Constellations in prime elements of number fields

Wataru Kai, Masato Mimura, Akihiro Munemasa, Shin-ichiro Seki, Kiyoto Yoshino

Abstract

Given any number field, we prove that there exist arbitrarily shaped constellations consisting of pairwise non-associate prime elements of the ring of integers. This result extends the celebrated Green–Tao theorem on arithmetic progressions of rational primes and Tao’s theorem on constellations of Gaussian primes. Furthermore, we prove a constellation theorem on prime representations of binary quadratic forms with integer coefficients. More precisely, for a non-degenerate primitive binary quadratic form $F$ which is not negative definite, there exist arbitrarily shaped constellations consisting of pairs of integers $(x,y)$ for which $F(x,y)$ is a rational prime. The latter theorem is obtained by extending the framework from the ring of integers to the pair of an order and its invertible fractional ideal.

1 Introduction

The following theorem proved by Green and Tao is a monumental work on additive number theory.

**Theorem 1.1** (The Green–Tao theorem [GT08]). *There exist arithmetic progressions of primes of arbitrary length.*

In order to consider multidimensional generalizations of this result, we introduce a terminology of *constellations*. For a finite subset $S$ of a $\mathbb{Z}$-module $\mathcal{Z}$ (we will consider only a free module of finite rank), we call a set of the form $\alpha + kS := \{\alpha + ks : s \in S\}$ a constellation.
with the shape $S$. Here, $\alpha$ is an element of $\mathbb{Z}$ and $k$ is a positive integer. In this paper, we abbreviate it as an $S$-constellation; it is also known as a homothetic copy of $S$. Note that, in the literature, some other authors allow $k$ to be a negative integer. Let $\mathcal{Z}$ be a $\mathbb{Z}$-module and $A$ a subset of $\mathcal{Z}$. When $A$ contains an $S$-constellation for any finite subset $S$ of $\mathcal{Z}$, we say that “there exist constellations of arbitrary shape in $\mathcal{Z}$ consisting of elements of $A$” or “the constellation theorem holds for $A$.” Note that for a subset $A \subseteq \mathbb{Z}$, the existence of arithmetic progressions of arbitrary length is equivalent to that of constellations of arbitrary shape.

As the Gaussian counterpart of the Green–Tao theorem, Tao established the following.

**Theorem 1.2** (Constellation theorem in the Gaussian primes [Tao06]). There exist constellations of arbitrary shape in the ring of Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ consisting of Gaussian primes.

In the same paper, Tao [Tao06 12 Discussion] conjectured that Theorem 1.1 could be extended in the following two ways.

1. Extension to the other number field (= the constellation theorem in the prime elements of an arbitrary number field).

2. Extension to a relatively dense subset $A$ of the direct product $\mathcal{P}^n$ of the set of primes (= the multidimensional Szemerédi theorem holds in the primes). More precisely, there exist constellations of arbitrary shape in $\mathbb{Z}^n$ consisting of elements of $A$.

Recently, the second conjecture has been settled independently by three research groups, Tao–Ziegler [TZ15], Fox–Zhao [FZ15] and Cook–Magyar–Titichetrakun [CMT18].

In this paper, we resolve the first conjecture in the affirmative. The main theorem in this paper is stated in its simplest form as follows; various refined statements will be introduced in Section 2. We denote by $\mathcal{O}_K$ the ring of integers of a number field $K$.

**Theorem 1.3** (Constellation theorem in the prime elements of a number field). Let $K$ be a number field. Then there exist constellations of arbitrary shape in $\mathcal{O}_K$ consisting of prime elements of $\mathcal{O}_K$.

In the above theorem, the statement for the case of $K = \mathbb{Q}$ is equivalent to the Green–Tao theorem (Theorem 1.1); that for the case of $K = \mathbb{Q}(\sqrt{-1})$ is exactly the constellation theorem in the Gaussian primes (Theorem 1.2). The definitions and facts on number fields that appear in this section are summarized in Section 3.

Tao remarks in [Tao06 12 Discussion] that his method of proving Theorem 1.2 is likely to extend to $K$ at least if the class number of $K$ is 1 and the unit group $\mathcal{O}_K^\times$ is finite. There exist only nine such number fields other than $\mathbb{Q}$ and all of them are imaginary quadratic by Dirichlet’s unit theorem and the Baker–Heegner–Stark theorem; see for instance, [Sta67]. For a general number field, the class number may be strictly greater than 1 or the unit group may be infinite. Both of these two cause problems for formulating an appropriate statement of generalizations of Theorem 1.2.

If the class number is greater than 1, then not all irreducible elements are prime elements. As already mentioned in Theorem 1.3, the prime elements suffice to guarantee the existence
of constellations of arbitrary shape. The unit group acts on the set of prime elements by multiplication. In Corollary 1.5 we strengthen Theorem 1.3 by showing the existence of constellations consisting of primes from distinct orbits. The original method of Tao [Tao06] does not extend to the proof of Theorem 1.2 in a straightforward manner, due to the above two obstacles. We will describe the difficulties in the latter part of this introduction.

In this paper, for a number field $K$, we denote by $\mathcal{P}_K$ the set of all prime elements of the ring of integers $\mathcal{O}_K$. We prepare some concepts in order to extend conjecture (1) to a ‘Szemerédi-type theorem’ and to refine the statement in the case that the unit group is infinite. For an integral basis $\omega$ of $K$, we denote by $\|\cdot\|_{\infty,\omega}:\mathcal{O}_K \to \mathbb{Z}_{\geq 0}$ the $\ell_\infty$-length with respect to the basis $\omega$; see Definition 2.2. For a non-empty set $X \subseteq \mathcal{O}_K$ and its subset $A \subseteq X$, we define the relative upper asymptotic density measured by the $\ell_\infty$-length $\|\cdot\|_{\infty,\omega}$ of $A$ with respect to $X$ by

$$d_{X,\omega}(A) := \limsup_{M \to \infty} \frac{|A \cap \mathcal{O}_K(\omega, M)|}{|X \cap \mathcal{O}_K(\omega, M)|},$$

where $\mathcal{O}_K(\omega, M) := \{\alpha \in \mathcal{O}_K : \|\alpha\|_{\infty,\omega} \leq M\}$. We say that two elements of $\mathcal{O}_K \setminus \{0\}$ are associate if they lie in the same orbit for the action $\mathcal{O}_K^\times \curvearrowright \mathcal{O}_K \setminus \{0\}$ by multiplication. We call a two-point subset $\{\alpha, \beta\}$ of $\mathcal{O}_K \setminus \{0\}$ an associate pair if $\alpha$ and $\beta$ are associate. The following theorem is a strengthening of Theorem 1.3.

**Theorem 1.4 (Szemerédi-type theorem in the prime elements of a number field).** Let $K$ be a number field and $\omega$ an integral basis of $K$. Assume that a subset $A$ of $\mathcal{P}_K$ has a positive relative upper asymptotic density measured by $\|\cdot\|_{\infty,\omega}$ with respect to $\mathcal{P}_K$, namely, $d_{X,\omega}(A) > 0$. Then there exist constellations of arbitrary shape in $\mathcal{O}_K$ consisting only of elements of $A$ without associate pairs.

In Subsection 2.1 we state Theorem A which may be seen as a version of Theorem 1.4 in a finitary setting. Theorem A is the first main theorem of the present paper. As a corollary to Theorem 1.4, we obtain the following.

**Corollary 1.5.** In the statement of Theorem 1.3, we can take constellations that do not admit associate pairs.

If the unit group is finite, then we see that Theorem 1.3 and Corollary 1.5 are equivalent in a simple argument using the pigeonhole principle. On the other hand, if the unit group is infinite, then Corollary 1.5 seems stronger than Theorem 1.3. Although Corollary 1.5 is derived immediately from Theorem 1.4, we prove it prior to Theorem 1.4. More precisely, we prove Corollary 1.5 by using Theorem 2.8 and the existence of a ‘good’ fundamental domain (Section 4); see Subsection 7.5.

Next, we briefly discuss the technical problems of the proofs in the case of general number fields. Recall that the class number of $K$ can be greater than 1, in which case prime element factorization in $\mathcal{O}_K$ fails. From this viewpoint, it may be seen that prime elements are ‘few.’ One of the key steps to the proofs of Theorem 1.1 and Theorem 1.2 is to prove Goldston–Yıldırım type asymptotic formulas; these are used to confirm the conditions for applying a
relative version of the multidimensional Szemerédi theorem. Since the proofs of Goldston–Yıldırım type asymptotic formulas involve the existence and uniqueness of factorizations, the proof breaks down if the class number of $K$ is at least 2. In the work of Green–Tao and Tao, they consider some variants of the von Mangoldt function to obtain Goldston–Yıldırım type asymptotic formulas. However, if the unit group $O_K^\times$ is infinite, naive generalizations of their variants do not make any sense; in their summations, an element would be summed for infinitely many times.

To address the two difficulties above, we switch the framework, from that of elements in $O_K$ to that of ideals. This is the standard approach in algebraic number theory since Dedekind. It enables us to treat our problems of all number fields in a unified manner.

To go back from the framework of ideals to that of elements in the final step of our proof, we employ the Chebotarev density theorem; it asserts that principal prime ideals have a certain proportion in prime ideals. From this viewpoint, the prime elements are ‘not too few.’ If we take a fundamental domain for $O_K^\times \curvearrowright O_K \setminus \{0\}$, then each prime element there exactly corresponds to each (non-zero) principal prime ideal. We need to count prime elements measured by $\ell_\infty$-length, while prime ideals are counted with respect to (ideal) norms. To connect these two scales, we introduce the notion of the $NL$-compatibility of fundamental domains. Thus, we have a desired estimate of numbers of prime elements measured by $\ell_\infty$-length in an $NL$-compatible fundamental domain. Then the relative multidimensional Szemerédi theorem applies, and we establish our constellation theorem for this domain. Next, we prove Theorem 1.4 whose statement does not involve fundamental domains. For the proof, we obtain a certain reduction theorem of this case to the case with a fundamental domain; see Theorem 2.11. The reduction theorem is proved with the aid of the geometry of numbers.

On the full resolution of the conjecture (1) in Tao’s paper [Tao06], the main novel points are summarized as follows.

- [Pseudorandom part] We formulate the Goldston–Yıldırım type asymptotic formula (Theorem 6.2) by focusing on ideals of $O_K$ instead of elements of $O_K$.

- [Counting part] We utilize an $NL$-compatible fundamental domain for counting of prime elements. Then we reduce a general case to this setting.

In this manner, we can treat the case where the class number is greater than 1, or the unit group is infinite.

In the last part of this section, we describe an application to binary quadratic forms with integer coefficients, which is related to the constellation theorems in prime elements of quadratic fields. We say that $F: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ is a primitive (binary) quadratic form if it is of the form $F(x, y) = ax^2 + bxy + cy^2$, where $a, b, c$ are integers with $\gcd(a, b, c) = 1$. A fundamental problem in number theory asks which primes, or $-1$ multiples of them, are represented by $F$. In this paper, motivated by this problem, we obtain a combinatorial theorem for pairs $(x, y) \in \mathbb{Z}^2$ satisfying $F(x, y) \in \mathcal{P}_Q$. The detailed statement is presented as Theorem C in Subsection 2.1, the following theorem is a simplified version of it. The discriminant $D_F$ of $F$ is defined by $D_F := b^2 - 4ac$. 

\[ D_F := b^2 - 4ac \]
Theorem 1.6 (Constellation theorem on prime representations of binary quadratic forms). Let $F : \mathbb{Z}^2 \to \mathbb{Z}$ be a primitive quadratic form. Assume that its discriminant $D_F$ is not a perfect square and that $F$ is not negative definite. Then, for a given finite set $S \subseteq \mathbb{Z}^2$, there exists an $S$-constellation $S$ in $\mathbb{Z}^2$ such that the function $F(x, y)$ takes distinct prime values on $S$.

The above condition on $D_F$ is necessary. Indeed, if $D_F$ is a perfect square, then $F(x, y)$ is not irreducible over $\mathbb{Z}$. If $F$ is indefinite, the above theorem also implies the existence of an $S$-constellation on which $F(x, y)$ takes distinct negative prime values. In order to prove Theorem 1.6 for general coefficients $(a, b, c)$, we extend the framework of our constellation theorem. More precisely, we consider a pair $(O, c)$, where $O$ is an order in $K$ and $c$ is an invertible fractional ideal of $O$. The original case is where $O$ and $c$ both equal $O_K$.

Acknowledgments

The authors are grateful to Toshiki Matsusaka and Kota Saito for discussions, and Yuta Suzuki for the reference [BHP01]. Wataru Kai, Masato Mimura, Akihiro Munemasa and Shin-ichiro Seki are supported in part by JSPS KAKENHI grant number, respectively, JP18K13382, JP17H04822, JP20K03527 and JP18J00151.

Contents

1 Introduction 1

2 Precise statements of main theorems and the outline of the proof 7

\hspace{0.5cm} 2.1 Main theorems 7

\hspace{0.5cm} 2.2 Constellations in prime elements inside a fundamental domain 11

\hspace{0.5cm} 2.3 The idea of proofs and the organization of this paper 13

3 Preliminaries on algebraic number theory 18

\hspace{0.5cm} 3.1 The ring of integers and its ideals 19

\hspace{0.5cm} 3.2 The unit group and ideal class group 21

\hspace{0.5cm} 3.3 $p$-Ideals 21

\hspace{0.5cm} 3.4 The Dedekind zeta function and density of ideals 24

\hspace{0.5cm} 3.5 Distribution of rational primes 26

4 Norm-length compatibility and geometry of numbers 27

\hspace{0.5cm} 4.1 Weighted multiplicative Minkowski embedding 28

\hspace{0.5cm} 4.2 Geometric characterization of the NL-compatibility 29

\hspace{0.5cm} 4.3 Construction of the domain $\mathcal{D}_K(e, \sigma)$ 31

\hspace{0.5cm} 4.4 Countings of elements in $O_K^\times$-orbits with respect to the $\ell_\infty$-length 34
5 Relative multidimensional Szemerédi theorem
5.1 The statement of the relative multidimensional Szemerédi theorem
5.2 Relative hypergraph removal lemma
5.3 Construction of pseudorandom weighted hypergraphs
5.4 The proof of the relative multidimensional Szemerédi theorem

6 Goldston–Yıldırım type asymptotic formula
6.1 Von Mangoldt function and its variants
6.2 Statement of Goldston–Yıldırım type asymptotic formula
6.3 The expectation of the characteristic function
6.4 The expectation of the characteristic function for $p$-ideals
6.5 Estimate for the error by a change of domain of integration
6.6 Calculation of the main term
6.7 Goldston–Yıldırım type asymptotic formula for ideals

7 Construction of pseudorandom measures and estimates of weighted densities
7.1 Outline of the proof of Theorem A
7.2 Construction of the pseudorandom measure
7.3 Comparison between countings with the norm scale and with the $\ell_{\infty}$-length scale
7.4 Estimates of weighted densities
7.5 Proof of Theorem 2.8

8 Szemerédi-type theorems in prime elements of number fields
8.1 Preliminaries on the axiomatizations for constellation theorems
8.2 Axiomatization for constellation theorems of type 1
8.3 Counting prime elements from above
8.4 Reduction to the case of fixing a fundamental domain

9 Szemerédi-type theorems for short intervals
9.1 Statements of the theorems for short intervals
9.2 Strong form for the case $K = \mathbb{Q}$
9.3 Slide trick
9.4 Axiomatization for short intervals
9.5 Proof of Theorems 9.15 and 9.16
9.6 Constellations whose norms are close

10 Constellations in ideals and quadratic forms
10.1 Strategy for the proof of Theorem 10.1
10.2 Preliminaries on invertible ideals of orders
10.3 Ideal norms of invertible fractional ideals
10.4 ‘Prime elements’ in ideals and subpseudorandom condition
10.5 Counting by the Chebotarev density theorem
2 Precise statements of main theorems and the outline of the proof

In this section, we state three main theorems in the present paper. Theorem A is a finitary version of Theorem 1.4. Theorem B is a short interval version of Theorem A. Theorem C is a precise version of Theorem 1.6.

In Subsection 2.3, we give an overview of the main argument to establish our constellation theorems. This is inspired by the ingenious method of Green–Tao and Tao; we simplify some of it with the use of a recent result of Conlon–Fox–Zhao. In our main argument, we build a fundamental diagram among ‘five worlds’; see Subsection 2.3 for details.

2.1 Main theorems

In this subsection, we present the statements of our main theorems, Theorems A, B, and C. First, we define the (ideal) norm of a non-zero element $\alpha$ of $O_K$ for a number field $K$; see also Remark 3.6. As mentioned in Introduction, the $\ell_\infty$-length of $\alpha \in O_K$ is defined for a fixed integral basis $\omega$ of $K$. Here we state the exact definitions of them. These are two distinct scales on $O_K$ used in this paper.

**Definition 2.1 (Norm).** Let $K$ be a number field of degree $n$. For $\alpha \in O_K \setminus \{0\}$, we define the norm $N(\alpha)$ by

$$N(\alpha) := \# (O_K / \alpha O_K) \quad (< +\infty).$$

For a non-negative real number $L$, we set

$$O_K(L) := \{ \alpha \in O_K \setminus \{0\} : N(\alpha) \leq L \}.$$

**Definition 2.2 ($\ell_\infty$-length).** Let $Z$ be a free $\mathbb{Z}$-module of rank $n \in \mathbb{N}$. Let $v = (v_1, v_2, \ldots, v_n)$ be a basis of $Z$. Then, we define the $\ell_\infty$-length of $\alpha \in Z$ for $v$ by

$$\|\alpha\|_{\infty, v} := \max_{1 \leq i \leq n} |a_i|,$$

where $\alpha = \sum_{1 \leq i \leq n} a_i v_i$. For a non-negative real number $M$, we set

$$Z(v, M) := \{ \alpha \in Z : \|\alpha\|_{\infty, v} \leq M \}.$$
As is well known, the ring of integers $\mathcal{O}_K$ of a number field $K$ of degree $n$ is a free $\mathbb{Z}$-module of rank $n$. We use the symbol $\omega$ for its integral basis in this paper. In particular, $\ell_\infty$-length $\| \cdot \|_\infty$ on $\mathcal{O}_K$ and the set $\mathcal{O}_K(\omega, M) \subseteq \mathcal{O}_K$ are defined by Definition 2.2. Furthermore, Definition 2.2 applies to the case where $\mathcal{O}_K$ is a non-zero ideal $a$ of $\mathcal{O}_K$. For $\alpha \in \mathcal{O}_K \setminus \{0\}$, its norm $N(\alpha)$ and its $\ell_\infty$-length $\|\alpha\|_\infty$, $\omega$ on $\mathcal{O}_K$ and the set $\mathcal{O}_K(\omega, M) \subseteq \mathcal{O}_K$ are defined by Definition 2.2. Furthermore, Definition 2.2 applies to the case where $\mathcal{O}_K$ is a non-zero ideal $a$ of $\mathcal{O}_K$. For $\alpha \in \mathcal{O}_K \setminus \{0\}$, its norm $N(\alpha)$ and its $\ell_\infty$-length $\|\alpha\|_\infty$, $\omega$ are both positive integers. Nevertheless, we allow the parameters $L, M$ to be non-negative real numbers in the definitions of $\mathcal{O}_K(L)$ and $\mathcal{O}_K(\omega, M)$ above. This is for avoiding an inessential issue from integrality.

We introduce the notion of standard shapes; this is useful for estimates of the number of constellations in our main theorems.

**Definition 2.3** (Standard shape, the number of $S$-constellations). Let $\mathcal{Z}$ be a $\mathbb{Z}$-module and $S \subseteq \mathcal{Z}$ a finite set.

1. The set $S$ is called a *standard shape* if the following hold: $0 \in S$, $S = -S$, and $S$ generates $\mathcal{Z}$ as a $\mathbb{Z}$-module.

2. Assume that $S \neq \emptyset$. For a finite subset $X \subseteq \mathcal{Z}$, $N_S(X)$ denotes the number of distinct $S$-constellations in $X$.

Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then, for $\alpha, \beta \in \mathfrak{a} \setminus \{0\}$ we say that they are *associate* if these elements lie in the same orbit of the action $\mathcal{O}_K^\times \curvearrowright \mathfrak{a} \setminus \{0\}$ by multiplication. For $A \subseteq \mathfrak{a} \setminus \{0\}$, we define an *associate pair* in $A$ to be a two-point subset $\{\alpha, \beta\}$ of $A$ consisting of associate elements. We have already defined this concept in Introduction in the case where $\mathfrak{a} = \mathcal{O}_K$. In this paper, we study the existence of constellations *without associate pairs*. Furthermore, if the shape $S$ is standard, then we evaluate the number of $S$-constellations without associate pairs.

**Definition 2.4.** Let $K$ be a number field and $\mathfrak{a}$ a non-zero ideal of $\mathcal{O}_K$. Let $S$ be a non-empty finite subset of $\mathcal{O}_K$. For a finite set $X \subseteq \mathfrak{a}$, $N^S_S(X)$ denotes the number of $S$-constellations in $X$ without associate pairs.

Now we exhibit our first main theorem. This is a finitary version of Theorem 1.4 in Introduction.

**Theorem A** (Szemerédi-type theorem in the prime elements of a number field: finitary version). Let $K$ be a number field and $\omega$ an integral basis of $K$. Let $\delta$ be a positive real number and $S$ a finite subset of $\mathcal{O}_K$. Then the following hold.

1. There exists a positive integer $M_0$ depending only on $\omega, \delta$ and $S$ such that the following holds: if $M \geq M_0$ and a subset $A$ of $\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)$ satisfies

$$\#A \geq \delta \cdot \#(\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)),$$

then there exists an $S$-constellation in $A$ without associate pairs.
(2) Furthermore, if $S$ is a standard shape, then there exist a constant $\gamma > 0$ and a positive integer $M'_0$ depending only on $\omega, \delta$ and $S$ such that the following holds: if $M \geq M'_0$ and a subset $A$ of $\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)$ satisfies (2.1), then

$$\mathcal{M}_S^2(A) \geq \gamma \cdot M^{n+1}(\log M)^{-(\#S + \sigma_M \to \infty, n(1))}$$

holds true. Here, $n$ is the degree of $K$.

On the estimate of the number of $S$-constellations in the main theorem, Theorem A (2), it seems natural that the negative power of log appears from the viewpoint of a natural density version of the Chebotarev density theorem (Theorem 3.22). For a given finite set $S \subseteq \mathcal{O}_K$, we can construct a standard shape by inflating $S$ as follows: add some elements of a basis of $\mathcal{O}_K$ to $S$ if $S$ does not generate $\mathcal{O}_K$. Let $\hat{S}$ be the resulting set, and consider $\hat{S} \cup (-\hat{S}) \cup \{0\}$. Note that for some $S$, the inflating process above may be done in a better manner. For this reason, the assumption on $S$ in Theorem A (2) does not lose its generality. In general, for a finite set $X \subseteq \mathcal{O}_K \setminus \{0\}$, the inequality $\mathcal{M}_S^2(X) \leq \mathcal{M}_S(X)$ holds. Hence, we have also a lower bound of $\mathcal{M}_S(A)$ by Theorem A (2).

We use the terms ‘finitary versions’ and ‘infinitary versions’ in the following manner: a statement of the existence of constellations in a certain subset of the set of the form $\mathcal{Z}(v, M)$ for sufficiently large $M$ is expressed as a ‘finitary version.’ A statement on the existence of constellations in a subset $A$ of a certain subset $X$ of $\mathcal{Z}$ where $A$ has a positive relatively upper asymptotic density in $X$ is expressed as an ‘infinitary version.’ Theorem A is an example of the former version; Theorem 1.4 is one of the latter. These usages are standard in this research field.

Our second main theorem may be seen as a ‘short interval version’ of Theorem A.

**Definition 2.5 ($\ell_\infty$-interval).** Let $\mathcal{Z}$ be a free $\mathbb{Z}$-module of finite rank and $v$ its $\mathbb{Z}$-basis. For $x \in \mathcal{Z}$ and a positive real number $M$, the $\ell_\infty$-interval $\mathcal{Z}(v, x, M)$ is defined to be

$$\mathcal{Z}(v, x, M) := \{ \alpha \in \mathcal{Z} : \|\alpha - x\|_\infty, v \leq M \}.$$  

**Theorem B** (A short interval version of the Szemerédi-type theorem in the prime elements of a number field: finitary version = Theorem 9.5). Let $K$ be a number field and $\omega$ an integral basis of $K$. Let $\delta$ be a positive real number and $S$ a finite subset of $\mathcal{O}_K$. Take a real number $a$ with $0 < a < 1$. Then the following hold.

(1) There exists a positive integer $M_0$ depending only on $\omega, \delta, S$ and $a$ such that the following holds: if $M \geq M_0$ and a subset $A$ of $\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)$ satisfies

$$\#A \geq \delta \cdot (\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)),$$

then there exists $x \in A$ with

$$\frac{M}{\log^{a^2} M} \leq \|x\|_\infty, \omega \leq M$$  

such that $A \cap \mathcal{O}_K(\omega, x, \|x\|_\infty, \omega)$ contains an $S$- constellation without associate pairs. Here, $\log^{a^2}$ means $\log \log$. 

\[ \]
(2) If \( S \) is a standard shape, then there exist a constant \( \gamma > 0 \) and a positive integer \( M_0 \) depending only on \( \omega, \delta, S \) and a such that the following holds: if \( M \geq M_0 \) and a subset \( A \) of \( \mathcal{P}_K \cap \mathcal{O}_K(\omega, M) \) satisfies \((2.2)\), then there exists \( x \in A \) with \((2.3)\) which satisfies

\[
\mathcal{N}_S^\ell(A \cap \mathcal{O}_K(\omega, x, \|x\|_{\infty, \omega})) \geq \gamma \cdot M^{a(n+1)}(\log M)^{-(\#S + \omega M^{-\infty, n}(1))}.
\]

An infinitary version of Theorem \([4]\) will be stated as Corollary \([9.6]\) in Section \([9]\). The case \( K = \mathbb{Q} \) of Corollary \([9.6]\) is written in \([TZ08, \text{Remark 2.4}]\) in more general ‘polynomial progression’ setting; see Remark \([9.7]\).

In the last part of this subsection, we state a precise version of Theorem \([1.6]\) as an application to binary quadratic forms with integer coefficients. Let \( F(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y] \) be a quadratic form and \( D_F = b^2 - 4ac \) its discriminant. Assume that \( D_F \) is not a perfect square. By multiplying \(-1\) if necessary, we may assume that \( a > 0 \). If \( D_F < 0 \), then \( F \) is positive definite and if \( D_F > 0 \), then \( F \) is indefinite. The symbol \( \| \cdot \|_\infty \) denotes the standard \( \ell_\infty \)-length on \( \mathbb{Z}^2 \). Namely, \( \|(x, y)\|_\infty := \max\{|x|, |y|\} \). For \( M \in \mathbb{R}_{\geq 0} \), set \( \mathbb{Z}^2(\| \cdot \|_\infty, M) := \{(x, y) \in \mathbb{Z}^2 : \|(x, y)\|_\infty \leq M\} \). In this paper, \( \mathcal{P} = \{2, 3, 5, 7, 11, \ldots\} \) denotes the set of positive rational prime numbers. We consider the set \( F^{-1}(\mathcal{P}) \) (respectively, \( F^{-1}(-\mathcal{P}) \)) of elements \((x, y)\) whose value of \( F \) (respectively, \(-F\)) represents a prime number:

\[
F^{-1}(\mathcal{P}) = \{(x, y) \in \mathbb{Z}^2 : F(x, y) \in \mathcal{P}\}, \quad \text{and} \quad F^{-1}(-\mathcal{P}) = \{(x, y) \in \mathbb{Z}^2 : -F(x, y) \in \mathcal{P}\}.
\]

The following is our third main theorem.

**Theorem C** (Szemerédi-type theorem on prime representations of binary quadratic forms). Let \( F: \mathbb{Z}^2 \to \mathbb{Z}; F(x, y) := ax^2 + bxy + cz^2 \) be a primitive quadratic form with integer coefficients such that its discriminant \( D_F \) is not a perfect square. Assume that \( a > 0 \).

1. Let \( A \subseteq F^{-1}(\mathcal{P}) \) be a set which has a positive relative upper asymptotic density measured by \( \| \cdot \|_\infty \) with respect to \( F^{-1}(\mathcal{P}) \), that means

\[
\overline{d}_{F^{-1}(\mathcal{P}), \infty}(A) := \limsup_{M \to \infty} \frac{\#(A \cap \mathbb{Z}^2(\| \cdot \|_\infty, M))}{\#(F^{-1}(\mathcal{P}) \cap \mathbb{Z}^2(\| \cdot \|_\infty, M))} > 0.
\]

Then, for every finite set \( S \subseteq \mathbb{Z}^2 \), there exists an \( S \)-constellation in \( A \).

2. Assume that \( D_F > 0 \). Let \( A \subseteq F^{-1}(-\mathcal{P}) \) be a set which has a positive relative upper asymptotic density measured by \( \| \cdot \|_\infty \) with respect to \( F^{-1}(-\mathcal{P}) \), that means

\[
\overline{d}_{F^{-1}(-\mathcal{P}), \infty}(A) := \limsup_{M \to \infty} \frac{\#(A \cap \mathbb{Z}^2(\| \cdot \|_\infty, M))}{\#(F^{-1}(-\mathcal{P}) \cap \mathbb{Z}^2(\| \cdot \|_\infty, M))} > 0.
\]

Then, for every finite set \( S \subseteq \mathbb{Z}^2 \), there exists an \( S \)-constellation in \( A \).

3. In both \((1)\) and \((2)\), we can take an \( S \)-constellation \( S \) in \( A \) such that \( F \mid_S: S \to \mathcal{P}_\mathbb{Q} \) is injective.
In particular, the constellation theorem holds for $F^{-1}(P)$ by Theorem C (1); and if $D_F > 0$, then the constellation theorem also holds for $F^{-1}(-P)$ by Theorem C (2). On the general statement of Theorem C, we can also take distinct primes in the $S$-constellation in $A$ such that they are sufficiently close to each other in some appropriate sense; see Theorem 10.1 for details. See also Theorem 10.36 for a general statement on norm forms associated with a pair of an order and an invertible fractional ideal of it.

2.2 Constellations in prime elements inside a fundamental domain

In this subsection, we state Theorem 2.8 (a finitary version) and Corollary 2.10 (an infinitary version) which appear as preludes to proving Theorem A and Theorem 1.4. Proving these theorems is the first goal of this paper, and their proofs contain the essence of the main arguments in this paper. See Subsection 2.3 on the relationship between Theorem 2.8 (respectively, Corollary 2.10) and Theorem A (respectively, Theorem 1.4). The difference between settings of them is whether we consider sets inside a fundamental domain for the action $O_K \times K \to O_K \setminus \{0\}$ by multiplication. If we take a fundamental domain $D$, then the correspondence $\alpha \mapsto \alpha O_K$ is injective on $D$ and hence counting of elements is reduced to that of ideals.

We call a fundamental domain for the action $O_K \times K \to O_K \setminus \{0\}$ an $O_K$-fundamental domain in this paper. We will use this terminology without referring to the action, as in the following definition.

**Definition 2.6** ($O_K$-fundamental domain). A set $D \subseteq O_K \setminus \{0\}$ is called an $O_K$-fundamental domain, if $O_K \setminus \{0\}$ is decomposed as the following disjoint union:

$$O_K \setminus \{0\} = \bigsqcup_{\eta \in O_K} \eta D.$$ 

We formulate a prime element constellation theorem in the setting of taking an $O_K$-fundamental domain $D$ as follows: we consider $P_K \cap D$ instead of $P_K$, and take a subset $A$ of it. Here we warn that if $\#(O_K) = \infty$, then there exists an $O_K$-fundamental domain $D$ such that the constellation theorem for $P_K \cap D$ does not hold. This fact will be proved as Proposition 4.13. Thus, the following question arises: “for which $O_K$-fundamental domain can we ensure that a constellation theorem holds?” We answer this question by introducing the notion of $NL$-compatible fundamental domains. The notion of the NL-compatibility is defined for a subset of $O_K \setminus \{0\}$ as follows.

**Definition 2.7** ($NL$-compatibility). Let $K$ be a number field of degree $n$. A set $X \subseteq O_K \setminus \{0\}$ is $NL$-compatible (norm-length compatible) if the following condition is satisfied: there exist an integral basis $\omega$ of $K$ and a constant $C = C(\omega, X) > 0$ such that, for every $\alpha \in X$,

$$C\|\alpha\|_{\infty, \omega} \leq N(\alpha)$$

holds.
The existence of a constant $C$ above is independent of the choice of an integral basis $\omega$; the exact value of $C$ depends. The NL-compatibility has a geometric interpretation in terms of the weighted multiplicative Minkowski embedding $L_R$, which is stated without taking an integral basis. See Definition 4.2 for $L$. If the unit group $O_K^\times$ is infinite, then not every $O_K^\times$-fundamental domain is NL-compatible. Note that there exists $C' = C'(\omega) > 0$ such that for all $\alpha \in O_K \setminus \{0\}$

$$N(\alpha) \leq C'||\alpha||_{\infty,\omega}^n$$

holds; see Lemma 4.8. In Section 4 we will show the existence of NL-compatible $O_K^\times$-fundamental domains. More precisely, given a system of fundamental units $\epsilon$ and a field embedding $\sigma: K \hookrightarrow \mathbb{C}$, we will explicitly construct such a domain $D_K(\epsilon, \sigma)$; see Definition 4.10 and Proposition 4.11 for details.

**Theorem 2.8** (Theorem A restricted to an NL-compatible fundamental domain = Theorem 7.10 + Theorem 7.11). Let $K$ be a number field, $\omega$ an integral basis of $K$ and $L$ an NL-compatible $O_K^\times$-fundamental domain. Let $\delta$ be a positive number and $S$ a finite subset of $O_K$. Then the following hold.

1. There exists a positive integer $M_0$ depending only on $\omega$, $D$, $\delta$ and $S$ such that the following hold: If $M \geq M_0$ and a subset $A$ of $P_K \cap D \cap O_K(\omega, M)$ satisfies

$$\#A \geq \delta \cdot \#(P_K \cap D \cap \mathcal{O}_K(\omega, M)),$$

(2.5) then there exists an $S$-constellation in $A$.

2. Furthermore, if $S$ is a standard shape, then there exist a constant $\gamma > 0$ and a positive integer $M'_0$ depending only on $\omega, \delta$ and $S$ such that the following holds: if $M \geq M'_0$ and a subset $A$ of $P_K \cap O_K(\omega, M)$ satisfies (2.5), then

$$\mathcal{N}_S(A) \geq \gamma \cdot M^{n+1}(\log M)^{-2} M^{n+1}(\log M)^{-2} \#S + o_M \rightarrow \infty, n(1))$$

holds true. Here $n$ is the degree of $K$.

In particular, for a given system $\epsilon$ of fundamental units of $K$ and a given embedding $\sigma: K \hookrightarrow \mathbb{C}$, we can take $D = D_K(\epsilon, \sigma)$, which is defined in Definition 4.10.

Note that, for a finite subset $A$ of an $O_K^\times$-fundamental domain, we have $\mathcal{N}_S(A) = \mathcal{N}_S(A)$ because constellations in $A$ never admit associate pairs. See Subsection 8.3 for the deduction of Theorem 2.8 from Theorem A Corollary 1.5 immediately follows from Theorem 2.8; see Subsection 7.3. The proof of Theorem 2.8 is completed in Section 7. In Section 8 we present the additional argument required by the proof of Theorem A.

We obtain the following Corollary 2.10 as an infinitary version of Theorem 2.8. In order to state it, we define the relative upper asymptotic density for both the norm scale and the $\ell_{\infty}$-length scale. The latter is defined also in Introduction.

**Definition 2.9.** Let $X$ be a non-empty subset of $O_K \setminus \{0\}$ and $A$ a subset of $X$. 
(1) Assume that, for every non-negative real number $L$, $X$ satisfies $\#(X \cap O_K(L)) < \infty$. Then the relative upper asymptotic density of $A$ measured by norm with respect to $X$ is defined by

$$d_X(A) := \limsup_{L \to \infty} \frac{\#(A \cap O_K(L))}{\#(X \cap O_K(L))}.$$ 

(2) Let $\omega$ be an integral basis of $K$. Then the relative upper asymptotic density of $A$ measured by $\ell_\infty$-length with respect to $X$ is defined by

$$d_{X, \omega}(A) := \limsup_{M \to \infty} \frac{\#(A \cap O_K(\omega, M))}{\#(X \cap O_K(\omega, M))}.$$ 

For an $O_K$-fundamental domain $D$, the set $X = P_K \cap D$ satisfies the assumption in (1), while $X = P_K$ does not if $\#(O_K^s) = \infty$. The norm scale naturally appears in algebraic number theory. However, to prove constellation theorems, we need to convert this setting to that of the $\ell_\infty$-length scale. The NL-compatibility enables this conversion.

**Corollary 2.10** (Corollary 1.5 restricted to an NL-compatible fundamental domain). Let $K$ be a number field and $D$ an NL-compatible $O_K^s$-fundamental domain. Assume that a set $A \subseteq P_K \cap D$ satisfies either $d_{P_K \cap D}(A) > 0$ or $d_{P_K \cap D, \omega}(A) > 0$ for an integral basis $\omega$ of $K$. Then there exist constellations of arbitrary shape in $O_K$ consisting of elements of $A$.

In fact, in the setting of Corollary 2.10, the conditions $d_{P_K \cap D}(A) > 0$ and $d_{P_K \cap D, \omega}(A) > 0$ are equivalent; see Subsection 7.3.

### 2.3 The idea of proofs and the organization of this paper

As mentioned in the previous section, Theorem 2.8 and Corollary 2.10 are the first major goals of this paper. We give an overview of proofs of them; they are based on the ‘fundamental diagram.’ See Figure 1. We use the relative hypergraph removal lemma due to Conlon–Fox–Zhao ([CFZ15, Theorem 2.12], Theorem 5.10) as a black box. Contrastingly, we do not appeal to Theorem 1.1 or Theorem 1.2 in the proof. Our proofs yield these theorems as special cases.

In what follows, we fix a number field $K$, its integral basis $\omega$ and a standard shape $S \subseteq O_K$. We will prove the existence of an $S$-constellation in $A$ by going back and forth among the ‘five worlds’ that appear in the horizontal sequence of the third line of Figure 1. We describe each world, in left-to-right order, as follows.

