Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann
Subseries: Mathematisches Institut der Universität und Max-Planck-Institut für Mathematik, Bonn – vol. 7
Adviser: F. Hirzebruch

1205

B.Z. Moroz

Analytic Arithmetic in Algebraic Number Fields

Springer-Verlag

Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann
Subseries: Mathematisches Institut der Universität und Max-Planck-Institut für Mathematik, Bonn – vol. 7
Adviser: F. Hirzebruch

1205

B. Z. Moroz

Analytic Arithmetic in Algebraic Number Fields

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo

Author

B.Z. Moroz
Max-Planck-Institut für Mathematik, Universität Bonn
Gottfried-Claren-Str. 26, 5300 Bonn 3, Federal Republic of Germany

Mathematics Subject Classification (1980): 11D57, 11R39, 11R42, 11R44, 11R45, 22C05

ISBN 3-540-16784-6 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-16784-6 Springer-Verlag New York Berlin Heidelberg

Library of Congress Cataloging-in-Publication Data. Moroz, B.Z. Analytic arithmetic in algebraic number fields. (Lecture notes in mathematics; 1205) "Subseries: Mathematisches Institut der Universität und Max-Planck-Institut für Mathematik, Bonn – vol. 7." Bibliography: p. Includes index.
1. Algebraic number theory. I. Title. II. Series: Lecture notes in mathematics (Springer-Verlag; 1205.
QA3.L28 no. 1205 [QA247] 510 [512'.74] 86-20335
ISBN 0-387-16784-6 (U.S.)

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2146/3140-543210

Introduction.

This book is an improved version of our memoir that appeared in Bonner Mathematische Schriften, [64]. Its purpose is twofold: first, we give a complete relatively self-contained proof of the theorem concerning analytic continuation and natural boundary of Euler products (sketched in Chapter III of [64]) and describe applications of Dirichlet series represented by Euler products under consideration; secondly, we review in detail classical methods of analytic number theory in fields of algebraic numbers. Our presentation of these methods (see Chapter I) has been most influenced by the work of E. Landau, [40], [42], E. Hecke, [24], and A. Weil, [91] (cf. also [87]). In Chapter II we develop formalism of Euler products generated by polynomials whose coefficients lie in the ring of virtual characters of the (absolute) Weil group of a number field and apply it to study scalar products of Artin-Weil L-functions. This leads, in particular, to a solution of a long-standing problem concerning analytic behaviour of the scalar products, or convolutions, of L-functions Hecke "mit Grössencharakteren" (cf. [63] for the history of this problem; one may regard this note as a résumé of Chapter II, if you like). Chapter III describes applications of those scalar products to the problem of asymptotic distribution of integral and prime ideals having equal norms and to a classical problem about distribution of integral points on a variety defined by a system of norm-forms. Chapter IV is designed to relate the contents of the book to the work of other authors and to acknowledge our indebtedness to these authors.

I should like to record here my sincere gratitude to Professor P. Deligne whose remarks and encouragement helped me to complete this work. This book, as well as [64], has been written in the quiet atmosphere of the Max-Planck-Institut für Mathematik (Bonn). We are grateful to the Director of the Institute Professor F. Hirzebruch for his hospitality and support of our work. The author acknowledges the hospitality of

the Mathematisches Institut Universität Zürich, where parts of the manuscript have been prepared.

Bonn-am-Rhein, im März 1986.

Notations and conventions.

We shall use the following notations and abbreviations:

