number field. Let us define its *zeta function* by the formula

$$(8.1) \quad \zeta_k(s) = \prod_{0 \neq \mathcal{P} \subset \mathcal{O}_k, \mathcal{P} \text{ prime}} (1 - N(\mathcal{P})^{-s})^{-1},$$

where the product is taken over all non-zero prime ideals in \mathcal{O}_k .

Example 8.2. If $k = \mathbf{Q}$, then $\mathcal{O}_k = \mathbf{Z}$, the prime ideals are (p) where p is a positive prime, $N((p)) = p$, and we see that $\zeta_{\mathbf{Q}}(s)$ is the Riemann zeta function

$$(8.2) \quad \zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

represented in the form of the Euler product.

The following formula is an analogue of (8.2) in the general case:

$$(8.3) \quad \zeta_k(s) = \sum_{0 \neq I \subset \mathcal{O}_k, I \text{ ideal}} N(I)^{-s},$$

the sum taken over all non-zero ideals in \mathcal{O}_k .

Proposition 8.3. *The product (8.1) and the series (8.3) are convergent if $\text{Re } s > 1$ and define the same function $\zeta_k(s)$ as a holomorphic function in the complex half-plane $\text{Re } s > 1$.*

Proof. In all future calculations p will always denote a positive prime, and \mathcal{P} a prime ideal in \mathcal{O}_k . It is sufficient to prove that the product (8.1) is convergent for all s with $\text{Re } s > 1$, then the convergence of the series (8.3) and its coincidence with (8.1) will follow if we present each factor in (8.1) as a geometric series

$$(1 - N(\mathcal{P})^{-s})^{-1} = \sum_{k=1}^{\infty} N(\mathcal{P})^{-sk}.$$

Multiplying all these series leads to (8.3) due to Theorem 7.8.

Let us divide all prime ideals by associated primes $p = p(\mathcal{P})$ defined as in Proposition 7.17, i.e so that $\mathcal{P} \cap \mathbf{Z} = (p)$. Then we obtain

$$(8.4) \quad \zeta_k(s) = \prod_p \prod_{\mathcal{P}: \mathcal{P} \cap \mathbf{Z} = (p)} (1 - N(\mathcal{P})^{-s})^{-1} = \prod_p \prod_{i=1}^{g(p)} (1 - p^{-f_i(p)s})^{-e_i(p)}.$$

To prove the convergence of the product it is sufficient to establish the convergence of the series

$$(8.5) \quad \sum_p \sum_{i=1}^{g(p)} e_i(p) p^{-f_i(p)s}.$$

Taking into account the estimates

$$f_i(p) \geq 1, \quad \sum_{i=1}^{g(p)} e_i(p) \leq \sum_{i=1}^{g(p)} e_i(p) f_i(p) = n = [k : \mathbf{Q}],$$

we see that the series (8.5) is dominated by

$$\sum_p np^{-\tau}, \quad \tau = \operatorname{Re} s,$$

and this series obviously converges when $\tau > 1$. \square

Let us choose a positive integer N and consider the ring $\mathbf{Z}/(N)$ whose elements are residues modulo N . Let $(\mathbf{Z}/(N))^\times$ is the multiplicative group of all invertible elements of this ring. The elements of this group can be identified with positive integers which are less than N and prime to N ; the multiplication is multiplication of integers modulo N . The order of the group $(\mathbf{Z}/(N))^\times$ is denoted $\varphi(N)$.

Denoting $\mathbf{C}^\times = \mathbf{C} \setminus \{0\}$, consider a homomorphism of multiplicative groups

$$(8.6) \quad \chi : (\mathbf{Z}/(N))^\times \longrightarrow \mathbf{C}^\times ,$$

which is also called a *character* of the group $(\mathbf{Z}/(N))^\times$. We will extend χ to a complex-valued function on \mathbf{Z} as follows

$$(8.7) \quad \chi(n) = \begin{cases} \chi(n \bmod N), & \text{if } (n, N) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Here (n, N) denotes the greatest common divisor of n and N .

Note that $|\chi(n)| = 0$ or 1 for all $n \in \mathbf{Z}$. Also

$$(8.8) \quad \chi(nm) = \chi(n)\chi(m) \text{ for all } n, m \in \mathbf{Z} .$$

Definition 8.4. Let us define the *L-function* associated with a character χ , by the formula

$$(8.9) \quad L(\chi, s) = \prod_p (1 - \chi(p)p^{-s})^{-1} .$$

(The product is taken over all positive primes.)