- **The world of hypergraphs $V$**: $V$ is an ($r$-uniform) hypergraph system which is constructed in Subsection 5.3 in the manner originated from Solymosi. Each vertex in $V$ represents a hyperplane in $\mathbb{Z}^r$. The mapping $T$, which connects two worlds $V$ and $\mathbb{Z}^r$, maps a hyperedge in $V$ to the intersection of the corresponding $r$ hyperplanes.

1 We do not actually consider the mapping $T$ whose domain is $V$, but we use this expression here instead of $T_j$ ($1 \leq j \leq r + 1$) introduced in Subsection 5.3. We use a similar convention for $E$ and $\nu$. See Subsection 5.3 for details.
A dense

\[ E \cap C \cap B \cap P_K \cap D_{(NL)} \cap V_T \rightarrow \nu \rightarrow \nu \rightarrow Z_r \phi \rightarrow \mathbb{R} \]

\[ \mathbb{Z}^r \rightarrow (O_K, \| \cdot \|_{\infty, \omega}, N) \rightarrow (O_K, \| \cdot \|_{\infty, \omega}, M) \rightarrow \text{id} \rightarrow (O_K, N, L) \]

Figure 1: The fundamental diagram

- **The world of higher dimension** \( \mathbb{Z}^r \): this is a free \( \mathbb{Z} \)-module of rank higher than (or equal to) that of \( O_K \simeq \mathbb{Z}^n \). The rank \( r \) is determined by \( r + 1 = \#S \). Via a homomorphism \( \phi_S : \mathbb{Z}^r \rightarrow O_K \) associated to \( S \), the standard basis and the origin of \( \mathbb{Z}^r \) provide a canonical lift of the shape \( S \). A constellation in \( \mathbb{Z}^r \) with this shape is called a *corner*.

- **The \( N \)-world** \( (O_K, \| \cdot \|_{\infty, \omega}, N) \): the following three worlds are all \( O_K \) as sets. In this world, we construct a pseudorandom measure \( \tilde{\lambda} \) by 'W-trick.' We use the \( \ell_\infty \)-length scale \( \| \cdot \|_{\infty, \omega} \) and the parameter \( N \).

- **The \( M \)-world** \( (O_K, \| \cdot \|_{\infty, \omega}, M) \): this is the world where the given set \( A \) lives, and it is connected to the \( N \)-world by an affine transformation. We use the \( \ell_\infty \)-length scale \( \| \cdot \|_{\infty, \omega} \) and the parameter \( M \).

- **The \( L \)-world** \( (O_K, N, L) \): this world is connected to the \( M \)-world by the identity map. The difference between these two worlds is that we take the (ideal) norm scale \( N \) in the \( L \)-world. We use the parameter \( L \).

The sketch of the proofs of Theorem 2.8 and Corollary 2.10 goes as follows.

**Step 1:** We start the proof from the ‘\( M \)-world.’ Take an NL-compatible \( O_K \)-fundamental domain \( D \) and a relatively dense subset \( A \) of \( P_K \cap D \). More precisely, the relative density of \( A \) measured by \( \ell_\infty \)-length \( \| \cdot \|_{\infty, \omega} \) with respect to \( P_K \cap D \) is greater than a certain positive constant. Our goal is to prove that if the parameter \( M \) is large enough, then there exists an \( S \)-constellation in \( A \). Since \( P_K \) is sparse in \( O_K \), we can not apply the classical multidimensional Szemerédi theorem (Theorem 5.2) directly to \( A \). Instead, we aim to show that the ‘weighted density’ of \( A \) with a certain weight function \( \lambda \) is not small. We define the weight function \( \lambda \) by using a variant of the von Mangoldt function. Since the norm scale \( N \) is easier to measure the desired density than the \( \ell_\infty \)-length scale \( \| \cdot \|_{\infty, \omega} \), we argue in the ‘\( L \)-world.'
Step 2: Apply the natural density version of the Chebotarev density theorem (Theorem 3.22) in the ‘\(L\)-world,’ and deduce the following: if \(A\) is relatively dense measured by the norm \(N\) with respect to \(\mathcal{P}_K \cap \mathcal{D}\), then the weighted density of \(A\) with \(\lambda\) is greater than a certain constant.

Step 3: Then we return to the ‘\(M\)-world.’ Here, the NL-compatibility of \(\mathcal{D}\) relates the density by norm to that by \(\ell_\infty\)-length. Hence, we conclude that the weighted density of \(A\) with \(\lambda\) measured by \(\ell_\infty\)-length is greater than a certain positive constant for the parameter \(M\). We warn that if \#(\mathcal{O}_K^\times) = \infty\), then the NL-compatibility of an \(\mathcal{O}_\times\)-fundamental domain is not automatic.

To the best of our knowledge, in order to apply known Szemerédi-type theorems to this \(A\), we need to confirm an extra condition on the measure \(\lambda\). More precisely, we aim to employ the relative multidimensional Szemerédi theorem, originated from Green–Tao [GT08]; \(\lambda\) is required to be a pseudorandom measure. Since it is difficult to show the pseudorandomness of \(\lambda\), we precompose a certain affine transformation to \(\lambda\) and investigate this modified function instead of \(\lambda\). Via this affine transformation, we switch from the ‘\(M\)-world’ to the ‘\(N\)-world.’

Step 4: We define \(B\) as the inverse image of \(A\) under the affine transformation \(\text{Aff}_{W,b}; \beta \mapsto W\beta + b\), where \(W\) is a positive integer determined by the parameter \(M\) and \(b\) is an element in \(\mathcal{O}_K\) determined by \(A\) and \(M\). We consider \(\lambda \circ \text{Aff}_{W,b}\) and define \(\tilde{\lambda}\) to be its normalization in an appropriate sense. Then we can prove the pseudorandomness of \(\tilde{\lambda}\) by using the Goldston–Yıldılım type asymptotic formula (Theorem 6.2). The proof utilizes the \(W\)-trick, which eliminates the bias caused by small prime numbers. In the ‘\(N\)-world,’ we can show that the weighted density of \(B\) with weight \(\tilde{\lambda}\) is still greater than a constant. Thus, it is possible to apply the relative multidimensional Szemerédi theorem (Theorem 5.4) and obtain an \(S\)-constellation in \(B\). In what follows, we also describe how this theorem is proved in this paper. For this purpose, the ‘world of higher dimension \(\mathbb{Z}^r\)’ shows up.

Step 5: Let \(C\) be the inverse image of \(B\) under \(\phi_S\) in the ‘world of higher dimension \(\mathbb{Z}^r\).’ Then the weighted density of \(C\) with weight \(\tilde{\lambda} \circ \phi_S\) is still greater than a constant.

Step 6: The weighted hypergraph \(\nu\) on \(V\) is constructed from \(\tilde{\lambda} \circ \phi_S\), and the pseudorandomness of \(\nu\) follows from that of \(\tilde{\lambda}\). Let \(E\) be the inverse image of \(C\) under \(T\). The elements of \(E\) are hyperedges. Since the weighted density of \(C\) is greater than a certain constant, removing hyperedges from \(E\) with small weighted density with weight \(\nu\) does not completely eliminate isomorphic copies of \(K_r^{(r)}\). Here \(K_r^{(r)}\) denotes the \((r + 1)\)-vertex complete \(r\)-graph. By the relative hypergraph removal lemma (Theorem 5.10), this implies that there exists an isomorphic copy of \(K_r^{(r)}\) whose \(r + 1\) hyperedges are sent to distinct \(r + 1\) points by \(T\), provided that \(M\) is large enough.

Step 7: By sending such a copy of \(K_r^{(r)}\) in \(E\) under \(T\), we obtain a corner consisting of elements of \(C\) in \(\mathbb{Z}^r\). The image of the resulting corner in \(C\) under \(\phi_S\) is an \(S\)-constellation in \(B\). This completes the rough description of the proof of our relative multidimensional
Szemerédi theorem.

Finally, the image of this $S$-constellation under $\text{Aff}_{W,b}$ is a desired $S$-constellation in $A$!

This is an overview of the proofs of Theorem 2.8 and Corollary 2.10, which are our first goals. It should be noted, however, that this paper is not actually written in the order described in Steps 1–7. At the beginning of Sections 5–7, we indicate the corresponding steps in this overview.

After achieving the first goal, we prove that Theorem $A$ (respectively, Corollary 2.10) and Theorem 2.8 (respectively, Theorem 1.4) are equivalent; see Remark 8.27. For this proof, we need a further counting argument, which is based on the geometry of numbers. In particular, Theorem $A$ is deduced from Theorem 2.8. Here we exhibit a key to this reduction; strictly speaking, we utilize the finitary version of Theorem 2.11.

**Theorem 2.11** (= Corollary 8.26). Let $K$ be a number field, $\omega$ its integral basis. Assume that $A \subseteq \mathcal{P}_K$ satisfies $d_{\mathcal{P}_K,\omega}(A) > 0$. Then, there exists an NL-compatible $O_K$-fundamental domain $D = D(A, \omega)$ such that

$$d_{\mathcal{P}_K \cap D, \omega}(A \cap D) > 0$$

holds.

See Theorem 8.19 in the case of the finitary version and Theorem 8.25 in the case of the infinitary version in full generality. In Section 8 where the above theorem is presented, we focus on the deduction ‘counting condition + pseudorandomness $\implies$ constellation theorem’ in our setting and axiomatize it. In Section 9 we refine the axiomatization as in Section 8 and prove Theorem 3 recall that this is a short interval version of Theorem $A$. There, a ‘slide trick,’ which follows from the pigeonhole principle, is in addition employed in order to take an appropriate $b$ in Step 4; see Lemma 9.9.

These axiomatizations can be furthermore extended to the case where the total space is a non-zero ideal $a$ of $O_K$. In Section 10 we prove our constellation theorem for a pair of an order in $K$ and its invertible fractional ideal with the aid of these extensions (Theorem 10.5). This theorem derives Theorem $C$ via the correspondence between binary quadratic forms and pairs of quadratic orders and their invertible fractional ideals (Theorem A.5). We present the proof of the correspondence in the appendix for the reader’s convenience. We remark that to define the counterpart of prime elements is non-trivial in our constellation theorem; see Definitions 10.4. For instance, if $a$ is not principal, then non-principal prime ideals show up in the definitions, in contrast to the case of Theorem 1.4.

We briefly summarize here the differences between the previous work [GT08, Tao06] and this paper. We have already discussed novelty and ideas for Goldston–Yıldırım type asymptotic formulas, the NL-compatibility and the setting without a fundamental domain in Introduction. The simplification of the proof of Goldston–Yıldırım type asymptotic formulas by using a smooth function $\chi$ was introduced by Tao subsequently to Green–Tao [GT08], and this method is also utilized in this paper.

There exist several different formulations of the ‘relative multidimensional Szemerédi theorem’ (RMST) in the literature. In this paper, we establish Theorem 5.4 seemingly, the
present paper may be the first place where the RMST of this form is explicitly stated. In the work of Green–Tao [GT08] and Tao [Tao06], a condition called the correlation condition was imposed on their definitions of pseudorandomness in addition to the linear forms condition. Conlon–Fox–Zhao [CFZ15] succeeded in removing this correlation condition from their formulations of the RMST. To do this, they proved the relative hypergraph removal lemma (RHRL) which only requires the linear forms condition. Note that the RMST in [CFZ15, Theorem 3.1] is stated in terms of finite additive groups, as is [GT08, Theorem 3.5] and [Tao06, Theorem 2.18]. For this reason, some additional arguments were needed in their work to switch from $\mathbb{Z}^n$ to finite additive groups, and to go back to the original setting of $\mathbb{Z}^n$. In this paper, although we appeal to the RHRL of Conlon–Fox–Zhao, we do not transfer our setting to that of finite additive groups. Instead, we follow the argument of Solymosi; see Steps 5–7 in the above overview. This enables us to remove the step of transferring a pseudorandom measure on $\mathbb{Z}^n$ to that on $(\mathbb{Z}/N\mathbb{Z})^n$. Moreover, our argument of estimating a weighted density seems more straightforward than that in the previous work. A slight disadvantage of our approach is that we need to take a ‘larger’ domain of variables to verify pseudorandomness. However, the Goldston–Yıldılım type asymptotic formula is strong enough to make this point negligible.

Due to the simplifications mentioned above, the complete proofs of Theorem A (the finitary version) and Theorem B (the short interval version) require no technical complication beyond that of Theorem 1.3. In some earlier work on constellation theorems for $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-1})$, detailed proofs of the corresponding theorems were omitted.

Plan. This paper is organized as follows: in Section 3 we briefly summarize some facts in algebraic number theory needed in this paper. In Section 4 we study the NL-compatibility by using the geometry of numbers, and give a geometric characterization of it (Theorem 4.7). We also construct an NL-compatible $O_K^\times$-fundamental domain $D_K(\epsilon, \sigma)$ from a fixed system of fundamental units $\epsilon$ of $K$ and a field embedding $\sigma: K \hookrightarrow \mathbb{C}$. We provide a proof of Lemma 4.14, which is a key to transferring our counting of ideals to that of elements. In Section 5 we formulate and prove our relative multidimensional Szemerédi theorem. In Section 6 we prove the Goldston–Yıldılım type asymptotic formula which is stated in terms of ideals. In Section 7 we present the full proof of Theorem 2.8. For this proof, we construct a pseudorandom measure with the aid of the Goldston–Yıldılım type asymptotic formula. Then we make an estimate of the weighted density of a well-chosen set and apply the relative multidimensional Szemerédi theorem. In Section 8 we prove Theorem A. In the proof, we axiomatize the argument in the proof of Theorem 2.8. By employing Lemma 4.14 we reduce the general setting of Theorem A to that with a fundamental domain; see Theorem 8.19 for details. Theorem 1.4 is also verified. In Section 9 we demonstrate Theorem B. The proof uses an additional argument, the ‘slide trick,’ to that of Theorem A. In Section 10 we formulate and prove our prime element constellation theorem with respect to the pair of an order and its invertible fractional ideal (Theorem 10.5). It derives a constellation theorem for a norm form (Theorem 10.36). By combining this with the classical correspondence between binary quadratic forms and the pairs where the orders are quadratic (Theorem A.5), we establish Theorem C. In Appendix, we present a proof of the correspondence above.
Notation. Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the set of positive integers, $\mathcal{P} = \{2, 3, 5, \ldots\}$ the set of rational prime numbers. A subset of $\mathcal{P}$ truncated by an inequality for a real number $x$ is expressed by putting a subscript with an inequality sign. For example,

$$\mathcal{P}_{\leq x} = \{p \in \mathcal{P} : p \leq x\}, \quad \text{and} \quad \mathcal{P}_{> x} = \{p \in \mathcal{P} : p > x\}.$$ 

For $m \in \mathbb{N}$, set $[m] := \{1, 2, 3, \ldots, m\}$. For $m_1, m_2 \in \mathbb{Z}$ satisfying $m_1 \leq m_2$, set $[m_1, m_2] := \{l \in \mathbb{Z} : m_1 \leq l \leq m_2\}$. When we use $[a_1, a_2]$ in the sense of a real closed interval, we write $[a_1, a_2]_{\mathbb{R}}$ to distinguish it. Similarly, in the case of (half-)open intervals, the real intervals are indicated by adding $\mathbb{R}$ as a subscript. For a finite set $A$, $\#A$ denotes the cardinality of $A$. We write $\#A = \infty$ to mean that the set $A$ is infinite. For a non-empty finite set $J$ and a positive integer $r$, $\binom{J}{r}$ denotes the set $\{e \in 2^J : \#e = r\}$. For a mapping $f$, $\text{Im}(f)$ denotes the image of $f$. For a set $A$, $1_A$ denotes the indicator function of $A$. For a function $f : X \to \mathbb{R}$ on a set $X$ and a non-empty finite subset $A \subseteq X$, we use the expectation symbol to denote the average of $f$ over $A$:

$$\mathbb{E}(f \mid A) = \mathbb{E}(f(a) \mid a \in A) := \frac{1}{\#A} \sum_{a \in A} f(a).$$

For functions $f, g : X \to \mathbb{R}$, if $f(x) \leq g(x)$ holds for all $x \in X$, then we express as $f \leq g$. For a $\mathbb{Z}$-module $\mathcal{O}$, $W \in \mathbb{Z}$ and $b \in \mathcal{O}$, the affine transformation $\text{Aff}_{W,b}$ is defined by

$$\text{Aff}_{W,b} : \mathcal{O} \to \mathcal{O} ; \; \beta \mapsto W\beta + b.$$ 

For $l \in \mathbb{N}$, $\log^l$ denotes the $l$ time composition of the natural logarithm $\log$.

We use big-$O$ and little-$o$ notation in the following sense for statements that take into account some parameters that are not necessarily ‘numbers.’ Let $x$ be a (natural, real or complex) numerical parameter and $t_1, \ldots, t_k$ a part of parameters under consideration. Let $a \in \mathbb{C}$. Let $f$ and $g$ be functions with parameters under consideration, where $g$ is non-negative. If there exists a positive valued function $C_{t_1,\ldots,t_k}$ depending only on $t_1, \ldots, t_k$ such that $|f| \leq C_{t_1,\ldots,t_k} \cdot g$, then we write $f = O_{t_1,\ldots,t_k}(g)$. If the inequality is valid only on a certain neighborhood of $a$, then we write $O_{x \to a;t_1,\ldots,t_k}(g)$. If there exists a positive valued function $c_{t_1,\ldots,t_k}(x)$ depending only on $x, t_1, \ldots, t_k$ and satisfying $\lim_{x \to a} c_{t_1,\ldots,t_k}(x) = 0$ such that $|f| \leq c_{t_1,\ldots,t_k} \cdot g$ on a certain neighborhood of $a$, then we write $f = o_{x \to a;t_1,\ldots,t_k}(g)$. The convergence of $c$ need not be uniform for $t_1, \ldots, t_k$. We use similar expressions for $a = +\infty$; in this case we only use a natural or positive real numerical parameter, and the symbol $+\infty$ is simply written as $\infty$ in this paper.

3 Preliminaries on algebraic number theory

In this section, we summarize necessary materials from algebraic number theory. All results in this section are known; see [Neu99] [Hec81] [HW08] for details.
Setting 3.1. Throughout this section, with the exception of Subsection 3.5, $K$ will denote a number field of degree $n$, that is, a finite extension of the rational number field $\mathbb{Q}$ with $n = [K : \mathbb{Q}]$.

3.1 The ring of integers and its ideals

The subset of $K$ consisting of elements which are integral over $\mathbb{Z}$ forms a subring called the ring of integers of $K$, and we denote it by $\mathcal{O}_K$. By [Neu99, Chapter I, Proposition 2.10], $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n$; a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is called an integral basis of $K$. We also denote by $\text{Idels}_K$ the set of nonzero ideals, and $|\text{Spec}(\mathcal{O}_K)|$ the set of nonzero prime ideals, of $\mathcal{O}_K$.

**Theorem 3.2** (Prime ideal decomposition, see [Neu99, Chapter I, Theorem 3.3]). The mapping

$$\bigoplus_{|\text{Spec}(\mathcal{O}_K)|} \mathbb{Z}_{\geq 0} \to \text{Idels}_K; \quad (e_p)_p \mapsto \prod_{p \in |\text{Spec}(\mathcal{O}_K)|} p^{e_p} \quad (3.1)$$

is an isomorphism of commutative monoids.

For two ideals $a \in \text{Idels}_K \cup \{(0)\}$ and $b \in \text{Idels}_K$, we write $b | a$ if $b \supseteq a$ holds. If $a \in \text{Idels}_K$, then this is equivalent to saying that the exponent of each $p$ appearing in the prime decomposition of $b$ is at most that of $a$.

In Section 10, we will treat fractional ideals of $\mathcal{O}_K$, which generalize ideals. A fractional ideal $a$ of $\mathcal{O}_K$ is a finitely generated $\mathcal{O}_K$-submodule of $K$. For a non-zero fractional ideal $a$ of $\mathcal{O}_K$, the set $a^{-1} := \{x \in K : xa \subseteq \mathcal{O}_K\}$ is again a non-zero fractional ideal, and $aa^{-1} = \mathcal{O}_K$ holds; see [Neu99, Chapter I, Proposition 3.8] for the proof. The following generalization of Theorem 3.2 will be employed in Section 10. Up to Section 9, fractional ideals will not show up.

**Theorem 3.3** (Prime ideal decomposition of fractional ideals, see [Neu99, Chapter I, Corollary 3.9]). The mapping from $\bigoplus_{|\text{Spec}(\mathcal{O}_K)|} \mathbb{Z}$ to the group of non-zero fractional ideals of $\mathcal{O}_K$ defined by

$$\bigoplus_{|\text{Spec}(\mathcal{O}_K)|} \mathbb{Z} \to \text{Idels}_K; \quad (v_p)_p \mapsto \prod_{p \in |\text{Spec}(\mathcal{O}_K)|} p^{v_p}$$

is an isomorphism of commutative groups.

We define the ideal norm of an ideal $a \in \text{Idels}_K$ by $N(a) := \#(\mathcal{O}_K/a)$. If $a$ is a principal ideal, that is, $a = \alpha \mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K \setminus \{0\}$, then $N(\alpha \mathcal{O}_K)$ coincides with the ideal norm $N(\alpha)$ of $\alpha$ defined in Definition 2.1.

Let $\sigma : K \to \mathbb{C}$ be a homomorphism of fields. If the image of $\sigma$ is contained in $\mathbb{R}$, then we call $\sigma$ a real embedding, and a complex embedding otherwise. If we denote by $r_1$ the number of real embeddings of $K$, and by $r_2$ that of conjugate pairs of complex embeddings of $K$, then $n = r_1 + 2r_2$ holds.

Setting 3.4. We denote by $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ the embeddings of $K$ into $\mathbb{C}$. We choose the numbering in such a way that $\sigma_1, \ldots, \sigma_{r_1}$ are real embeddings, while conjugate pairs of complex embeddings are $(\sigma_{r_1+1}, \sigma_{r_1+r_2+1}), (\sigma_{r_1+2}, \sigma_{r_1+r_2+2}), \ldots, (\sigma_{r_1+r_2}, \sigma_{r_1+2r_2})$. 
Lemma 3.5 (see [Neu99, Chapter 1, Proposition 2.6]). Under Setting 3.4, we have

\[ N(\alpha) = \prod_{i \in [r_1]} |\sigma_i(\alpha)| \prod_{j \in [r_2]} |\sigma_{r_1+j}(\alpha)|^2 \]

for \( \alpha \in \mathcal{O}_K \setminus \{0\} \).

In particular, \( N(W) = W^n \) for \( W \in \mathbb{N} \).

Remark 3.6. Conventionally, the norm of an element \( \alpha \in \mathcal{O}_K \) is defined to be the rational integer \( \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_{r_1+2r_2}(\alpha) \). In this paper, however, we denote by \( N(\alpha) \) the absolute value of this conventional norm. In Section 10, we use the symbol \( N_{K/\mathbb{Q}}(\alpha) \) for the conventional norm above. We remark that the ideal norm \( N(0) \) is undefined.

Lemma 3.7 (see [Neu99, Chapter I, Proposition 6.1]). Let \( a = \prod_{p \in |\text{Spec}(\mathcal{O}_K)|} p^{e_p} \) be the prime ideal decomposition of an ideal \( a \in \text{Ideals}_K \). Then

\[ N(a) = \prod_{p \in |\text{Spec}(\mathcal{O}_K)|} N(p)^{e_p}. \]

Next we introduce two number theoretic functions.

Definition 3.8. The \textit{totient function} \( \varphi_K \) of \( K \) is defined by

\[ \varphi_K : \text{Ideals}_K \to \mathbb{N}; \quad a \mapsto \#((\mathcal{O}_K/a)^\times). \]

For \( \alpha \in \mathcal{O}_K \setminus \{0\} \), we write \( \varphi_K(\alpha) := \varphi_K(\alpha \mathcal{O}_K) \).

Proposition 3.9 (see [Hec81, Theorem 80 in §27]). For \( a \in \text{Ideals}_K \), we have

\[ \varphi_K(a) = N(a) \prod_{p \in |\text{Spec}(\mathcal{O}_K)|, p|a} (1 - N(p)^{-1}). \]

Definition 3.10. We define the \textit{Möbius function} \( \mu_K : \text{Ideals}_K \to \{0, \pm 1\} \) by

\[ \mu_K(a) = \begin{cases} (-1)^r & \text{if } a \text{ is a product of } r \text{ distinct prime ideals,} \\ 0 & \text{otherwise.} \end{cases} \]

It follows from the definition that the Möbius function is \textit{multiplicative}, that is, \( \mu_K(ab) = \mu_K(a)\mu_K(b) \) for relatively prime ideals \( a \) and \( b \).

Proposition 3.11. Given a function \( f : \text{Ideals}_K \to \mathbb{C} \), define \( g : \text{Ideals}_K \to \mathbb{C} \) by

\[ g(a) := \sum_{b \in \text{Ideals}_K, b|a} f(b). \]

Then

\[ f(a) = \sum_{b,c \in \text{Ideals}_K, b \cdot c = a} \mu_K(b) \cdot g(c). \]
Proof. Since \( \text{Ideals}_K \) is isomorphic to \( \text{Ideals}_\mathbb{Q} \) as monoids by Theorem 3.2, the result follows from the property of the standard M"obius function \( \mu_{\mathbb{Q}} \).

The next lemma may be regarded as a refinement of complete multiplicativity of the ideal norm (Lemma 3.7), and will be employed in Section 8. We will present a proof of a more general statement of this lemma in Section 10; see Proposition 10.10.

Lemma 3.12. For \( a, b \in \text{Ideals}_K \), we have an isomorphism \( \mathcal{O}_K / b \simeq a / ab \) of \( \mathcal{O}_K \)-modules.

3.2 The unit group and ideal class group

The multiplicative group \( \mathcal{O}_K^{\times} \) of \( \mathcal{O}_K \) is called the unit group of \( K \). The subgroup of \( \mathcal{O}_K^{\times} \) consisting of torsion elements is denoted by \( \mu(K) \) (not to be confused with the M"obius function \( \mu_K \)). We continue to assume Settings 3.1 and 3.4.

Lemma 3.13 (see [Neu99, Chapter I, Proposition 7.1]). The group \( \mu(K) \) is finite. Moreover, an element \( \alpha \in \mathcal{O}_K \setminus \{0\} \) is a unit if and only if \( |\sigma_i(\alpha)| = 1 \) for all \( i \in [r_1 + r_2] \).

We define \( \overline{\mathcal{O}_K^{\times}} := \mathcal{O}_K^{\times} / \mu(K) \). The group \( \overline{\mathcal{O}_K^{\times}} \) is torsion-free with rank \( r_1 + r_2 - 1 \) by the celebrated theorem of Dirichlet (see [Neu99, Chapter I, Theorem 7.4]). See also Theorem 4.5.

A sequence \( \mathbf{e} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r_1+r_2-1}) \) which gives a basis \( (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r_1+r_2-1}) \) of \( \overline{\mathcal{O}_K^{\times}} \) is called fundamental units of \( K \).

There is an invariant of \( K \) called the class number which is a positive integer; this will show up in the Chebotarev density theorem. For the sake of completeness, let us give a quick definition. Define an equivalence relation \( \sim \) on \( \text{Ideals}_K \) as follows. We declare \( a \sim b \) if there exist \( \gamma, \delta \in \mathcal{O}_K \setminus \{0\} \) such that \( (\gamma) \cdot a = (\delta) \cdot b \) holds. The set of equivalence classes \( \text{Ideals}_K / \sim \) inherits the monoid structure from \( \text{Ideals}_K \). It is known that this is indeed a group (see [Neu99, Chapter I, Definition 3.7 to Proposition 3.8]), called the ideal class group. It is furthermore known that this is a finite group (see [Neu99, Chapter I, Theorem 6.3]), and its order, written \( h = h_K \), is the class number.

3.3 \( p \)-Ideals

Recall from Notation in Subsection 2.3 that the set of rational primes is denoted by \( \mathcal{P} = \{2, 3, 5, \ldots\} \). For \( p \in \text{Spec}(\mathcal{O}_K) \), the intersection \( p \cap \mathbb{Z} \) is a nonzero prime ideal of \( \mathbb{Z} \). Hence, there exists a unique \( p \in \mathcal{P} \) such that \( p \cap \mathbb{Z} = p\mathbb{Z} \). In this case, we call \( p \) a \( p \)-ideal, and the set of prime \( p \)-ideals is denoted by \( |\text{Spec}(\mathcal{O}_K)|(p) \). For \( p \in |\text{Spec}(\mathcal{O}_K)|(p) \), the quotient \( \mathcal{O}_K / p \) is a finite extension field of the finite prime field \( \mathbb{F}_p \). The extension degree \( f_p := [\mathcal{O}_K / p : \mathbb{F}_p] \) is called the degree of \( p \). Then \( N(p) = p^{f_p} \) holds.

For the prime ideal decomposition \( a = \prod_{p \in |\text{Spec}(\mathcal{O}_K)|(p)} p^{e_p} \) of \( a \in \text{Ideals}_K \), for each \( p \in \mathcal{P} \), we define

\[
a^{(p)} := \prod_{p \in |\text{Spec}(\mathcal{O}_K)|(p)} p^{e_p};
\]
it is called the $p$-part of $a$. Then we have

$$a = \prod_{p \in \mathcal{P}} a^{(p)}.$$ 

An ideal $a \in \text{Ideals}_K$ is called a $p$-ideal if $a^{(\ell)} = \mathcal{O}_K$ holds for all $\ell \in \mathcal{P} \setminus \{p\}$, or equivalently, $N(a)$ is a power of $p$. Observe that $\mathcal{O}_K$ is a $p$-ideal for every $p \in \mathcal{P}$. We denote the set of $p$-ideals of $\mathcal{O}_K$ by $\text{Ideals}^{(p)}_K$. For $a, b \in \text{Ideals}_K$ and $p \in \mathcal{P}$, we have $(a \cap b)^{(p)} = a^{(p)} \cap b^{(p)}$.

When $K = \mathbb{Q}$, we have $\mathcal{O}_K = \mathbb{Z}$, and the positive generator of the $p$-part of the ideal $D\mathbb{Z}$ for $D \in \mathbb{N}$ is denoted by $D^{(p)}$. We then have

$$D = \prod_{p \in \mathcal{P}} D^{(p)},$$

which is the prime factorization of $D$.

We now exhibit two lemmas needed in Section 6. Let $Z$ be a finite abelian group. Then $Z$ admits a unique decomposition into finite direct products $Z = \bigoplus_{p \in \mathcal{P}} Z^{(p)}$, where $Z^{(p)}$ is a $p$-group for each $p$. More explicitly, $Z^{(p)} = \{z \in Z : \exists e \geq 0, \, p^e \cdot z = 0\}$. We call $Z^{(p)}$ the $p$-part of $Z$.

**Lemma 3.14.** Let $p \in \mathcal{P}$.

1. Let $c \in \text{Ideals}_K$. The $p$-part $(\mathcal{O}_K/c)^{(p)}$ of the finite abelian group $\mathcal{O}_K/c$ is isomorphic to $\mathcal{O}_K/(c^{(p)})$ by the composition

$$(\mathcal{O}_K/c)^{(p)} \hookrightarrow \mathcal{O}_K/c \twoheadrightarrow \mathcal{O}_K/(c^{(p)}),$$

of the inclusion followed by the canonical surjection.

2. Let $Z$ and $W$ be finite abelian groups. Then the following map gives a bijection

$$\text{Hom}(Z, W) \xrightarrow{\sim} \bigoplus_{p \in \mathcal{P}} \text{Hom}(Z^{(p)}, W^{(p)}); \quad \psi \mapsto (\psi^{(p)})_{p \in \mathcal{P}},$$

where $\psi^{(p)}$ is defined as the restriction of $\psi$ to $Z^{(p)}$.

**Proof.** To prove (1), simply take the $p$-part of both sides of the isomorphism by the Chinese remainder theorem:

$$\mathcal{O}_K/c \xrightarrow{\sim} \prod_{p \in \mathcal{P}} \mathcal{O}_K/c^{(p)}.$$ 

Next we prove (2). Since $Z$ and $W$ are finite abelian groups, we have decompositions into finite direct products $Z \simeq \bigoplus_{p \in \mathcal{P}} Z^{(p)}$ and $W \simeq \bigoplus_{\ell \in \mathcal{P}} W^{(\ell)}$. This implies the direct sum decomposition

$$\text{Hom}(Z, W) \xrightarrow{\sim} \bigoplus_{p, \ell \in \mathcal{P}} \text{Hom}(Z^{(p)}, W^{(\ell)}) = \bigoplus_{p \in \mathcal{P}} \text{Hom}(Z^{(p)}, W^{(p)}),$$
where the last equality follows by observing that \( \text{Hom}(\mathbb{Z}^{(p)}, W^{(\ell)}) = 0 \) for \( p \neq \ell \). Thus, a homomorphism \( \psi : Z \to W \) is determined by its \( p \)-components \( \psi^{(p)} : Z^{(p)} \to W^{(p)} \). Since \( \psi^{(p)} \) is the composition of the three homomorphisms \( Z^{(p)} \xrightarrow{\psi_{|Z^{(p)}}} W^{(p)} \xhookrightarrow{} W \xrightarrow{} W^{(p)} \) in which the composition of the last two is the identity, the claimed correspondence follows.

An ideal \( a \in \text{Ideals}_K \) is said to be square-free if, in the prime ideal decomposition \( a = \prod_{p \in |\text{Spec}(\mathcal{O}_K)|} p^{e_p} \), the condition \( e_p \in \{0, 1\} \) holds for all \( p \in |\text{Spec}(\mathcal{O}_K)| \).

**Lemma 3.15.** For \( p \in \mathcal{P} \), we have \( \#(|\text{Spec}(\mathcal{O}_K)|^{(p)}) \leq n \). In particular, the number of square free \( p \)-ideals is at most \( 2^n \).

**Proof.** Every \( p \in |\text{Spec}(\mathcal{O}_K)|^{(p)} \) appears in the prime ideal decomposition of \( p\mathcal{O}_K \). Thus

\[
p\mathcal{O}_K = \prod_{p \in |\text{Spec}(\mathcal{O}_K)|^{(p)}} p^{e_p}, \quad e_p \in \mathbb{N}.
\]

Taking the norm of both sides using Lemma 3.7 we find

\[
n = \sum_{p \in |\text{Spec}(\mathcal{O}_K)|^{(p)}} f_p e_p \geq \#(|\text{Spec}(\mathcal{O}_K)|^{(p)}).
\]

This proves the first statement. The second statement follows from the first by the definition of square-freeness.

Despite that the following lemma itself is not on \( p \)-ideals, we present a corollary to the Chinese remainder theorem. Lemma 3.16 will be employed in Subsection 6.7 and Section 10.

In Lemma 3.16 by a ‘ring \( A \),’ we mean an associative commutative ring with unit.

**Lemma 3.16 (Chinese Remainder Theorem for modules).** Let \( M \) be a module over a ring \( A \) and \( a_1, \ldots, a_s \) mutually coprime ideals of \( A \). Then we have an equality of ideals

\[
\bigcap_{i \in [s]} a_i = \prod_{i \in [s]} a_i
\]

and the next natural maps of rings and \( A \)-modules are isomorphisms:

\[
A/(\prod_{i \in [s]} a_i) \xrightarrow{\sim} \prod_{i \in [s]} A/a_i, \tag{3.3}
\]

\[
M/(\prod_{i \in [s]} a_i) M \xrightarrow{\sim} \prod_{i \in [s]} M/a_i M. \tag{3.4}
\]

**Proof.** The Chinese remainder theorem provides \( \text{(3.2)} \) and \( \text{(3.3)} \). For \( \text{(3.4)} \), consider the tensor product of \( \text{(3.3)} \) and \( M \) over \( A \) and apply [AM16, Chapter 2, Exercise 2].
3.4 The Dedekind zeta function and density of ideals

In this subsection, we present some results on the Dedekind zeta function and density of ideals for a number field \( K \).

**Definition 3.17** (Dedekind zeta function; see [Neu99, Chapter VII, Definition 5.1]). The sum

\[
\sum_{a \in \text{Ideals}_K} \frac{1}{N(a)^s}
\]

converges absolutely and uniformly on every compact subset of the domain \( \Re(s) > 1 \) in the complex plane. Here we take the branch of log defined on \( \mathbb{C} \setminus \mathbb{R}_{\leq 0} \sqrt{-1} \), in order to define \( N(a)^s = e^{s \log N(a)} \). We call the analytic function defined by this sum the Dedekind zeta function of \( K \), and denote it by \( \zeta_K \).

**Proposition 3.18** (see [Neu99, Chapter VII, Proposition 5.2]). The infinite product

\[
\prod_{p \in |\text{Spec}(O_K)|} \left( 1 - \frac{1}{N(p)^s} \right)^{-1}
\]

converges absolutely on the domain \( \Re(s) > 1 \), and coincides with \( \zeta_K(s) \).

It is known that the Dedekind zeta function \( \zeta_K \) has analytic continuation to a meromorphic function on \( \mathbb{C} \). In this paper, however, we need only the property of \( \zeta_K \) around \( s = 1 \): it has a pole of order 1 at \( s = 1 \). More precisely, we only need the behaviour of \( \zeta_K(s) \) when \( s \) tends to 1 inside the domain \( \Re(s) > 1 \).

**Theorem 3.19** (The class number formula; [Hec81, Theorem 121 in §40]). There exists a constant \( \kappa = \kappa_K > 0 \) such that

\[
\zeta_K(s) = \frac{\kappa}{s-1} + O_{s \to 1; K}(1).
\]

The residue \( \kappa = \kappa_K \) can be expressed in terms of the class number \( h = h_K \) (Subsection 3.2) and an invariant called the regulator of \( K \). This is why Theorem 3.19 is known as the class number formula (see [Neu99, Chapter VII, Corollary 5.11 (ii)]). In this paper, however, we do not need the explicit form of \( \kappa \).