$\emptyset$	empty set
$:=$	"is defined as"
$A \setminus B$	the set theoretic difference
$\mathbb{N}$	the set of natural numbers (including zero)
$\mathbb{Z}$	the ring of natural integers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{R}$	the field of real numbers
$\mathbb{R}_+$	the set of positive real numbers
$\mathbb{C}$	the field of complex numbers
A^*	the group of invertible elements in a ring A
$\hat{G}$	the set of all the simple (continuous) characters of a (topological) group G
$\hat{k}$	a fixed algebraic closure of the field k
1	denotes the unit element in any of the multiplicative groups to be considered
$\{x \mid P(x)\}$	is the set of objects x satisfying the property $P(x)$
card S, or simply $\lvert S \rvert$,	stands for the cardinality of a finite set S;
$E \mid F$	is an extension of number fields: $E \supseteq F$
$[E:F]$	denotes the degree of $E \mid F$
$G(E \mid F)$	denotes the Galois group of a finite extension $E \mid F$
(α)	is a principal ideal generated by α
$\mathfrak{a} \mid \mathfrak{b}$	means divisor $\mathfrak{a}$ divides $\mathfrak{b}$
$\lvert \mathfrak{a} \rvert$	is the absolute norm, that is $N_{E/\mathbb{Q}}\mathfrak{a}$, of a divisor $\mathfrak{a}$ in a number field E
$\lvert x \rvert$	is the absolute value of a complex number x
$\vec{\alpha}, \vec{\chi}, \vec{k}$	stand for finite sequences (of a fixed length) of divisors, characters, fields, etc.
Im φ	is the image of the map φ

$\operatorname{Ker} \varphi$	is the kernel of the homomorphism φ
$\operatorname{Re} s$	is the real part of s in $\mathbb{C}$
$\operatorname{Im} s$	is the imaginary part of s in $\mathbb{C}$
$f \circ g$	denotes the composition of two maps, so that $(f \circ g)(a) = f(g(a))$
$\Gamma(s)$	is the Euler's gamma-function
l.c.m.	is the least common multiple
g.c.d.	is the greatest common divisor
$\rho\|_H$	denotes the restriction of a map ρ to the set H
G^c	denotes sometimes (the closure of) the commutator subgroup of a (topological) group G
$A \otimes B$	is the tensor product of A and B
$A \oplus B$	is the direct sum of A and B

References of the form: theorem I.2.3, lemma 1.1, proposition 2, corollary I.A2.1 mean theorem 3 in §2 of Chapter I, lemma 1 in §1 of the same chapter, proposition 2 in the same paragraph and corollary 1 in Appendix 2 of Chapter I, respectively; the same system is used for references to numbered formulae. Relations proved under the assumption that Riemann Hypothesis, Artin-Weil conjecture or Lindelöf Hypothesis are valid shall be marked by the letters R, AW, L, respectively, before their number.

Every paragraph is regarded as a distinct unit, a brief relatively self-contained article; thus we try to be consistent in our notations throughout a paragraph but not necessarily over the whole chapter. In the first three chapters we avoid bibliographical and historical references which are collected in the Chapter IV.

Table of contents

Chapter I. Classical background.

§1. On the multidimensional arithmetic in the sense of E. Hecke.

Let k be an algebraic number field of degree $n = [k:\mathbb{Q}]$. Consider the following objects:

v is the ring of integers of k;

S_1 and S_2 are the sets of real and complex places of k respectively, $S_\infty = S_1 \cup S_2$;

S_o is the set of prime divisors of k identified with the set of non-archimedean valuations;

$S := S_o \cup S_\infty$ is the set of all primes in k;

$r_j := |S_j|$, $j = 1,2$, so that $n = r_1 + 2r_2$;

k_p is the completion of k at p for $p \in S$;

U_p is the group of units of k_p for $p \in S_o$;

w_p is the valuation function on k_p normalised by the condition $w_p(k_p^*) = w_p(k^*) = \mathbb{Z}$, $p \in S_o$;

$I_o(k)$ is the monoid of integral ideals of k;

$I(k)$ is the group of fractional ideals of k;

$(\alpha) = \prod_{p \in S_o} p^{w_p(\alpha)}$ is the principal ideal generated by α in k^*,

we extend the valuation function w_p to I and write $\mathfrak{a} = \prod_{p \in S_o} p^{w_p(\mathfrak{a})}$ for $\mathfrak{a} \in I$;

J_k is the idèle group of k;

$C_k := J_k / k^*$ is the idèle-class group of k, where k^* is embedded diagonally in J_k;