Using the same argument as in the proof of Proposition 8.3, we easily see that the product (8.9) converges for all s with $\operatorname{Re} s > 1$ and for these s we also have

$$(8.10) \quad L(\chi, s) = \sum_{n=1}^{\infty} \chi(n)n^{-s} .$$

The series in (8.10) is an example of a Dirichlet series.

Example 8.5. Consider the field k of Gaussian numbers: $k = \mathbf{Q}(i) = \mathbf{Q}[i] = \mathbf{Q} + \mathbf{Q}i$, where $i = \sqrt{-1}$. Then $\mathcal{O}_k = \mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i$ (the ring of Gaussian integers) and $n = [k : \mathbf{Q}] = 2$. Consider a prime $p \in \mathbf{Z}$ and the ideal $p\mathcal{O}_k$, and let us try to describe the decomposition

of $p\mathcal{O}_k$ into the product of prime ideals. Using the relation (7.15) from Proposition 7.17, we see that the number of prime ideals can not be greater than 2, i.e $g \leq 2$, and there are the following possibilities:

- (a) $g = 1$, $e_1 = 2$, $f_1 = 1$, i.e. $p\mathcal{O}_k = \mathcal{P}^2$, where \mathcal{P} is a prime ideal in \mathcal{O}_k (“ramified” case);
- (b) $g = 2$, $e_1 = e_2 = f_1 = f_2 = 1$, i.e. $p\mathcal{O}_k = \mathcal{P}_1\mathcal{P}_2$, where $\mathcal{P}_1, \mathcal{P}_2$ are different prime ideals in \mathcal{O}_k (“split” case);
- (c) $g = 1$, $e_1 = 1$, $f_1 = 2$, i.e. $p\mathcal{O}_k = \mathcal{P}$, where \mathcal{P} is a prime ideal in \mathcal{O}_k ($p\mathcal{O}_k$ “remains prime”).

Let us investigate how the primes $p \in \mathbf{Z}$ distribute between the cases (a), (b), (c).

Note that $\mathcal{O}_k = \mathbf{Z}[i] = \mathbf{Z}[X]/(X^2 + 1)$ and $\mathbf{Z}[i]/(p\mathbf{Z}[i]) = (\mathbf{Z}/(p))[X]/(X^2 + 1)$.

Lemma 8.6. *In the notations above*

- (a) holds if and only if $X^2 + 1 = (X - a)^2 \pmod p$ for some $a \in \mathbf{Z}$;
- (b) holds if and only if $X^2 + 1 = (X - a)(X - b) \pmod p$, where $a, b \in \mathbf{Z}$, $a \not\equiv b \pmod p$;
- (c) holds if and only if $X^2 + 1$ is irreducible $\pmod p$.

Here the equality of polynomials $\pmod p$ means equality of all coefficients $\pmod p$.

Proof. Denote $\mathcal{O}_{k,p} = \mathcal{O}_k/(p) = \mathbf{Z}[i]/(p\mathbf{Z}[i]) = (\mathbf{Z}/(p))[X]/(X^2+1)$. The ideals $I \supset (p)$ in \mathcal{O}_k are in one-one correspondence with the ideals $I_p \subset \mathcal{O}_{k,p}$. But $\mathcal{O}_{k,p}$ is a 2-dimensional vector space over $\mathbf{Z}/(p)$, so a proper ideal in $\mathcal{O}_{k,p}$ can be either $\{0\}$ or 1-dimensional subspace in $\mathcal{O}_{k,p}$. In the first case the corresponding ideal in \mathcal{O}_k is just the principal ideal $(p) = p\mathcal{O}_k$. In the second case the ideal I_p should be a one-dimensional subspace in $\mathcal{O}_{k,p}$. It can not coincide with $\mathbf{Z}/(p)$ because this is not ideal, hence it is generated by $X - a \pmod p$, where $a \in \mathbf{Z}/(p)$. The statement of the Lemma immediately follows. \square

It is possible to describe explicitly the distribution of primes p between the categories (a), (b), (c) above.