**Proposition 3.20** (Density of ideals; see [Hec81] Theorem 121 in §40]). The residue \( \kappa \) of \( \zeta_K \) at \( s = 1 \) coincides with the limit of the density of ideals in the following sense:

\[
\lim_{L \to \infty} \frac{\# \{ a \in \text{Ideals} : N(a) \leq L \}}{L} = \kappa > 0.
\]

As for the density of prime ideals, the following theorem is known. This theorem will be used to bound from the above the number of prime elements. See, for example, Proposition 8.14.
Theorem 3.21 (Landau’s prime ideal theorem, see [Hei67, Theorem 3]). We have

\[
\#\{p \in |\text{Spec}(\mathcal{O}_K)| : N(p) \leq L\} = (1 + o_{L \to \infty;K}(1)) \cdot \frac{L}{\log L}.
\]

The ring of integers \(\mathcal{O}_K\) is not necessarily a principal ideal domain. There may be a prime ideal which is not generated by a single element. A special case of the natural density version of the Chebotarev density theorem (Theorem 3.22 below) implies that, principal prime ideals constitute a positive fraction among all prime ideals. This fact plays a key role in this paper.

We denote by \(|\text{Spec}(\mathcal{O}_K)|^{PI}\) the set of nonzero principal prime ideals of \(\mathcal{O}_K\). For the sake of completeness, we provide a proof of the following theorem because its statement differs from that of [Hei67, Theorem 4].

**Theorem 3.22** (Special case of the natural density version of the Chebotarev density theorem). Let \(h\) be the class number of \(K\). Then

\[
\#\{p \in |\text{Spec}(\mathcal{O}_K)|^{PI} : N(p) \leq L\} = (1 + o_{L \to \infty;K}(1)) \cdot \frac{1}{h} \cdot \frac{L}{\log L}.
\]

**Proof.** We can define a modified ideal class group \(\text{Cl}_m^m\) for each ideal \(m \in \text{Ideals}_K\); see [Neu99, Chapter VI, before Proposition 1.9]. The finite group \(\text{Cl}_m^m\) is a quotient of the monoid

\[
\text{Ideals}_m^m := \{a \in \text{Ideals}_K : a \text{ is relatively prime to } m\},
\]

and it has \(\text{Cl}_K\) as a homomorphic image. We use this fact only for \(m = 1 := \mathcal{O}_K\); see [Neu99, Chapter VI, Proposition 1.11].

In [Hei67], the order of the group \(\text{Cl}_m^m\) is denoted by \(h_m\), although no name is given to the group itself ([Hei67, p.209]). For \(C \in \text{Cl}_K\), let \(|\text{Spec}(\mathcal{O}_K)|_C\) denote the subset of \(|\text{Spec}(\mathcal{O}_K)|\) consisting of prime ideals \(p \in |\text{Spec}(\mathcal{O}_K)|\) with \(p \nmid m\) such that \(p\) is mapped to \(C\) by the canonical surjection \(\text{Ideals}_m^m \rightarrow \text{Cl}_m^m\). The density theorem, see [Hei67, Theorem 4 on p.214], asserts that, for every \(C \in \text{Cl}_K\),

\[
\#\{p \in |\text{Spec}(\mathcal{O}_K)|_C : N(p) \leq L\} = (1 + o_{L \to \infty;m}(1)) \cdot \frac{1}{h_m} \cdot \frac{L}{\log L}.
\]

Specializing this formula to the case \(m = 1\) and taking the sum over all \(C \in \text{Cl}_K\) whose image is the identity under the epimorphism \(\text{Cl}_m^m \rightarrow \text{Cl}_K\), we obtain the desired result. \(\square\)

**Remark 3.23.** The analytic density version of the Chebotarev density theorem given below may look more familiar to some readers (see [Neu99, Chapter VII, Theorem 13.2]):

\[
\lim_{s \to 1+0} \frac{\prod_{p \in |\text{Spec}(\mathcal{O}_K)|^{PI}} \left(1 - \frac{1}{N(p)^s}\right)^{-1}}{\log \left(\frac{1}{s-1}\right)} = \frac{1}{h}.
\]
In general, if \( f(s) = \sum_{n \geq 1} \frac{a_n}{n^s} \) is a Dirichlet series convergent in the domain \( \text{Re}(s) > 1 \), the following inequality is known:

\[
\limsup_{x \to +\infty} \frac{\sum_{1 \leq n \leq x} a_n}{\log \left( \frac{x}{\log x} \right)} \geq \limsup_{s \to 1+0} f(s) \log \left( \frac{1}{s-1} \right).
\]

The proof is straightforward in Abel’s summation method. See, for example, [Lan53, Theorem on p.118]. Combining this with (3.5), we obtain the following estimate for the number of principal prime ideals holds for infinitely many \( x \in \mathbb{N} \):

\[
\# \{ p \in |\text{Spec}(\mathcal{O}_K)|^{\mathrm{PI}} : N(p) \leq x \} \geq \frac{1}{2h} \cdot \frac{x}{\log x}.
\]

Whereas the assertion above is weaker than that of Theorem 3.22, this suffices to prove Theorem 1.3 and Corollary 1.5.

### 3.5 Distribution of rational primes

In this subsection we list three results concerning on the distribution of primes in \( K = \mathbb{Q} \). We use the notation introduced in Subsection 2.3. As in Subsection 3.4, \( L \) will denote a real parameter greater than 1. The number of rational primes not exceeding \( L \) is denoted by \( \pi(L) \).

The first result, Lemma 3.24 below, will be used in the proof of Lemma 6.24.

**Lemma 3.24.** For \( L > 1 \), we have

\[
\sum_{p \in \mathcal{P} > L} \frac{1}{p^2} = O \left( \frac{1}{L \log L} \right).
\]

**Proof.** It follows from inequality (3.6) below and [HW08, (22.4.2)] that

\[
\pi(L) \leq L^{3/2} + \frac{5}{3} \cdot \frac{\vartheta(L)}{\log L} \leq \left( 1 + \frac{10}{3} \log 2 \right) \cdot \frac{L}{\log L} < \frac{3.5L}{\log L}.
\]

By Abel’s summation formula (see [HW08, Theorem 421]), we obtain

\[
\sum_{p \in \mathcal{P} > L} \frac{1}{p^2} = -\frac{\pi(L)}{L^2} + 2 \int_L^\infty \frac{\pi(t)}{t^3} \, dt \leq 7 \int_L^\infty \frac{dt}{t^2 \log t} \leq \frac{7}{L \log L},
\]

as desired.

The second result is known as Mertens’s first theorem. It will be used in the proof of Lemma 6.26.
Proposition 3.25 (Mertens’s first theorem; see [HW08, Theorem 425]). For \( L \geq 2 \),
\[
\sum_{p \in \mathcal{P} \leq L} \frac{\log p}{p} = \log L + O(1).
\]
The third result is an upper bound on the first Chebyshev function \( \vartheta(L) \) defined by
\[
\vartheta(L) = \sum_{p \in \mathcal{P} \leq L} \log p.
\]
Proposition 3.26 (Chebyshev’s theorem; see [HW08, Theorem 415]). For \( L \geq 1 \), we have
\[
\vartheta(L) \leq 2(\log 2)L. \tag{3.6}
\]
The estimate in the proposition above will be employed for the choice of \( w = w(M) \) in Section 7. In fact, the celebrated prime number theorem provides a sharper estimate; but we do not utilize it in the present paper.

Theorem 3.27 (The prime number theorem; see [HW08, Theorem 7, Theorem 420]). We have
\[
\vartheta(L) = (1 + o_{L \to \infty}(1))L \tag{3.7}
\]
and
\[
\pi(L) = (1 + o_{L \to \infty}(1)) \cdot \text{Li}(L), \tag{3.8}
\]
where \( \text{Li}(L) \) denotes the logarithmic integral
\[
\text{Li}(L) := \int_{2}^{L} \frac{dt}{\log t} = (1 + o_{L \to \infty}(1)) \cdot \frac{L}{\log L}. \tag{3.9}
\]
Note that the asymptotic formulas (3.7) and (3.8) are equivalent. The former gives the ultimate improvement of the inequality (3.6) when \( L \to \infty \), while the latter can be considered as the special cases of Theorem 3.21 and of Theorem 3.22 when \( K = \mathbb{Q} \).

4 Norm-length compatibility and geometry of numbers

In this section, we study the NL-compatibility of subsets of \( \mathcal{O}_K \setminus \{0\} \), which is introduced in Definition 2.7. For this, we employ the geometry of numbers; in Subsection 4.1 we recall some related definitions, including Minkowski embeddings. We characterize the NL-compatibility in terms of the weighted multiplicative Minkowski embedding (Theorem 4.7) in Subsection 4.2. Then we provide a way of constructing an NL-compatible \( \mathcal{O}_K^\times \)-fundamental domain (Definition 4.10, Proposition 4.11) in Subsection 4.3. The existence of an NL-compatible fundamental domain plays a key role throughout the present paper. In Subsection 4.4 we estimate the size of a part of an \( \mathcal{O}_K^\times \)-orbit of the action \( \mathcal{O}_K^\times \acts \mathcal{O}_K \setminus \{0\} \), bounded by an \( \ell_\infty \)-length. The results, Lemma 4.14 and Corollary 4.16, enable us to switch from ideal countings to element countings in Sections 8–10. Here is the setting of this section.
Setting 4.1. Let $K$ be a number field of degree $n$, and let $\omega = (\omega_1, \ldots, \omega_n)$ be an integral basis of $K$. Let $\epsilon$ be fundamental units of $K$. We also use the notation defined in Setting 3.4 for embeddings. We say that a subset of a finite-dimensional real vector space is bounded if it is bounded with respect to some norm.

The notion of boundedness is independent of the choice of a norm. Indeed, it is equivalent to relative compactness in the natural topology.

4.1 Weighted multiplicative Minkowski embedding

Throughout this subsection, we use Setting 4.1. In this section, we introduce the additive Minkowski embedding and weighted multiplicative Minkowski embedding. Here, we consider a weight on the multiplicative Minkowski embedding, which may not be standard in the literature; see Remark 4.9 for more details. We define

\[ \sigma_{i,\mathbb{R}} : K \otimes \mathbb{Q} \to \mathbb{R} \quad (i \in [r_1]), \]
\[ \sigma_{r_1+j,\mathbb{R}} : K \otimes \mathbb{Q} \to \mathbb{C} \quad (j \in [2r_2]) \]

as extensions of $\sigma_i$ ($i \in [r_1]$) and $\sigma_{r_1+j}$ ($j \in [2r_2]$), respectively. Then we define $N_{\mathbb{R}} : K \otimes \mathbb{Q} \to \mathbb{R}$ by

\[ N_{\mathbb{R}}(x) := \prod_{i \in [r_1]} |\sigma_{i,\mathbb{R}}(x)| \prod_{j \in [r_2]} |\sigma_{r_1+j,\mathbb{R}}(x)|^2. \quad (4.1) \]

Compare this with Lemma 3.5. Note that $N_{\mathbb{R}}(0) = 0$ while the ideal norm $N(0)$ is undefined.

Definition 4.2. We define the additive Minkowski embedding

\[ \mathcal{M}_{\mathbb{R}} : K \otimes \mathbb{Q} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \]

by

\[ \mathcal{M}_{\mathbb{R}}(x) := (\sigma_{1,\mathbb{R}}(x), \ldots, \sigma_{r_1,\mathbb{R}}(x); \sigma_{r_1+1,\mathbb{R}}(x), \ldots, \sigma_{r_1+r_2,\mathbb{R}}(x)) \quad (x \in K \otimes \mathbb{Q}). \]

The restriction of $\mathcal{M}_{\mathbb{R}}$ to $K$ will be denoted by $\mathcal{M}$. We also define the weighted multiplicative Minkowski embedding

\[ \mathcal{L}_{\mathbb{R}} : (K \otimes \mathbb{Q}) \setminus \{x \in K \otimes \mathbb{Q} : N_{\mathbb{R}}(x) = 0\} \to \mathbb{R}^{r_1+r_2} \]

by

\[ \mathcal{L}_{\mathbb{R}}(x) := \log(\mathcal{M}_{\mathbb{R}}(x)), \quad (4.2) \]

where $x \in K \otimes \mathbb{Q}$ with $N_{\mathbb{R}}(x) \neq 0$, and $\log : (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \to \mathbb{R}^{r_1+r_2}$ is defined by

\[ \log(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) = (\log|x_1|, \ldots, \log|x_{r_1}|, \sqrt{2}\log|z_1|, \ldots, \sqrt{2}\log|z_{r_2}|). \]

The restriction of $\mathcal{L}_{\mathbb{R}}$ to $K^\times$ will be denoted by $\mathcal{L}$.

Lemma 4.3. The additive Minkowski embedding $\mathcal{M}_{\mathbb{R}}$ is an isomorphism of $\mathbb{R}$-vector spaces.
Proof. This follows from \cite{Neu99} Chapter I, Proposition 5.2. \qed

It follows from Lemma 4.3 that $L : K^\times \to \mathbb{R}^{r_1+r_2}$ is a homomorphism of groups, with $\mu(K) \subseteq \ker L$. In fact, it induces an injection $\overline{Z} : \overline{O}_K^\times \to \mathbb{R}^{r_1+r_2}$ by Lemma 3.13.

**Definition 4.4** (The hyperplane $H$ and vector $u_0$). We define a vector $u_0 \in \mathbb{R}^{r_1+r_2}$ by

$$u_0 := (1, 1, \ldots, 1, \sqrt{2}, \sqrt{2}, \ldots, \sqrt{2}).$$

Then we define the hyperplane $H$ in $\mathbb{R}^{r_1+r_2}$ by

$$H := \{ x \in \mathbb{R}^{r_1+r_2} : \langle x, u_0 \rangle = 0 \}.$$ 

Here, $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{R}^{r_1+r_2}$. We denote by $P_H$ the orthogonal projection from $\mathbb{R}^{r_1+r_2}$ onto the hyperplane $H$.

Observe $P_H(u_0) = 0$, since $\mathbb{R}^{r_1+r_2} = H \oplus \mathbb{R}u_0$ (orthogonal direct sum).

**Theorem 4.5.** The image $\overline{Z}(\overline{O}_K^\times)$ is a lattice of full rank in the hyperplane $H$.

Proof. This follows from \cite{Neu99} Chapter I, Theorem 7.3. \qed

### 4.2 Geometric characterization of the NL-compatibility

We continue to use Setting 4.1.

**Lemma 4.6.** Let $Z$ be a subset of $K \otimes_\mathbb{Q} \mathbb{R}$. Then the following statements hold.

1. The set $Z$ is bounded if and only if $M_\mathbb{R}(Z)$ is bounded.
2. If $Z \subseteq (K \otimes_\mathbb{Q} \mathbb{R}) \setminus \{ x : N_{K,\mathbb{R}}(x) = 0 \}$ and $L_\mathbb{R}(Z)$ is bounded, then so is $Z$.
3. Assume that $Z \subseteq (K \otimes_\mathbb{Q} \mathbb{R}) \setminus \{ x : N_{K,\mathbb{R}}(x) = 0 \}$ is bounded and $\inf\{ N_{\mathbb{R}}(x) \mid x \in Z \} > 0$. Then $L_\mathbb{R}(Z)$ is bounded.

Proof. Item [1] is obvious by Lemma 4.3. To prove [2], since $L_\mathbb{R}(Z)$ is bounded, we see that $\log^{-1}(L_\mathbb{R}(Z))$ is bounded. Since $M_\mathbb{R}(Z) \subseteq \log^{-1}(L_\mathbb{R}(Z))$ by (4.2), $M_\mathbb{R}(Z)$ is also bounded. Hence, $Z$ is bounded by [1]. To show [3], since $Z$ is bounded, $M_\mathbb{R}(Z)$ is also bounded by [1]. This implies that the set

$$C = \sup\{|\sigma_{j,\mathbb{R}}(x)| : x \in Z, j \in [r_1 + r_2]\}$$

is finite. Let

$$c = \inf\{ N_{K,\mathbb{R}}(x) \mid x \in Z \}.$$

Then by assumption, we have $c > 0$. Thus, for $x \in Z$ and $j \in [r_1 + r_2],$

$$|\sigma_{j,\mathbb{R}}(x)| \geq \frac{N_{K,\mathbb{R}}(x)}{\prod_{i \in [n] \setminus \{j\}} |\sigma_{i,\mathbb{R}}(x)|} \geq \frac{c}{C^{n-1}}.$$
This implies
\[ \mathcal{L}_R(Z) \subseteq \left[ \log \frac{C}{C^{n-1}}, \log C \right]_R \times \left[ \sqrt{2} \log \frac{C}{C^{n-1}}, \sqrt{2} \log C \right]_R, \]
and hence \( \mathcal{L}_R(Z) \) is bounded. \( \square \)

**Theorem 4.7** (Geometric characterization of the NL-compatibility). With reference to Setting 4.1, the following statements are equivalent for \( X \subseteq \mathcal{O}_K \setminus \{0\} \).

(i) \( X \) is NL-compatible;

(ii) \( (\mathbf{P}_H \circ \mathbf{L})(X) \subseteq \mathcal{H} \) is bounded. Here \( \mathcal{H} \) and \( \mathbf{P}_H \) are defined in Definition 4.4.

**Proof.** Note that the \( \ell_\infty \)-length \( \| \cdot \|_{\infty, \omega} \) defined in Definition 2.2 can be naturally extended to \( K \) with values in \( \mathbb{Q} \), and then to \( K \otimes \mathbb{Q} \mathbb{R} \) with values in \( \mathbb{R} \). We denote the latter by
\[ \| \cdot \|_{\infty, \omega, \mathbb{R}} : K \otimes \mathbb{Q} \mathbb{R} \to \mathbb{R} \]
\[ \alpha \otimes t \mapsto \max_{i \in [n]} |t \alpha_i|, \]
where \( \alpha = \sum_{i \in [n]} a_i \omega_i, (a_1, \ldots, a_n) \in \mathbb{Q}^n \). This makes \( K \otimes \mathbb{Q} \mathbb{R} \) into a normed vector space over \( \mathbb{R} \), which is finite dimensional. Let
\[ \tilde{X} := \{ N(\alpha)^{-1/n} \alpha : \alpha \in X \} \subseteq K \otimes \mathbb{Q} \mathbb{R}. \]

It follows from Definition 2.7 that (i) is equivalent to boundedness of \( \tilde{X} \). Since
\[ N_{K, \mathbb{R}}(\tilde{\alpha}) = 1 \quad (\tilde{\alpha} \in \tilde{X}), \]
we can use Lemma 4.6 (2) and (3) to conclude that \( \tilde{X} \) is bounded if and only if \( \mathcal{L}_R(\tilde{X}) \) is bounded. Therefore, it only remains to establish
\[ \mathcal{L}_R(\tilde{X}) = (\mathbf{P}_H \circ \mathbf{L})(X). \]

Observe that, for \( t > 0 \) and \( x \in K \otimes \mathbb{Q} \mathbb{R} \) with \( N_{K, \mathbb{R}}(x) \neq 0 \), we have
\[ \mathcal{L}_R(t \cdot x) = \mathcal{L}_R(x) + (\log t) \cdot u_0. \]

By (4.3), we have \( \mathcal{L}_R(\tilde{X}) \subseteq \mathcal{H} \), and hence
\[ \mathcal{L}_R(\tilde{X}) = \mathbf{P}_H(\mathcal{L}_R(\tilde{X})) \]
\[ = \{ \mathbf{P}_H(\mathcal{L}_R(N(\alpha)^{-1/n} \alpha)) : \alpha \in X \} \]
\[ = \{ \mathbf{P}_H(\mathcal{L}_R(\alpha)) + (\log N(\alpha)^{-1/n})u_0 : \alpha \in X \} \quad \text{(by 4.4)} \]
\[ = \{ \mathbf{P}_H(\mathcal{L}(\alpha)) : \alpha \in X \} \]
\[ = (\mathbf{P}_H \circ \mathbf{L})(X). \]

This completes the proof. \( \square \)
We regard $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as a normed real vector space by introducing the norm $\| \cdot \|_\infty$ defined by
\[
\|(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})\|_\infty = \max\{|x_1|, \ldots, |x_{r_1}|, |z_1|, \ldots, |z_{r_2}|\}.
\]

**Lemma 4.8.** Define
\[
\Theta := \max_{i \in [n]} \sum_{j \in [n]} |\sigma_i(\omega_j)|.
\]
Then, for all $\alpha \in \mathcal{O}_K \setminus \{0\}$, we have inequalities
\[
\|\mathcal{M}(\alpha)\|_\infty \leq \Theta \|\alpha\|_{\infty, \omega}, \quad (4.7)
\]
\[
\mathcal{N}(\alpha) \leq \Theta^n \|\alpha\|_{\infty, \omega}^n. \quad (4.8)
\]

**Proof.** For $\alpha \in \mathcal{O}_K$, we have $|\sigma_i(\alpha)| \leq \Theta \|\alpha\|_{\infty, \omega}$ for all $i \in [n]$. This implies (4.7). Then (4.8) follows from (4.7) and Lemma 3.5. 

Let $\mathcal{D}$ be an NL-compatible $\mathcal{O}_K^\times$-fundamental domain on $\mathcal{O}_K \setminus \{0\}$. Then there exist constants $C = C(\omega; \mathcal{D}) > 0$ and $C' = C'(\omega) > 0$ such that
\[
C \|\alpha\|_{\infty, \omega}^n \leq \mathcal{N}(\alpha) \leq C' \|\alpha\|_{\infty, \omega}^n \quad (\alpha \in \mathcal{D}). \quad (NLC)
\]
Indeed, the existence of $C$ follows from Definition 2.7 while that of $C'$ is ensured by Lemma 4.8. The inequality (NLC) will be used frequently in Sections 7 and 9.

**Remark 4.9.** In a conventional definition of the multiplicative Minkowski embedding, the coefficients of the logarithm of the imaginary embeddings are 2, instead of $\sqrt{2}$ in our Definition 4.2. It has an advantage that the conditions $\mathcal{L}(\mathcal{O}_K^\times) \subseteq \mathcal{H}$, $\mathbb{R}u_0 \perp \mathcal{H}$ and (4.4) all hold. The vector $u_0$ will be used in the counting of elements of $\mathcal{O}_K^\times$-orbits in Subsection 4.4, as well as in the discussion of the NL-compatibility in Subsections 4.2 and 4.3.

### 4.3 Construction of the domain $\mathcal{D}_K(\epsilon, \sigma)$

We continue to use Setting 4.1. We fix fundamental units $\epsilon = (\epsilon_1, \ldots, \epsilon_{r_1+r_2-1})$, and define
\[
u_i = L(\pi_i) \quad (i \in [r_1 + r_2 - 1]).
\]
Then $u_1, u_2, \ldots, u_{r_1+r_2-1}$ form a basis of $\mathcal{H}$, and hence $u_0, u_1, \ldots, u_{r_1+r_2-1}$ form a basis of $\mathbb{R}^{r_1+r_2}$.

In this subsection, we first introduce a domain $\tilde{\mathcal{D}}_K(\epsilon)$. The construction of $\tilde{\mathcal{D}}_K(\epsilon)$ is closely related to density of ideals in Subsection 3.4. See for instance, [Hec81, §40]. Given an embedding $\sigma: K \hookrightarrow \mathbb{C}$, we then construct a fundamental domain $\mathcal{D}_K(\epsilon, \sigma)$ for the action $\mu(K) \curvearrowright \tilde{\mathcal{D}}_K(\epsilon)$. The domain $\mathcal{D}_K(\epsilon, \sigma)$ will turn out to be an NL-compatible $\mathcal{O}_K^\times$-fundamental domain in Proposition 4.11.

**Definition 4.10 (The fundamental domain $\mathcal{D}(\epsilon, \sigma)$).** We define
\[
\mathcal{C}_K(\epsilon) = \left\{ \left( \sum_{i \in [r_1+r_2-1]} y_i u_i \right) + y_0 u_0 : y_i \in [0, 1) \ (i \in [r_1 + r_2 - 1]), \ y_0 \in \mathbb{R} \right\}.
\]
By Definition 4.10 (1), we have

\[ \tilde{D}_K(\mathfrak{e}) := L_\mathbb{R}^{-1}(C_K(\mathfrak{e})) \cap (O_K \setminus \{0\}). \]

(2) For an embedding \( \sigma : K \hookrightarrow \mathbb{C} \), we define a subset \( D_K(\mathfrak{e}, \sigma) \) of \( O_K \setminus \{0\} \) as

\[ D_K(\mathfrak{e}, \sigma) := \left\{ \alpha \in \tilde{D}_K(\mathfrak{e}) : 0 \leq \arg(\sigma(\alpha)) < \frac{2\pi}{\#\mu(K)} \right\}, \]

where \( \arg \) denotes the argument of a nonzero complex number.

**Proposition 4.11.** For an embedding \( \sigma : K \hookrightarrow \mathbb{C} \), the set \( D_K(\mathfrak{e}, \sigma) \subseteq O_K \setminus \{0\} \) is an \( O_K^\times \)-fundamental domain which is NL-compatible.

**Proof.** By Definition 4.10 (1), we have

\[ (P_{\mathfrak{e}} \circ L)(\tilde{D}_K(\mathfrak{e})) \subseteq C_K(\mathfrak{e}) \cap \mathcal{H}. \]

Since \( C_K(\mathfrak{e}) \) is bounded, this implies that \( (P_{\mathfrak{e}} \circ L)(\tilde{D}_K(\mathfrak{e})) \) is bounded. Then by Theorem 4.7, \( \tilde{D}_K(\mathfrak{e}) \) is NL-compatible. Since \( D_K(\mathfrak{e}, \sigma) \subseteq \tilde{D}_K(\mathfrak{e}) \), \( D_K(\mathfrak{e}, \sigma) \) is also NL-compatible.

Next we show that \( D_K(\mathfrak{e}, \sigma) \) is an \( O_K^\times \)-fundamental domain. It is clear from Definition 4.10 that \( D_K(\mathfrak{e}, \sigma) \subseteq O_K \setminus \{0\} \). Since \( \mu(K) \) is a cyclic group, we can write \( \sigma(\mu(K)) = \langle \zeta \rangle \), where \( \zeta = e^{2\pi \sqrt{-1}/(\#\mu(K))} \in \mathbb{C} \). Thus

\[ \sigma(\tilde{D}_K(\mathfrak{e})) = \bigsqcup_{\xi \in \mu(K)} \sigma(\xi D_K(\mathfrak{e}, \sigma)). \quad (4.10) \]

Since \( \mathbb{R}^{r_1 + r_2} = \bigsqcup_{\eta \in O_K^\times} (\mathcal{L}(\eta) + \mathcal{C}(\mathfrak{e})) \), we have

\[ O_K \setminus \{0\} = \bigsqcup_{\eta \in O_K^\times} \mathcal{L}^{-1}(\mathcal{L}(\eta) + \mathcal{C}(\mathfrak{e})) \cap (O_K \setminus \{0\}) = \bigsqcup_{\eta \in O_K^\times} \eta \bigsqcup_{\xi \in \mu(K)} \eta D_K(\mathfrak{e}, \sigma) \]

by (4.10). Therefore, \( D_K(\mathfrak{e}, \sigma) \) is an \( O_K^\times \)-fundamental domain.

**Example 4.12.** For \( K = \mathbb{Q}(\sqrt{2}) \), the ring of integers is \( O_K = \mathbb{Z}[\sqrt{2}] \), and we may take fundamental units to be \( \mathfrak{e} = (1 + \sqrt{2}) \). We illustrate \( \tilde{D}_K(\mathfrak{e}) \) by depicting \( L_\mathbb{R}^{-1}(C_K(\mathfrak{e})) \) and its image \( C_K(\mathfrak{e}) \) under \( L_\mathbb{R} \) (see Figure 2). Define an embedding \( \sigma : K \hookrightarrow \mathbb{C} \) by \( \sigma(x + y\sqrt{2}) = x + \sqrt{2}y \ (x, y \in \mathbb{Q}) \). Since \( \mu(K) = \{ \pm 1 \} \), the \( O_K^\times \)-fundamental domain \( D_K(\mathfrak{e}, \sigma) \) consists of the upper right half of \( \tilde{D}_K(\mathfrak{e}) \) in Figure 2. Indeed,

\[ C_K(\mathfrak{e}) = \{ y_0(1, 1) + y_1(\log(\sqrt{2} + 1), \log(\sqrt{2} - 1) : y_0 \in \mathbb{R}, y_1 \in [0, 1) \}
\]

\[ = \{(x, y) : x, y \in \mathbb{R}, 0 \leq x - y < \log(3 + 2\sqrt{2}) \}, \]

\[ L_\mathbb{R}^{-1}(C_K(\mathfrak{e})) = \{ a + b\sqrt{2} : a, b \in \mathbb{R}, a > 2b \geq 0 \text{ or } b > a \geq 0 \}
\]

\[ \cup \{ a + b\sqrt{2} : a, b \in \mathbb{R}, a < 2b \leq 0 \text{ or } b < a \leq 0 \}, \]

and

\[ D_K(\mathfrak{e}, \sigma) = \{ a + b\sqrt{2} : a, b \in \mathbb{Z}, a > 2b \geq 0 \text{ or } b > a \geq 0 \}. \]
The following statement explains why we need the notion of the NL-compatibility.

**Proposition 4.13.** Assume the unit group of $K$ is infinite, equivalently, $r_1 + r_2 \geq 2$. Let $S \subseteq \mathcal{O}_K$ be a finite subset with $\#S \geq 3$. Then there exists an $\mathcal{O}_K^\times$-fundamental domain $\mathcal{D}_S \subseteq \mathcal{O}_K \setminus \{0\}$ such that $\mathcal{D}_S$ contains no $S$-constellation.

**Proof.** By Lemma 3.13, we have $(\mathcal{O}_K \setminus \{0\}) \cap \ker \mathcal{L} = \mu(K)$. Since $\mathcal{O}_K^\times$ is infinite, there exists $\varepsilon \in \mathcal{O}_K^\times \setminus \ker \mathcal{L}$. We claim, for all $\alpha \in \mathcal{O}_K \setminus \{0\}$,

$$\lim_{m \to \infty} \|M_{\mathbb{R}}(\varepsilon^m \alpha)\|_{\infty} = \infty. \quad (4.11)$$

Indeed, since $\varepsilon \in \mathcal{O}_K^\times$, we have $1 = N(\varepsilon)$, while $\mathcal{L}(\varepsilon) \neq 0$ implies that $|\sigma_i(\varepsilon)| \neq 1$ for some $i \in [n]$. Thus, there exists $i_0 \in [r_1 + r_2]$ such that $|\sigma_{i_0}(\varepsilon)| > 1$. Then for $m \in \mathbb{N}$,

$$\|M_{\mathbb{R}}(\varepsilon^m \alpha)\|_{\infty} \geq |\sigma_{i_0}(\varepsilon^m \alpha)| = |\sigma_{i_0}(\varepsilon)|^m |\sigma_{i_0}(\alpha)| \to \infty \quad (m \to \infty).$$

We enumerate the elements of the countable set $(\mathcal{O}_K \setminus \{0\})/\mathcal{O}_K^\times$ as $\{v_m : m \in \mathbb{N}\}$. Fix $\alpha_1$ for a representative for $v_1$. By (4.11), the image of the set $v_m$ under the embedding $M_{\mathbb{R}}$ is unbounded. Thus, we may take a sequence $(\alpha_m)_{m \in \mathbb{N}}$, chosen inductively on $m$, such that for all $m \in \mathbb{N}$, $\alpha_m$ is a representative of $v_m$ and

$$\|M_{\mathbb{R}}(\alpha_{m+1})\|_{\infty} \geq (2 \mathcal{R} + 2)\|M_{\mathbb{R}}(\alpha_m)\|_{\infty} \quad (4.12)$$

holds. Let $\mathcal{D}_S := \{\alpha_m : m \in \mathbb{N}\}$. By construction, $\mathcal{D}_S$ is an $\mathcal{O}_K^\times$-fundamental domain.

Define

$$\mathcal{R} := \max_{(s_1, s_2, s_3) \in \mathcal{S}} \|M_{\mathbb{R}}(s_3) - M_{\mathbb{R}}(s_2)\|_{\infty}/\|M_{\mathbb{R}}(s_3) - M_{\mathbb{R}}(s_1)\|_{\infty},$$
where \((S^3)\) is the family of all three-element subsets of \(S\). Note that the denominator above is never zero by Lemma 4.3. We will show that \(\mathcal{D}_S\) contains no \(S\)-constellation. Suppose, by way of contradiction, \(\mathcal{D}_S\) contains an \(S\)-constellation \(S\). By Lemma 4.3, we have

\[
\mathcal{R} = \max_{(s'_1, s'_2, s'_3) \in (S^3)} \frac{\|M_R(s'_3) - M_R(s'_2)\|_\infty}{\|M_R(s'_2) - M_R(s'_1)\|_\infty}. \tag{4.13}
\]

Let \(\beta_1, \beta_2, \beta_3 \in S\) be distinct. Since \(\mathcal{D}_S\) is an \(O_K \times K\)-fundamental domain, there exist distinct \(m_1, m_2, m_3 \in \mathbb{N}\) such that \(\beta_j = \alpha_{m_j}\) for \(j = 1, 2, 3\). We may assume without loss of generality that \(m_1 < m_2 < m_3\). Since

\[
\|M_R(\beta_3) - M_R(\beta_2)\|_\infty \geq \|M_R(\alpha_{m_3})\|_\infty - \|M_R(\alpha_{m_2})\|_\infty \\
\geq ((2R + 2)^{m_3-m_2} - 1)\|M_R(\beta_2)\|_\infty \quad \text{(by (4.12))} \geq (2R + 1)\|M_R(\beta_2)\|_\infty,
\]

and

\[
\|M_R(\beta_2) - M_R(\beta_1)\|_\infty \leq \|M_R(\beta_2)\|_\infty + \|M_R(\beta_1)\|_\infty \\
\leq \|M_R(\beta_2)\|_\infty + \frac{1}{2R + 2}\|M_R(\beta_2)\|_\infty \quad \text{(by (4.12))} \leq 2\|M_R(\beta_2)\|_\infty,
\]

we have

\[
\frac{\|M_R(\beta_3) - M_R(\beta_2)\|_\infty}{\|M_R(\beta_2) - M_R(\beta_1)\|_\infty} > \frac{2R + 1}{2} > \mathcal{R}.
\]

This contradicts (4.13).

### 4.4 Countings of elements in \(O_K^\times\)-orbits with respect to the \(\ell_\infty\)-length

In this subsection, we give an estimate on the size of part of the orbit \(O_K^\times \cdot \alpha\) of the action \(O_K^\times \curvearrowright O_K \setminus \{0\}\) bounded by \(\ell_\infty\)-length. More precisely, for \(M \geq 1\), we give an upper bound on \(\#((O_K^\times \cdot \alpha) \cap O_K(\omega, M))\). The results in this subsection are not needed to prove Theorem 2.8 the mapping \(O_K \setminus \{0\} \ni \alpha \mapsto \alpha O_K \in \text{Ideals}_K\) restricted to an \(O_K^\times\)-fundamental domain is injective. This injectivity allows us to transfer the estimate of the number of ideals by Theorem 3.22 to that of prime elements. However, to prove Theorem A an estimate of the size of a preimage when the domain is restricted by \(\ell_\infty\)-length is in addition required. Lemma 4.14 below will serve this purpose. For the convenience of the reader, we give our estimate in a self-contained manner. A sharper estimate could be obtained, for instance with the help of [Wid10, Corollary 5.3].

We continue to use Setting 4.1. Recall from Definition 4.2 the additive and weighted multiplicative Minkowski embeddings, and from Definition 4.4 the hyperplane \(\mathcal{H}\) and vector...
Further, recall the $\infty$-norm on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ defined in (4.5), and the constant $\Theta$ defined in (4.6). We define the following sets:

$$Q := (-\infty, 0]^{r_1+r_2}, \quad T := \frac{1}{n}(u_0 + Q) \cap \mathcal{H}.$$ 

The following lemma is a key to counting the number of associates of a given element $\alpha \in \mathcal{O}_K \setminus \{0\}$ in $\mathcal{O}_K(\omega, M)$. The assumption $N(\alpha) \leq \Xi M^n$ in Lemma 4.14(1) is not essential, as is seen from Lemma 4.8. We write $k := r_1 + r_2 - 1$.

**Lemma 4.14.** (1) There exists $\Xi > 0$ depending only on $\omega$, such that for all $M \geq 1$ and $\alpha \in \mathcal{O}_K \setminus \{0\}$ with $N(\alpha) \leq \Xi M^n$,

$$\#(\mathcal{O}_K^x \cdot \alpha \cap \mathcal{O}_K(\omega, M)) \leq \Xi \cdot \left( \log \frac{\Xi M^n}{N(\alpha)} \right)^k$$

holds.

(2) There exists $\Xi' > 0$ depending only on $\omega$, such that for all $M \geq 2$ and $\alpha \in \mathcal{O}_K \setminus \{0\}$,

$$\#(\mathcal{O}_K^x \cdot \alpha \cap \mathcal{O}_K(\omega, M)) \leq \Xi' \cdot (\log M)^k$$

holds.

The proof of Lemma 4.14 will be provided after the following auxiliary lemma. In these proofs, see Figure 4.4:

**Lemma 4.15.** For $\alpha \in \mathcal{O}_K \setminus \{0\}$, the following statements hold.

(1) $\mathcal{L}(\alpha) \in (\log(\Theta \|\alpha\|_{\infty, \omega}))u_0 + \mathcal{Q}$,
(2) if \( M > 0, \alpha \in \mathcal{O}_K(\Theta^n M^n) \) and \( \beta \in \mathcal{O}_K^\times \cdot \alpha \cap \mathcal{O}_K(\omega, M) \), then
\[
\mathcal{L}(\beta) - \frac{\log N(\alpha)}{n} u_0 \in \left( \log \frac{\Theta^n M^n}{N(\alpha)} \right) \cdot \mathcal{T}.
\]

**Proof.** Item (1) follows from (4.7). Since \( \alpha \in \mathcal{O}_K(\Theta^n M^n) \), we have
\[
(\log(\Theta^n M^n) - \log N(\alpha)) \mathcal{Q} = \mathcal{Q}.
\]
Thus, by (1), we have
\[
\mathcal{L}(\beta) - \frac{\log N(\alpha)}{n} u_0 \in \left( \frac{1}{n} (\log(\Theta^n M^n) - \log N(\alpha)) u_0 + \mathcal{Q} \right) \cap \mathcal{H}
\]
\[
= \frac{1}{n} (\log(\Theta^n M^n) - \log N(\alpha))(u_0 + \mathcal{Q}) \cap \mathcal{H}
\]
\[
= \left( \log \frac{\Theta^n M^n}{N(\alpha)} \right) \cdot \mathcal{T}.
\]
This completes the proof.