$X := \prod_{p \in S_\infty} k_p$ is regarded as a n-dimensional $\mathbb{R}$-algebra. The group of units v^* acts freely as a discrete group of transformations on the multiplicative group X^*, the action being given by

$$x \mapsto \varepsilon x, \quad x \in X^*, \ \varepsilon \in v^*,$$

where k is embedded diagonally in X. Obviously,

$$X^* \cong (\mathbb{Z}/2\mathbb{Z})^{r_1} \times T^{r_2} \times \mathbb{R}_+^{r_1+r_2} , \tag{1}$$

where $T = \{\exp(2\pi i\varphi) \mid 0 \leq \varphi < 1\}$ denotes the unit circle in $\mathbb{C}^*$. Let m be the order of the maximal finite subgroup of k^*; by a theorem of Dirichlet,

$$v^* \cong \mathbb{Z}^{r_1+r_2-1} \times \mathbb{Z}/m\mathbb{Z} . \tag{2}$$

One can show that, in accordance with (1) and (2),

$$X^*/v^* \cong (\mathbb{Z}/2\mathbb{Z})^{r_o} \times \mathbb{R}_+ \times \mathcal{T} , \tag{3}$$

where $r_o \leq \max\{0, r_1-1\}$ and $\mathcal{T}$ is a real $(n-1)$-dimensional torus. The diagonal embedding of k into X gives rise to a monomorphism

$$f_o: k^*/v^* \to X^*/v^*$$

of the group of principal ideals of k into the group (3). Let $g: X^*/v^* \to \mathcal{T}$ denote the natural projection map of X^*/v^* on the torus $\mathcal{T}$. The composition of these maps $g \cdot f_o$ can be continued to a homomorphism

$$f: I(k) \to \mathcal{T} , \quad f_{|P_k} = g \cdot f_o , \tag{4}$$

where $P_k := k^*/v^*$. Let $\mathfrak{m} \in I_o(k)$ and let $\mathfrak{m}_\infty \subseteq S_1$. One defines a subgroup

$$I(\mathfrak{m}) = \{\mathfrak{a} \mid \mathfrak{a} \in I(k),\ w_p(\mathfrak{a}) = 1 \text{ for } p|\mathfrak{m},\ p \in S_o\}$$

of $I(k)$ and a subgroup

$$P(\mathfrak{m}) = \{(\alpha) \mid \alpha \in k^*,\ \alpha \equiv 1 (\mathfrak{m}),\ \sigma_p(\alpha) > 0 \text{ for } p \in \mathfrak{m}_\infty\}$$

of P_k, where σ_p denotes the natural embedding of k in k_p for $p \in S$, and $\tilde{\mathfrak{m}} := (\mathfrak{m}, \mathfrak{m}_\infty)$. The ray class group

$$H(\tilde{\mathfrak{m}}) := I(\mathfrak{m})/P(\tilde{\mathfrak{m}})$$

is a finite group of order

$$|H(\tilde{\mathfrak{m}})| = h\varphi(\tilde{\mathfrak{m}}),$$

where

$$h = |H(1,\emptyset)|\ ,\quad H(1,\emptyset) = I(k)/P_k$$

are the class number and the class group of k respectively, and

$$\varphi(\tilde{\mathfrak{m}}) := \text{card } (I(\mathfrak{m}) \cap P_k)/P(\tilde{\mathfrak{m}}).$$

For a smooth subset τ of $\mathcal{T}$ and a ray class A in $H(\tilde{\mathfrak{m}})$ one defines two functions

$$\iota(\cdot;A,\tau): \mathbb{R}_+ \to \mathbb{N}\ ,$$
$$\pi(\cdot;A,\tau): \mathbb{R}_+ \to \mathbb{N}\ ,$$

by letting

$$\iota(x;A,\tau) = \text{card } \{\mathfrak{a} \mid \mathfrak{a} \in A \cap I_o,\ f(\mathfrak{a}) \in \tau, |\mathfrak{a}| < x\}$$

and

$$\pi(x;A,\tau) = \text{card}\,\{p \mid p \in A \cap S_o,\ f(p) \in \tau,\ |p| < x\}.$$

We are interested in obtaining asymptotic estimates for $\iota(x;A,\tau)$ and $\pi(x;A,\tau)$ as $x \to \infty$. To this end one defines grossencharacters and studies L-functions associated with these characters.