Clearly, (a) holds if and only if there exists $a \in \mathbf{Z}$ such that $a^2 \equiv 1 \pmod p$ and $2a \equiv 0 \pmod p$. This is true if $p = 2$, and not true for any odd p .

The case (b) can be obviously characterized by the conditions:

- (b’): p is odd, and there exists $a \in \mathbf{Z}/(p)$ such that $a^2 = -1$.

Indeed, according to our consideration of the case (a), p is odd if and only if the equation $x^2 + 1 = 0$ can not have a double root in $\mathbf{Z}/(p)$, so if we require that it *has* a root, then it has in fact 2 distinct roots.

So (b) takes place if and only if -1 is a square $\pmod p$. The description of such p is a particular case of the famous quadratic reciprocity law (the Gauss Theorema Aureum) - see e.g. an elementary exposition in [I-R]. The result is

Proposition 8.7. *-1 is a square $\pmod p$ if and only if either $p = 2$ or p is odd and $(-1)^{(p-1)/2} = 1$ (or, in other words, $p \equiv 1 \pmod 4$).*

Let us sketch the use of the *Legendre quadratic symbol* which is defined as follows:

$$(8.11) \quad \left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \pmod{p}; \\ 1, & \text{if } a \equiv b^2 \pmod{p}, \ b \in \mathbf{Z}; \\ -1, & \text{otherwise.} \end{cases}$$

Here $a, p \in \mathbf{Z}$, p is a prime.

It depends only on $a \pmod{p}$ and has the following properties:

$$(8.12) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right);$$

$$(8.13) \quad a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

(Note that if $a \not\equiv 0 \pmod{p}$ then by the small Fermat theorem $a^{p-1} \equiv 1 \pmod{p}$, so

$$(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Therefore obviously $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.)

In particular, (8.13) implies that

$$(8.14) \quad \left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

The statement of Proposition 8.7 is equivalent to (8.14).

Summing up, we conclude that a prime p falls into a category (a), (b) or (c) above if and only if $p = 2$, $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$ respectively.

Now we are in a position to calculate the zeta function of the Gauss number field $k = \mathbf{Q}[i]$ by use of (8.4). We obtain

$$\begin{aligned} \zeta_k(s) &= \prod_p \prod_{\mathcal{P} \cap \mathcal{O}_k = (\mathcal{P})} (1 - N(\mathcal{P})^{-s})^{-1} = (1 - 2^{-s})^{-1} \prod_{p \equiv 1 \pmod{4}} (1 - p^{-s})^{-2} \prod_{p \equiv 3 \pmod{4}} (1 - p^{-2s})^{-1} \\ &= \zeta_{\mathbf{Q}}(s) \prod_{p \equiv 1 \pmod{4}} (1 - p^{-s})^{-1} \prod_{p \equiv 3 \pmod{4}} (1 + p^{-s})^{-1} = \zeta_{\mathbf{Q}}(s) L(\chi, s), \end{aligned}$$

where $\chi : (\mathbf{Z}/(4))^\times \rightarrow \{\pm 1\}$ is the only non-trivial character of the group $(\mathbf{Z}/(4))^\times$ (which has the order 2), namely, $\chi(1 \pmod{4}) = 1$, $\chi(3 \pmod{4}) = -1$, the L -function $L(\chi, s)$ is defined by (8.9) or (8.10). We can also rewrite this formula as

$$(8.15) \quad \zeta_k(s) = (1 - 2^{-s})^{-1} \prod_{\chi} L(\chi, s),$$

where the product is taken over all characters $\chi : (\mathbf{Z}/(4))^\times \longrightarrow \mathbf{C}^\times$.

Our next goal will be a generalization of the Example 8.5. For any integer $N \geq 2$ consider a number field $k_N = \mathbf{Q}[\zeta_N]$ where $\zeta_N = \exp(2\pi i/N)$, $i = \sqrt{-1}$.

Definition 8.8. Let $k \supset K$ is a field extension. Its *Galois group* $\text{Gal}(k/K)$ is the group of all field automorphisms of k which are identical on K .

In a particular case $K = \mathbf{Q}$ the group $\text{Gal}(k/\mathbf{Q})$ is just the group of all automorphisms of k because any field automorphism of $k \supset \mathbf{Q}$ is automatically identical on \mathbf{Q} .