**Proof of Lemma 4.14.** Pick a relatively compact Borel measurable fundamental domain \( \mathcal{F} \) of the lattice \( \mathcal{L}(\mathcal{O}_K^\times) \) in \( \mathcal{H} \). Since 0 is an interior point of \( \mathcal{T} \) in \( \mathcal{H} \), we may choose \( c > 0 \) in such a way that \( \mathcal{F} \subseteq c \cdot \mathcal{T} \). Let
\[
\Xi := \max \left\{ \# \mu(K) \cdot \frac{\text{Leb}(k)(\mathcal{T})}{\text{Leb}(k)(\mathcal{F})}, c^e \Theta^n \right\},
\]
where \( \text{Leb}(k) \) denotes the \( k \)-dimensional Lebesgue measure.

If \( N(\alpha) > \Theta^n M^n \), then \( \mathcal{O}_K^\times \cdot \alpha \cap \mathcal{O}_K(\omega, M) = \emptyset \) by Lemma 4.8. Thus, we assume \( N(\alpha) \leq \Theta^n M^n \).

We define \( L(\alpha, M) \) and \( \tilde{L}(\alpha, M) \) by
\[
L(\alpha, M) := \mathcal{L}(\mathcal{O}_K^\times \cdot \alpha \cap \mathcal{O}_K(\omega, M)) - \frac{\log N(\alpha)}{n} u_0,
\]
\[
\tilde{L}(\alpha, M) := \bigcup_{v \in L(\alpha, M)} (v + \mathcal{F}).
\]
(4.14)

Since
\[
L(\alpha, M) \subseteq \mathcal{L}(\mathcal{O}_K^\times) + \mathcal{L}(\alpha) - \frac{\log N(\alpha)}{n} u_0 \subseteq \mathcal{H}
\]
and \( \mathcal{F} \) is a fundamental domain of the lattice \( \mathcal{L}(\mathcal{O}_K^\times) \) in \( \mathcal{H} \), the union in the right-hand side of (4.14) is indeed disjoint. Since the restriction of \( \mathcal{L} \) to \( \mathcal{O}_K^\times \setminus \{0\} \) has kernel \( \mu(K) \), we have
\[
\# (\mathcal{O}_K^\times \cdot \alpha \cap \mathcal{O}_K(\omega, M)) = \# \mu(K) \cdot \# L(\alpha, M).
\]
(4.15)
By Lemma 4.15 (2), we have

\[ L(\alpha, M) \subseteq \left( \log \frac{\Theta M^n}{N(\alpha)} \right) \cdot \mathcal{T}. \]

Hence

\[ \tilde{L}(\alpha, M) = L(\alpha, M) + \mathcal{F} \subseteq \left( \log \frac{\Theta M^n}{N(\alpha)} + c \right) \cdot \mathcal{T}, \]

since \( \mathcal{T} \) is convex. Therefore, by (4.14), we obtain

\[ \#L(\alpha, M) \cdot \text{Leb}(\mathcal{F}) = \text{Leb}(\tilde{L}(\alpha, M)) \leq \text{Leb}(\mathcal{T}) \left( \log \frac{\Theta M^n}{N(\alpha)} + c \right)^k. \]

This, together with (4.15) implies the inequality in (1).

To prove (2), let \( \Xi' := (\log_2 \Xi + n)^k \cdot \Xi \). Assuming \( M \geq 2 \), we have \( \log(\Xi M^n) \leq (\log_2 \Xi + n) \log M \). Since \( N(\alpha) \geq 1 \), the desired inequality follows from (1). \( \square \)

In Section 10, we need to extend the statement of Lemma 4.14 from \( \mathcal{O}_K \) to its nonzero ideal. The corresponding statement can be proved as a corollary to Lemma 4.14; it will be used in Sections 8 and 9 in order to prove our main result on quadratic forms in Section 10.

For a \( \mathbb{Z} \)-basis \( v = (v_1, \ldots, v_n) \) of an ideal \( a \in \text{Ideals}_K \), write

\[ v_j = \sum_{i \in [n]} c_{ij} \omega_i \quad (j \in [n]), \]

where \( c_{ij} \in \mathbb{Z} \) for \( i, j \in [n] \). Define

\[ C_v := \max_{i \in [n]} \sum_{j \in [n]} |c_{ij}|. \]

Recall from Definition 2.2 the \( \ell_{\infty} \)-length \( \| \cdot \|_{\infty, v} \) and the set \( a(v, M) \) for \( M \geq 0 \).

**Corollary 4.16.** Let \( a \in \text{Ideals}_K \), and let \( v \) be a \( \mathbb{Z} \)-basis of \( a \).

1. There exists a constant \( \Xi(v) > 0 \) depending on \( v \) such that for all \( M \in \mathbb{R}_{\geq 2} \) and for all \( \alpha \in a \cap \mathcal{O}_K(\Xi(v)M^n) \), the inequality

   \[ \#(\mathcal{O}_K^{\times} \cdot \alpha \cap a(v, M)) \leq \Xi(v) \cdot \left( \log \frac{\Xi(v)M^n}{N(\alpha)} \right)^k \]

   holds.

2. There exists a constant \( \Xi'(v) > 0 \) depending on \( v \) such that, for all \( M \in \mathbb{R}_{\geq 2} \) and for all \( \alpha \in a \setminus \{0\} \), the inequality

   \[ \#(\mathcal{O}_K^{\times} \cdot \alpha \cap a(v, M)) \leq \Xi'(v) \cdot (\log M)^k \]

   holds.
Proof. Let $\Xi(v) := \Xi C^n v$. Let $M \geq 1$ and $\alpha \in a \setminus \{0\}$. Since $a(v, M) \subseteq O_K(\omega, C_v M)$, we have
\[
\#(O_K^\infty \cdot \alpha \cap a(v, M)) \leq \#(O_K^\infty \cdot \alpha \cap O_K(\omega, C_v M)).
\] (4.16)

To prove (1), suppose further that $\alpha \in O_K(\Xi(v) M^n) = O_K(\Xi C^n v M^n)$. Since $C_v \geq 1$, the desired inequality follows from Lemma 4.14 (1) and (4.16).

To prove (2), let $\Xi'(v) := \Xi' \cdot (\log 2 C_v + 1)^k$ and assume $M \geq 2$. Then we have $\Xi'(v) (\log(C_v M))^k \leq \Xi'(v) (\log M)^k$. Now the desired inequality follows from Lemma 4.14 (2) and (4.16).

5 Relative multidimensional Szemerédi theorem

We develop an axiomatic framework that enables us to carry out Steps 5–7 in Subsection 2.3. More specifically, the goal of this Section is to prove the relative multidimensional Szemerédi theorem (Theorem 5.4) below.

Setting 5.1. Let $Z$ be a free $\mathbb{Z}$-module of rank $n$. Let $v = (v_i)_{i \in [n]}$ be a basis for $Z$. Fix a finite subset $S \subseteq Z$ which is the shape of constellations we are looking for and assume it is a standard shape (Definition 2.3). Namely, $S$ generates $Z$ as a $\mathbb{Z}$-module and satisfies $0 \in S$ and $S = -S$. Let $r$ be the positive integer defined by $\#S = r + 1$ and write $S = \{s_1, \ldots, s_r, s_{r+1} = 0\}$. For $j \in [r+1]$, set $e_j := [r+1] \setminus \{j\}$.

Recall that for a given positive integer $N$, we define $Z(v, N) = \{\sum_{i \in [n]} a_i v_i \in Z \mid a_i \in [-N, N]\}$. We often denote elements of direct products $(a_i)_{i \in I} \in \prod_{i \in I} A_i$ by $a_I$ for short.

5.1 The statement of the relative multidimensional Szemerédi theorem

The following is a multidimensional generalization of the celebrated theorem of Szemerédi. It was first established by Furstenberg–Katznelson [FK78], whose proof is based on ergodic theory. See Gowers [Gow07, Theorems 10.2, 10.3] and Rödl–Schacht–Tengan–Tokushige [RSTT06, Section 2] for a proof using the hypergraph removal lemma.

Theorem 5.2 (Multidimensional Szemerédi theorem). Let $n$ be a positive integer, $\delta$ a positive real number and $S$ a finite subset of $\mathbb{Z}^n$. Then, there exists a positive integer $N_{MS}(\delta, S)$ such that for every $N \geq N_{MS}(\delta, S)$ and every subset $B \subseteq [-N, N]^n$ with
\[ E(1_B \mid [-N, N]^n) \geq \delta, \]
there exist $S$-constellations in $B$.

In this article, we prove a relative version (in terms of weight) of the above theorem, Theorem 5.4, and use it in the proof of the main theorems. To state Theorem 5.4 we now introduce a condition on weight functions $\lambda: Z \to \mathbb{R}_{\geq 0}$. 

**Definition 5.3 ((ρ, N, S)-linear forms condition).** Assume Setting \[5.1\] For each \( \omega \in \bigcup_{j \in [r+1]} \{0, 1\}^{e_j} \), we define a \( \mathbb{Z} \)-linear map \( \psi_S^{(\omega)} : \mathbb{Z}^{2r+2} \to \mathbb{Z} \) as follows: if \( j \in [r] \), the map associated to \( \omega = (\omega_i)_{i \in e_j} \in \{0, 1\}^{e_j} \) is

\[
\psi_S^{(\omega)}(a_1^{(0)}, \ldots, a_{r+1}^{(0)}, a_1^{(1)}, \ldots, a_{r+1}^{(1)}) := \left( \sum_{i \in [r]\setminus\{j\}} (s_i - s_j)a_i^{(\omega_i)} \right) + s_ja_{r+1}^{(\omega_{r+1})}
\]

and if \( \omega = (\omega_i)_{i \in e_{r+1}} \in \{0, 1\}^{e_{r+1}} \), we define

\[
\psi_S^{(\omega)}(a_1^{(0)}, \ldots, a_{r+1}^{(0)}, a_1^{(1)}, \ldots, a_{r+1}^{(1)}) := \sum_{i \in [r]} s_i a_i^{(\omega_i)}.
\]

Let \( 0 < \rho < 1 \) be a real number and \( N \) a positive integer. A function \( \lambda : \mathbb{Z} \to \mathbb{R}_{\geq 0} \) is said to satisfy the \((\rho, N, S)\)-linear forms condition if for every subset \( \mathcal{B} \subseteq \mathbb{Z}^{r+1} \) that is the product of intervals of lengths \( \geq N \) and every \( (n_\omega) \omega \in \{0, 1\}^{\bigcup_{j \in [r+1]} \{0, 1\}^{e_j}} \), we have

\[
\left| \mathbb{E} \left( \prod_{j \in [r+1]} \prod_{\omega \in \{0, 1\}^{e_j}} (\lambda \circ \psi_S^{(\omega)})^{n_\omega} \right) \right| \leq \rho.
\]

A function \( \lambda : \mathbb{Z} \to \mathbb{R}_{\geq 0} \) satisfying the \((\rho, N, S)\)-linear forms condition is also called a \((\rho, N, S)\)-pseudorandom measure on \( \mathbb{Z} \).

We note that this terminology differs from the usage in preceding work of \[GT08\] and \[CFZ15\]. The role of this definition will be clear in the proof of Proposition \[5.14\].

The goal in this section is the following theorem, whose proof will be completed in Subsection \[5.4\].

**Theorem 5.4 (Relative multidimensional Szemerédi theorem).** Assume Setting \[5.1\]. Then for every \( \delta > 0 \), there exist positive real numbers \( \gamma = \gamma_{\text{RMS}}(v, \delta, S) \) and \( \rho = \rho_{\text{RMS}}(v, \delta, S) \) such that the following holds: let \( N \) be a positive integer and \( \lambda \) a \((\rho, N, S)\)-pseudorandom measure on \( \mathbb{Z} \). Let \( B \subseteq \mathbb{Z}(v, N) \) be a subset satisfying the next two conditions:

(i) (Weighted density) \( \mathbb{E}(1_B \cdot \lambda \mid \mathbb{Z}(v, N)) \geq \delta, \)

(ii) (Smallness) \( \mathbb{E}(1_B \cdot \lambda^{r+1} \mid \mathbb{Z}(v, N)) \leq \gamma N. \)

Then \( B \) contains an \( S \)-constellation.

This covers Theorem \[5.2\]. Indeed, consider \( \mathcal{Z} := \mathbb{Z}^n \) with the standard basis \( v \) and \( \lambda := 1_z \). Then Theorem \[5.4\] implies Theorem \[5.2\] with threshold \( N_{\text{MS}}(\delta, S) = (\gamma_{\text{RMS}}(v, \delta, S))^{-1} \).

In some Szemerédi-type theorems, it is possible to obtain lower bounds of the asymptotic number of \( S \)-constellations with respect to the parameter \( N \). Results of this sort date back to Varnavides’s \[Var59\] work on Roth’s theorem. This is also the case for our Theorem \[5.4\] in a weighted sense we now state.
Theorem 5.5. In the setting of Theorem 5.4, in addition to the existence of $S$-constellations in $B$, we have the following inequality:

$$
\mathbb{E} \left( \prod_{s \in S} (1_B \cdot \lambda)(\alpha + ks) \bigg| (\alpha, k) \in \mathcal{Z}(v, N) \times [N] \right) > \gamma.
$$

Remark 5.6. The smallness condition guarantees that the contribution of the ‘trivial’ $S$-constellations (those of the form $a + 0 \cdot S = \{a\}$) is small. This condition is necessary to prove the existence of ‘non-trivial’ $S$-constellations. The classical Szemerédi theorem as in [GT08, Theorem 3.5] and the relative multidimensional Szemerédi theorems in [Tao06, Theorem 2.18], [CFZ15, Theorem 3.1] do not impose the smallness condition on their formulations of the relative multidimensional Szemerédi theorem; instead, in the step of applications, they argue that the smallness condition is satisfied if the parameter $N$ is sufficiently large.

Remark 5.7. Our main problem is to show the existence of $S$-constellations in a subset $A \subseteq \mathcal{Z}$. In this article, the subset $A$ is the set of prime elements of the ring of integers in a number field $K$. In this case, it seems difficult to construct directly a pseudorandom measure on $\mathcal{Z} = \mathcal{O}_K$ to make the relative multidimensional Szemerédi theorem applicable. We will instead employ the so-called $W$-trick, where we choose suitable $W \in \mathbb{N}$ and $b \in \mathcal{O}_K$ and try to apply the relative multidimensional Szemerédi theorem to the inverse image of $A$ by the affine transformation $\text{Aff}_{W,b} : \mathcal{O}_K \to \mathcal{O}_K$. If we can find an $S$-constellation in the inverse image $\text{Aff}^{-1}_{W,b}(A)$, we may send it back by $\text{Aff}_{W,b}$ to obtain one in $A$. This approach was also used effectively by Green–Tao [GT08].

Before ending this subsection, let us prove the following elementary fact. This implies that the family of maps $(\psi_S^{(\omega)})_\omega$ in Definition 5.3 satisfies the conditions on kernels in Theorem 6.2 in Section 6.

Lemma 5.8. (1) For a given $j$ and $\omega \in \{0, 1\}^{e_j}$, consider the defining formulas (5.1) and (5.2) for the map $\psi_S^{(\omega)}$. Then the indices $(i, \sigma) \in [r+1] \times \{0, 1\}$ where the coordinate $a^{(\omega)}_i(\sigma)$ has a non-trivial coefficient are precisely those in the following set:

$$A^{(\omega)} := \{(i, \omega_i)\}_{i \in e_j}.
$$

(2) For distinct $\omega, \omega' \in \bigsqcup_{j \in [r+1]} \{0, 1\}^{e_j}$, we have $A^{(\omega)} \not\subseteq A^{(\omega')}$. 

(3) For distinct $\omega, \omega' \in \bigsqcup_{j \in [r+1]} \{0, 1\}^{e_j}$, we have $\ker(\psi_S^{(\omega)}) \not\subseteq \ker(\psi_S^{(\omega')})$.

Proof. Item [1] is clear from the definition. To show [2], if $j \neq j'$, we have $(j, \omega_j) \in A^{(\omega')} \setminus A^{(\omega)}$. If $j = j'$, there is an $i \in e_j$ with $\omega_i \neq \omega_i'$. For this $i$, we have $(i, \omega_i) \in A^{(\omega')} \setminus A^{(\omega)}$.

The assertion [3] follows from [2]. Indeed, we know there is an element $(i, \sigma) \in A^{(\omega')} \setminus A^{(\omega)}$ by assertion [2]. The vector whose $(i, \sigma)$-entry is 1 and the others are 0 belongs to $\ker(\psi_S^{(\omega)}) \setminus \ker(\psi_S^{(\omega')})$. This completes the proof. \qed
5.2 Relative hypergraph removal lemma

As is the case for the other versions [Tao06 Theorem 2.18], [CFZ15 Theorem 3.1], Theorem [5.4] is derived from the relative hypergraph removal lemma. We use the version of Conlon–Fox–Zhao [CFZ15 Theorem 2.12] which is a refinement of Tao’s [Tao06 Theorem 2.17], which in turn is a relative generalization of the hypergraph removal lemma of Gowers [Gow07] and Nagle–Rödl–Schacht–Skokan [RS06, NRS06, RS07b, RS07a]. Cook–Magyar–Titichetrakun have proved a further strengthening of the relative hypergraph removal lemma [CMT18, Theorem 1.4] to prove the multidimensional Szemerédi theorem in the primes, although we do not need this in this paper.

Let $J$ be a non-empty finite set and $r$ a positive integer. The pair of $J$ and a subset $E \subseteq \binom{J}{r}$ is called an $r$-uniform hypergraph (r-graph for short). Here, recall $\binom{J}{r} = \{ e \in 2^J : \# e = r \}$ from our notation. If further for each $j \in J$ a finite set $V_j$ is given, then we call the tuple $((J, E); (V_j)_{j \in J})$ an $r$-graph system. For a subset $e \subseteq J$ of indices, we write $V_e \coloneqq \prod_{j \in e} V_j$ for short and $x_e \coloneqq (x_j)_{j \in e} \in V_e$. Let $V = ((J, E); (V_j)_{j \in J})$ be an $r$-graph system. We say $g$ is a weighted hypergraph on $V$ if $g$ is a tuple $g = (g_e)_{e \in E}$ of functions $g_e : V_e \rightarrow \mathbb{R}_{\geq 0}$. For two weighted hypergraphs $g = (g_e)_{e \in E}$ and $g' = (g'_e)_{e \in E}$ on $V$, we write $g \leq g'$ if for all $e \in E$, we have $g_e \leq g'_e$ pointwise.

**Definition 5.9.** Let $\rho$ be a positive real number and $V = ((J, E); (V_j)_{j \in J})$ an $r$-graph system. We say a weighted hypergraph $\nu$ on $V$ is $\rho$-pseudorandom if the following inequality holds for every tuple $(n_\omega)_\omega \in \{0, 1\}^{\bigcup_{e \in E} \{0, 1\}^e}$:

$$\left| \mathbb{E} \left( \prod_{e \in E} \prod_{\omega \in \{0, 1\}^e} \nu_e(x^{(\omega)}_e)^{n_\omega} \middle| (x^{(0)}_j, x^{(1)}_j) \in V_j \times V_j \right) - 1 \right| \leq \rho. \quad (5.4)$$

Here, the symbol $x^{(\omega)}_e$ denotes the tuple $(x^{(\omega_j)}_j)_{j \in e} \in V_e$.

Now we are ready to state the relative hypergraph removal lemma.

**Theorem 5.10** (Relative hypergraph removal lemma [CFZ15 Theorem 2.12]). For every positive integer $k$ and every positive $\varepsilon > 0$, there are positive real numbers $\gamma = \gamma_{\text{RHR}}(k, \varepsilon) > 0$ and $\rho = \rho_{\text{RHR}}(k, \varepsilon) > 0$ such that the following holds: let $V = ((J, E); (V_j)_{j \in J})$ be an $r$-graph system with $r \leq k = \# J$ and $g, \nu$ two weighted hypergraphs on $V$ with $g \leq \nu$. If $\nu$ is $\rho$-pseudorandom and the estimate

$$\mathbb{E} \left( \prod_{e \in E} g_e(x_e) \middle| x_j \in V_j \right) \leq \gamma \quad (5.5)$$

holds, then there is a family of subsets $E_e \subseteq V_e$ for $e \in E$ such that the following hold:

$$\bigcap_{e \in E} (E_e \times V_{j \setminus e}) = \emptyset$$

and for all $e \in E$,

$$\mathbb{E} \left( g_e \cdot 1_{V_e \setminus E_e} \mid V_e \right) \leq \varepsilon.$$
Remark 5.11. It will be useful later that the only requirement on the weighted hypergraph $\nu$ is $\rho$-randomness, with $\rho$ depending only on $k$ and $\varepsilon$. This fact might not be clear from the reference $[CFZ15]$, where they consider a family $(\nu^{(N)})_{N \in \mathbb{N}}$ and state the above result for $N$ large enough without explicitly mentioning how the threshold for $N$ is determined.

Theorem 5.10 can be verified by examining the proof of Conlon–Fox–Zhao $[CFZ15$, Theorem 2.12$]$ as follows: first, note that the dependence on $N$ stems solely from the relative counting lemma $[CFZ15$, Theorem 2.17$]$. Also note that their proof actually shows Theorem 5.12 below by examining each $o(1)$ related to $\nu$ in the proof. This verifies Theorem 5.10 above. Such a family-free argument has already appeared in Romanić–Wolf $[RW19]$ for the study of a quantitative version of the 1-dimensional relative Szemerédi theorem.

Theorem 5.12 (Relative counting lemma). Let $r$ be a positive integer, and $\varepsilon$ and $\rho$ positive real numbers with $\rho < 1$. Let $V = ((J, E); (V_j)_{j \in J})$ be an $r$-graph system and $\nu$ a $\rho$-pseudorandom weighted hypergraph on $V$.

Let $g$ and $\tilde{g}$ be two weighted hypergraphs on $V$ with $g \leq \nu$ and $\tilde{g} \leq 1$ such that $(g, \tilde{g})$ is a $\varepsilon$-discrepancy pair; see $[CFZ15$, Definition 2.13$]$ for this notion. Then we have

$$\left| \mathbb{E} \left( \prod_{e \in E} g_e(x_e) \bigg| x_J \in V_J \right) - \mathbb{E} \left( \prod_{e \in E} \tilde{g}_e(x_e) \bigg| x_J \in V_J \right) \right| = O_r(\varepsilon + \sqrt{\rho}).$$

5.3 Construction of pseudorandom weighted hypergraphs

Assume Setting 5.1. Let $\phi_S \colon \mathbb{Z}^r \rightarrow \mathbb{Z}$ be the homomorphism of $\mathbb{Z}$-modules sending the $i$-th standard vector $\epsilon_i \in \mathbb{Z}^r$ to $s_i \in \mathbb{Z}$ for each $i \in [r]$. Let $\epsilon_{r+1} \in \mathbb{Z}^r$ denote the zero vector for a notational purpose. Since $S$ generates $\mathbb{Z}$ by assumption, we have the following exact sequence

$$0 \rightarrow \ker(\phi_S) \rightarrow \mathbb{Z}^r \xrightarrow{\phi_S} \mathbb{Z} \rightarrow 0,$$

which splits because $\mathbb{Z}$ is a free $\mathbb{Z}$-module.

Lemma 5.13. There exists a positive integer $U = U(\nu, S)$ such that the following holds: for every positive integer $N$ and every $\alpha \in \mathbb{Z}(\nu, N)$, we have the inequality

$$(2N + 1)^{r-n} \leq \#(\phi_S^{-1}(\alpha) \cap [-UN, UN]^r) \leq (2UN + 1)^{r-n}.$$ 

Proof. Choose a $\mathbb{Z}$-linear section $\sigma \colon \mathbb{Z} \rightarrow \mathbb{Z}^r$ to $\phi_S$. Choose a basis $w_1, \ldots, w_{r-n}$ for the rank $r - n$ free $\mathbb{Z}$-module $\ker(\phi_S)$. Then the vectors $\sigma(v_1), \ldots, \sigma(v_n), w_1, \ldots, w_{r-n}$ form a basis for $\mathbb{Z}^r$. Let $U$ be $r$ times the maximum of the absolute values of the entries of the basis.

The second inequality easily follows from the fact that $\ker(\phi_S)$ is has rank $r - n$. Next, by the choice of $U$, we have an inclusion of sets

$$\left\{ \sigma(\alpha) + \sum_{i \in [r-n]} b_i w_i : b_i \in [-N, N] \ (i \in [r-n]) \right\} \subseteq \phi_S^{-1}(\alpha) \cap [-UN, UN]^r,$$

which shows the first inequality. \qed
Let $U$ be an integer given by Lemma 5.13. Let $N$ be a positive integer and $\lambda: \mathbb{Z} \to \mathbb{R}_{\geq 0}$ a function. By following Solymosi [Sol03], we construct a weighted hypergraph $\nu = \nu(\lambda, N, v, S)$ as follows. Denote by $K_{r+1}^{(r)} = ([r + 1], \binom{[r+1]}{r})$ the complete $r$-hypergraph with $r + 1$ vertices. By our notation $e_j = [r + 1] \setminus \{j\}$, we have $\binom{[r+1]}{r} = \{e_j : j \in [r + 1]\}$. For each integer $a$ and index $j \in [r + 1]$, we define a hyperplane $H_j(a)$ of $\mathbb{Z}^r$ by
\[
H_j(a) := \begin{cases} 
\{(x_1, \ldots, x_r) \in \mathbb{Z}^r : x_j = a\} & \text{if } j \in [r], \\
\{(x_1, \ldots, x_r) \in \mathbb{Z}^r : \sum_{i \in [r]} x_i = a\} & \text{if } j = r + 1
\end{cases}
\]
and a set $V_j$ by
\[
V_j := \begin{cases} 
\{H_j(a) : a \in [-UN, UN]\} & \text{if } j \in [r], \\
\{H_{r+1}(a) : a \in [-rUN, rUN]\} & \text{if } j = r + 1.
\end{cases}
\]
We define an $r$-graph system $V$ by $V := (K_{r+1}^{(r)}; (V_j)_{j \in [r+1]})$. Let $j \in [r + 1]$. For every tuple $(H_i)_i \in \prod_{i \in e_j} V_i$, the intersection $\bigcap_{i \in e_j} H_i$ consists of a single point. Let $T_j: V_{e_j} \to \mathbb{Z}^r$ be the map sending the given tuple to the point. We define a weighted hypergraph $\nu = (\nu_{e_j})_{j \in [r + 1]}$ on $V$ by the following composition:
\[
\nu_{e_j}: V_{e_j} \xrightarrow{T_j} \mathbb{Z}^r \xrightarrow{\phi_S} \mathbb{Z} \xrightarrow{\lambda} \mathbb{R}_{\geq 0}.
\]
Here, we exhibit an explicit form of the map $T_j$. Set $B = B(N, v, S) := [-UN, UN]^r \times [-rUN, rUN]$. Then, for every point $a_{[r+1]} \in B$, we have
\[
T_j((H_i(a))_{i \in e_j}) = \begin{cases} 
\left( a_1, \ldots, a_{j-1}, a_{j+1} - \sum_{i \in [r]\setminus\{j\}} a_i, a_{j+1}, \ldots, a_r \right) & \text{if } j \in [r], \\
(a_1, \ldots, a_r) & \text{if } j = r + 1.
\end{cases}
\]

**Proposition 5.14.** Let $\rho$ be a positive real number. If the function $\lambda: \mathbb{Z} \to \mathbb{R}_{\geq 0}$ satisfies the $(\rho, N, S)$-linear forms condition, then the weighted hypergraph $\nu$ constructed in (5.6) and (5.7) is $\rho$-pseudorandom.

**Proof.** In the current situation, the expectation in (5.4) is equal to
\[
\mathbb{E} \left( \prod_{j \in [r+1]} \prod_{\omega \in \{0,1\}^{e_j}} (\lambda \circ \phi_S \circ T_j)(H_{e_j}^{(\omega)})^{n_{\omega}} \right) \left( H_{[r+1]}^{(0)}, H_{[r+1]}^{(1)} \right) \in V_{[r+1]} \times V_{[r+1]}
\]
\[
= \mathbb{E} \left( \prod_{j \in [r+1]} \prod_{\omega \in \{0,1\}^{e_j}} (\lambda \circ \phi_S \circ T_j)((H_i(a_i^{(\omega)}))_{i \in e_j})^{n_{\omega}} \right) \left( (a_{[r+1]}^{(0)}, a_{[r+1]}^{(1)}) \in B \times B \right).
\]
By (5.8) and defining formulas (5.1), (5.2), we have for each $\omega \in \bigcup_{j \in [r+1]} \{0,1\}^{e_j}$,
\[
(\phi_S \circ T_j)((H_i(a_i^{(\omega)}))_{i \in e_j}) = \psi_{S}^{(\omega)} (a_{[r+1]}^{(0)}, a_{[r+1]}^{(1)})
\]
and hence the expectation above equals
\[
E \left( \prod_{j \in [r+1]} \prod_{\omega \in \{0,1\}^*} \left( \lambda \circ \psi_\omega^{(\omega)} \right)^{n_\omega} \left| B \times B \right) \right).
\]
Since \( \lambda \) satisfies the \((\rho, N, S)\)-linear forms condition, the difference of the above value and 1 is at most \( \rho \). This verifies the desired \( \rho \)-pseudorandomness.

\section{The proof of the relative multidimensional Szemerédi theorem}

We use notation in Theorem 5.4. We prove Theorems 5.4 and 5.5 simultaneously.

\begin{proof}[Proof of Theorems 5.4 and 5.5]
For a positive real number \( \delta > 0 \), set
\[
\epsilon = \epsilon(v, \delta, S) := \frac{\delta}{(r+1)(rU+2-1)^r},
\]
where \( U \) is the integer given by Lemma 5.13. Also, using Theorem 5.10, set
\[
\gamma = \gamma_{\text{RMS}}(v, \delta, S) := \frac{2}{3} \gamma_{\text{RHR}}(r+1, \epsilon), \quad \rho = \rho_{\text{RMS}}(v, \delta, S) := \rho_{\text{RHR}}(r+1, \epsilon).
\]
Let \( N \) be a positive integer, \( \lambda \) a \((\rho, N, S)\)-pseudorandom measure on \( Z \) and \( B \subseteq Z(v, N) \) a subset satisfying the weighted density and the smallness conditions in Theorem 5.4. Let \( \nu = \nu(\lambda, N, v, S) \) be the weighted hypergraph defined in (5.7), which is \( \rho \)-pseudorandom by Proposition 5.14. Define a subset \( E_{e_j} \subseteq V \) for each \( j \in [r+1] \) by
\[
E_{e_j} = \left( \varphi_{S} \circ T_j \right)^{n_{\epsilon_j}} \left| -B \right|
\]
and a weighted hypergraph \( g = (g_{e_j})_{j \in [r+1]} \) on \( V \) by
\[
g_{e_j} := 1_{E_{e_j}} \cdot \nu_{e_j}.
\]
Then we have \( g \leq \nu \) in the sense discussed at the beginning of Subsection 5.2.

By the definitions and (5.8), we have
\[
\left| H_{e_j} \right|_{[r+1]} \in V_{[r+1]}
\]

\begin{equation}
\left| H_{e_j} \right|_{[r+1]} \in V_{[r+1]}
\end{equation}

\[
E \left( \prod_{j \in [r+1]} g_{e_j} \left| H_{[r+1]} \in V_{[r+1]} \right) \right).
\]

\begin{equation}
E \left( \prod_{j \in [r+1]} \left( 1_{E_{e_j}} \cdot \nu_{e_j} \right) \left[ H_\varphi(a_i)_{i \in e_j} \right] \left| a_{[r+1]} \in B \right) \right).
\end{equation}

\begin{equation}
E \left( \prod_{j \in [r+1]} \left( 1_{\phi_{S}^{-1}(B)} \cdot (\lambda \circ \phi_{S})_{[r]}(a_{[r]} + k_{e_j}) \right) \left| a_{[r+1]} \in B \right) \right),
\end{equation}

where \( k := a_{r+1} - \sum_{i \in [r]} a_i \). By the upper bound in Lemma 5.13 and the smallness condition, the contribution of those \( a_{[r+1]} \)’s with \( k = 0 \) in the above expectation is bounded from above by

\begin{equation}
\frac{1}{2rUN + 1} \left( (2UN + 1)^{r-n} \cdot (2N + 1)^n \cdot \left( 1_B \cdot \lambda^{r+1} \right) \left| \mathcal{Z}(v, N) \right) \right) \leq \frac{\gamma}{2}.
\end{equation}
By way of contradiction, suppose that the contribution of those $a_{[r+1]}$'s with $k \neq 0$ in (5.9) is at most $\gamma$, that is

$$E \left( \prod_{j \in [r+1]} (1_{\phi_S^{-1}(B)} \cdot (\lambda \circ \phi_S))(a_{[r]} + k\epsilon_j) \Big| a_{[r+1]} \in B \text{ with } k \neq 0 \right) \leq \gamma. \quad (5.11)$$

Combined with (5.10), it implies that the value (5.9) does not exceed $\frac{3}{2} \gamma = \gamma_{RHR}(r + 1, \epsilon)$. Therefore, Theorem 5.10 applies, and there exists a family $(E'_{e_j})_{j \in [r+1]}$ of subsets $E'_{e_j} \subseteq V_{e_j}$ for $j \in [r+1]$ such that

$$\bigcap_{j \in [r+1]} (E'_{e_j} \times V_j) = \emptyset \quad (5.12)$$

and

$$E(1_{E_{e_j}} \setminus E'_{e_j} \cdot \nu_{e_j} \mid V_{e_j}) \leq \epsilon \quad \text{for all } j \in [r+1]. \quad (5.13)$$

We will argue that this contradicts the assumption of the weighted density condition.

Define a map $\iota_0: \phi_S^{-1}(B) \cap [-UN, UN]^r \to V_{[r+1]}$ by

$$\iota_0(a_{[r]}) := \left( H_1(a_1), \ldots, H_r(a_r), H_{r+1}\left( \sum_{i \in [r]} a_i \right) \right).$$

Denote by $pr_{e_j}: V_{[r+1]} \to V_{e_j}$ the projection which forgets the $j$-th entry. Then, for all $j \in [r+1]$, the map $T_j \circ pr_{e_j} \circ \iota_0$ coincides with the inclusion map from $\phi^{-1}(B) \cap [-UN, UN]^r$ to $\mathbb{Z}^r$. Hence by the definition of $E_{e_j}$, it follows that $\iota_0$ maps into $\bigcap_{j \in [r+1]} (E_{e_j} \times V_j)$.

Let us write $\widetilde{E}_{e_j} := E_{e_j} \times V_j$ and $\widetilde{E}'_{e_j} := E'_{e_j} \times V_j$ for short. Consider the following decreasing sequence of subsets

$$\bigcap_{j \in [r+1]} \widetilde{E}_{e_j} \supseteq \left( \bigcap_{j \in [r]} \widetilde{E}_{e_j} \cap \widetilde{E}'_{e_{r+1}} \right) \supseteq \left( \bigcap_{j \in [r-1]} \widetilde{E}_{e_j} \cap \bigcap_{j \in [r,r+1]} \widetilde{E}'_{e_j} \right) \supseteq \cdots \supseteq \bigcap_{j \in [r+1]} \widetilde{E}'_{e_j} = \emptyset,$$

where the last equality is (5.12). Consider also the associated partition

$$\bigcap_{j \in [r+1]} \widetilde{E}_{e_j} = \bigcup_{j \in [r+1]} \left( \widetilde{E}_{e_j} \cap \cdots \cap \left( \bigcap_{j \in [r,r+1]} \widetilde{E}_{e_j} \setminus \widetilde{E}'_{e_j} \right) \cap \cdots \cap \widetilde{E}'_{e_{r+1}} \right).$$

Composing the projection $pr_{e_j}: \widetilde{E}_{e_j} \setminus \widetilde{E}'_{e_j} \to E_{e_j} \setminus E'_{e_j}$, we obtain the following composite map

$$\iota: \phi_S^{-1}(B) \cap [-UN, UN]^r \xrightarrow{\iota_0} \bigcap_{j \in [r+1]} \widetilde{E}_{e_j} \xrightarrow{} \bigcup_{j \in [r+1]} E_{e_j} \setminus E'_{e_j},$$

which is injective since $T_j \circ pr_{e_j} \circ \iota_0$ is an inclusion map.