A <u>grossencharacter modulo</u> $\tilde{\mathfrak{m}} = (\mathfrak{m}, \mathfrak{m}_\infty)$ is, by definition, a character χ of $I(\mathfrak{m})$ for which there is λ in $\hat{X}^*$ such that

$$\chi((\alpha)) = \lambda(\alpha) \quad \text{whenever} \quad \alpha \in k^*, \quad (\alpha) \in P(\tilde{\mathfrak{m}}). \tag{5}$$

Let $\tilde{\mathfrak{m}}_i = (\mathfrak{m}_i, \mathfrak{m}_{\infty i})$ and let χ_i be a grossencharacter modulo $\tilde{\mathfrak{m}}_i$, $i = 1,2$. If $\mathfrak{m}_1 \mid \mathfrak{m}_2$, $\mathfrak{m}_{\infty 1} \leq \mathfrak{m}_{\infty 2}$, and $\chi_1(\mathfrak{a}) = \chi_2(\mathfrak{a})$ for $\mathfrak{a} \in I(\mathfrak{m}_2)$, we write $\chi_1 \leq \chi_2$. A grossencharacter χ is called a <u>proper grossencharacter</u> if $\chi_1 \leq \chi$ implies $\chi_1 = \chi$. Given a proper grossencharacter χ modulo $\tilde{\mathfrak{m}} = (\mathfrak{m}, \mathfrak{m}_\infty)$ we call $\tilde{\mathfrak{m}}$ the <u>conductor</u> of χ and write

$$\tilde{\mathfrak{m}} = \widetilde{\mathfrak{f}(\chi)}, \quad \mathfrak{m} = \mathfrak{f}(\chi), \quad \mathfrak{m}_\infty = \mathfrak{f}_\infty(\chi).$$

One continues a proper grossencharacter χ to a multiplicative function $\chi: I_o(k) \cup I(\mathfrak{f}(\chi)) \to T \cup \{0\}$ by letting $\chi(\mathfrak{a}) = 0$ for $\mathfrak{a} \in I_o(k) \setminus I(\mathfrak{f}(\chi))$. To simplify our notations we write $\alpha \equiv 1(\tilde{\mathfrak{m}})$ for $\alpha \in k^*$ whenever $\alpha \equiv 1(\mathfrak{m})$, $\sigma_p(\alpha) > 0$ for $p \in \mathfrak{m}_\infty$. Let $v^*(\tilde{\mathfrak{m}}) = \{\varepsilon \mid \varepsilon \equiv 1(\tilde{\mathfrak{m}})\}$; it is a subgroup (of finite index) of v^* regarded as a transformation group of X^*. We embed $\mathbb{R}_+$ diagonally in X^*: $t \mapsto (t^{1/n}, \ldots, t^{1/n})$, $t \in \mathbb{R}_+$, $t^{1/n} \in \mathbb{R}_+$. The following result is a generalisation of (3).

Lemma 1. The character group

$$\hat{X}^*(\mathfrak{m}) = \{\lambda \mid \lambda \in X^*;\ \lambda(\varepsilon x) = \lambda(x) \text{ for } x \in X^*,\ \varepsilon \in v^*(\mathfrak{m});$$

$$\lambda(t) = 1 \quad \text{for} \quad t \in \mathbb{R}_+\}$$

is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{r_o} \times \mathbb{Z}^{n-1}$ with $r_o \leq r_1$.