Lemma 8.9. *There is an isomorphism*

$$(8.16) \quad \text{Gal}(k_N/\mathbf{Q}) \cong (\mathbf{Z}/(N))^\times$$

which maps $\sigma \in \text{Gal}(k_N/\mathbf{Q})$ to a unique $a = a(\sigma) \in (\mathbf{Z}/(N))^\times$ such that $\sigma(\zeta_N) = \zeta_N^a$.

Proof. Clearly $\sigma(\zeta_N)$ completely determines σ . But $\sigma(\zeta_N)$ should be a primitive N^{th} root of unity, therefore it is ζ_N^a where $a \in (\mathbf{Z}/(N))^\times$ is uniquely determined by σ . Moreover, $\sigma(\zeta_N^m) = (\zeta_N^m)^a$ for any $m \in \mathbf{Z}/(N)$. It follows that the map $\sigma \mapsto a(\sigma)$ is a group homomorphism because $(\zeta_N^a)^b = \zeta_N^{ab}$. \square

Let us consider a number field $k \supset \mathbf{Q}$ and the ring of integers $\mathcal{O}_k \subset k$. Since the group $\text{Gal}(k/\mathbf{Q})$ maps \mathbf{Z} to \mathbf{Z} , its action on k restricts to an action on \mathcal{O}_k by ring automorphisms. It follows that $\text{Gal}(k/\mathbf{Q})$ acts on the set of prime ideals of \mathcal{O}_k .

Let us chose a prime $p \in \mathbf{Z}$ and consider the prime decomposition (7.14) for the ideal $p\mathcal{O}_k$. Since $\sigma(p) = p$ for any $\sigma \in \text{Gal}(k/\mathbf{Q})$, and the prime decomposition of the ideals is unique, the group $\text{Gal}(k/\mathbf{Q})$ acts on the set of prime factors $\{\mathcal{P}_1, \dots, \mathcal{P}_g\}$ by permutations.

Proposition 8.10. *The action of $\text{Gal}(k/\mathbf{Q})$ on $\{\mathcal{P}_1, \dots, \mathcal{P}_g\}$ is transitive.*

Using the notations e_j, f_j from Proposition 7.17, we obtain

Corollary 8.11. *For any prime $p \in \mathbf{Z}$ we have*

$$(8.17) \quad e_1 = \dots = e_g,$$

$$(8.18) \quad f_j = [\mathcal{O}_k/\mathcal{P}_j : \mathbf{Z}/(p)], \quad j = 1, \dots, g,$$

and

$$(8.19) \quad f_1 = \dots = f_g .$$

Proof. For any $\sigma \in \text{Gal}(k/\mathbf{Q})$

$$\prod_{j=1}^g (\sigma(\mathcal{P}_j))^{e_j} = \prod_{j=1}^g \mathcal{P}_j^{e_j} ,$$

hence $\sigma(\mathcal{P}_j) = \mathcal{P}_k$ implies $e_j = e_k$, so the equalities (8.17), (8.19) follow from Proposition 8.10. The equality (8.18) follows from Propositions 7.5 and 7.17. \square

Corollary 8.12. *Denote $e := e_1 = \dots = e_g$, $f := f_1 = \dots = f_g$. Then $efg = n = [k : \mathbf{Q}]$.*

Proof. It follows from the formula (7.15). \square

Proposition 8.13. *For all but finitely many primes $p \in \mathbf{Z}$ we have $e = 1$.*

Definition 8.14.

If $e > 1$ then p is called *ramified*.

If $e = 1$ then p is called *unramified*.

So if we take p unramified, then

$$(8.20) \quad p\mathcal{O}_k = \mathcal{P}_1 \dots \mathcal{P}_g ,$$

where $\mathcal{P}_1, \dots, \mathcal{P}_g$ are distinct prime ideals. Also $\mathcal{O}_k/\mathcal{P}_j$ is a vector space of dimension f over $\mathbf{Z}/(p)$, hence

$$(8.21) \quad \mathcal{O}_k/\mathcal{P}_j = \mathbf{F}_{p^f} ,$$

where \mathbf{F}_{p^f} is the finite field with p^f elements.

In the example 8.5 above only $p = 2$ was unramified, all odd primes were ramified.