If $a_{[r]} \in \phi_S^{-1}(B) \cap [-UN, UN]^r$ is mapped by $\iota$ into $E_{e_j} \setminus E'_{e_j}$, then we have by definition of $\nu_{e_j}$,

$$(\lambda \circ \phi_S)(a_{[r]}) = \nu_{e_j}(\iota(a_{[r]})).$$
Therefore by the injectivity of \( \iota \) and the lower bound in Lemma 5.13 we have that
\[
(2N + 1)^{r-n} \sum_{\alpha \in \mathcal{Z}(\mathbf{v}, N)} (1_B \cdot \lambda)(\alpha) \leq \sum_{a[n] \in [-UN,UN]^r} (1_{\phi^{-1}(B)} \cdot (\lambda \circ \phi_S))(a[n])
\]
\[
\leq \sum_{j \in [r+1]} (1_{E_{e_j} \setminus E_{e_j}} \cdot \nu_{e_j})(H_{e_j}).
\]
We divide this formula by \((2N + 1)^r\) and apply (5.13). Since \( \#V_{e_j} \leq (2rUN + 1)^r \), we have
\[
\mathbb{E}(1_B \cdot \lambda \mid \mathcal{Z}(\mathbf{v}, N)) \leq \frac{1}{(2N + 1)^r} \sum_{j \in [r+1]} \#V_{e_j} \cdot \mathbb{E}(1_{E_{e_j} \setminus E_{e_j}} \cdot \nu_{e_j} \mid V_{e_j}) < (r + 1)(rU + 2^{-1})^r \varepsilon = \delta.
\]
This contradicts the assumption of the weighted density condition. Therefore our supposition (5.11) turns out false and we conclude:
\[
\sum_{a[n] \in [-UN,UN]^r \atop a_r+1 \in [-rUN,rUN]} \prod_{j \in [r+1]} (1_{\phi^{-1}_S(B)} \cdot (\lambda \circ \phi_S))(a[n] + k\epsilon_j) > \gamma \cdot \#B, \tag{5.14}
\]
where we recall \( k = a_{r+1} - \sum_{i \in [r]} a_i \). By the upper bound in Lemma 5.13 and the assumptions \( 0 \in S \) and \( S = -S \), we have
\[
\text{L.H.S. of (5.14)} \leq \sum_{a[n] \in [-UN,UN]^r \atop k \in [-2rUN,2rUN] \setminus \{0\}} \prod_{j \in [r+1]} (1_{\phi^{-1}_S(B)} \cdot (\lambda \circ \phi_S))(a[n] + k\epsilon_j)
\]
\[
\leq 2(2UN + 1)^{r-n} \sum_{\alpha \in \mathcal{Z}(\mathbf{v}, N) \atop s \in S} \prod_{k \in [2rUN]} (1_B \cdot \lambda)(\alpha + ks)
\]
\[
= 2(2UN + 1)^{r-n} \sum_{\alpha \in \mathcal{Z}(\mathbf{v}, N) \atop s \in S} \prod_{k \in [N]} (1_B \cdot \lambda)(\alpha + ks).
\]
The last equality holds because the summand can be non-zero only when \( \alpha + ks \subseteq B \subseteq \mathcal{Z}(\mathbf{v}, N) \) and because \( S = -S \). Therefore we conclude
\[
\mathbb{E}\left( \prod_{s \in S} (1_B \cdot \lambda)(\alpha + ks) \right)_{(\alpha, k) \in \mathcal{Z}(\mathbf{v}, N) \times [N]} > \left( \frac{2UN + 1}{2N + 1} \right)^n \cdot \frac{2rUN + 1}{N} \cdot \frac{\gamma}{2} \geq \gamma.
\]
This completes the proof of Theorems 5.4 and 5.5. \( \square \)

A slight modification of the argument in the proof above yields the following result. Theorem 5.15 estimates a weighted expectation for a shape \( S \) satisfying the conditions of a standard shape except \( 'S = -S' \); in this case, we allow the scaling factor also to be negative for the estimation. This theorem enables us to obtain the estimate of the numbers of arithmetic progressions of length \( k \) in Theorem 9.2 even for the case where \( k \) is even.
Theorem 5.15. In the setting of Theorem \[5.14\] instead of assuming \(S\) is a standard shape, we only assume that a finite subset \(S \subseteq \mathbb{Z}\) generates \(\mathbb{Z}\) as a \(\mathbb{Z}\)-module, and that \(0 \in S\). Then we have that

\[
\mathbb{E}\left( \prod_{s \in S} (1_B \cdot \lambda)(\alpha + ks) \middle| (\alpha, k) \in \mathbb{Z}(v, N) \times ([2N, 2N] \setminus \{0\}) \right) > \frac{\gamma}{2}.
\]

Proof. Almost all parts of the proof of Theorem \[5.3\] remain to work under the current weaker assumptions on \(S\). However, since the condition \('S = -S'\) is dropped, the estimate of the left-hand side of \[5.14\] may not hold in the original form. This is the only point to be modified in the present proof; the modification can be done in the following manner.

L.H.S. of \[5.14\] ≤ \(\sum_{a[r] \in [-UN, UN]} \prod_{j=1}^{r} (1_{\phi_{-1}(B)} \cdot (\lambda \circ \phi_{S}))(a[r] + k \epsilon_{j})\)

\(\leq (2UN + 1)^{r-n} \sum_{\alpha \in \mathbb{Z}(v, N)} \prod_{s \in S} (1_B \cdot \lambda)(\alpha + ks)\)

\(= (2UN + 1)^{r-n} \sum_{\alpha \in \mathbb{Z}(v, N)} \prod_{s \in S} (1_B \cdot \lambda)(\alpha + ks).\)

This provides the desired estimate. \(\square\)

6 Goldston–Yıldırım type asymptotic formula

The main result in this section is a Goldston–Yıldırım type asymptotic formula (Theorem \[6.2\]). It shows pseudorandomness of the weight function \(\tilde{\lambda}\) in the ‘\(N\)-world,’ which is required in Step 4 of the strategy to prove Theorem \[2.8\] in Subsection \[2.3\] Note that the notion of pseudorandomness of weighted functions is presented in Definition \[5.3\] and \(\tilde{\lambda}\) is constructed in Definition \[7.3\]

Goldston–Yıldırım type asymptotic formulas are ingeniously proved by the W-trick. As described in Remark \[5.7\] an affine transformation appears from the use of the W-trick. If we directly use the relative multidimensional Szemerédi theorem (Theorem \[5.4\]) in the ‘\(M\)-world,’ then we need to derive an asymptotic formula without W-trick. It has difficulties in terms of analytic number theory, and hence we consider an asymptotic formula through an affine transformation. For this reason, we need to transfer the setting in the ‘\(M\)-world’ to that in the ‘\(N\)-world.’ This is related to Steps 3 and 4 in Subsection \[2.3\] We emphasize that in our asymptotic formula, the choices of \(b_1, \ldots, b_m\) has large flexibility; it is of significance in our applications.

To state our Goldston–Yıldırım type estimate, we define a variant of the von Mangoldt function for a number field. We ‘truncate’ and ‘smoothen’ the original function, and obtain a weight function. This idea appeared in Tao \[Tao06\] (and Conlon–Fox–Zhao \[CFZ14\]).
defined such a weight function on the ring of Gaussian integers. In this paper, we introduce an \((R, \chi)\)-von Mangoldt function on the ideals of the ring of integers. We establish the asymptotic formula for this function in a similar manner to that in Conlon–Fox–Zhao. The main difference here is that we focus on this variant of the von Mangoldt functions defined on ideals, not on elements, to show the asymptotic formula. For instance, we consider \(p\)-ideals for each rational prime \(p\) in our proof, while in [CFZ14] they studied \(p\)-summands. If we consider weight functions on elements instead of ideals, then obstacles arise in the latter part of this section; see Remark 6.30.

### 6.1 Von Mangoldt function and its variants

For a number field \(K\), recall that the symbols in Subsection 3.1 such as \(\text{Ideals}_K\) and \(|\text{Spec}(\mathcal{O}_K)|\). Recall also the von Mangoldt function \(\Lambda(= \Lambda_K)\). The von Mangoldt function \(\Lambda\) for \(K\) is defined as

\[
\Lambda(a) := \begin{cases} 
\log N(p) & \text{if } a \text{ is a power of a prime ideal } p, \\
0 & \text{otherwise}
\end{cases}
\]

for each nonzero ideal \(a \in \text{Ideals}_K\).

Recall that the norm \(N\) is multiplicative by Lemma 3.7. Hence, by considering the decomposition of an ideal \(a\) into prime elements we have \(\sum_{b|a} \Lambda(b) = \log N(a)\). The Möbius inversion formula (Proposition 3.11) implies

\[
\Lambda(a) = \sum_{b|a} \mu(b) \log \left( \frac{N(a)}{N(b)} \right) = \log N(a) \cdot \sum_{b|a} \mu(b) \left( 1 - \frac{\log N(b)}{\log N(a)} \right),
\]

where \(\mu := \mu_K\). Next we consider an analogy of the Goldston–Yıldırım truncated divisor sum. More precisely we take a sufficiently large \(R > 0\) as necessary, and consider sum over the ideals \(b\) with \(N(b) \leq R\). Moreover we replace \(\log N(a)\) with \(\log R\):

\[
\log R \cdot \sum_{b|a, N(b) \leq R} \mu(b) \left( 1 - \frac{\log N(b)}{\log R} \right).
\]

This is the Goldston–Yıldırım truncated divisor sum on ideals of the ring of integers. Following the method of Tao [Tao06], we first regard \(1 - \log N(b)/\log R\) as the function obtained by substituting \(\log N(b)/\log R\) for \(x\) into \(\max\{1 - |x|, 0\}\). We secondly consider the sum over the ideals of norm at most \(R\) because its support is contained in \([-1, 1]_\mathbb{R}\). Thirdly, we replace the function \(\max\{1 - |x|, 0\}\) with a non-negative \(C^\infty\)-function \(\chi\) whose support is contained in \([-1, 1]_\mathbb{R}\). Note that the values of \(\chi\) on \([-1, 0]_\mathbb{R}\) do not influence the sum. Thus we derive the following definition.

**Definition 6.1.** Let \(R\) be a real number greater than 1, and \(\chi\) a non-negative \(C^\infty\)-function whose support is contained in \([-1, 1]_\mathbb{R}\). For convenience of later calculation, we assume that \(\chi(0) = 1\) and \(\chi(x) \leq 1\) for every \(x\). Then the \((R, \chi)\)-von Mangoldt function \(\Lambda_{R, \chi}: \text{Ideals}_K \cup\)
\{0\} \to \mathbb{R} is defined to be
\[
\Lambda_{R,\chi}(a) := \log R \cdot \sum_{b \in \text{Ideals}_K \text{ with } b \mid a} \mu(b) \chi \left( \frac{\log N(b)}{\log R} \right).
\]  
(6.1)

By abuse of notation, we define for each \( \alpha \in O_K \),
\[
\Lambda_{R,\chi}(\alpha) := \Lambda_{R,\chi}(\alpha O_K).
\]

Let \( c_\chi \) be a positive real number defined to be
\[
c_\chi := \int_0^\infty \chi'(x)^2 \, dx,
\]
(6.2)

where \( \chi' \) is the derivative of \( \chi \).

Note that \( \Lambda_{R,\chi}(0) \) is finite by the assumption about \( \chi \) and Proposition 3.20.

### 6.2 Statement of Goldston–Yildirim type asymptotic formula

The following asymptotic formula implies that the measure constructed in Definition 7.3 satisfies the linear forms condition (Definition 5.3). The main point here is to find an appropriate formula for a general number field. Once it is successfully done, the proof of it will be completed by following strategies in [Tao06, Section 9] and [CFZ14, Section 10]. Recall that \( \kappa \) is the positive real number in Theorem 3.19, \( c_\chi \) is the positive real number in (6.2) determined by \( \chi \), and \( \varphi_K \) is the totient function (Definition 3.8).

**Theorem 6.2** (Goldston–Yildirim type asymptotic formula). Let \( K \) be a number field of degree \( n \). Let \( m \) and \( t \) be positive integers, and \( \psi_1, \ldots, \psi_m : \mathbb{Z}^t \to O_K \) be \( \mathbb{Z} \)-module homomorphisms. Let \( w \) be a positive real number, and \( W \) a positive integer of which the set of prime divisors is \( \mathcal{P}_{\leq w} = \{ p \in \mathcal{P} \mid p \leq w \} \). Let \( b_1, \ldots, b_m \) be elements in \( O_K \) each of which is prime to \( W \), and define affine transformations \( \theta_1, \ldots, \theta_m : \mathbb{Z}^t \to O_K \) as
\[
\theta_j(x) := \text{Aff}_{W,b_j}(\psi_j(x)) = W\psi_j(x) + b_j.
\]

Let \( R \) be a positive real number, and \( I_1, \ldots, I_t \subseteq \mathbb{Z} \) intervals of length at least \( R^{4m+1} \). Set \( B := I_1 \times \cdots \times I_t \subseteq \mathbb{Z}^t \). Fix a \( C^\infty \)-function \( \chi : \mathbb{R} \to [0,1]_\mathbb{R} \) which satisfies \( \chi(0) = 1 \) and \( \supp(\chi) \subseteq [-1,1]_\mathbb{R} \). Assume that

all \( \ker(\psi_j) \) are finite, and for all \( i, j \in [m] \), \( \ker(\psi_j) \subseteq \ker(\psi_i) \) implies \( i = j \).  
(6.3)

Then there exist positive real numbers \( R_0 = R_0(m,K) \), \( F_0 = F_0(m,n) \) and \( w_0 = w_0((\psi_j)_{j \in [m]}) \) such that if \( R \geq R_0 \), \( w \geq w_0 \) and \( w \leq F_0 \cdot \sqrt{\log R} \), then
\[
\mathbb{E}(\Lambda_{R,\chi}(\theta_1(x))^2 \cdots \Lambda_{R,\chi}(\theta_m(x))^2 \mid x \in B)
= \left( 1 + O_{m,n} \left( \frac{1}{w \log w} \right) + O_{\chi,m,t,K} \left( \frac{\log w}{\sqrt{\log R}} \right) \right) \cdot \left( \frac{W^n c_\chi \log R}{\varphi_K(W) \cdot \kappa} \right)^m
\]
holds true. In particular, the error terms \( O_{m,n} \left( \frac{1}{w \log w} \right) \) and \( O_{\chi,m,t,K} \left( \frac{\log w}{\sqrt{\log R}} \right) \) are bounded uniformly on \( W \) and \( (b_j)_{j \in [m]} \).
In the rest of this section is devoted to the proof of this theorem. In this section, we use ‘Propositions’ to rewrite the expectation on the left-hand side of (6.4); during the rewriting processes, we describe partial estimates as ‘Lemmas.’ We divide this section into subsections according to the particular aspect of estimate we focus on, such as $p$-parts of ideals. We clarify our setting as ‘Setting’ at the beginning of each subsection.

Recall the symbols and definitions given in Subsection 2.3 ‘Notation’ and Subsection 3.3. In particular, the following symbols are frequently used:

- the set $\mathcal{P}$ of all prime numbers, and subsets of form $\mathcal{P}_{\leq x}$ and $\mathcal{P}_{> x}$,
- the set $\mathfrak{I}_K^{(p)}$ of all $p$-ideals of $\mathcal{O}_K$,
- and the set $|\text{Spec}(\mathcal{O}_K)|^{(p)}$ of all prime $p$-ideals of $\mathcal{O}_K$.

Under Setting 6.3 below, we transform the following expectation

$$
\mathbb{E}\left( \prod_{j \in [m]} (\Lambda_{R,\chi} \circ \theta_j)^2 \bigg| \mathcal{B} \right),
$$

which appears on the left-hand side of (6.4).

**Setting 6.3.** Assume the setting in Theorem 6.2, and fix the function $\chi$ as in Definition 6.1. In addition, $w_0$, $R_0$ and $F_0$ are arbitrary positive real numbers with $R_0 > 1$.

**Proposition 6.4.** Expectation (6.5) is equal to

$$(\log R)^{2m} \sum_{(a_j, b_j) \in [m]} \Pi_{R,\chi} ((a_j, b_j)_{j \in [m]}) \cdot \mathbb{E}\left( \prod_{j \in [m]} (1_{a_j \cap b_j} \circ \theta_j) \bigg| \mathcal{B} \right),$$

where

$$
\Pi_{R,\chi} ((a_j, b_j)_{j \in [m]}) := \prod_{j \in [m]} \mu(a_j)\mu(b_j) \chi \left( \frac{\log N(a_j)}{\log R} \right) \chi \left( \frac{\log N(b_j)}{\log R} \right).
$$

**Proof.** Let $x \in \mathcal{B}$. Substituting (6.1) for $\Lambda_{R,\chi}(\theta_j(x))$ in (6.5) and expanding it, we have that

$$(\log R)^{-2m} \prod_{j \in [m]} \Lambda_{R,\chi}(\theta_j(x))^2
$$

$$
= \sum_{(a_j, b_j) \in [m]} \prod_{j \in [m]} \mu(a_j)\mu(b_j) \chi \left( \frac{\log N(a_j)}{\log R} \right) \chi \left( \frac{\log N(b_j)}{\log R} \right)
$$

$$
= \sum_{(a_j, b_j) \in [m]} \left( \prod_{j \in [m]} 1_{a_j \cap b_j}(\theta_j(x)) \right) \cdot \Pi_{R,\chi} ((a_j, b_j)_{j \in [m]}).
$$

Only the characteristic functions $\prod_{j \in [m]} 1_{a_j \cap b_j}(\theta_j(x))$ depend on $x \in \mathcal{B}$, and hence the desired result holds. \qed
Next we focus on the expectation in (6.6). Although a statement similar to the following lemma might be standard in this research area, we write down a proof for the convenience of the reader.

**Lemma 6.5.** Let \((a_j, b_j)_{j \in [m]} \in \text{Ideals}_K^{2m}\), and define a positive integer \(D = D ((a_j, b_j)_{j \in [m]})\) such that

\[
DZ = \mathbb{Z} \cap \left( \bigcap_{j \in [m]} (a_j \cap b_j) \right). \tag{6.7}
\]

If for every \(j \in [m], N(a_j), N(b_j) \leq R\), then the following hold.

1. \(D \leq R^{2m}\).
2. The following holds:

\[
\mathbb{E} \left( \prod_{j \in [m]} (1_{a_j \cap b_j} \circ \theta_j) \mid B \right) = \mathbb{E} \left( \prod_{j \in [m]} (1_{a_j \cap b_j} \circ \theta_j) \mid (\mathbb{Z}/D\mathbb{Z})^t \right) + O(R^{−2m−1}).
\]

Note that for every \(x \in (\mathbb{Z}/D\mathbb{Z})^t, 1_{a_j \cap b_j}(\theta_j(x)) \in \{0, 1\}\) is well-defined.

**Proof.** First we prove \([1]\). For each \(a \in \{a_j, b_j\}_{j \in [m]}\), the injection \(\mathbb{Z}/(\mathbb{Z} \cap a) \hookrightarrow \mathcal{O}_K/a\) shows \(#(\mathbb{Z}/(\mathbb{Z} \cap a)) \leq #(\mathcal{O}_K/a) = N(a) \leq R\). This together with

\[
DZ = \bigcap_{j \in [m]} ((\mathbb{Z} \cap a_j) \cap (\mathbb{Z} \cap b_j)) \supseteq \prod_{j \in [m]} ((\mathbb{Z} \cap a_j) \cdot (\mathbb{Z} \cap b_j))
\]

implies that

\[
D = #(\mathbb{Z}/D\mathbb{Z}) \leq \prod_{j \in [m]} (\#(\mathbb{Z}/\mathbb{Z} \cap a_j) \cdot \#(\mathbb{Z}/\mathbb{Z} \cap b_j)) \leq R^{2m}.
\]

Next we prove \([2]\). Since \(B\) contains pairwise disjoint \(\prod_{i \in [t]} \left\lfloor \frac{\#I_i}{D} \right\rfloor\) translates of \([D]^t\) in \(\mathbb{Z}^t\), we see that

\[
\#B \cdot \mathbb{E} \left( \prod_{j \in [m]} (1_{a_j \cap b_j} \circ \theta_j) \mid B \right) = \left( \prod_{i \in [t]} \left\lfloor \frac{\#I_i}{D} \right\rfloor \right) \cdot D^t \cdot \mathbb{E} \left( \prod_{j \in [m]} (1_{a_j \cap b_j} \circ \theta_j) \mid (\mathbb{Z}/D\mathbb{Z})^t \right) + O \left( \#B - \left( \prod_{i \in [t]} \left\lfloor \frac{\#I_i}{D} \right\rfloor \right) \cdot D^t \right). \tag{6.8}
\]

Since \(\left\lfloor \frac{\#I_i}{D} \right\rfloor \cdot D > \#I_i - D\), we have

\[
\frac{1}{\#B} \left( \#B - \left( \prod_{i \in [t]} \left\lfloor \frac{\#I_i}{D} \right\rfloor \right) \cdot D^t \right) < 1 - \frac{1}{\#B} \prod_{i \in [t]} (\#I_i - D) = 1 - \prod_{i \in [t]} \left( 1 - \frac{D}{\#I_i} \right).
\]
Note that \( D/\#I_i \leq R^{2m}/R^{4m+1} = R^{-2m-1} \) follows from (1). By Bernoulli’s inequality, we conclude that
\[
1 - \prod_{i \in [t]} \left( 1 - \frac{D}{\#I_i} \right) \leq 1 - (1 - R^{-2m-1})^t \leq t R^{-2m-1}.
\]

Furthermore,
\[
\frac{1}{\#B} \cdot \left( \prod_{i \in [t]} \left| \frac{\#I_i}{D} \right| \right) \cdot D' = 1 + O_t(R^{-2m-1})
\]
follows, and we derive the desired equality.

We write for short the following expectation
\[
e((a_j, b_j)_{j \in [m]}) = e((a_j, b_j)_{j \in [m]}; (\theta_j)_{j \in [m]}) := \mathbb{E} \left( \prod_{j \in [m]} (1_{a_j \cap b_j} \circ \theta_j) \mid (\mathbb{Z}/D\mathbb{Z})^t \right), \tag{6.9}
\]
which depends on \((\theta_j)_{j \in [m]}\) and \((a_j, b_j)_{j \in [m]}\). Here the positive integer \(D = D((a_j, b_j)_{j \in [m]})\) is taken as in Lemma 6.5. In what follows, we prove the multiplicativity of \(e\) in Lemma 6.8 and the estimates as in Lemma 6.12 for \(e\). Once these two properties are established, we will no longer need the definition of \(e\) for the proof of Theorem 6.2.

**Proposition 6.6.** Expectation \((6.6)\) equals
\[
(\log R)^{2m} \sum_{(a_j, b_j)_{j \in [m]} \in \text{(Ideals}_K)^{2m}} \Pi_{R,\chi} \left((a_j, b_j)_{j \in [m]}\right) \cdot e\left((a_j, b_j)_{j \in [m]}\right) \tag{6.10}
\]
with an additive error term \(O_t,K \left( \frac{(\log R)^{2m}}{R} \right)\), where \(\Pi_{R,\chi} \left((a_j, b_j)_{j \in [m]}\right)\) is defined in Proposition 6.4.

**Proof.** By Lemma 6.5 (2), the the subtracting \((6.6)\) from \((6.10)\), we obtain
\[
(\log R)^{2m} \sum_{(a_j, b_j)_{j \in [m]} \in \text{(Ideals}_K)^{2m}} \Pi_{R,\chi} \left((a_j, b_j)_{j \in [m]}\right) \cdot O_t(R^{-2m-1}). \tag{6.11}
\]

Since the support of the function \(\chi\) is contained in \([-1, 1]_\mathbb{R}\) it suffices to consider the sum over pairs \((a_j, b_j)_{j \in [m]}\) with \(N(a_j), N(b_j) \leq R\) for all \(j \in [m]\). Moreover, Proposition 3.20 asserts that the number of such pairs \((a_j, b_j)_{j \in [m]}\) is \(O_K(R^{2m})\). Since \(|\Pi_{R,\chi}((a_j, b_j)_{j \in [m]}|) \leq 1\), we have the desired estimate for the difference \((6.11)\) above.

It is seen that the contribution of all error terms are permissible in the proof of Theorem 6.2. Next we focus on the expectation \(e\left((a_j, b_j)_{j \in [m]}\right)\) in \((6.10)\).
6.3 The expectation of the characteristic function

In this subsection, we assume the following setting:

**Setting 6.7.** Assume Setting 6.3. Fix a tuple \((a_j, b_j)_{j \in [m]}\) of arbitrary nonzero ideals of \(\mathcal{O}_K\) each of which is not necessary of norm at most \(R\), and write \(c_j := a_j \cap b_j\) for short. Note that \(c_j^{(p)} = a_j^{(p)} \cap b_j^{(p)}\) (see Subsection 3.3 where \(p\)-parts are defined). Let \(D\) be the positive integer defined in Lemma 6.5. Then note that \(DZ = Z \cap (\bigcap_{j \in [m]} c_j)\) and \(D^{(p)}Z = Z \cap (\bigcap_{j \in [m]} c_j^{(p)})\).

The following symbols and an easy equality are helpful to estimate (6.9). We consider the \(\mathbb{Z}\)-module homomorphisms and affine transformations

\[
\overline{\psi}_j, \overline{\theta}_j : (\mathbb{Z}/DZ)^t \to \mathcal{O}_K/c_j
\]

induced by \(\psi_j\) and \(\theta_j\), respectively. Let

\[
\overline{\psi}, \overline{\theta} : (\mathbb{Z}/DZ)^t \to \prod_{j \in [m]} \mathcal{O}_K/c_j
\]

be the two maps defined by \(\overline{\psi}(x) = (\overline{\psi}_1(x), \ldots, \overline{\psi}_m(x))\) and \(\overline{\theta}(x) = (\overline{\theta}_1(x), \ldots, \overline{\theta}_m(x))\). Then we see that

\[
e((a_j, b_j)_{j \in [m]}) = \mathbb{E}\left( \prod_{j \in [m]} (1_{c_j} \circ \theta_j) \bigg| (\mathbb{Z}/DZ)^t \right) = \mathbb{E}\left( 1_{\{0\}} \circ \overline{\theta} \bigg| (\mathbb{Z}/DZ)^t \right). \tag{6.12}
\]

**Lemma 6.8.** The expectation \(\mathbb{E}\left( (a_j, b_j)_{j \in [m]} \right)\) is decomposed into its \(p\)-parts. Namely,

\[
\mathbb{E}\left( (a_j, b_j)_{j \in [m]} \right) = \prod_{p \in \mathcal{P}} \mathbb{E}\left( (a_j^{(p)}, b_j^{(p)})_{j \in [m]} \right).
\]

**Proof.** Recall the definition of \(\mathbb{E}\). It suffices to prove that

\[
\mathbb{E}\left( \prod_{j \in [m]} (1_{c_j} \circ \theta_j) \bigg| (\mathbb{Z}/DZ)^t \right) = \prod_{p \in \mathcal{P}} \mathbb{E}\left( \prod_{j \in [m]} (1_{c_j^{(p)}} \circ \theta_j) \bigg| (\mathbb{Z}/D^{(p)}Z)^t \right).
\]

By the Chinese remainder theorem (Lemma 3.14), the \(\mathbb{Z}\)-module homomorphism \(\overline{\psi}\) equals the product of its restrictions \(\overline{\psi}^{(p)}\) to \((\mathbb{Z}/D^{(p)}Z)^t\), that means

\[
\overline{\psi} = \prod_{p \in \mathcal{P}} \overline{\psi}^{(p)} : \prod_{p \in \mathcal{P}} (\mathbb{Z}/D^{(p)}Z)^t \to \prod_{p \in \mathcal{P}} \left( \prod_{j \in [m]} \mathcal{O}_K/c_j^{(p)} \right).
\]

Hence the affine transformation \(\overline{\theta}\) is the product of the restrictions

\[
\overline{\theta}^{(p)} : (\mathbb{Z}/D^{(p)}Z)^t \to \prod_{j \in [m]} \mathcal{O}_K/c_j^{(p)}.
\]
Applying (6.12) to the ideals \((c_j)_{j \in [m]}\) and \((c_p)_{j \in [m]}\), we see that it suffices to prove
\[
\mathbb{E} \left( 1_{\{0\}} \circ \bar{\theta} \mid (\mathbb{Z}/D\mathbb{Z})^t \right) = \prod_{p \in \mathcal{P}} \mathbb{E} \left( 1_{\{0\}} \circ \bar{\theta}^{(p)} \mid (\mathbb{Z}/D^{(p)}\mathbb{Z})^t \right).
\] (6.13)

Since \(c_j = \prod_{p \in \mathcal{P}} c_j^{(p)} = \bigcap_{p \in \mathcal{P}} c_j^{(p)}\), for each element
\[
x = (x_p)_{p \in \mathcal{P}} \in \prod_{p \in \mathcal{P}} (\mathbb{Z}/D^{(p)}\mathbb{Z})^t,
\]
we have \(\bar{\theta}(x) = 0\) if and only if \(\bar{\theta}^{(p)}(x_p) = 0\) holds for every \(p \in \mathcal{P}\). Hence
\[
\mathbb{E} \left( 1_{\{0\}}(\bar{\theta}(x)) \mid x \in (\mathbb{Z}/D\mathbb{Z})^t \right) = \mathbb{E} \left( \prod_{p \in \mathcal{P}} 1_{\{0\}}(\bar{\theta}^{(p)}(x_p)) \mid (x_p)_{p \in \mathcal{P}} \in \prod_{p \in \mathcal{P}} (\mathbb{Z}/D^{(p)}\mathbb{Z})^t \right).
\]
This coincides with the right-hand side of (6.13).

From this lemma, in the next subsection, we may restrict our attention to a tuple of \(p\)-ideals for each rational prime number \(p\).

### 6.4 The expectation of the characteristic function for \(p\)-ideals

In this subsection, we assume the following setting. We use symbols such as \(\alpha_j, \beta_j\) and \(\gamma_j\) for \(p\)-ideals.

#### Setting 6.9
Let \(K, n, t, m, (\psi_j)_{j \in [m]}\) be as in Theorem 6.2; we assume (6.3). In addition, \(w_0\) will be given in Setting 6.10 below and then we take \(w, W, (\theta_j)_{j \in [m]}\) as in Theorem 6.2. Let \((\alpha_j, \beta_j)_{j \in [m]} \in (\text{Ideals}_K^{(p)})^{2m}\) be the tuple of \(p\)-ideals for some prime number \(p\). Write \(\gamma_j := \alpha_j \cap \beta_j\). Let \(D\) be the positive integer such that \(D\mathbb{Z} = \mathbb{Z} \cap \left( \bigcap_{j \in [m]} \gamma_j \right)\). Then the ideals \(\gamma_j\) are \(p\)-ideals, and \(D\) is a power of \(p\). The two maps \(\bar{\psi}, \bar{\theta}: (\mathbb{Z}/D\mathbb{Z})^t \to \prod_{j \in [m]} \mathcal{O}_K/\gamma_j\) are defined in Subsection 6.3.

#### Setting 6.10
Let \(w_0\) be a positive real number at least \(w'_0\) and \(w''_0\), which are defined as follows:

1. For every \(j \in [m]\), the cardinality of \(\text{coker}(\psi_j)\) is finite by assumption (6.3). Hence we let \(w'_0\) be the largest prime factor of \(\prod_{j \in [m]} \# \text{coker}(\psi_j)\).

2. By assumption (6.3), for each \((j, k) \in [m]^2\) with \(j \neq k\), we may take \(x_{jk} \in \text{ker}(\psi_j) \setminus \text{ker}(\psi_k)\). Then let
\[
w''_0 := \max \left\{ \ell \in \mathcal{P} : \exists p \in |\text{Spec} \mathcal{O}_K|^{(\ell)}, p \mid \prod_{(j, k) \in [m]^2, j \neq k} \psi_k(x_{jk}) \right\}.
\]
We take the elements \(x_{jk}\) which minimizes \(w''_0\), and then \(w''_0\) depends only on \((\psi_j)_{j \in [m]}\).
Below we estimate the expectation

$$e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) = \mathbb{E} \left( \prod_{j \in [m]} (1_{\gamma_j} \circ \theta_j) \mid (\mathbb{Z}/D\mathbb{Z})^t \right) = \mathbb{E} \left( 1_{\{0\}} \circ \overline{\theta} \mid (\mathbb{Z}/D\mathbb{Z})^t \right).$$

We prove the following without assuming Setting 6.10.

**Lemma 6.11.** If $p > w$, then

$$e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) = \begin{cases} \#\text{Im}(\overline{\psi})^{-1} & \text{if } 0 \in \text{Im}(\overline{\theta}), \\ 0 & \text{otherwise}. \end{cases}$$

**Proof.** In general, for an affine transformation $\theta: Z \rightarrow Z'$ between two finite abelian groups $Z$ and $Z'$,

$$\mathbb{E} \left( 1_{\{0\}} \circ \theta \mid Z \right) = \begin{cases} \#\text{Im}(\theta)^{-1} & \text{if } 0 \in \text{Im}(\theta), \\ 0 & \text{otherwise}. \end{cases}$$

By applying this to $\overline{\theta}: (\mathbb{Z}/D\mathbb{Z})^t \rightarrow \prod_{j \in [m]} \mathcal{O}_K/\gamma_j$, we see that the expectation $e \left( (\alpha_j, \beta_j)_{j \in [m]} \right)$ equals $(\#\text{Im}(\overline{\theta}))^{-1}$ if $0 \in \text{Im}(\overline{\theta})$, and 0 otherwise. Consider the first case. By $p > w$, $W$ and $p$ are coprime. Since the order of each $\mathcal{O}_K/\gamma_j$ is a power of $p$, this implies that the multiplication by $W$ on $\prod_{j \in [m]} \mathcal{O}_K/\gamma_j$ is an automorphism. Therefore $\#\text{Im}(\overline{\theta}) = \#\text{Im}(\overline{\psi})$ follows. \(\square\)

Only the following lemma and its consequences exploit assumption (6.3).

**Lemma 6.12.** For each prime number $p$ and each tuple $(\alpha_j, \beta_j)_{j \in [m]}$ of $p$-ideals, the following hold:

1. If $\gamma_j = \mathcal{O}_K$ holds for every $j \in [m]$, then $e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) = 1$.

2. Suppose that $p \leq w$ and there exists $j_0 \in [m]$ such that $\gamma_{j_0} \subseteq \mathcal{O}_K$. Then $e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) = 0$.

3. Suppose that $p > w$ and there exists $j_0 \in [m]$ such that $\gamma_{j_0} \subseteq \mathcal{O}_K$ and $\gamma_j = \mathcal{O}_K$ for all $j \in [m] \setminus \{j_0\}$. Then $e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) = 1/\mathbb{N}(\gamma_{j_0})$.

4. Suppose that $p > w$ and there exist two distinct $j_1$ and $j_2 \in [m]$ such that $\gamma_{j_1}, \gamma_{j_2} \nsubseteq \mathcal{O}_K$. Then $e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) \leq 1/p^2$.

**Proof.** First we prove (1). If $\gamma_j = \mathcal{O}_K$ for every $j \in [m]$, then $\prod_{j \in [m]} (1_{\gamma_j} \circ \theta_j)$ is identical with the constant function 1, and hence $e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) = 1$.

Secondly, we prove (2). Then it suffices to show that for all $x \in (\mathbb{Z}/D\mathbb{Z})^t$, $\theta_{j_0}(x) = W\psi_{j_0}(x) + b_{j_0} \notin \gamma_{j_0}$. Let $p$ be an arbitrary prime ideal $p \supseteq \gamma_{j_0}$. Since $\gamma_{j_0}$ is a $p$-ideal, we have $p \cap \mathbb{Z} = p\mathbb{Z}$. From $p \leq w$, $p$ divides $W$, and hence $W \in p$ follows. In addition, the assumption $b_{j_0}\mathcal{O}_K + W\mathcal{O}_K = \mathcal{O}_K$ implies that $b_{j_0} \notin p$. Hence we see that for all $x \in \mathbb{Z}^t$, $\theta_{j_0}(x) = W\psi_{j_0}(x) + b_{j_0} \notin p$. This together with $\gamma_{j_0} \subseteq p$ implies that $\theta_{j_0}(x) \notin \gamma_{j_0}$, as desired.
Thirdly, we prove (3). Set \( C_{j_0} := \# \text{coker}(\psi_{j_0}) \). Note that for every \( x \in \mathcal{O}_K \), \( C_{j_0} \cdot x \) is contained in the image of \( \psi_{j_0} \). By Setting 6.10 (1), \( p \) and \( C_{j_0} \) are coprime. Since the order of \( \mathcal{O}_K / \gamma_{j_0} \) is a power of \( p \), this implies that the multiplication by \( C_{j_0} \) on \( \mathcal{O}_K / \gamma_{j_0} \) is an automorphism. Hence we see that \( \psi_{j_0} : (\mathbb{Z} / D\mathbb{Z})^t \to \mathcal{O}_K / \gamma_{j_0} \) is surjective. By Setting 6.10 (1), \( p \) and \( C_{j_0} \) are coprime. Since the order of \( \mathcal{O}_K / \gamma_{j_0} \) is a power of \( p \), this implies that the multiplication by \( C_{j_0} \) on \( \mathcal{O}_K / \gamma_{j_0} \) is an automorphism. Hence we see that \( \psi_{j_0} : (\mathbb{Z} / D\mathbb{Z})^t \to \mathcal{O}_K / \gamma_{j_0} \) is surjective. Since \( W \) and \( p \) are coprime, the map \( \theta_{j_0} = \text{Aff}_{W,b_{j_0}} \circ \psi_{j_0} : (\mathbb{Z} / D\mathbb{Z})^t \to \mathcal{O}_K / \gamma_{j_0} \) is also surjective. Then Lemma 6.11 yields that \( \left| \left( \alpha_j, \beta_j \right)_{j \in [m]} \right| = \left( \#(\text{Im}(\psi)) \right) - 1 \); recall that \( \gamma_j = \mathcal{O}_K \) for all \( j \in [m] \setminus \{j_0\} \). We have

\[ \#(\text{Im}(\psi)) = \#(\text{Im}(\psi_{j_0})) = \#(\mathcal{O}_K / \gamma_{j_0}) = N(\gamma_{j_0}). \]

This is the desired result.

Finally we prove (4). By Lemma 6.11, it suffices to show that \( \#(\text{Im}(\psi)) \geq p^2 \). Without loss of generality, we may assume that \( \gamma_1, \gamma_2 \subseteq \mathcal{O}_K \). Recall that two elements \( x_{12} \) and \( x_{21} \) are chosen in Setting 6.10 (2). Since \( p > w \geq w'' \), both \( \psi_2(x_{12}) \) and \( \psi_1(x_{21}) \) are prime to all \( p \)-ideals. We focus on the mapping \( (\psi_1, \psi_2) \), which is defined as

\[ (\psi_1, \psi_2) : (\mathbb{Z} / D\mathbb{Z})^t \to \mathcal{O}_K / \gamma_1 \times \mathcal{O}_K / \gamma_2 \]

\[ x \mapsto (\psi_1(x), \psi_2(x)). \]

This maps \( x_{12} \) and \( x_{21} \) to nonzero elements \( (0, \psi_2(x_{12})) \) and \( (\psi_1(x_{21}), 0) \), respectively. The order of the linear span of these two images is at least \( p^2 \). Hence

\[ p^2 \leq \#(\text{Im}(\psi_1, \psi_2)) \leq \#(\text{Im}(\psi)), \]

and (4) follows.

### 6.5 Estimate for the error by a change of domain of integration

In this subsection, we estimate expectation (6.5). Its main term is equal to (6.10) by Proposition 6.6. In this subsection, we prove Proposition 6.14, which provides an integral representation of the main term.

First, we use the Fourier transform to derive an integral representation of \( \chi \), which is given in Definition 6.1. Let \( \hat{\chi} \) be the inverse Fourier transform of the function \( x \mapsto e^x \chi(x) \). Here we normalize it to satisfy

\[ e^x \chi(x) = \int_{\mathbb{R}} \hat{\chi}(\xi) e^{-x(1+\xi\sqrt{-1})} d\xi, \quad \text{or equivalently,} \quad \chi(x) = \int_{\mathbb{R}} \hat{\chi}(\xi) e^{-x(1+\xi\sqrt{-1})} d\xi. \quad (6.14) \]

Then for all \( \mathfrak{c} \in \text{Ideals}_K \) and \( R > 1 \), we have that

\[ \chi \left( \log \frac{N(\mathfrak{c})}{\log R} \right) = \int_{\mathbb{R}} \hat{\chi}(\xi) N(\mathfrak{c})^{-\left((1+\xi\sqrt{-1})/\log R \right) / \log R} d\xi. \quad (6.15) \]

Assume the following:
Setting 6.13. Assume the setting in Theorem 6.2 and fix $\chi$ as in Definition 6.1. In addition, assume that $R_0 \geq \epsilon$, $F_0 > 0$ and $w_0 \geq \max\{4^{2m}, w_0', w_0''\}$, where $w_0'$ and $w_0''$ are defined in Setting 6.10.