Proof. For $\lambda \in \hat{X}^*$, $x \in X^*$ we have

$$\lambda(x) = \prod_{p \in S_\infty} |x_p|^{it_p} \left(\frac{x_p}{|x_p|}\right)^{a_p} \tag{6}$$

with $t_p \in \mathbb{R}_+$, $a_p \in \mathbb{Z}$; moreover $a_p \in \{0,1\}$ when $p \in S_1$. Here x_p denotes the p-component of x, so that $x_p \in k_p$. Condition $\lambda(t) = 1$ is equivalent to the equation

$$\sum_{p \in S_\infty} t_p = 0.$$

The second condition $\lambda(\varepsilon x) = \lambda(x)$ for $x \in X^*$, $\varepsilon \in v^*(\mathfrak{m})$ leads, in view of the Dirichlet theorem on units, to a system of linear equations for the exponents $\{t_p, a_p\}$. Solving these equations one finds a system of generators for $\hat{X}^*(\mathfrak{m})$. We refer for these calculations to [24] (cf. also [23], §9).

A grossencharacter χ satisfying (5) is said to be normalised if $\lambda \in \hat{X}^*(\mathfrak{m})$.

Lemma 2. For every λ in $\hat{X}^*(\mathfrak{m})$ there is a grossencharacter χ modulo $\mathfrak{m}$ such that $\chi((\alpha)) = \lambda(\alpha)$ whenever $\alpha \in k^*$ and $(\alpha) \in P(\mathfrak{m})$.

Proof. See [24] (cf. also [23], §9; [91]).

The following assertion can be easily deduced from Lemma 1 and Lemma 2.

Proposition 1. The group of normalised grossencharacters modulo $\mathfrak{m}$ is

isomorphic to

$$(\mathbb{Z}/2\mathbb{Z})^{r_o} \times \mathbb{Z}^{n-1} \times \hat{H}(\mathfrak{m}).$$

For $x \in k_p$ one writes

$$\|x\|_p = \begin{cases} |x| & \text{when } p \in S_1 \\ |x|^2 & \text{when } p \in S_2 \\ |p|^{-w_p(x)} & \text{when } p \in S_o \end{cases}$$

Let $x \in J_k$ and let x_p be the p-component of x, we set then $\|x\| = \prod_{p \in S} \|x_p\|_p$. By the product formula,

$$\|\alpha\| = 1 \quad \text{for } \alpha \in k^*,$$

therefore the map $\alpha \mapsto \|\alpha\|$ is well defined on C_k. Let

$$C_k^1 = \{\alpha \mid \alpha \in C_k, \ \|\alpha\| = 1\}$$

be the subgroup of idèle-classes having unit volume. The group C_k^1 is known to be compact. The group X^* can be identified with the subgroup $\{x \mid x \in J_k, \ x_p = 1 \text{ for } p \in S_o\}$ of J_k, so that $\mathbb{R}_+$ embedded diagonally in X^* may be regarded as a subgroup of C_k. It follows then that

$$C_k = \mathbb{R}_+ \times C_k^1. \tag{7}$$

There is a natural homomorphism id: $J_k \to I(k)$ of J_k on $I(k)$ given by the equation

$$\mathrm{id}\, x = \prod_{p \in S_o} p^{w_p(x_p)} \quad \text{for} \quad x \in J_k.$$

Let $\mu \in \hat{C}_k$, let $\mathfrak{f}(\mu)$ be the conductor of μ (defined as, e.g., in [93], p. 133) and let $\mathfrak{f}_\infty(\mu)$ be set of those primes in S_1 at which μ is ramified; write $\widetilde{\mathfrak{f}(\mu)} = \{\mathfrak{f}(\mu), \mathfrak{f}_\infty(\mu)\}$. One can define a character χ_μ on $I(\mathfrak{f}(\mu))$ by the equation

$$\chi_\mu(\mathfrak{a}) = \mu(x) \quad \text{for} \quad \mathfrak{a} \in I(\mathfrak{f}(\mu)), \quad x \in \mathrm{id}^{-1}(\mathfrak{a}),$$

if one regards μ as a character of J_k (trivial on k^*). It follows from definitions that χ_μ is well defined since μ is constant on $\mathrm{id}^{-1}(\mathfrak{a})$ for $\mathfrak{a} \in I(\mathfrak{f}(\mu))$.