Let us fix $\mathcal{P} = \mathcal{P}_j$ in the prime decomposition (7.14) for $p\mathcal{O}_k$. Denote

$$(8.22) \quad D(\mathcal{P}/p) = \{ \sigma \in \text{Gal}(k/\mathbf{Q}) \mid \sigma(\mathcal{P}) = \mathcal{P} \} .$$

Consider $\sigma \in D(\mathcal{P}/p)$. Then σ maps \mathcal{O}_k to \mathcal{O}_k and \mathcal{P} to \mathcal{P} , hence it induces an automorphism

$$(8.23) \quad \bar{\sigma} : \mathbf{F}_{p^f} \cong \mathcal{O}_k/\mathcal{P} \longrightarrow \mathcal{O}_k/\mathcal{P} \cong \mathbf{F}_{p^f} .$$

This automorphism is obviously trivial on $\mathbf{F}_p = \mathbf{Z}/(p)$, hence $\bar{\sigma}$ defines an element in $\text{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p)$, so we obtain a group homomorphism

$$(8.24) \quad \Phi_p : D(\mathcal{P}/p) \longrightarrow \text{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p) .$$

Proposition 8.15.

(i) Φ_p is surjective;

(ii) If p is unramified, then Φ_p is an isomorphism.

Consider the Frobenius endomorphism $\text{Frob}(p, f) \in \text{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p)$:

$$(8.25) \quad \text{Frob}_{p,f}(x) = x^p .$$

It defines a Frobenius element

$$(8.26) \quad \text{Frob}(\mathcal{P}/p) = \Phi_p^{-1}(\text{Frob}_{p,f}) \in D(\mathcal{P}/p) \subset \text{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p) .$$

Lemma 8.16. *If $\sigma \in \text{Gal}(k/\mathbf{Q})$, $\mathcal{P} \subset \mathcal{O}_k$ is a prime ideal and $\sigma(\mathcal{P}) = \mathcal{P}'$, then*

$$(8.27) \quad \text{Frob}(\mathcal{P}'/p) = \sigma \text{Frob}(\mathcal{P}/p) \sigma^{-1} .$$

Definition 8.17. A finite field extension $k \supset K$ is called *abelian* if $\text{Gal}(k/K)$ is abelian.

Corollary 8.18. *If the extension $k \supset \mathbf{Q}$ is abelian then $\text{Frob}(\mathcal{P}/p)$ depends only on p .*

Therefore we will use notation $\text{Frob}_p = \text{Frob}(\mathcal{P}/p)$ in case of abelian extension $k \supset \mathbf{Q}$.

Example 8.19. Let us take $k = k_N$ and choose a prime $p \in \mathbf{Z}$ such that p does not divide N . Then it is easy to see that $\zeta_N, \zeta_N^2, \dots, \zeta_N^{N-1}$ are still distinct mod p . We also have $\mathcal{O}_k = \mathbf{Z}[\zeta_N]$. In this case

$$(8.28) \quad \text{Frob}_p = \{\zeta \mapsto \zeta^p\} .$$

Theorem 8.20 (E.Kummer). *Every abelian extension is a subfield of $\mathbf{Q}(\zeta_N)$ for some N .*

References.

- [C-F] J.W.S. Cassels, A. Fröhlich (eds.): “Algebraic number theory”. Academic Press, 1967.
- [I-R] K. Ireland, M. Rosen: “A classical introduction to modern number theory”, Springer-Verlag, 1982.
- [K] N. Koblitz: “ p -adic numbers, p -adic analysis, and zeta-functions. Springer-Verlag, 1977.
- [L1] S. Lang: “Algebra”. Addison-Wesley, 1965.
- [L2] S. Lang: “Algebraic numbers”, Addison-Wesley, 1964.
- [V-V-Z] V.S. Vladimirov, I.V. Volovich, E.I. Zelenov: “ p -adicheskie analiz i matematicheskaya fizika”. Izdatel'skaya firma “Fiziko-matematicheskaya literatura”, VO Nauka, Moscow, 1994 (Russian). English translation: “ p -adic analysis and mathematical physics”. Series on Soviet and East European Mathematics, 1. World Scientific Publishing Co., Inc., River Edge, NJ, 1994.
- [W.A.] A. Weil: “Basic number theory”. Springer-Verlag, 1967.
- [W.H.] H. Weyl: “Algebraic theory of numbers”. Princeton University Press, 1940.