Recall that $e ((a_j, b_j)_{j\in[m]}$ is defined as (6.9). Let $I = \{\sqrt{\log R}, +\sqrt{\log R}\}_{\mathbb{R}}$, and $\xi_j$ and $\eta_j$ be variables of integration. For short, write $d\xi = d\xi_1 \cdots d\xi_m$ and $d\eta = d\eta_1 \cdots d\eta_m$. Let

\[ z_j := \frac{1 + \xi_j \sqrt{-1}}{\log R}, \quad w_j := \frac{1 + \eta_j \sqrt{-1}}{\log R}. \]

Note that the real number $w \geq w_0$ and complex variable $w_j$ are unrelated.

The goal in this subsection is to prove the following. We define

\[ E := \sum_{(a_j, b_j)_{j\in[m]} \in \text{Ideals}^{2m}} \left( \prod_{j\in[m]} \{ \mu(a_j)\mu(b_j)N(a_j)^{-\xi_j}N(b_j)^{-\eta_j} \} \right) e ((a_j, b_j)_{j\in[m]}). \]

(6.16)

Proposition 6.14. The series $E = E ((\xi_j, \eta_j)_{j\in[m]}; R)$ converges uniformly on $(\xi_j, \eta_j)_{j\in[m]} \in I^{2m}$. Furthermore, for every positive real number $\epsilon$, (6.10) is equal to

\[ (\log R)^{2m} \int_{I^{2m}} d\xi d\eta \left[ \prod_{j\in[m]} (\xi_j) \cdot E ((\xi_j, \eta_j)_{j\in[m]}; R) \right] \]

(6.17)

with an additive error term $O_{A,\chi;m,n} ((\log R)^{-\epsilon})$.

We estimate the error caused by the change of the domain of integration from $\mathbb{R}^{2m}$ to $I^{2m}$. Then it turns out that this error is sufficiently small for our purpose. To show this, we provide several estimates as lemmas. First we recall the following estimate in Fourier analysis; we write down a proof for the convenience of the reader.

Lemma 6.15. For every real-valued $C^N$-function $f$ whose support with compact support, we have

\[ \mathcal{F}^*(f)(x) := \int_{\mathbb{R}} f(\xi) e^{\pi \xi \sqrt{-1}} d\xi = O_{N,f} ((1 + |x|)^{-N}), \]

where $\mathcal{F}^*(f)$ denotes the inverse Fourier transform of $f$.

Proof. Since the support of $f$ is compact, $f \in L^1(\mathbb{R})$ holds, and then $\|\mathcal{F}^*(f)\|_{\infty} \leq \|f\|_1 < \infty$ follows. For every $k \in [0, N]$, since the $k$th derivative of $f$ has a compact support, there exists a real number $C_{N,f}$ such that $\|\mathcal{F}^*(f(k))\|_{\infty} \leq C_{N,f}$. By integration by parts, we have $\mathcal{F}^*(f')(x) = -\sqrt{-1} x \mathcal{F}^*(f)(x)$. Applying this repeatedly, we see that for all $k \in [0, N], \|\mathcal{F}^*(f(k))(x)\| = |x|^k |\mathcal{F}^*(f)(x)|$. Hence

\[ |\mathcal{F}^*(f)(x)| \sum_{k\in[0, N]} |x|^k \leq \sum_{k\in[0, N]} |\mathcal{F}^*(f(k))(x)| \leq (N + 1)C_{N,f} =: C'_{N,f}. \]

By the binomial theorem, there exists $c_N > 0$ such that $c_N (1 + |x|)^N \leq \sum_{k\in[0, N]} |x|^k$. Therefore we obtain the desired estimate $|\mathcal{F}^*(f)(x)| \leq \frac{C'_{N,f}}{c_N} (1 + |x|)^{-N}$. 

\[ \square \]
Corollary 6.16. For every positive real number $A$, we have
\[
\int_{\mathbb{R}} |\hat{\chi}(\xi)|d\xi = O_{A,\chi}(1). \tag{6.18}
\]
In addition, for all positive real numbers $b$ and $A$, we have
\[
\int_{b}^{\infty} |\hat{\chi}(\xi)|d\xi = O_{A,\chi}(b^{-A}) \quad \text{and} \quad \int_{-\infty}^{-b} |\hat{\chi}(\xi)|d\xi = O_{A,\chi}(b^{-A}). \tag{6.19}
\]

Proof. The $C^\infty$-function $\chi$ has a compact support. Applying Lemma 6.15 with $f(x) = e^{x}\chi(x)$, we have $$\hat{\chi}(\xi) = O_{B,\chi}((1 + |\xi|)^{-B}) \text{ for all } B \geq 0.$$ Let $b \geq 0$, $B = A + 1$, and $I_b = [b, \infty]_\mathbb{R}$ or $[-\infty, -b]_\mathbb{R}$. Then we have that
\[
\int_{I_b} |\hat{\chi}(\xi)|d\xi = \int_{I_b} O_{B,\chi}((1 + |\xi|)^{-B}) d\xi = O_{B,\chi}\left(\int_{I_b} (1 + \xi)^{-B}d\xi\right)
\]
\[
= O_{B,\chi}\left(\frac{1}{B - 1}(1 + b)^{1 - B}\right) = \begin{cases} O_{A,\chi}(b^{-A}) & \text{if } b > 0, \\ O_{A,\chi}(1) & \text{otherwise}. \end{cases}
\]
\[\square\]

Lemma 6.17. For every positive real number $A$ and every tuple $(a_j, b_j)_{j \in [m]} \in \text{Ideals}_{\mathbb{R}}^{2m}$, we have that
\[
\prod_{j \in [m]} \chi \left(\frac{\log N(a_j)}{\log R}\right) \chi \left(\frac{\log N(b_j)}{\log R}\right) = \int_{I^{2m}} d\xi d\eta \left[ \prod_{j \in [m]} N(a_j)^{-z_j} N(b_j)^{-w_j} \hat{\chi}(\xi) \hat{\chi}(\eta) \right] + O_{A,\chi,m} \left( (\log R)^{-A} \prod_{j \in [m]} N(a_j)^{-\frac{1}{\log R}} N(b_j)^{-\frac{1}{\log R}} \right). \tag{6.21}
\]

Proof. Let $\mathfrak{c} \in \text{Ideals}_{\mathbb{R}}$. Integral representation (6.15) of $\chi$ is decomposed as
\[
\chi \left(\frac{\log N(\mathfrak{c})}{\log R}\right) = \int_{I} \hat{\chi}(\xi) N(\mathfrak{c})^{-\left(1+\xi\sqrt{-1}\right)/\log R} d\xi + \int_{R\setminus I} \hat{\chi}(\xi) N(\mathfrak{c})^{-\left(1+\xi\sqrt{-1}\right)/\log R} d\xi. \tag{6.20}
\]

The two term on the right-hand side are estimated in the following manner: the first equality (6.18) in Corollary 6.16 implies that
\[
\left| \int_{I} \hat{\chi}(\xi) N(\mathfrak{c})^{-\left(1+\xi\sqrt{-1}\right)/\log R} d\xi \right| \leq N(\mathfrak{c})^{-1/\log R} \int_{I} |\hat{\chi}(\xi)|d\xi = O_{A,\chi} \left( N(\mathfrak{c})^{-1/\log R} \right).
\]
Similarly, the second equality (6.19) in Corollary 6.16 implies that
\[
\left| \int_{R\setminus I} \hat{\chi}(\xi) N(\mathfrak{c})^{-\left(1+\xi\sqrt{-1}\right)/\log R} d\xi \right| = O_{A,\chi} \left( N(\mathfrak{c})^{-1/\log R}(\log R)^{-A} \right). \tag{6.21}
\]
Note that \( O_{A, \chi} \left( N(\mathbf{c})^{-1/\log R} (\log R)^{-A} \right) = O_{A, \chi} \left( N(\mathbf{c})^{-1/\log R} \right) \) by \( R \geq R_0 \geq e \). We decompose each of the \( 2m \) factors of

\[
\prod_{j \in [m]} \chi \left( \frac{\log N(a_j)}{\log R} \right) \chi \left( \frac{\log N(b_j)}{\log R} \right)
\]

as (6.20), and expand this product. As a result, this product is expressed as the sum of the main term whose domain of integration is \( I^{2m} \) and other \( 2m - 1 \) error terms. Then we focus on each error term, which is the product of \( 2 \) factors. We apply (6.21) to one of these \( 2m \) factors whose domain of integration is \( \mathbb{R} \setminus I \). Moreover the other factors can be estimated as \( O_{A, \chi} \left( N(\mathbf{c})^{-1/\log R} \right) \). Hence the desired conclusion follows.

Using this lemma, we show an integral representation of (6.10) up to a sufficiently small additive error. Each term of the series (6.10) has \( \chi(\log N(\cdot)/\log R) \) as a factor. Hence it suffices to consider this series over \( (a_j, b_j)_{j \in [m]} \) all of whose entries have norm at most \( R \). Hence it is a finite series. However, the term represented by integral in Lemma 6.17 should be considered over all the \( (a_j, b_j)_{j \in [m]} \), and hence \( E \) defined in (6.16) is an infinite series over all the \( (a_j, b_j)_{j \in [m]} \). This causes a subtlety on exchanging the order of summations and integrations; we will overcome it by proving that \( E \) converges absolutely and uniformly. In the rest of this subsection, we mainly show that the error caused by application of Lemma 6.17 is small enough. It suffices to estimate the error roughly; however we prepare a precise lemma for an estimate for the main term.

For each prime number \( p \in \mathcal{P} \), we define

\[
E_p = E_p \left( (\xi_j, \eta_j)_{j \in [m]}; R \right)
= \sum_{(\alpha_j, \beta_j)_{j \in [m]} \in \text{Ideals}^2_{\mathcal{K}}} \left( \prod_{j \in [m]} \{ \mu(\alpha_j) \mu(\beta_j) N(\alpha_j)^{-z_j} N(\beta_j)^{-w_j} \} \right) e \left( (\alpha_j, \beta_j)_{j \in [m]} \right) .
\]

(6.22)

Since each summand of this sum contains \( \mu(\alpha_j) \mu(\beta_j) \) as a factor, it suffices to consider the sum over the tuples \( (\alpha_j, \beta_j)_{j \in [m]} \) consisting of square free \( p \)-ideals. The number of such tuples is at most \( 4^m \) by Lemma 3.15. The absolute value of summand for every \( (\alpha_j, \beta_j)_{j \in [m]} \neq (\mathcal{O}_K, \ldots, \mathcal{O}_K) \) is at most \( 1/p \). Hence for every prime number \( p \) greater than \( w \ (\geq 4^m) \), \( E_p \) is a non-zero finite value by Lemma 6.12. More precisely, we prove the following.

**Lemma 6.18.** For every prime number \( p \) greater than \( w \), we have

\[
E_p = 1 - \Sigma_p \left( (\xi_j, \eta_j)_{j \in [m]}; R \right) + O(4^m/p^2),
\]

(6.23)

where

\[
\Sigma_p \left( (\xi_j, \eta_j)_{j \in [m]}; R \right) := \sum_{j \in [m]} \sum_{p \in \text{Spec}(\mathcal{O}_K) \setminus \{p\}} \left( N(p)^{-1-z_j} + N(p)^{-1-w_j} - N(p)^{-1-z_j-w_j} \right).
\]

The infinite series \( E \) defined by (6.16) and the infinite product \( \prod_{p \in \mathcal{P} > w} E_p \) converge absolutely and uniformly on \( (\xi_j, \eta_j)_{j \in [m]} \in I^{2m} \). Furthermore, they coincide, that is,

\[
E = \prod_{p \in \mathcal{P} > w} E_p .
\]

(6.24)
Proof. Let $p$ be a prime number greater than $w$. Consider the case of Lemma 6.12, namely, there exists $j_0 \in [m]$ such that $p := \alpha_{j_0} \cap \beta_{j_0} \in |\text{Spec}(O_K)|^{(p)}$ and $\alpha_j = \beta_j = O_K$ for all $j \in [m] \setminus \{j_0\}$. Then Lemma 6.12 asserts that $e((\alpha_j, \beta_j)_{j \in [m]}) = N(p)^{-1}$. Moreover we have

$$(\alpha_{j_0}, \beta_{j_0}) \in \{(p, O_K), (O_K, p), (p, p)\}.$$ 

Hence (6.23) follows from Lemma 6.12. 

Let $\tilde{E}$ be the sum of the absolute values of the summands of $E$, and for each prime number $p$, let $\tilde{E}_p$ be that of $E_p$. Applying Lemma 6.12 to the summands of $\tilde{E}_p$, we have

$$\tilde{E}_p = \begin{cases} 1 + O_{m,n} \left( p^{-1 - \frac{1}{\log R}} \right) & \text{if } p > w, \\ 1 & \text{otherwise.} \end{cases}$$ 

and

$$\prod_{p \in \mathcal{P}} \tilde{E}_p = \prod_{p \in \mathcal{P} > w} \left( 1 + O_{m,n} \left( p^{-1 - \frac{1}{\log R}} \right) \right). \quad (6.25)$$

Since

$$\sum_{p \in \mathcal{P} > w} O_{m,n} \left( p^{-1 - \frac{1}{\log R}} \right) = O_{m,n} \left( \zeta \left( 1 + \frac{1}{\log R} \right) \right) < \infty,$$

product (6.25) converges uniformly on $(\xi_j, \eta_j)_{j \in [m]} \subseteq I^{2m}$. This implies that $\prod_{p \in \mathcal{P} > w} E_p$ converges absolutely and uniformly. By the multiplicativity of the Möbius function, norm (Lemma 3.7) and $e$ (Lemma 6.8), we see that for each $(a_j, b_j)_{j \in [m]} \subseteq \text{Ideals}_{2m}^{\mathcal{P}_R}$,

$$\left( \prod_{j \in [m]} \mu(a_j) \mu(b_j) N(a_j)^{-z_j} N(b_j)^{-w_j} \right) e((a_j, b_j)_{j \in [m]})$$

$$= \prod_{p \in \mathcal{P}} \left( \prod_{j \in [m]} \mu(a_j^{(p)}) \mu(b_j^{(p)}) N(a_j^{(p)})^{-z_j} N(b_j^{(p)})^{-w_j} \right) e((a_j^{(p)}, b_j^{(p)})_{j \in [m]}) \right].$$

Hence

$$\tilde{E} = \prod_{p \in \mathcal{P}} \tilde{E}_p = \prod_{p \in \mathcal{P} > w} \tilde{E}_p.$$

Therefore $E$ converges absolutely and uniformly on $(a_j, b_j)_{j \in [m]} \subseteq \text{Ideals}_{2m}^{\mathcal{P}_R}$, and we have $E = \prod_{p \in \mathcal{P} > w} E_p.$ \hfill \Box

The following lemma provides a further estimate of (6.25).

Lemma 6.19. Let $C$ be a positive real number. Then for each positive real number $w$, we have

$$\prod_{p \in \mathcal{P} > w} \left( 1 + C \cdot p^{-1 - \frac{1}{\log R}} \right) \leq (\log R + O(1))^C.$$
Proof. It suffices to prove this lemma in the case of \( w = 1 \). By the generalized binomial theorem, we have
\[
1 + C \cdot p^{-1 - \frac{1}{\log R}} \leq \left( 1 - p^{-1 - \frac{1}{\log R}} \right)^{-C}.
\]
Hence
\[
\prod_{p \in P} \left( 1 + C \cdot p^{-1 - \frac{1}{\log R}} \right) \leq \prod_{p \in P} \left( 1 - p^{-1 - \frac{1}{\log R}} \right)^{-C} = \zeta \left( 1 + \frac{1}{\log R} \right)^C.
\]
The Riemann zeta function \( \zeta \) satisfies that for every \( s > 1 \), \( |\zeta(s) - \frac{1}{1-s}| \leq 1 \) holds. Since \( \zeta \left( 1 + \frac{1}{\log R} \right) = \log R + O(1) \), the desired result follows. \( \square \)

We will prove Proposition 6.14 by combination of the above lemmas.

Proof of Proposition 6.14. We apply Lemma 6.17 to \( \prod_{j \in [m]} \chi(\log N(a_j)) \chi(\log N(b_j)) \) in (6.10), and then (6.10) is decomposed into the main term represented by integral and the following error term:
\[
O_{A,\chi,m} \left( (\log R)^{2m-A} \sum_{(a_j, b_j) \in [m]} \left( \prod_{j \in [m]} N(a_j)^{-\frac{1}{\log R}} N(b_j)^{-\frac{1}{\log R}} \right) e \left( (a_j, b_j)_{j \in [m]} \right) \right).
\]
Since \( E \) converges absolutely and uniformly by Lemma 6.18, we can interchange integral and the series in the main term. Then it turns out that the main term is equal to (6.17). Next we estimate the error term. Recall that \( \tilde{E} \) and \( \tilde{E}_p \) are defined in the proof of Lemma 6.18, and \( \tilde{E} = \prod_{p \in P > w} \tilde{E}_p \) is estimated in (6.25). We see that the series in big-O of the error term is equal to \( \tilde{E} \), and hence apply Lemma 6.19 to \( \tilde{E} \). Then the error term is rewritten as
\[
O_{A,\chi,m} \left( (\log R)^{2m-A} (\log R + O(1))^O_{m,n}(1) \right). \tag{6.26}
\]
By replacing \( A \) with some sufficiently large \( A \) depending on \( m \) and \( n \), we may rewrite this error as \( O_{A,\chi,m,n}(\log R)^{-A} \).

6.6 Calculation of the main term

In the above, we first have replaced the box \( B \), where the expectation is estimated, with \( (\mathbb{Z}/D\mathbb{Z})^t \) for each \( (a_j, b_j)_{j \in [m]} \). Secondly we have obtained an integral representation of \( \chi \), and replaced the domain \( \mathbb{R}^{2m} \) of integration with \( I^{2m} \). Thirdly we have calculated the main term and controlled the error terms, which have been accumulated up to Proposition 6.14.

In this section, we continue calculation of the main term, which is written as (6.27) by using (6.24)

Proposition 6.20. Assume Setting 6.13. Let \( A \) be a positive real number. Then (6.10) equals
\[
(\log R)^{2m} \int_{I^{2m}} d\xi d\eta \left[ \left( \prod_{j \in [m]} \tilde{\chi}(\xi_j) \tilde{\chi}(\eta_j) \right) \cdot \prod_{p \in P > w} E_p \right]. \tag{6.27}
\]
with an additive error term $O_{A,\chi,m,n}((\log R)^{-A})$.

In this subsection, we assume the following setting, which finalizes the choice of the three parameters in Theorem 6.2.

**Setting 6.21.** Assume the setting in Theorem 6.2, and fix $\chi$ as in Definition 6.1. Set the positive real numbers $w_0, R_0$ and $F_0$ as in Theorem 6.2 in the following manner:

1. $w_0 = w_0((\psi_j)_{j\in[m]}):=\max\{c_14^{mn}, w'_0, w''_0\}$, where $c_1$ is a sufficiently large constant. Both $w'_0$ and $w''_0$ are given in Setting 6.10.

2. $R_0 = R_0(m, K) := c_K e^{m^2}$, where $c_K$ is a sufficiently large constant depending only on $K$.

3. $F_0 = F_0(m, n) := c_2(\min\{R_0, w_0\})^{-1}$, where $c_2$ is a sufficiently small constant.

The choices of $c_1$, $c_2$ and $c_K$ will become clear in the course of this section. In this paper, since the exact values of them are not of importance in the rest, we do not specify them explicitly.

Recall that two parameters $w$ and $R$ are positive real numbers such that $w \geq w_0$, $R \geq R_0$ and $\log w \leq F_0 \cdot \sqrt{\log R}$. In addition we continue to use the symbols as in Subsection 6.5.

Let $I = I(R) := [-\sqrt{\log R}, +\sqrt{\log R}]$, and $\xi_j$ and $\eta_j$ be variables of integration. For short, write $d\xi = d\xi_1 \cdots d\xi_m$ and $d\eta = d\eta_1 \cdots d\eta_m$. Let $z_j = \frac{1 + \xi_j \sqrt{-1}}{\log R}$ and $w_j = \frac{1 + \eta_j \sqrt{-1}}{\log R}$. The function $\widehat{\chi}$ is the inverse Fourier transform of the function $x \mapsto e^{x} \chi(x)$. For each prime number $p \in \mathcal{P}$, $E_p = E_p((\xi_j, \eta_j)_{j\in[m]}; R)$ is defined in (6.22). In order to calculate (6.27), we fix $(\xi_j, \eta_j)_{j\in[m]} \in I^{2m}$, and for each prime number $p \in \mathcal{P}$, define $E'_p = E'_p((\xi_j, \eta_j)_{j\in[m]}; R)$ by

$$E'_p := \prod_{j\in[m]} \prod_{p \in \operatorname{Spec}(O_K)(p)} \frac{(1 - N(p)^{-w_j})}{(1 - N(p)^{1-w_j})}.$$ 

We first show estimates for $E_p$ and $E'_p$ and their relation. The following lemma provides elementary estimates.

**Lemma 6.22.** The following estimates hold.

1. For all complex number $\varepsilon$ with $|\varepsilon| \leq 1/2$, we have
   \[
   \log(1 + \varepsilon) = O(|\varepsilon|),
   \]
   \[
   \frac{1}{1 - \varepsilon} = 1 + \varepsilon + O(|\varepsilon|^2) = 1 + O(|\varepsilon|).
   \]

2. For all complex number $\varepsilon$ with $|\varepsilon| \leq 1$, we have
   \[
   e^\varepsilon = 1 + O(|\varepsilon|).
   \]

3. For all positive integer $k$ and all complex numbers $\varepsilon_1, \ldots, \varepsilon_k$ with $|\varepsilon_1|, \ldots, |\varepsilon_k| \leq 1/k$, we have
   \[
   \prod_{i\in[k]} (1 + \varepsilon_i) = 1 + \sum_{i\in[k]} \varepsilon_i + O\left(k^2 \cdot \max_{i\in[k]} |\varepsilon_i|^2\right) = 1 + O\left(k \cdot \max_{i\in[k]} |\varepsilon_i|\right).
   \]
Lemma 6.23. For every prime number $p$ greater than $w$, we have

$$E_p E_p' = 1 + O(4^{mn}/p^2).$$

Proof. By Lemma 6.22 (1), we obtain that

$$1/E'_p = \prod_{j \in [m]} \prod_{p \in \Spec(O_K)(p)} \frac{(1 - N(p)^{-1-z_j-w_j})}{(1 - N(p)^{-1-z_j})(1 - N(p)^{-1-w_j})} = \prod_{j \in [m]} \prod_{p \in \Spec(O_K)(p)} (1 + N(p)^{-1-z_j} + O(1/p^2)) \cdot (1 + N(p)^{-1-w_j} + O(1/p^2)) (1 - N(p)^{-1-z_j-w_j}).$$

Since the number of prime $p$-ideals is at most $n = [K : \mathbb{Q}]$ by Lemma 3.15, the product above consists of at most $3mn$ factors. In addition, the difference between 1 and each factor is at most $2/p$. Hence, in the case of $p > w$ ($\geq 6mn$), we may apply Lemma 6.22 (3) to the product, and then obtain that

$$1/E'_p = 1 + \Sigma_p ((\xi_j, \eta_j)_{k \in [m]}; R) + O(m^2 n^2/p^2).$$

Recall that $\Sigma_p = \Sigma_p ((\xi_j, \eta_j)_{k \in [m]}; R)$ is given by

$$\Sigma_p = \sum_{j \in [m]} \sum_{p \in \Spec(O_K)(p)} (N(p)^{-1-z_j} + N(p)^{-1-w_j} - N(p)^{-1-z_j-w_j}) .$$

Note that $|\Sigma_p| \leq 3mn/p$ holds. Recall from (6.23) in Lemma 6.18 that

$$E_p = 1 - \Sigma_p ((\xi_j, \eta_j)_{k \in [m]}; R) + O(4^{mn}/p^2).$$

We set

$$\varepsilon_1 = 1/E'_p - 1 = \Sigma_p + O(m^2 n^2/p^2), \quad \varepsilon_2 = E_p - 1 = -\Sigma_p + O(4^{mn}/p^2).$$

Then, $|\varepsilon_i| \leq (3mn + 1)/p \leq 1/2$ follows from $p > w$ ($\geq c_14^{mn}$), provided that the universal constant $c_1$ is big enough. Hence Lemma 6.22 (3) can be applied to (6.28), and then the desired result follows.
Lemma 6.24. We have

\[
\prod_{p \in \mathcal{P}_{>w}} E_p = \left(1 + O \left( \frac{4mn}{w \log w} \right) \right) \cdot \prod_{p \in \mathcal{P}_{>w}} E'_p.
\]

Proof. Take \( c_1 \) to be sufficiently large. By Lemma 6.23 we have

\[
\prod_{p \in \mathcal{P}_{>w}} E_p = \prod_{p \in \mathcal{P}_{>w}} \left(1 + O \left( \frac{4mn}{p^2} \right) \right) \cdot \prod_{p \in \mathcal{P}_{>w}} E'_p.
\]

In the case of \( p > w \) (\( \geq c_1 2^{mn} \)), all \( O \left( \frac{4mn}{p^2} \right) \) in the above equality is bounded by \( 1/2 \).

Hence, by Lemma 6.22 (1) and Lemma 3.24 we have that

\[
\log \left( \prod_{p \in \mathcal{P}_{>w}} E_p \right) - \log \left( \prod_{p \in \mathcal{P}_{>w}} E'_p \right) = \log \left( \prod_{p \in \mathcal{P}_{>w}} \left(1 + O \left( \frac{4mn}{p^2} \right) \right) \right)
= \sum_{p \in \mathcal{P}_{>w}} \log \left(1 + O \left( \frac{4mn}{p^2} \right) \right)
= \sum_{p \in \mathcal{P}_{>w}} O \left( \frac{4mn}{p^2} \right) = O \left( \frac{4mn}{w \log w} \right).
\]

Since \( w \log w \geq c_1 4^{mn} \), the absolute value of the value of the equalities above is at most 1.

Hence by Lemma 6.22 (2), we derive the desired estimate

\[
\frac{\prod_{p \in \mathcal{P}_{>w}} E_p}{\prod_{p \in \mathcal{P}_{>w}} E'_p} = e^{O \left( \frac{4mn}{w \log w} \right)} = 1 + O \left( \frac{4mn}{w \log w} \right),
\]
as desired.

From this lemma, the calculation of \( \prod_{p \in \mathcal{P}_{>w}} E_p \) is reduced to that of \( \prod_{p \in \mathcal{P}_{>w}} E'_p \). Thus we continue to calculate the numerator and the denominator of

\[
\prod_{p \in \mathcal{P}_{>w}} E'_p = \frac{\prod_{p \in \mathcal{P}_{>w}} E'_p}{\prod_{p \in \mathcal{P}_{\leq w}} E'_p}.
\]

Lemma 6.25. We have

\[
\prod_{p \in \mathcal{P}} E'_p = \prod_{j \in [m]} \frac{\zeta_K(1 + z_j + w_j)}{\zeta_K(1 + z_j) \zeta_K(1 + w_j)} = \left(1 + O_K \left( \frac{m}{\sqrt{\log R}} \right) \right) \cdot \prod_{j \in [m]} \frac{1}{\kappa} \cdot \frac{z_j w_j}{z_j + w_j}.
\]

Proof. Take \( c_K \) to be sufficiently large depending on \( K \). Recall that the definition of \( E'_p \) and the Euler product of Dedekind zeta function (Proposition 3.18). We see that

\[
\prod_{p \in \mathcal{P}} E'_p = \prod_{j \in [m]} \frac{\zeta_K(1 + z_j + w_j)}{\zeta_K(1 + z_j) \zeta_K(1 + w_j)}.
\]
Let $j$ be an arbitrary integer in $[m]$. Since $\xi_j, \eta_j \in I = [-\sqrt{\log R}, \sqrt{\log R}]_R$, we have

$$|z_j|, |w_j| \leq \frac{\sqrt{1 + \log R}}{\log R} \leq \sqrt{\frac{2}{\log R}}.$$  

The class number formula (Theorem 3.19) implies that, for every complex number $\varepsilon$ whose absolute value is bounded by a constant depending only on $K$,

$$\zeta_K(1 + \varepsilon) = \frac{\kappa}{\varepsilon} (1 + O_K(\varepsilon)). \quad (6.29)$$

Note that $R \geq R_0 (\geq c_K)$. Lemma 6.22 (1) and (6.29) imply that for $\varepsilon = z_j$ or $w_j$,

$$\frac{1}{\zeta_K(1 + \varepsilon)} = \frac{\varepsilon}{\kappa} \frac{1}{1 + O_K(1/\sqrt{\log R})} = \frac{\varepsilon}{\kappa} \left(1 + O_K(1/\sqrt{\log R})\right).$$

Similarly, it follows from (6.29) that

$$\zeta_K(1 + z_j + w_j) = \frac{\kappa}{z_j + w_k} \left(1 + O_K(1/\sqrt{\log R})\right).$$

Hence applying Lemma 6.22 (3) to the product of these three functions, we obtain that

$$\frac{\zeta_K(1 + z_j + w_j)}{\zeta_K(1 + z_j)\zeta_K(1 + w_j)} = \frac{1}{\kappa} \cdot \frac{z_jw_j}{z_j + w_j} \cdot \left(1 + O_K(1/\sqrt{\log R})\right).$$

These estimates for all $j \in [m]$ together with Lemma 6.22 (3) provide the desired estimate. \qed

**Lemma 6.26.** We have

$$\prod_{p \in \mathcal{P}, \leq w} E'_p = \left(1 + O\left(\frac{mn^2 \log w}{\sqrt{\log R}}\right)\right) \cdot \left(\frac{\varphi_K(W)}{N(W)}\right)^m.$$

**Proof.** Take $c_2$ to be sufficiently small. Let $p$ be a prime number at most $w$, and $\mathfrak{p} \in \operatorname{Spec}(O_K)(p)$ a prime $p$-ideal. Let $j \in [m]$, and suppose that $\varepsilon = z_j$ or $w_j$. Then note that $\varepsilon = O(1/\sqrt{\log R})$, $N(p) \leq p^n$ and $\log w/\sqrt{\log R} \leq F_0 (\leq c_2^{n^{-1}})$. By Lemma 6.22 (2), we see that

$$1 - N(p)^{-1-\varepsilon} = 1 - N(p)^{-1} \exp(-\varepsilon \log N(p)) = 1 - N(p)^{-1} \left(1 + O\left(\frac{\log N(p)}{\sqrt{\log R}}\right)\right) = \left(1 - N(p)^{-1}\right) \left(1 + O\left(\frac{\log N(p)}{N(p)\sqrt{\log R}}\right)\right) = \left(1 - N(p)^{-1}\right) \left(1 + O\left(\frac{n \log p}{p \sqrt{\log R}}\right)\right).$$
Similarly, we have
\[
\frac{1}{1 - N(p)^{-1}z_j - w_j} = \frac{1}{1 - N(p)^{-1}} \left(1 + O\left(\frac{n \log p}{p\sqrt{\log R}}\right)\right).
\]
Since \(\log w/\sqrt{\log R} \leq F_0 = c_2(mn^2)^{-1}\), the equality above together with Lemma 6.22 (3) implies that
\[
E'_p = \prod_{j \in [m]} \prod_{p \in \Spec(O_K) \mid \{p\}} \frac{(1 - N(p)^{-1}z_j)(1 - N(p)^{-1}w_j)}{(1 - N(p)^{-1}z_j - w_j)} = \left(1 + O\left(\frac{mn^2 \log p}{p\sqrt{\log R}}\right)\right) \cdot \prod_{j \in [m]} \prod_{p \in \Spec(O_K) \mid \{p\}} (1 - N(p)^{-1}).
\]
Recall that the set of prime divisors of \(W\) equals \(P \leq w\). It follows from Proposition 3.9 that
\[
\prod_{p \in P \leq w} \prod_{p \in \Spec(O_K) \mid \{p\}} (1 - N(p)^{-1}) = \frac{\varphi_K(W)}{N(W)}.
\]
Therefore, we have
\[
\prod_{p \in P \leq w} E'_p = \left(\prod_{p \in P \leq w} \left(1 + O\left(\frac{mn^2 \log p}{p\sqrt{\log R}}\right)\right)\right) \cdot \left(\frac{\varphi_K(W)}{N(W)}\right)^m.
\]
Below we estimate the product over \(P \leq w\) on the right-hand side of this equality under the assumption \(\log w/\sqrt{\log R} \leq F_0 = c_2(mn^2)^{-1}\). By Lemma 6.22 (1) and Proposition 3.25 we have
\[
\log \left(\prod_{p \in P \leq w} E'_p\right) - \log \left(\frac{\varphi_K(W)}{N(W)}\right)^m = \log \left(\prod_{p \in P \leq w} \left(1 + O\left(\frac{mn^2 \log p}{p\sqrt{\log R}}\right)\right)\right)
= \sum_{p \in P \leq w} \log \left(1 + O\left(\frac{mn^2 \log p}{p\sqrt{\log R}}\right)\right)
= \sum_{p \in P \leq w} O\left(\frac{mn^2 \log p}{p\sqrt{\log R}}\right) = O\left(\frac{mn^2 \log w}{\sqrt{\log R}}\right).
\]
This together with Lemma 6.22 (2) implies that
\[
\frac{\prod_{p \in P \leq w} E'_p}{\left(\frac{\varphi_K(W)}{N(W)}\right)^m} = e \left(\frac{mn^2 \log w}{\sqrt{\log R}}\right) = 1 + O\left(\frac{mn^2 \log w}{\sqrt{\log R}}\right),
\]
and this completes the proof.
We combine Lemmas 6.24, 6.25 and 6.26 and use Lemma 6.22 under the assumptions $w \geq w_0$, $R \geq R_0$ and $\log w \leq F_0 \cdot \sqrt{\log R}$. Then we obtain that
\[
\prod_{p \in \mathcal{P} > w} E_p = \left(1 + O \left(\frac{4mn}{w \log w}\right) + O_K \left(\frac{m \log w}{\sqrt{\log R}}\right)\right) \cdot \left(\frac{W_n}{\varphi_K(W) \cdot K}\right)^m \prod_{j \in [m]} \frac{z_j w_j}{z_j + w_j}.
\]
This concludes an estimate for every fixed $(\xi_j, \eta_j)_{j \in [m]} \in I^{2m}$. Now we integrate over $(\xi_j, \eta_j)_{j \in [m]} \in I^{2m}$. Then the main term of Proposition 6.20 provides the following result.

**Proposition 6.27.** The main term (6.27) is equal to
\[
(\log R)^{2m} \left(\frac{W_n}{\varphi_K(W) \cdot K}\right)^m \int_{I^{2m}} d\xi d\eta \left[\prod_{j \in [m]} \hat{\chi}(\xi_j) \hat{\chi}(\eta_j) \frac{z_j w_j}{z_j + w_j}\right] \tag{6.30}
\]
with a multiplicative error $1 + O \left(\frac{4mn}{w \log w}\right) + O_K \left(\frac{m \log w}{\sqrt{\log R}}\right)$.

Finally, in order to calculate the integral in the above proposition, we switch the domain of integration from $I^{2m}$ back to $\mathbb{R}^{2m}$.

**Proposition 6.28.** For every positive real number $A$, we have
\[
\int_{I^{2m}} d\xi d\eta \left[\prod_{j \in [m]} \hat{\chi}(\xi_j) \hat{\chi}(\eta_j) \frac{z_j w_j}{z_j + w_j}\right] = \int_{\mathbb{R}^{2m}} d\xi d\eta \left[\prod_{j \in [m]} \hat{\chi}(\xi_j) \hat{\chi}(\eta_j) \frac{z_j w_j}{z_j + w_j}\right] + O_{A,\chi,m} \left((\log R)^{-m-A}\right).
\]

**Proof.** We decompose the integral as $\int_{I^{2m}} = \int_{\mathbb{R}^{2m}} - \int_{\mathbb{R}^{2m} \setminus I^{2m}}$, and estimate $\int_{\mathbb{R}^{2m} \setminus I^{2m}}$. For every $(\xi_j, \eta_j)_{j \in [m]} \in \mathbb{R}^{2m}$, we have
\[
\frac{z_j w_j}{z_j + w_j} = O \left( (\log R)^{-1} \left(1 + |\xi_j|\right) \left(1 + |\eta_j|\right) \right).
\]

By Lemma 6.15, for all $B \geq 0$, it follows that
\[
\prod_{j \in [m]} \hat{\chi}(\xi_j) \hat{\chi}(\eta_j) \frac{z_j w_j}{z_j + w_j} = O_{B,\chi} \left((\log R)^{-m} \prod_{j \in [m]} \left(1 + |\xi_j|\right)^{-B} \left(1 + |\eta_j|\right)^{-B}\right).
\]
We let $B = 2A + 1$ and note that the following:
\[
\int_{\mathbb{R}} (1 + \xi)^{-B} d\xi = O_A(1) \quad \text{and} \quad \int_{\mathbb{R} \setminus I} (1 + \xi)^{-B} d\xi = O_A \left( (\log R)^{-A}\right).
\]
In an argument similar to that of the proof of Lemma 6.17, we see that
\[
\int_{\mathbb{R}^2} d\xi d\eta \left[ \prod_{j \in [m]} \hat{\chi}(\xi_j) \hat{\chi}(\eta_j) \frac{z_j w_j}{z_j + w_j} \right] = O_{A,\chi,m} \left( (\log R)^{-m-A} \right).
\]
This is the desired result.

We write down a proof of the following lemma for the convenience of the reader.