Proposition 2. The function $\mathfrak{a} \mapsto \chi_\mu(\mathfrak{a})$ is a proper grossencharacter and $\widetilde{\mathfrak{f}(\chi_\mu)} = \widetilde{\mathfrak{f}(\mu)}$; it satisfies (5) with $\mathfrak{m} = \widetilde{\mathfrak{f}(\mu)}$ and λ equal to the restriction of μ to X^* (regarded as a subgroup of J_k), in particular, χ_μ is normalised if and only if $\mathbb{R}_+ \subseteq \mathrm{Ker}\, \mu$. If χ is a proper grossencharacter, there is one and only one μ in $\hat{C}_k$ such that $\chi = \chi_\mu$.

Proof. See [91], p. 9 - 10 (or [23], §9).
We denote the group of proper normalised grossencharacters by $\mathrm{gr}(k)$ and remark that

$$\mathrm{gr}(k) \cong \hat{C}_k^1.$$

Proposition 1 defines a fibration of $\mathrm{gr}(k)$ over the set of (generalised) conductors. Let $\chi \in \mathrm{gr}(k)$ and suppose that χ satisfies (5) with λ of the shape (6); we call a_p, t_p appearing in (6) exponents of χ and write $a_p = a_p(\chi)$, $t_p = t_p(\chi)$.

Let now

$$s_p(\chi) = \begin{cases} a_p(\chi) + it_p(\chi) & , \quad p \in S_1 \\ \frac{1}{2}(|a_p(\chi)| + it_p(\chi)), & p \in S_2 \end{cases} ,$$

and let

$$G_p(s) = \begin{cases} \pi^{-s/2}\Gamma(s/2), & p \in S_1 \\ (2\pi)^{1-s}\Gamma(s), & p \in S_2 \end{cases} .$$

For $s \in \mathbb{C}$, $\chi \in gr(k)$ one defines a Dirichlet series

$$L(s,\chi) = \sum_{n=1}^{\infty} c_n(\chi) n^{-s} , \tag{8}$$

where

$$c_n(\chi) = \sum_{|\mathfrak{a}|=n} \chi(\mathfrak{a}), \qquad \mathfrak{a} \in I_o(k), \tag{9}$$

is a finite sum extended over the integral ideals of k whose norm is equal to n. The series (8) converges absolutely for $\mathrm{Re}\, s > 1$ and in this half-plane it can be decomposed in an Euler product:

$$L(s,\chi) = \prod_{p \in S_o} (1-\chi(p)|p|^{-s})^{-1}. \tag{10}$$

One extends (10) by adding the gamma-factors at infinite places:

$$\Lambda(s,\chi) = L(s,\chi) \prod_{p \in S_\infty} G_p(s+s_p). \tag{11}$$

By a theorem of E. Hecke, [24] (cf. also [93], VII §7) the function

$$s \mapsto \Lambda(s,\chi)$$

can be meromorphically continued to the whole complex plane $\mathbb{C}$ and satisfies a functional equation:

$$\Lambda(s,\chi) = W(\chi)a(\chi)^{\frac{1}{2}-s}\Lambda(1-s,\bar{\chi}), \tag{12}$$

where $a(\chi) = |D|\cdot|\mathfrak{f}(\chi)|$, D denotes the discriminant of k and $|W(\chi)| = 1$. The function

$$s \mapsto L(s,\chi) - \frac{\omega(k)g(\chi)}{s-1},$$

where $g(\chi) = 0$ for $\chi \neq 1$ and $g(1) = 1$, is holomorphic in $\mathbb{C}$. The residue of $L(s,1)$ at $s = 1$ is given by the equation: $\omega(k) = 2^{r_1+r_2}\pi^{r_2}R\,h(m\sqrt{|D|})^{-1}$, where R is the regulator of k and m denotes the order of the group of roots of unity contained in k^*. We write, for brevity,

$$\zeta_k(s) = L(s,1),\ \zeta_{\mathbb{Q}}(s) = \zeta(s),$$

and let

$$L_\infty(s,\chi) = \prod_{p\in S_\infty} G_p(s+s_p(\chi)), \tag{13}$$

so that

$$\Lambda(s,\chi) = L(s,\chi)L_\infty(s,\chi). \tag{14}$$