**Lemma 6.29** ([CFZ14, (38)] or [Tao06, p.170]). We have
\[
\int_{\mathbb{R}^2} d\xi d\eta \left[ \hat{\chi}(\xi) \hat{\chi}(\eta) \frac{(1 + \xi \sqrt{-1})(1 + \eta \sqrt{-1})}{2 + (\xi + \eta) \sqrt{-1}} \right] = c_\chi.
\]

**Proof.** Since
\[
\frac{1}{2 + (\xi + \eta) \sqrt{-1}} = \int_0^{\infty} e^{-x(1+\xi \sqrt{-1})} e^{-x(1+\eta \sqrt{-1})} dx,
\]
the left-hand side of (6.31) equals
\[
\int_0^{\infty} \left( \int_{\mathbb{R}} \hat{\chi}(\xi)(1 + \xi \sqrt{-1}) e^{-x(1+\xi \sqrt{-1})} d\xi \right)^2 dx.
\]

Then the integral over $\xi \in \mathbb{R}$ is equal to $-\chi'(x)$ by the integral representation (6.14) of $\chi$. Since $c_\chi$ is defined in (6.2) as $c_\chi = \int_0^{\infty} \chi'(x)^2 dx$, it ends the proof.

Now we are ready to complete the proof of Theorem 6.2.

**Proof of Theorem 6.2**. First, note that by Lemma 6.29, the main term is calculated as follows
\[
(\log R)^{2m} \left( \frac{W^n}{\varphi_K(W) \cdot \kappa} \right)^m \int_{\mathbb{R}^2} d\xi d\eta \left[ \prod_{j \in [m]} \hat{\chi}(\xi_j) \hat{\chi}(\eta_j) \frac{z_j w_j}{z_j + w_j} \right] = \left( \frac{W^n c_\chi \log R}{\varphi_K(W) \cdot \kappa} \right)^m.
\]

Combining Propositions 6.4, 6.6, 6.20, 6.27, 6.28 and (6.32), we have that for all $A > 0$,
\[
\mathbb{E} \left( \prod_{j \in [m]} (\Lambda_{R,\chi} \circ \theta_j)^2 \bigg| \mathcal{B} \right) = \left( 1 + O \left( \frac{4^{mn}}{w \log w} \right) + O_K \left( \frac{m \log w}{\sqrt{\log R}} \right) \right) \cdot (1 + O_{A,\chi,m} ((\log R)^{-A})) \left( \frac{W^n c_\chi \log R}{\varphi_K(W) \cdot \kappa} \right)^m
\]
\[
+ O_{A,\chi,m,n} ((\log R)^{-A}) + O_{t,K} \left( \frac{(\log R)^{2m}}{R} \right).
\]
We write the first, second and third term of the right-hand side of the equality above, respectively, as $\mathcal{E}_1$, $\mathcal{E}_2$ and $\mathcal{E}_3$. Set $A = 1/2$. Since $w \geq w_0$ and $\log w \leq F_0 \cdot \sqrt{\log R}$, we obtain that

$$\mathcal{E}_1 \cdot \left( \frac{W^n c_\chi \log R}{\varphi_K(W) \cdot \kappa} \right)^{-m} = \left( 1 + O \left( \frac{4^{m n}}{w \log w} \right) + O_K \left( \frac{m \log w}{\sqrt{\log R}} \right) \right) \cdot \left( 1 + O_{\chi,m} \left( (\log R)^{-1/2} \right) \right)$$

$$= 1 + O \left( \frac{4^{m n}}{w \log w} \right) + O_{\chi,m,K} \left( \frac{\log w}{\sqrt{\log R}} \right).$$

Since $R \geq R_0 (= c_K e^{m^2})$ and $\varphi_K(W) \leq W^n$, we in addition have that

$$\mathcal{E}_2 + \mathcal{E}_3 = O_{\chi,m,n} \left( (\log R)^{-1/2} \right) + O_{t,K} \left( \frac{(\log R)^{2m}}{R} \right) = O_{\chi,m,t,K} \left( \frac{\log w}{\sqrt{\log R}} \right) \cdot \left( \frac{W^n c_\chi \log R}{\varphi_K(W) \cdot \kappa} \right)^m.$$

Therefore, the proof is completed.

We remark that, by replacing the definition of $I = [-\sqrt{\log R}, \sqrt{\log R}]_R$ with $[-(\log R)^\varepsilon, (\log R)^\varepsilon]_R$, $1/\sqrt{\log R}$ in a big-$O$ term in (6.4) is improved to $1/(\log R)^{1-\varepsilon}$.

In the remaining part of this subsection, we summarize differences from the previous work on Goldston–Yıldırım type estimates in this research field.

**Remark 6.30.** It may be possible to formulate another variant of $(R, \chi)$-functions, which also avoids taking sums of terms for infinitely many times, as follows

$$\log R \cdot \sum_{\beta \mid \alpha}^{'} \mu(\beta) \chi \left( \frac{\log N(\beta)}{\log R} \right).$$

Here, the sum $\sum^{'}$ means that $\beta$ runs over the subset of a complete list of representatives of $(\mathcal{O}_K \setminus \{0\})/\mathcal{O}_K^\times$ consisting of elements which divide $\alpha$. This alternative solution bypasses considering ideals. Nevertheless, our present approach has a great technical advantage in the following sense. If we employ the above variant of the $(R, \chi)$-function, then a partial Euler product shows up in place of the Dedekind zeta function, in which $p$ runs over all principal prime ideals. In [KMTB15] Lemma 8, such partial Euler products were studied; around $s = 1$, the partial Euler product above is a multi-valued complex function which is proportional to $(s - 1)^{-1/h}$. For this reason, treatments of this variant may be more delicate than those of our $(R, \chi)$-function.

**Remark 6.31.** Assumption [6.3] in Theorem 6.2 is stronger than the corresponding assumption in [Tao06] Proposition 9.1]. However, this condition is always fulfilled in our applications. Furthermore, one of the great advantages of Theorem 6.2 is that it applies to all number fields $K$, including those where $K/\mathbb{Q}$ is not Galois. In Theorem 6.2, we have in addition assumed that for all $j \in [m]$, $\psi_j$ has a finite cokernel.

**Remark 6.32.** The condition `$#I_i \geq R^{4m+1}$' in Theorem 6.2 corresponds to `$#I_i \geq R^{5m}$' in [Tao06] Proposition 9.1], and to `$#I_i \geq R^{10m}$' in [CFZ14] Proposition 8.3]. Here note that the convention in [Tao06] is slightly different from ours; Tao bounded ideal norms from above by $R^2$, not by $R$. In the present paper, we do not optimize the order of this bound on $#I_i$; the proof of Theorem 6.2 remains to work, provided that $#I_i \geq R^{4m} \cdot (\log R)^{2m} \cdot \sqrt{\log R} \cdot \log w$. 
6.7 Goldston–Yıldırım type asymptotic formula for ideals

In this subsection, we present a generalization of Theorem 6.2 to the setting of ideals. We may consider a further generalization to that of fractional ideals in a similar manner, but we state for ideals for simplicity. The result, Theorem 6.33, will be employed in Section 10 in order to establish Theorem C. The reader who is interested in the proofs of results before Theorem C may skip this subsection.

Let \( a \) be a non-zero ideal of \( \mathcal{O}_K \). Then \( a^{-1} = \{ x \in K : xa \subseteq \mathcal{O}_K \} \) is a non-zero fractional ideal; recall the discussion before Theorem 3.3. Let \( \chi \) be a function as in Theorem 6.2 and let \( R \geq 1 \). From the \((R, \chi)\)-von Mangoldt function \( \Lambda_{R, \chi}^a : \text{Ideals}_K \cup \{(0)\} \to \mathbb{R} \), we construct a new function \( \Lambda_{R, \chi}^a : a \to \mathbb{R} \) in the following manner:

\[
\Lambda_{R, \chi}^a(\alpha) := \Lambda_{R, \chi}(\alpha a^{-1}) \quad \text{for all } \alpha \in a. \tag{6.33}
\]

Here, note that \( \alpha a^{-1} \in \text{Ideals}_K \cup \{(0)\} \) holds true. Also, note that unless \( a \) is principal or \( \alpha = 0 \), the ideal \( \alpha a^{-1} \) is not principal.

**Theorem 6.33** (Goldston–Yıldırım type asymptotic formula for ideals). Let \( K \) be a number field of degree \( n \). Let \( a \in \text{Ideals}_K \). Let \( m \) and \( t \) be positive integers, and \( \psi_1, \ldots, \psi_m : \mathbb{Z}^t \to a \) be \( \mathbb{Z} \)-module homomorphisms. Let \( w \) be a positive real number, and \( W \) a positive integer of which the set of prime divisors is \( \mathcal{P}_{\leq w} \). Let \( b_1, \ldots, b_m \) be elements in \( a \) such that

\[
b_i \mathcal{O}_K + Wa = a \quad \text{for all } i \in [m]. \tag{6.34}
\]

Define affine transformations \( \theta_1, \ldots, \theta_m : \mathbb{Z}^t \to a \) as

\[
\theta_j(x) := \text{Aff}_{W, b_j}(\psi_j(x)) = W \psi_j(x) + b_j.
\]

Let \( R \) be a positive real number, and \( I_1, \ldots, I_t \subseteq \mathbb{Z} \) intervals of length at least \( R^{4m+1} \). Set \( \mathcal{B} := I_1 \times \cdots \times I_t \subseteq \mathbb{Z}^t \). Fix a \( C^\infty \)-function \( \chi : \mathbb{R} \to [0, 1]_\mathbb{R} \) which satisfies \( \chi(0) = 1 \) and \( \text{supp}(\chi) \subseteq [-1, 1]_\mathbb{R} \). Assume \( [6.3] \). Then there exist positive real numbers \( R_0 = R_0(m, K) \), \( F_0 = F_0(m, n) \) and \( w_0 = w_0((\psi_j)_{j \in [m]}) \) such that if \( R \geq R_0 \), \( w \geq w_0 \) and \( w \leq F_0 \cdot \sqrt{\log R} \), then

\[
\mathbb{E}(\Lambda_{R, \chi}^a(\theta_1(x))^2 \cdots \Lambda_{R, \chi}^a(\theta_m(x))^2 \mid x \in \mathcal{B})
\]

\[
= \left( 1 + O_{m, n} \left( \frac{1}{w \log w} \right) + O_{\chi, m, t, K} \left( \frac{\log w}{\sqrt{\log R}} \right) \right) \cdot \left( \frac{W^n \chi \log R}{\varphi_K(W) \cdot \kappa} \right)^m \tag{6.35}
\]

holds true. In particular, the error terms \( O_{m, n} \left( \frac{1}{w \log w} \right) \) and \( O_{\chi, m, t, K} \left( \frac{\log w}{\sqrt{\log R}} \right) \) are bounded uniformly on \( W \) and \( (b_j)_{j \in [m]} \).

We remark that condition \( (6.34) \) is the counterpart of the coprime condition imposed on \( b_1, \ldots, b_m \) in Theorem 6.2; see Section 8 more specifically, Lemma 8.4, for more details.

In the rest of this subsection, we prove Theorem 6.33 under the setting of Theorem 6.33.
Proposition 6.34. Expectation (6.35) is equal to

\[(\log R)^{2m} \sum_{(a_j, b_j) \in [m] \cap \text{Ideals}_K^{2m}} \Pi_{R, \chi} \left( (a_j, b_j)_{j \in [m]} \right) \cdot \mathbb{E} \left( \prod_{j \in [m]} \left( 1_{a_j \cap b_j} \circ \theta_j \right) \bigg| \mathcal{B} \right). \tag{6.36} \]

where

\[\Pi_{R, \chi} \left( (a_j, b_j)_{j \in [m]} \right) = \prod_{j \in [m]} \mu(a_j) \mu(b_j) \chi \left( \frac{\log N(a_j)}{\log R} \right) \chi \left( \frac{\log N(b_j)}{\log R} \right).\]

Proof. Let \(x \in \mathcal{B}.\) We have that

\[(\log R)^{-2m} \prod_{j \in [m]} \Lambda_{R, \chi}^{\alpha} (\theta_j(x))^2 = \sum_{(a_j, b_j) \in [m] \cap \text{Ideals}_K^{2m}} \prod_{j \in [m]} \mu(a_j) \mu(b_j) \chi \left( \frac{\log N(a_j)}{\log R} \right) \chi \left( \frac{\log N(b_j)}{\log R} \right) \]

\[= \sum_{(a_j, b_j) \in [m] \cap \text{Ideals}_K^{2m}} \left( \prod_{j \in [m]} 1_{a_j \cap b_j} \left( \theta_j(x) \right) \right) \cdot \Pi_{R, \chi} \left( (a_j, b_j)_{j \in [m]} \right).\]

Only the characteristic functions \( \prod_{j \in [m]} 1_{a_j \cap b_j} \left( \theta_j(x) \right) \) depend on \(x \in \mathcal{B},\) and hence the desired result holds. \(\square\)

The following lemma is verified in the same way as the proof of Lemma 6.35. Indeed, observe that for every \(x \in (\mathbb{Z}/D\mathbb{Z})^t,\) the value \(1_{a \cap b}(\theta_j(x)) \in \{0, 1\}\) is well-defined.

Lemma 6.35. Let \((a_j, b_j)_{j \in [m]} \in \text{Ideals}_K^{2m}.\) Let \(D = D ((a_j, b_j)_{j \in [m]}\) be the positive integer defined in (6.7). If \(N(a_j), N(b_j) \leq R\) holds for every \(j \in [m],\) then the following hold true:

\[\mathbb{E} \left( \prod_{j \in [m]} \left( 1_{a_j \cap b_j} \circ \theta_j \right) \bigg| \mathcal{B} \right) = \mathbb{E} \left( \prod_{j \in [m]} \left( 1_{a_j \cap b_j} \circ \theta_j \right) \bigg| (\mathbb{Z}/D\mathbb{Z})^t \right) + O_1(R^{-2m-1}).\]

As in (6.9), we write for short the following expectation

\[e^a \left( (a_j, b_j)_{j \in [m]} \right) = e^a \left( (a_j, b_j)_{j \in [m]}; (\theta_j)_{j \in [m]} \right) := \mathbb{E} \left( \prod_{j \in [m]} \left( 1_{a_j \cap b_j} \circ \theta_j \right) \bigg| (\mathbb{Z}/D\mathbb{Z})^t \right), \tag{6.37} \]

which depends on \((\theta_j)_{j \in [m]}, (a_j, b_j)_{j \in [m]}\) and \(a.\) Here a positive integer \(D = D ((a_j, b_j)_{j \in [m]}\) is taken as in Lemma 6.35. Then we derive the following proposition in the same way as the proof of Proposition 6.6.
Proposition 6.36. **Expectation** (6.36) equals

\[(\log R)^{2m} \sum_{(a_j, b_j) \in [m]} \Pi_{R, X} \left( (a_j, b_j)_{j \in [m]} \right) \cdot e^{a} \left( (a_j, b_j)_{j \in [m]} \right) \tag{6.38} \]

with an additive error term \(O_{t, K} \left( \frac{(\log R)^{2m}}{R} \right) \).

Recall that (6.4) and (6.35) equal (6.10) and (6.38), respectively. In addition, the properties of \(e\) required in the proof of Theorem 6.2 are the multiplicativity of \(e\) as in Lemma 6.8 and the estimates as in Lemma 6.12 for \(e\). Hence, in order to show Theorem 6.33, it suffices to prove that \(e^{a}\) has the same properties of \(e\). Namely, we show Lemmas 6.37 and 6.40 below.

**Lemma 6.37.** Let \((a_j, b_j)_{j \in [m]}\) be a tuple of arbitrary nonzero ideals of \(O_K\). Then Lemma 6.8 with \(e\) replace by \(e^{a}\) holds. Namely, we have that

\[e^{a} \left( (a_j, b_j)_{j \in [m]} \right) = \prod_{p \in P} e^{a} \left( (a_j^{(p)}, b_j^{(p)})_{j \in [m]} \right). \tag{6.39} \]

**Proof.** We write \(c_j := a_j \cap b_j\) for short, and then we have \(DZ = \mathbb{Z} \cap \bigcap_{j \in [m]} c_j\). Note that \(c_j^{(p)} = a_j^{(p)} \cap b_j^{(p)}\) and \(D^{(p)}Z = \mathbb{Z} \cap \bigcap_{j \in [m]} c_j^{(p)}\). We consider the \(\mathbb{Z}\)-module homomorphisms and affine transformations \(\overline{\psi}_j, \overline{\theta}_j : (\mathbb{Z}/DZ)^t \rightarrow \mathbb{Z}/ac_j\) induced by \(\psi_j\) and \(\theta_j\), respectively. Let

\[\overline{\psi}, \overline{\theta} : (\mathbb{Z}/DZ)^t \rightarrow \prod_{j \in [m]} a/ac_j\]

be the two maps defined by \(\overline{\psi}(x) = (\overline{\psi}_1(x), \ldots, \overline{\psi}_m(x))\) and \(\overline{\theta}(x) = (\overline{\theta}_1(x), \ldots, \overline{\theta}_m(x))\). Then we see that

\[e^{a} \left( (a_j, b_j)_{j \in [m]} \right) = \mathbb{E} \left( \prod_{j \in [m]} (1_{ac_j} \circ \theta_j) \bigg| (\mathbb{Z}/DZ)^t \right) = \mathbb{E} \left( 1_{\{0\}} \circ \overline{\theta} \bigg| (\mathbb{Z}/DZ)^t \right). \tag{6.39} \]

By Lemma 3.16, the \(\mathbb{Z}\)-module homomorphism \(\overline{\psi}\) equals the product of its restrictions \(\overline{\psi}^{(p)}\) to \((\mathbb{Z}/D^{(p)}Z)^t\), that means

\[\overline{\psi} = \prod_{p \in P} \overline{\psi}^{(p)} : \prod_{p \in P} (\mathbb{Z}/D^{(p)}Z)^t \rightarrow \prod_{p \in P} \left( \prod_{j \in [m]} a/ac_j^{(p)} \right).\]

Hence the affine transformations \(\overline{\theta}\) is the product of the restrictions

\[\overline{\theta}^{(p)} : (\mathbb{Z}/D^{(p)}Z)^t \rightarrow \prod_{j \in [m]} a/ac_j^{(p)}.\]
Therefore, by \((6.39)\), we obtain that
\[
e^a ((a_j, b_j)_{j \in [m]}) = E (1_{\{0\}} \circ \theta | (\mathbb{Z}/D\mathbb{Z})^t) = \prod_{p \in \mathcal{P}} E \left(1_{\{0\}} \circ \theta^{(p)} | (\mathbb{Z}/p\mathbb{Z})^t\right)
= \prod_{p \in \mathcal{P}} e^a ((a_j^{(p)}, b_j^{(p)})_{j \in [m]}).
\]
This is the desired conclusion. \(\square\)

In what follows, we assume the following setting.

**Setting 6.38.** Let \((\alpha_j, \beta_j)_{j \in [m]} \in (\text{Ideals}_{K}^{(p)})^{2m}\) be a tuple of \(p\)-ideals for some prime number \(p\). Write \(\gamma_j := \alpha_j \cap \beta_j\). Let \(D\) be the positive integer such that \(D\mathbb{Z} = \mathbb{Z} \cap \bigcap_{j \in [m]} \gamma_j\).

Let \(\overline{\psi}_j, \overline{\theta}_j : (\mathbb{Z}/D\mathbb{Z})^t \to a/ac_j\) be the \(\mathbb{Z}\)-module homomorphisms induced by \(\psi_j\) and \(\theta_j\), respectively. Let \(\overline{\psi}, \overline{\theta} : (\mathbb{Z}/D\mathbb{Z})^t \to \prod_{j \in [m]} a/ac_j\) be the two maps defined by \(\overline{\psi}(x) = (\overline{\psi}_1(x), \ldots, \overline{\psi}_m(x))\) and \(\overline{\theta}(x) = (\overline{\theta}_1(x), \ldots, \overline{\theta}_m(x))\).

Note the equality \(N(\gamma) = \#(a/ac)\) for all ideal \(\gamma \in \text{Ideals}_{K}\). The arguments in the proof of Lemma \(6.11\) hence shows the following lemma.

**Lemma 6.39.** Under Setting \(6.38\), Lemma \(6.11\) with \(e\) replaced by \(e^a\) holds.

Although the next lemma is also verified by following the proof of Lemma \(6.12\) we write down a proof for the convenience of the reader.

**Lemma 6.40.** Under Settings \(6.10\) and \(6.38\), Lemma \(6.12\) with \(e\) replaced by \(e^a\) holds.

**Proof.** First we prove \(\Box\). If \(\gamma_j = \mathcal{O}_K\) for every \(j \in [m]\), then \(\prod_{j \in [m]} (1_{a\gamma_j} \circ \theta_j)\) is identical with the constant function 1, and hence \(e^a ((\alpha_j, \beta_j)_{j \in [m]}) = 1\).

Secondly, we prove \(\Box\). It suffices to show that for all \(x \in (\mathbb{Z}/D\mathbb{Z})^t\), \(\theta_{j_0}(x) = W\psi_{j_0}(x) + b_{j_0} \not\in a\gamma_{j_0}\). Let \(p\) be an arbitrary prime ideal \(p \supseteq \gamma_{j_0}\). Since \(\gamma_{j_0}\) is a \(p\)-ideal, we have \(p \cap \mathbb{Z} = p\mathbb{Z}\). From \(p \leq w\), \(p\) divides \(W\), and hence \(W \in p\) follows. In addition, the assumption \(b_{j_0}\mathcal{O}_K + W\mathcal{A} = \mathcal{A}\) implies that \(b_{j_0} \not\in a\mathcal{A}\). Hence we see that for all \(x \in \mathbb{Z}^t\), \(\theta_{j_0}(x) = W\psi_{j_0}(x) + b_{j_0} \not\in a\mathcal{A}\). This together with \(\gamma_{j_0} \subseteq \mathcal{A}\) implies that \(\theta_{j_0}(x) \not\in a\gamma_{j_0}\), as desired.

Thirdly, we prove \(\Box\). Set \(C_{j_0} := \# \text{coker}(\psi_{j_0}).\) Note that for every \(x \in \mathcal{A}\), the element \(C_{j_0} \cdot x\) is contained in the image of \(\psi_{j_0}\). By Setting \(6.10\) \(\Box\), \(p\) and \(C_{j_0}\) are coprime. Since the order of \(a/ac_{j_0}\) is a power of \(p\), this implies that the multiplication by \(C_{j_0}\) on \(a/ac_{j_0}\) is an automorphism. Hence we see that \(\overline{\psi}_{j_0} : (\mathbb{Z}/D\mathbb{Z})^t \to a/ac_{j_0}\) is surjective. Since \(W\) and \(p\) are coprime, the map \(\overline{\theta}_{j_0} = \text{Aff}_{W,b_{j_0}} \circ \psi_{j_0} : (\mathbb{Z}/D\mathbb{Z})^t \to a/ac_{j_0}\) is also surjective. Then Lemma \(6.11\) yields that \(e^a ((\alpha_j, \beta_j)_{j \in [m]}) = (\# \text{Im}(\overline{\psi}))^{-1};\) recall that \(\gamma_j = \mathcal{O}_K\) for all \(j \in [m] \setminus \{j_0\}\). We have
\[
\# \text{Im}(\overline{\psi}) = \# \text{Im}(\overline{\psi}_{j_0}) = \#(a/ac_{j_0}) = N(\gamma_{j_0}).
\]
This is the desired result.
Finally we prove (4). By Lemma 6.11, it suffices to show that \( \#\text{Im}(\psi) \geq p^2 \). Without loss of generality, we may assume that \( \gamma_1, \gamma_2 \subsetneq O_K \). Recall that two elements \( x_{12} \) and \( x_{21} \) are chosen in Setting 6.10 (2). Since \( p > w \geq w''_0 \), both \( \psi_2(x_{12}) \not\in a\gamma_2 \) and \( \psi_1(x_{21}) \not\in a\gamma_1 \) hold. We focus on the mapping \((\psi_1, \psi_2)\), which is defined as
\[
(\psi_1, \psi_2) : (\mathbb{Z}/D\mathbb{Z})^t \to a/a\gamma_1 \times a/a\gamma_2
\]
\[
x \mapsto (\psi_1(x), \psi_2(x)).
\]
This maps \( x_{12} \) and \( x_{21} \) to nonzero elements \((0, \psi_2(x_{12}))\) and \((\psi_1(x_{21}), 0)\), respectively. The order of the linear span of these two images is at least \( p^2 \). Hence
\[
p^2 \leq \#\text{Im}(\psi_1, \psi_2) \leq \#\text{Im}(\psi),
\]
and (4) follows.

This provides the desired estimate for \( e^a \), and a proof of Theorem 6.33 is completed.

7 Construction of pseudorandom measures and estimates of weighted densities

In the present section, we will prove our first goal Theorem 2.8 as mentioned in Subsection 2.2. The main argument in this section consists of two parts: switching our ‘worlds,’ which treat \( O_K \), among three worlds appearing in Steps 1–4 in Subsection 2.3 and estimations of weighted densities corresponding to these switches. Let us recall the three worlds above.

- \textit{The N-world} \((O_K, \| \cdot \|_{\infty, \omega}, N)\): it is an auxiliary world in order to apply the relative multidimensional Szemerédi theorem (Theorem 5.4). We use the \( \ell_{\infty} \)-length scale and the parameter \( N \). Starting from a set \( A \) in the \( M \)-world, we choose appropriate \( W \in \mathbb{Z} \) and \( b \in O_K \), and connect the \( M \)-world (range) and the \( N \)-world (domain) via the affine transformation
\[
\text{Aff}_{W,b} : O_K \to O_K; \quad \beta \mapsto W\beta + b.
\]
Then we construct a set \( B \) from \( A \) in this \( N \)-world; we will apply Theorem 5.4 to this set \( B \).

- \textit{The M-world} \((O_K, \| \cdot \|_{\infty, \omega}, M)\): this is the world where the set \( A \) in the setting of Theorem 2.8 lives. We use the \( \ell_{\infty} \)-length scale and the parameter \( M \in \mathbb{R}_{\geq 1} \). We choose the parameter \( N \) above appropriately depending on \( M \).

- \textit{The L-world} \((O_K, N, L)\): the underlying space is the same as that of the \( M \)-world. The differences between these two worlds are the scales we take: in the \( L \)-world, we consider the (ideal) norm \( N \). We use the parameter \( L \in \mathbb{R}_{\geq 1} \). We appeal to Theorem 3.22 for counting elements in a given set \( A \) with respect to a certain scale; since Theorem 3.22 is stated in terms of ideals, this \( L \)-world is suited for this counting procedure.
We assume the following setting throughout the current section.

**Setting 7.1.** Let $K$ be a number field of degree $n$ and $\omega$ an integral basis of $K$. Let $D$ be an NL-compatible $O_K$-fundamental domain; recall Definitions 2.6 and 2.7. Let $C = C(\omega, D) > 0$ and $C' = C'(\omega) > 0$, respectively, be constants which satisfy (NLC). Let $S$ be a finite subset of $O_K$. We moreover assume that $S$ is a standard shape; recall Definition 2.3. As mentioned after Theorem [A] we may assume this without loss of generality. Set $r := \# S - 1$.

In this section and Sections 8 and 9, we use the following convention on cosets without mentioning it: each element of $O_K/WO_K$ may be seen as a subset of $O_K$. In particular, if $b \in O_K$ is sent to $\overline{b} \in O_K/WO_K$ by the natural projection, then we may express it as ‘$b \in \overline{b}$.’ Thus we frequently regard $b \in O_K/WO_K$ as a subset of $O_K$. In our arguments in these sections, we often take $\overline{b} \in O_K/WO_K$ first, and then choose $b$ in $\overline{b}$.

Hereafter, for $l \in \mathbb{N}$, we denote by $\log \circ l$ the $l$-time composition of log; see Subsection 2.3.

### 7.1 Outline of the proof of Theorem [A]

Let $\delta > 0$. Assume that for a sufficiently large real number $M$, $A \subseteq P_K \cap D \cap O_K(\omega, M)$ satisfies

$$\# A \geq \delta \cdot \# (P_K \cap D \cap O_K(\omega, M)).$$

The goal is to show that $A$ contains an $S$-constellation. Here we outline the argument to achieve this goal.

- For the main parameter $M$, choose $W \in \mathbb{N}$ and an auxiliary parameter $N$ appropriately in order to apply Theorem 5.4.

- Construct a pseudorandom measure $\tilde{\lambda}: O_K \to \mathbb{R}_{\geq 0}$ with the following condition: if $M$ (and hence $N$) are sufficiently large depending on a given $\rho > 0$, then $\tilde{\lambda}$ satisfies the $(\rho, N, S)$-linear forms condition in the sense of Definition 5.3.

The exact argument will be presented in Subsection 7.2. The proof of pseudorandomness of $\tilde{\lambda}$ is based on the Goldston–Yıldırım type asymptotic formula (Theorem 6.2). To switch from the $M$-world to the $N$-world, we need to take $b \in O_K$ as well as $W \in \mathbb{N}$. Although in Subsection 7.2 we argue with an arbitrarily taken $b$ which is prime to $W$, we will eventually choose $b$ according to the given set $A$. In Subsection 7.3, we prove Proposition 7.6, which describes the switch between the $L$-world and the $M$-world in the setting of the upper dense version of Theorem 2.8 (Corollary 2.10). Next, we proceed to the following two steps:

- trim $A$ by deleting an ‘exceptional set’ to obtain $A'$, choose an appropriate $b \in O_K$ according to $A'$,

- and set $B \subseteq O_K(\omega, N)$ as $B := (\text{Aff}_{W,b})^{-1}(A') \cap O_K(\omega, N)$, and establish the following estimate of the weighted density of $B$,

$$\mathbb{E} \left( 1_B \cdot \tilde{\lambda} \mid O_K(\omega, N) \right) \geq \tilde{\delta},$$
provided that $M$ is sufficiently large. Here, $\tilde{\delta}$ is a strictly positive constant depending on $\delta$, $\omega$, $D$ and $S$.

In Subsection 7.4, we will take these two steps by switching among the three worlds; see Proposition 7.9. To define $\lambda$, we also need to choose $\chi$ as in Setting 7.2. However, we can fix it as we like, and hence in what follows we sometimes omit writing the dependence on $\chi$ explicitly; see also Remark 7.13.

Finally, in Subsection 7.5, we confirm (ii) (the smallness condition); then we appeal to Theorem 5.4 and verify that $B$ contains an $S$-constellation. As we argued in Remark 5.7, we conclude that $A$ contains an $S$-constellation, thus proving Theorem 2.8.

### 7.2 Construction of the pseudorandom measure

To construct the pseudorandom measure mentioned in Subsection 7.1, we choose parameters $w$, $W$, $R$ and $N$ according to the main parameter $M$, and a function $\chi$ in the following manner.

**Setting 7.2 (The choice of the parameters).** Let $f$ be a real-valued function defined for sufficiently large real numbers $t$ with $\lim_{t \to +\infty} f(t) = +\infty$ and $f(t) \leq \frac{1}{2} \log t$ for all $t$. Let $M \in \mathbb{R}_{\geq 1}$ be the parameter with $M \geq M_f$, where $M_f$ is the smallest positive integer which satisfies that for all $t \geq M_f$, the condition $f(t) \geq 2$ holds. Then set $w = w_{f,M} \in \mathbb{R}$, $W = W_{f,M} \in \mathbb{N}$ and $R = R_{r,M} \in \mathbb{R}$ as follows:

$$w := f(M), \quad W := \prod_{p \in \mathcal{P} \leq w} p, \quad R := M^{\frac{1}{17(r+1)^2}}.$$  \hspace{1cm} (7.1)

Also, set $N = N_M \in \mathbb{N}$ as

$$N := \left\lceil \frac{M}{W} \right\rceil.$$  \hspace{1cm} (7.2)
Fix a $C^\infty$-function $\chi: \mathbb{R} \to \mathbb{R}_{\geq 0}$ which satisfies the conditions $\chi(0) = 1$, $\text{supp}(\chi) \subseteq [-1, 1]$, and $\chi(x) \leq 1$ for every $x \in \mathbb{R}$. Let $c_\chi := \int_0^\infty \chi'(x)^2 dx$.

In practice, we choose $f$ as follows in the present paper: to ensure the existence of constellations (to show Theorem 7.10), we set $f(t) = \frac{1}{2} \log t$. When we make an estimate of the number of constellations (to show Theorem 7.11), we set $f(t) = \frac{1}{2} \log^3 t$. See Remark 7.12 for more details on these choices.

We will employ the following estimate frequently in the remaining part of this paper:

$$W \leq e^{2(\log 2)f(M)}. \tag{7.3}$$

Indeed, this follows from the definitions of $w$ and $W$, and (3.6) in Proposition 3.26.

Here is the construction of the pseudorandom measure $\lambda$, which plays a key role in the proof of the main theorems in the present paper.

**Definition 7.3** (The pseudorandom measure $\tilde{\lambda}$). We use Settings 7.1 and 7.2 Let $\kappa = \kappa_K > 0$ be the constant as in Theorem 3.19. Let $\varphi_K$ be the totient function of $K$ (Definition 3.8) and $\Lambda_{R,\chi}$ be the $(R, \chi)$-von Mangoldt function (Definition 6.1). Then, define a function $\lambda = \lambda_{M;f,\chi,r,K}: \mathcal{O}_K \to \mathbb{R}_{\geq 0}$ by

$$\lambda(\alpha) := \frac{\kappa \cdot \Lambda_{R,\chi}(\alpha)^2}{c_\chi \log R}. \tag{7.4}$$

For a fixed $b \in \mathcal{O}_K$, define a function $\tilde{\lambda} = \tilde{\lambda}_{M;f,\chi,r,K,b}: \mathcal{O}_K \to \mathbb{R}_{\geq 0}$ by

$$\tilde{\lambda}(\beta) := \frac{\varphi_K(W)}{W_n}(\lambda \circ \text{Aff}_{W,b})(\beta). \tag{7.5}$$

The following theorem states that the function $\tilde{\lambda}$ indeed satisfies the linear forms condition, provided that $b$ is prime to $W$ and that $M$ is sufficiently large. For the proof, we appeal to the Goldston–Yıldılım type asymptotic formula (Theorem 6.2).

**Theorem 7.4** (Pseudorandomness of $\tilde{\lambda}$). Assume Settings 7.1 and 7.2. Fix $\rho > 0$ and $b \in \mathcal{O}_K$ prime to $W$. Then there exists a real number $M_{\text{PR}}(f, \chi, S, \rho)$ depending only on $f$, $\chi$, $S$ and $\rho$ such that the following holds: if $M \geq M_{\text{PR}}(f, \chi, S, \rho)$, then $\tilde{\lambda} = \tilde{\lambda}_{M;f,\chi,r,K,b}$, constructed in Definition 7.3, is a $(\rho, N, S)$-pseudorandom measure.

**Proof.** We will check that the conditions of Theorem 6.2 are fulfilled. Let $m$ be a positive integer at most $(r + 1)2^r$ and let $t = 2r + 2$. Take an arbitrary subset $J$ of $\bigcup_{j \in [r+1]} \{0, 1\}$ with $#J = m$, where for each $j \in [r+1]$, $e_j = [r+1] \setminus \{j\}$. Write $S$ as $S = \{s_1, \ldots, s_r\} \cup \{0\}$. Then for each $\omega \in J$, define a homomorphism $\psi_{S}^{(\omega)}: \mathbb{Z}^r \to \mathcal{O}_K$ of $\mathbb{Z}$-modules by (5.1) and (5.2) in Definition 5.3. (Thus we consider $m$ homomorphisms in total for a fixed $J$.) Since $S$ is assumed to be a standard shape, these $\psi_{S}^{(\omega)}$ are all surjective. Hence, by Lemma 5.8, condition (6.3) holds for $(\psi_{S}^{(\omega)})_{\omega \in J}$.

Consider the constants $w_0$ (depending on $S$), $R_0$ (depending on $r$ and $K$) and $F_0$ (depending on $r$ and $n$) for $(\psi_{S}^{(\omega)})_{\omega \in J}$ in the statement of Theorem 6.2. In our choices of $f$, $w_0$
and \( R \) in (7.1), if \( M \) is sufficiently large depending on \( f \) and \( S \), we have that \( w \geq w_0 \) and that \( R \geq R_0 \). From (7.3) and \( f(M) \leq \frac{1}{2} \log M \), we obtain that

\[
W \leq M^{\log 2}. \tag{7.6}
\]

Take an arbitrary subset \( B \) of \( \mathbb{Z}^{r+1} \) which is the product of intervals of length at least \( N \). Note that by the choice of \( R \) in (7.1), that of \( N \) in (7.2) and condition (7.6), \( N \geq M^{\frac{5}{17}} \geq R^{4m+1} \). In addition, by the choices of \( w \) and \( R \) in (7.1) and by \( f(M) \leq \frac{1}{2} \log M \), we have

\[
\frac{\log w}{\sqrt{\log R}} = O_r \left( \frac{\log^2 M}{\sqrt{\log M}} \right) = o_{M \to \infty, r}(1); \tag{7.7}
\]

this implies that if \( M \) is sufficiently large depending on \( r \) and \( n \), then \( \log w \leq F_0 \cdot \sqrt{\log R} \) holds.

Therefore, we may appeal to Theorem 6.2 and we conclude that

\[
E \left( \prod_{\omega \in J} (\tilde{\lambda} \circ \psi^{(\omega)}_S) \bigg| \mathcal{B} \times \mathcal{B} \right) = 1 + O_{r,n} \left( \frac{1}{w \log w} \right) + O_{\chi,r,K} \left( \frac{\log w}{\sqrt{\log R}} \right); \tag{7.8}
\]

recall that \( b \) is assumed to be prime to \( W \). By the conditions above on \( M \), (7.1) and \( \lim_{M \to +\infty} f(M) = +\infty \), we have the following: if \( M \) is sufficiently large depending only on \( f \), \( \chi \), \( S \) and \( \rho \), then the absolute value of the difference between the left-hand side of (7.8) and 1 does not exceed \( \rho \). This proves that \( \tilde{\lambda} \) satisfies the \((\rho,N,S)\)-linear forms condition in the sense of Definition 5.3. \( \square \)

### 7.3 Comparison between countings with the norm scale and with the \( \ell_\infty \)-length scale

In Subsection 7.4 we will estimate the weighted density of the set \( B \) appearing in Subsection 7.1. Before that, in this subsection, for a subset of \( \mathcal{P}_K \cap \mathcal{D} \), we make a comparison of the relative upper asymptotic density measured by norm and that measured by \( \ell_\infty \)-length; see Proposition 7.6. This relates to Corollary 2.10, which is the upper dense version of Theorem 2.8. The key to this comparison is the following lemma for an NL-compatible \( \mathcal{O}_K \)-fundamental domain \( \mathcal{D} \).

**Lemma 7.5.** Let \( \mathcal{D}, C \) and \( C' \) be as in Setting 7.1. Then the following hold true.

1. For \( L, M \in \mathbb{R}_{\geq 0} \) with \( L \leq CM^n \),

\[
\mathcal{D} \cap \mathcal{O}_K(L) \subseteq \mathcal{D} \cap \mathcal{O}_K(\omega, M). \]

2. For \( L, M \in \mathbb{R}_{\geq 0} \) with \( L \geq C'M^n \),

\[
\mathcal{D} \cap \mathcal{O}_K(\omega, M) \subseteq \mathcal{D} \cap \mathcal{O}_K(L). \]
Proof. Both items may be easily seen by inequality (NLC) for all \( \alpha \in \mathcal{D} \),
\[
C \| \alpha \|^n_{\infty, \omega} \leq N(\alpha) \leq C' \| \alpha \|^n_{\infty, \omega},
\]
mentioned after Lemma 4.8.

We will derive the following proposition from Lemma 7.5 and Theorem 3.22. Recall the definition of the relative upper asymptotic densities from Definition 2.9.

**Proposition 7.6.** Assume Setting 7.1. Then for every \( A \subseteq \mathcal{P}_K \cap \mathcal{D} \), the density \( \overline{d}_{\mathcal{P}_K \cap \mathcal{D}}(A) \) is strictly positive if and only if \( \overline{d}_{\mathcal{P}_K \cap \mathcal{D}, \omega}(A) \) is strictly positive.

**Proof.** Since \( \mathcal{D} \) is an \( \mathcal{O}_K \)-fundamental domain, the following holds true: for a finite subset \( \mathcal{A} \subseteq \text{Ideals}_K \) consisting of principal ideals, we have
\[
\# \{ \alpha \in \mathcal{D} : (\alpha) \in \mathcal{A} \} = \# \mathcal{A}.
\]
(7.9)

Apply (7.9) to \( \mathcal{A} = \{ p \in |\text{Spec}(\mathcal{O}_K)|^n : N(p) \leq L \} \). Then by a special case of the natural density version of the Chebotarev density theorem (Theorem 3.22), for a sufficiently large \( L \), we obtain that
\[
\frac{1}{2h} \cdot \frac{L}{\log L} \leq \#(\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(L)) \leq \frac{2}{h} \cdot \frac{L}{\log L}.
\]
(7.10)

Here \( h = h_K \) denotes the class number of \( K \).

First, we will prove \( \overline{d}_{\mathcal{P}_K \cap \mathcal{D}, \omega}(A) > 0 \) if \( \overline{d}_{\mathcal{P}_K \cap \mathcal{D}}(A) > 0 \). Let \( \delta := \overline{d}_{\mathcal{P}_K \cap \mathcal{D}}(A) > 0 \). Then there exists a strictly increasing real sequence \( (L_k)_{k \in \mathbb{N}} \) with \( \lim_{k \to \infty} L_k = \infty \) such that for all \( k \in \mathbb{N} \),
\[
\#(A \cap \mathcal{O}_K(L_k)) \geq \frac{\delta}{2} \cdot \#(\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(L_k))
\]
holds. By (7.10), if \( k \) is sufficiently large, then we have
\[
\#(A \cap \mathcal{O}_K(L_k)) \geq \delta \cdot \frac{1}{4h} \cdot \frac{L_k}{\log L_k}.
\]
Now set \( M_k := (L_k/C)^{1/n} \). Then \( \lim_{k \to \infty} M_k = \infty \) holds. By Lemma 7.5 (1), for a sufficiently large \( k \),
\[
\#(A \cap \mathcal{O}_K(\omega, M_k)) \geq \delta \cdot \frac{1}{4h} \cdot \frac{C M_k^n}{\log(C M_k^n)}
\]
holds. In addition, by Lemma 7.5 (2) and by (7.10), we have
\[
\#(\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M_k)) \leq \frac{2}{h} \cdot \frac{C' M_k^n}{\log(C' M_k^n)}.
\]
By combining them, we have that for a sufficiently large \( k \),
\[
\frac{\#(A \cap \mathcal{O}_K(\omega, M_k))}{\#(\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M_k))} \geq \frac{C}{8C'} \delta;
\]
here recall that $C' \geq C$. This implies that
\[
\overline{d}_{P_K \cap D}(A) \geq \frac{C}{8C'} \cdot \overline{d}_{P_K \cap D, \omega}(A)
\]
and hence that $\overline{d}_{P_K \cap D, \omega}(A) > 0$.

Finally, we will prove $\overline{d}_{P_K \cap D}(A) > 0$ if $\overline{d}_{P_K \cap D, \omega}(A) > 0$. This time, we set $\delta := \overline{d}_{P_K \cap D, \omega}(A) > 0$. Then there exists a strictly increasing real sequence $(M_k)_{k \in \mathbb{N}}$ with $\lim_{k \to \infty} M_k = \infty$ such that for every $k \in \mathbb{N}$,
\[
\#(A \cap \mathcal{O}_K(\omega, M_k)) \geq \frac{\delta}{2} \cdot \#(\mathcal{P}_K \cap D \cap \mathcal{O}_K(\omega, M_k))
\]
holds. Set $L_k := C'M_k^n$. Then $\lim_{k \to \infty} L_k = \infty$. By Lemma 7.5 and (7.10), if $k$ is sufficiently large, then we have that
\[
\#(A \cap \mathcal{O}_K(L_k)) \geq \#(A \cap \mathcal{O}_K(\omega, M_k))
\]
\[
\geq \frac{\delta}{2} \cdot \#(\mathcal{P}_K \cap D \cap \mathcal{O}_K(\omega, M_k))
\]
\[
\geq \frac{\delta}{2} \cdot \#(\mathcal{P}_K \cap D \cap \mathcal{O}_K(CM_k^n)) \geq \delta \cdot \frac{1}{4h} \cdot \frac{CM_k^n}{\log(CM_k^n)}.
\]
Again by (7.10), for a sufficiently large $k$, we obtain
\[
\frac{\#(A \cap \mathcal{O}_K(L_k))}{\#(\mathcal{P}_K \cap D \cap \mathcal{O}_K(L_k))} \geq \delta \cdot \frac{1}{4h} \cdot \frac{CM_k^n}{\log(CM_k^n)} \cdot \frac{h}{2} \cdot \frac{\log L_k}{L_k} \geq \frac{C}{8C'} \cdot \frac{1}{
}
This implies that
\[
\overline{d}_{P_K \cap D}(A) \geq \frac{C}{8C'} \cdot \overline{d}_{P_K \cap D, \omega}(A)
\]
and hence that $\overline{d}_{P_K \cap D}(A) > 0$.

We remark that in the above proof of Proposition 7.6, the multiplicative constant $\frac{C}{8C'}$, appearing twice, may be improved to $\frac{C}{C'}$. Indeed, for every $\varepsilon > 0$, take $L$ and $k$ both sufficiently large according to $\varepsilon$, and improve the factors $\frac{1}{2h}$, $\frac{2}{h}$ and $\frac{\delta}{2}$ in the proof to $\frac{1-\varepsilon}{h}$, $\frac{1+\varepsilon}{h}$ and $(1-\varepsilon)\delta$, respectively. Finally, let $\varepsilon \to 0$.

The following result of counting will be employed in Subsection 7.4.

**Proposition 7.7.** Under Setting 7.1, we have that
\[
\lim inf_{M \to \infty} \frac{\#(\mathcal{P}_K \cap D \cap \mathcal{O}_K(\omega, M))}{M^n(\log M)^{-1}} \geq \frac{C}{(n+1)h},
\]
where $h$ is the class number of $K$.

**Proof.** Utilize the estimate from below in (7.10) (with a finer constant $(1-\varepsilon)/h$ for each $\varepsilon > 0$ and for a sufficiently large $L$ depending on $\varepsilon$) with $L = CM^n$. Then, the desired result follows from Lemma 7.5(1) and $CM^n \leq M^{n+1}$, which is valid for $M \geq C$. \qed
7.4 Estimates of weighted densities

Let \( A \) be a subset of \( \mathcal{O}_K \) in which we hope to find an \( S \)-constellation. In Subsection 7.2, we have constructed a pseudorandom measure \( \tilde{\lambda} \) corresponding to suitable parameters and for a (yet unspecified) \( b \in \mathcal{O}_K \) prime to \( W \). In this subsection, we specify a suitable \( b \) and make an estimation of the weighted density of \( B \), whose construction is outlined in Subsection 7.1, with weight \( \tilde{\lambda} \). As mentioned in Subsection 7.1, to construct \( B \) from \( A \), we will trim \( A \) by removing an exceptional set \( T \), which behaves badly in our proof. The following lemma collects the properties of the exceptional set \( T \) employed in this section.

**Lemma 7.8 (Exceptional set).** Assume Settings 7.1 and 7.2. Let \( A \subseteq \mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M) \). Then

\[
T := A \cap \mathcal{O}_K(R) \tag{7.11}
\]

satisfies the following, provided that \( M \) is sufficiently large depending on \( r \) and \( K \):

1. \( \#T \leq M^{1/16} \),
2. for every \( \alpha \in A \setminus T \),
   \[
   \lambda(\alpha) = \frac{\kappa}{17(r+1)2^r c_\chi} \cdot \log M,
   \]
3. every \( \alpha \in A \setminus T \) is prime to \( W \).

**Proof.** First, we will prove (1). By Proposition 3.20, if \( M \) is sufficiently large depending on \( r \), then the number of ideals whose ideal norms are at most \( R \) does not exceed \( 2^\kappa R \). By (7.9), \( \#T \leq 2^\kappa R \) holds. From the choice of \( R \), if \( M \) is sufficiently large depending on \( K \), then \( R \leq \frac{1}{2^\kappa} M^{1/16} \) holds.

Secondly, we will prove (2). Here note that for every \( \alpha \in A \setminus T \), we have \( N(\alpha) > R \) and \( \alpha \) is a prime element. Since \( \chi(0) = 1 \) and \( \text{supp}(\chi) \subseteq [-1, 1]_R \), we have

\[
\sum_{b | \alpha \mathcal{O}_K} \mu(b) \chi \left( \frac{\log N(b)}{\log R} \right) = 1,
\]

which ensures (2).

Finally, we will prove (3). Since \( w \leq \frac{1}{2} \log M \), for a sufficiently large \( M \) depending on \( r \) and \( K \), we have \( w^m \leq R \). Hence, every \( \alpha \in A \setminus T \) satisfies that \( N(\alpha) > w^m \). Since \( \alpha \) is a prime element, \( \alpha \) is prime to \( W \); recall the choice of \( W \) from (7.1).

The next proposition is the goal of the present subsection.

**Proposition 7.9 (Estimate of the weighted density with weight \( \tilde{\lambda} \)).** Assume Settings 7.1 and 7.2. Then there exist positive real number \( M_{DS} = M_{DS}(\omega, \mathcal{D}, \delta, r) \), depending only on \( \omega, \mathcal{D}, \delta \) and \( r \), and positive real number \( u = u(\omega, \mathcal{D}, \chi, r) > 0 \), depending only on \( \omega, \mathcal{D}, \chi \) and \( r \), such that the following holds true: let \( \delta > 0 \) and \( M \geq M_{DS} \). Assume that a set \( A \subseteq \mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M) \) satisfies

\[
\#A \geq \delta \cdot \#(\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M)). \tag{7.12}
\]
Let $A' := A \setminus T$, where $T$ is the exceptional set defined in (7.11). Then there exists $b = b(M,A)$ such that $b$ is prime to $W$ and that for

$$B := (\text{Aff}_{W,b})^{-1}(A') \cap \mathcal{O}_K(\omega,N),$$

(7.13)

the following estimate

$$\mathbb{E}(1_B \cdot \tilde{\lambda} \mid \mathcal{O}_K(\omega,N)) \geq \tilde{\delta}$$

of the weighted density of $B$ with weight $\tilde{\lambda} = \tilde{\lambda}_{M,f,r,K,b}$ holds true. Here, $\tilde{\delta} := u \cdot \delta$.

An important point here is that not all $b \in \mathcal{O}_K$ prime to $W$ satisfy the estimate of the weighted density in Proposition 7.9, whereas Theorem 7.4 holds true for all $b \in \mathcal{O}_K$ prime to $W$. We will go back to this point in Section 9 in more detail. In the proof of Proposition 7.9 below, note that $C = C(\omega,D)$ only depends on $\omega$ and $D$.

Proof. By Proposition 7.7, for a sufficiently large $M$ depending on $\omega, D$ and $\delta$, we have that

$$\# A \geq \frac{C}{2(n+1)h} \cdot \frac{M^n}{\log M}.$$ 

Since $M \tilde{\pi} = o_{M \to \infty}(M^n)$, Lemma 7.8 (1) implies that for a sufficiently large $M$ depending on $\omega, D$ and $\delta$,

$$\# A' \geq \frac{C}{3(n+1)h} \cdot \frac{M^n}{\log M}$$

(7.14)

holds true.

Next, we will choose an appropriate $b \in \mathcal{O}_K$. By Lemma 7.8 (3), if $M$ is sufficiently large depending on $r$ and $K$, then the image of $A'$ by the natural projection $\mathcal{O}_K \to \mathcal{O}_K/W\mathcal{O}_K$ is a subset of $(\mathcal{O}_K/W\mathcal{O}_K)^\times$. Hence $A'$ is partitioned as

$$A' = \bigsqcup_{\bar{e} \in (\mathcal{O}_K/W\mathcal{O}_K)^\times} (A' \cap \bar{e});$$

(7.15)

here, we regard $\bar{e} \subseteq \mathcal{O}_K$ as mentioned at the beginning of the current section. Apply the pigeonhole principle to (7.15). Then (7.14) implies that there exists $\bar{b} \in (\mathcal{O}_K/W\mathcal{O}_K)^\times$ such that

$$\#(A' \cap \bar{b}) \geq \frac{1}{\varphi_K(W)} \cdot \frac{C}{3(n+1)h} \cdot \frac{M^n}{\log M}$$

(7.16)

holds. Fix such a coset $\bar{b} \in \mathcal{O}_K/W\mathcal{O}_K$, and choose $b \in \bar{b}$ which satisfies

$$\|b\|_{\infty,\omega} < W.$$ 

(7.17)

We set $\tilde{\lambda} = \tilde{\lambda}_{M,f,r,K,b}$ corresponding to this $b$.

In what follows, we will make estimates of weight densities in the $N$-world. Define $B$ by (7.13), corresponding to the element $b$ above. Since $\text{Aff}_{W,b} : \mathcal{O}_K \to \mathcal{O}_K$ is injective,

$$\mathbb{E}(1_B \cdot \tilde{\lambda} \mid \mathcal{O}_K(\omega,N)) = \frac{\varphi_K(W)}{W^n} \cdot \mathbb{E}(1_{\text{Aff}_{W,b}(B)} \cdot \tilde{\lambda} \mid \text{Aff}_{W,b}(\mathcal{O}_K(\omega,N)))$$
holds true. Note that \( \text{Aff}_{W,b}(B) = A' \cap \text{Aff}_{W,b}(\mathcal{O}_K(\omega, N)) \). Hence, by Lemma 7.8, we have that

\[
\mathbb{E}(\mathbf{1}_B \cdot \lambda \mid \mathcal{O}_K(\omega, N)) \geq \frac{\varphi_K(W)}{W^n} \cdot \frac{\kappa}{17(r+1)2^r c_{\chi}} \cdot \frac{\#(A' \cap \text{Aff}_{W,b}(\mathcal{O}_K(\omega, N)))}{(2N+1)^n} \cdot \log M. \tag{7.18}
\]

Here observe by the choice of \( N \) in (7.2), (7.17) and by the triangle inequality for \( \|\cdot\|_{\infty,\omega} \),

\[
\text{Aff}_{W,b}(\mathcal{O}_K(\omega, N)) \supseteq \mathcal{O}_K(\omega, M) \cap (W\mathcal{O}_K + b)
\]

holds true; indeed, our choice (7.2) of \( N \) is made in such a way that the inclusion above is satisfied.

Therefore, by (7.16) and (7.18), we conclude that

\[
\mathbb{E}(\mathbf{1}_B \cdot \lambda \mid \mathcal{O}_K(\omega, N)) \geq \frac{\kappa}{17(r+1)2^r c_{\chi}} \cdot \frac{C}{3(n+1)h} \cdot \frac{M^n}{W^n(2N+1)^n}. \tag{7.19}
\]

Finally, since \( N \leq \frac{2M}{W} \) and \( (2N+1)^n \leq 3^n N^n \), we obtain that

\[
\mathbb{E}(\mathbf{1}_B \cdot \lambda \mid \mathcal{O}_K(\omega, N)) \geq \frac{\kappa}{51h(n+1)6^n} \cdot \frac{C}{(r+1)2^r c_{\chi}} \cdot \delta. \tag{7.19}
\]

Hence we can take \( u = \frac{\kappa C}{51h(n+1)6^n(r+1)2^r c_{\chi}} \). \qed

### 7.5 Proof of Theorem 2.8

In this subsection, we present the proof of Theorem 2.8 which is the first goal of the present paper. We will divide the statement of Theorem 2.8 into the following two parts: Theorem 7.10 (the existence of \( S \)-constellations) and Theorem 7.11 (the estimate of the numbers of \( S \)-constellations).

**Theorem 7.10** (The first half of Theorem 2.8). Assume Setting 7.1. Let \( \delta > 0 \). Then, there exists a positive integer \( M_{\text{FES}} = M_{\text{FES}}(\omega, \mathcal{D}, \delta, S) \) depending only on \( \omega, \mathcal{D}, \delta \) and \( S \) such that the following holds true: assume that \( M \geq M_{\text{FES}} \) and that a subset \( A \) of \( \mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M) \) satisfies

\[
\#A \geq \delta \cdot \#(\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M)).
\]

Then there exists an \( S \)-constellation in \( A \).

**Proof.** Utilize Setting 7.2; recall that, in particular, we assume that \( M \geq M_f \). For \( A \) in the assumption, let \( A', b, B, \lambda \) and \( \tilde{\delta} \) be as in Proposition 7.9. Take \( \gamma = \gamma_{\text{RMS}}(\omega, \tilde{\delta}, S) \) and \( \rho = \rho_{\text{RMS}}(\omega, \tilde{\delta}, S) \), which are determined from the relative multidimensional Szemerédi theorem (Theorem 5.4); note that we here substitute \( \tilde{\delta} \) for \( \delta \). We will verify the following three items in order to appeal to Theorem 5.4.
• (Pseudorandomness) Define $M^{(1)}_{\text{PES}}(f, \omega, D, \delta, \chi, S)$ by

$$M^{(1)}_{\text{PES}}(f, \omega, D, \delta, \chi, S) := M_{\text{PR}}(f, \chi, S, \rho).$$

Then by Theorem 7.4, if $M \geq M^{(1)}_{\text{PES}}$, then $\tilde{\lambda}$ is a $(\rho, N, S)$-pseudorandom measure. Here observe that $\delta$ only depends on $\omega, D, \chi$ and $r$, and not on $f$; this observation will be used in the proof of Theorem 7.11.

• (Weighted density) Define $M^{(2)}_{\text{PES}} := M_{\text{DS}}(\omega, D, \delta, r)$. By Proposition 7.9, if $M \geq M^{(2)}_{\text{PES}}$, then the weighted density condition

$$\mathbb{E}(1_B \cdot \tilde{\lambda} \mid O_K(\omega, N)) \geq \tilde{\delta}$$

is fulfilled.

• (Smallness) By Lemma 7.8, we have that

$$\mathbb{E}(1_B \cdot \tilde{\lambda}^{r+1} \mid O_K(\omega, N)) \leq \mathbb{E}(1_{A'} \cdot \lambda^{r+1} \mid \text{Aff}_{W,b}(O_K(\omega, N))) \leq \left(\frac{\kappa}{17(r+1)2^r c_\chi}\right)^{r+1} (\log M)^{r+1}.$$

In particular, it follows from (7.6) that $N \geq M^{0.3}$; we obtain that

$$\frac{1}{N} \mathbb{E}(1_B \cdot \tilde{\lambda}^{r+1} \mid O_K(\omega, N)) \leq \left(\frac{\kappa}{17(r+1)2^r c_\chi}\right)^{r+1} (\log M)^{r+1} \leq o_{M \to \infty; \chi, r, K}(1).$$

Hence, there exists $M^{(3)}_{\text{PES}} = M^{(3)}_{\text{PES}}(\omega, D, \delta, \chi, S)$ such that the following holds: if $M \geq M^{(3)}_{\text{PES}}$, then the smallness condition

$$\mathbb{E}(1_B \cdot \tilde{\lambda}^{r+1} \mid O_K(\omega, N)) \leq \gamma \cdot N$$

is fulfilled; here note that $\gamma$ only depends on $\omega, D, \chi$ and $S$.

Finally, set $M'_{\text{PES}} = M'_{\text{PES}}(f, \omega, D, \delta, \chi, S)$ as

$$M'_{\text{PES}} := \max\{M_f, M^{(1)}_{\text{PES}}, M^{(2)}_{\text{PES}}, M^{(3)}_{\text{PES}}\}.$$ 

Then, for every $M$ with $M \geq M'_{\text{PES}}$, Theorem 5.4 applies to the set $B$ above. This implies that there exists an $S$-constellation in $B$. By sending it by $\text{Aff}_{W,b}$, we obtain an $S$-constellation in $A'$; recall Remark 5.7. Since $A' \subseteq A$, in particular, there exists an $S$-constellation in $A$, as desired.

On dependence on parameters, first observe that $\chi$ is taken in order to construct $\tilde{\lambda}$; it does not appear in the setting itself of Theorem 7.10. Secondly, we can take an arbitrary $f$ as long as $\lim_{t \to +\infty} f(t) = +\infty$ and $f(t) \leq \frac{1}{2} \log t$. Hence, once we take $f_1(M) = \frac{1}{2} \log M$ (in this case, $M_{f_1} = 55$), we may set

$$M_{\text{PES}} := \min_{\chi} [M'_{\text{PES}}(f_1, \omega, D, \delta, \chi, S)].$$

Then $M_{\text{PES}}$ only depends on $\omega, D, \delta$ and $S$. It completes our proof. □
Proof of Corollary 2.10. Note that Proposition 7.6 implies that the two conditions in Corollary 2.10 are equivalent to each other. Take an arbitrary finite subset $S$ of $\mathcal{O}_K$. Assume that $d_{P \cap \mathcal{D}, \omega}(A) > \delta > 0$. Then there exists a sequence $M_1 < M_2 < M_3 < \cdots$ of positive reals with $\lim_{n \to \infty} M_n = \infty$ such that for all $n \in \mathbb{N}$, the set $A \cap \mathcal{O}_K(\omega, M_n)$ witnesses the relative density at least $\delta$. There exists $m$ such that $M_m \geq M_{PES}(\omega, \mathcal{D}, \delta, S)$. Apply Theorem 7.10 to $A \cap \mathcal{O}_K(\omega, M_m)$ with the parameter $M_m$ with such $m$, we can find an $S$-constellation in $A \cap \mathcal{O}_K(\omega, M_m) \subseteq A$.

Since $S$ is arbitrarily taken, it completes the proof; note that $m$ itself does depend on $S$ but $A \supseteq A \cap \mathcal{O}_K(\omega, M_n)$ for all $n \in \mathbb{N}$.

Proof of Corollary 1.5. Proposition 4.11 ensures the existence of an NL-compatible $\mathcal{O}_K^x$-fundamental domain $\mathcal{D}$. Apply Corollary 2.10 with $A = \mathcal{P}_K \cap \mathcal{D}$; since $\mathcal{D}$ is an $\mathcal{O}_K^x$-fundamental domain, $\mathcal{D}$ itself admits no associate pairs.

In the last part of this subsection, we will present the proof of the estimate of the number of $S$-constellations in Theorem 2.8. The key to the estimation is Theorem 5.5. Theorem 5.5 implies that if the main parameter $M$ in Theorem 7.10 satisfies $M \geq M_{PES}$, then the following estimate holds true:

$$\frac{\mathcal{N}_S(B) \times \left( \frac{\kappa}{17(\ref{7.20}) \log M} \log M \right)^{r+1}}{N(2N+1)^n} \geq \gamma,$$

where $\gamma = \gamma_{RMS}(\omega, \delta, S) > 0$. Indeed, for each $S$-constellation $S$ in $B$, the value $\prod_{s' \in S}(1_B \cdot \bar{\lambda})(s')$ is at most $\left( \frac{\kappa}{17(\ref{7.20}) \log M} \log M \right)^{r+1}$ by Lemma 7.8. Furthermore, the final part of the proof above of Theorem 7.10 implies that $\mathcal{N}_S(B) \leq \mathcal{N}_S(A') \leq \mathcal{N}_S(A)$. Therefore, we conclude that there exists $\gamma' = \gamma_{PES}(\omega, \mathcal{D}, \delta, \chi, S) > 0$ such that for all $M \geq M_{PES}$,

$$\mathcal{N}_S(A) \geq \gamma' \cdot N^{n+1}(\log M)^{-(r+1)} \tag{7.20}$$

holds true. Here $\gamma'$ depends on $\chi$, but this dependence is harmless once we choose and fix $\chi$; see also Remark 7.13.

We here warn that (7.20) does not complete our desired estimate: this is because the right-hand side of (7.20) involves $N$, whereas our original parameter is $M$. For instance, for the choice $f(t) = f_1(t) = \frac{1}{2} \log t$, (3.7) in Theorem 3.27 implies that $W = M^{0.5+o_{M \to \infty}(1)}$; then $N = M^{0.5+o_{M \to \infty}(1)}$ and the estimate provided by (7.20) is much worse than $M^{n+1}(\log M)^{-(r+1)+o(1)}$. To obtain a better estimate, we replace $f$ with a function of a much slower growth in the proof of Theorem 7.10. The following theorem is the outcome of the discussion above.

**Theorem 7.11** (The latter half of Theorem 2.8). Assume Setting 7.2. Let $\chi$ be as in Setting 7.2. Let $\delta > 0$. Then, there exist a positive integer $M_{PES}^\delta = M_{PES}(\omega, \mathcal{D}, \delta, S)$ and a positive real $\gamma = \gamma_{PES}(\omega, \mathcal{D}, \delta, \chi, S) > 0$ such that the following holds true: assume that $M \geq M_{PES}^\delta$ and that a subset $A$ of $\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M)$ satisfies

$$\#A \geq \delta \cdot \#(\mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M)).$$
Then we have the following estimate

\[ \mathcal{N}_S(A) \geq \gamma \cdot M^{n+1}(\log M)^{-\#S+o_M \to \infty, n(1)} \]

of the number of \( S \)-constellations in \( A \).

**Proof.** Utilize Setting 7.2 with setting \( f \) as

\[ f_2(t) = \frac{1}{2} \log^3 t \leq \frac{1}{2} \log t \]

(then \( M_{f_2} = \lceil e^{e^4} \rceil \)). Also fix \( \chi \). Repeat the argument of the proof of Theorem 7.10 in this setting. Then the corresponding estimate, provided by Theorem 5.5, to (7.20) in this case is the following: for every \( M \geq M'_{\text{PES}}(f_2, \omega, \mathcal{D}, \delta, \chi, S) \), we have

\[ \mathcal{N}_S(A) \geq \gamma \cdot N^{n+1}(\log M)^{-(r+1)}; \]

here note that we may take \( \gamma = \gamma' \) because \( \tilde{\delta} \) does not depend on the choice of \( f \). Since \( f = f_2 \) and \( \chi \) are both fixed, we may write \( M'_{\text{PES}}(\omega, \mathcal{D}, \delta, \chi, S) \) for \( M'_{\text{PES}}(f_2, \omega, \mathcal{D}, \delta, \chi, S) \). By (7.3) and by the choice of \( f_2 \), we have

\[ N \geq \frac{M}{\log^2 M}. \]

Therefore, we conclude that

\[ \mathcal{N}_S(A) \geq \gamma \cdot M^{n+1}(\log M)^{-(\#S+o_M \to \infty, n(1))}. \]

(7.21)

The right-hand side of (7.21) can be expressed as

\[ \gamma \cdot M^{n+1}(\log M)^{-(\#S+o_M \to \infty, n(1))}, \]

this completes our proof.

**Remark 7.12** (Remark on the choice of \( f \)). We remark the following trade-off on the choice of \( f \): if we choose a smaller \( f \), then (7.20), which is valid for a ‘sufficiently large’ \( M \) (depending on \( f \)), provides a better estimate of the number of \( S \)-constellations in \( A \). On the other hand, the supremum of \( M \) for which the existence of \( S \)-constellations is not guaranteed may get larger. The latter point arises from (7.8); more precisely, the error term \( O_{r,n}\left(\frac{1}{w \log w}\right) \) there may become larger if \( w \) gets smaller.

**Remark 7.13** (Remark on the choice of \( \chi \)). The effect of \( \chi \) on the quantitative aspects of the proof of Theorem 7.10 consists of the following two factors: first, \( c_\chi \) in the denominator of (7.19); secondly, the term \( O_{\chi,r,K}\left(\frac{\log w}{\sqrt{\log R}}\right) \) in (7.8). To optimize the first factor, we may take \( c_\chi > 1 \) arbitrarily close to 1 by smoothening the function \( \chi_0(t) = \max\{1 - |t|, 0\} \). Note also that \( c_\chi > 1 \) by Cauchy–Schwarz. The second factor comes from the Fourier transform, and is more delicate. For this reason, the optimization of the total factors over all choices of \( \chi \) might not be straightforward.
8 Szemerédi-type theorems in prime elements of number fields

In this section, we will establish Theorem A, which is the first main theorem in the present paper. Recall the proof of Theorem 2.8 in Section 7: the first key to the proof is the existence of a suitable pseudorandom measure. Once this is ensured, the main part of the rest of the proof is counting arguments of elements. In this section, before proceeding to the proof of Theorem A, we will axiomatize deductions of constellation theorems from the existence of appropriate pseudorandom measures and from certain countings. In fact, our axiomatizations have two types, as follows.

(i) Axiomatizations for constellation theorems of type 1: Theorem 8.7, Theorem 8.8, Corollary 8.10.

(ii) Axiomatizations for constellation theorems of type 2: Theorem 8.20, Theorem 8.21, Corollary 8.22.

Here by constellation theorems of type 1, we mean those that guarantee the mere existence of constellations; constellation theorems of type 2 those that guarantee the existence of constellations without associate pairs. A constellation theorem of type 2 is stronger than the corresponding one of type 1. In our axiomatizations, that of type 2 requires an additional condition to that of type 1. More precisely, in both axiomatizations, we assume a certain condition on countings from below of elements; in the axiomatization of constellation theorems of type 2, we furthermore impose a certain condition on countings from above of elements according to their ideal norms.

To establish Theorem A, we will first prove Theorem 8.13, which is the type 1 version of it. The proof of Theorem 8.13 will be done by axiomatization [i]. Then, with the aid of axiomatization [ii], we will secondly prove the full statements of Theorem A and Theorem 1.4. For these proofs, a counting from below which is needed in axiomatization [i] will be verified in Proposition 8.12; a counting from above which is additionally required in axiomatization [ii] is provided in Proposition 8.14. On these propositions, it may be possible to obtain finer results if we exploit the generalized prime number theorem of Mitsui [Mit56, Main Theorem], which is an even deeper result than Theorem 3.22. See also Remark 8.16.

Nevertheless, in the present paper, we employ Landau’s prime ideal theorem (Theorem 3.21) and (a special case of) the natural density version of the Chebotarev density theorem (Theorem 3.22) for our counting arguments, rather than appealing to Mitsui’s theorem. There are two reasons for this: first, in the present work, it only suffices to have certain order estimates for countings, and precise information on the multiplicative constants of the main term is not needed. Our less involved approach fits this purpose. (It is similar to the situation on estimating the first Chebyshev function: (3.7) provides the exact main term of $\vartheta(L)$, whereas Proposition 3.26 only gives the order of the main term, but it is considerably less involved.) Secondly and more importantly, our approach in this paper is based on taking an NL-compatible fundamental domain. This approach has a great advantage in the proofs.
of constellation theorems of type 2; recall that a fundamental domain should admit no associate pairs. For the proofs of constellation theorems for a general case, in the current paper, we reduce the general case to finding constellations inside a fixed fundamental domain; see Theorem 8.19 and Theorem 8.25 for the precise meaning of this reduction. Thus, we will establish constellation theorems both of type 1 and type 2, such as Theorem A, in a unified manner by taking a ‘good’ $\mathcal{O}_K$-fundamental domain. The key argument to our approach, the reduction to the case of fixing a fundamental domain, will be presented in Subsection 8.4.

We collect the setting in this section.

**Setting 8.1.** Let $K$ be a number field, and $n$ the degree. Let $\phi_K$ be the totient function of $K$ (Definition 3.8). Let $a \subseteq \mathcal{O}_K$ be a non-zero ideal of $\mathcal{O}_K$. Then $a$ is a free module of rank $n$ as a $\mathbb{Z}$-module; we fix a $\mathbb{Z}$-basis $v$ of $a$.

In Section 5, the $(\rho, N, S)$-pseudorandom condition on measures (Definition 5.3) is stated for a non-negative integer parameter $N$. Hereafter, we relax the range of the parameter $N$ and consider $N$ to be a non-negative real parameter. More precisely, for a non-negative real number $N$, we define the $(\rho, \lceil N \rceil, S)$-pseudorandom condition as the $(\rho, \lceil N \rceil, S)$-pseudorandom condition in the original sense. This relaxation enables us to avoid inessential issues caused by the integrality of the parameters. In the present paper, when we express dependences of constants, we omit writing that on $K$ if the constant depends on $v$. This is because $K$ equals the $\mathbb{Q}$-span of $v$, and hence $v$ remembers $K$.

### 8.1 Preliminaries on the axiomatizations for constellation theorems

Under Setting 8.1 let $S \subseteq a$ be a finite subset and let $\delta > 0$. For a parameter $M \in \mathbb{R}_{\geq 1}$, consider a subset $A \subseteq a(v, M)$. Suppose that

$$\#A \geq \delta M^n$$

holds. Then, for a sufficiently large parameter $M$, $A$ may be regarded as a ‘dense’ subset of $a(v, M)$. In this case, the multidimensional Szemerédi theorem (Theorem 5.2) ensures the existence of $S$-constellations in $A$.

However, for subsets in $a(v, M)$ of our interest in the current paper, such as $A = \mathcal{P}_K \cap \mathcal{O}_K(\omega, M)$ for $a = \mathcal{O}_K$, we only have the following counting estimate

$$\#A \geq \delta \frac{M^n}{\log M}, \quad (8.1)$$

which is mainly derived from the natural density version of the Chebotarev density theorem (Theorem 3.22). In many cases of our interest, $A$ is indeed ‘sparse’ for a large $M$. Consider the case where $a = \mathcal{O}_K$. As we proved in Section 6 (and Section 7), we can construct a suitable pseudorandom measure for $A$ based on the $W$-trick. Then, if $A \subseteq \mathcal{P}_K \cap \mathcal{D} \cap \mathcal{O}_K(\omega, M)$ for some NL-compatible fundamental domain $\mathcal{D}$, then with the aid of a certain counting argument as in Section 7 we may appeal to the relative multidimensional Szemerédi theorem (Theorem 5.4).
and prove that $A$ admits an $S$-constellation. It might be a problem of significance to ask whether the counting estimate [8.1] in fact ensures the existence of $S$-constellations; if $n = 1$, then this is closely related to the well-known conjecture of Erdős–Turán (also known as Erdős’s conjecture). Recently, Bloom and Sisask [BS20] have resolved the Erdős–Turán conjecture in the affirmative for the case of three-term arithmetic progressions, namely, the case where $n = 1$ and $S = \{-1, 0, 1\}$. However, to the best of the authors’ knowledge, the problem above seems to be widely open if $\#S \geq 4$ or $n \geq 2$.

In this subsection and Subsection 8.2, we will axiomatize the arguments in Section 7. At the same time, we extend the setting to a more general case; more precisely, we consider a general $a$ rather than the whole $O_K$. Here, a certain argument related to an affine transformation $\text{Aff}_{W,b}$ shows up from the $W$-trick in our construction of pseudorandom measures. To extend the arguments in Section 7 to a general setting of $a$, we need to formulate a suitable generalization of being coprime for $W$ and $b$. Since the mere structure of $\mathbb{Z}$-modules does not suffice for this purpose, we impose an additional structure on the setting of Theorem 5.4. More precisely, we treat a non-zero ideal $a$ of a ring of integers $O_K$, rather than a free $\mathbb{Z}$-module of finite rank, as our ambient space. It suffices to deal with the case of $a = O_K$ for the proofs of Theorem $A$ and Theorem $B$; however, to establish Theorem $C$ in the full generality, we will employ our axiomatizations for a general non-zero ideal $a$, including non-principal ones. Except for Lemma 8.4, the arguments in our axiomatizations for a general $a$ go along exactly the same lines as ones for $O_K$, with no extra complications. Our axiomatization which ensures the existence of $S$-constellations for $A$ with (8.1) (for a large enough $M$) is formulated as the $(\rho, M, v, S)$-condition. The counterpart in the infinite version is described as the family $S_{\Psi_{\log}(a)}$ of subsets of $a$. These two notions will be explained in Definitions 8.2 and 8.3 below.

**Definition 8.2** ($(\rho, M, v, S)$-condition). Assume Setting 8.1. Let $S \subseteq a$ be a standard shape. Let $\rho > 0$, $M \in \mathbb{R}_{\geq 1}$, $D_1, D_2 > 0$, and $\varepsilon \in (0, 1)_{\mathbb{R}}$. A subset $A \subseteq a$ is said to satisfy the $(\rho, M, v, S)$-condition with parameters $(D_1, D_2, \varepsilon)$ if $A \subseteq a(v, M)$, and there exist $W \in \mathbb{N}$ with $W \leq M^{-\varepsilon}$ and $\lambda : a \to \mathbb{R}_{\geq 0}$ such that the following hold.

1. For every $b \in a$ with $bO_K + Wa = a$, the function $\beta \mapsto \varphi_K(W) \lambda(\text{Aff}_{W,b})(\beta)$ on $a$ is a $(\rho, M, W, S)$-pseudorandom measure.

2. There exists $T \subseteq A$ with $\#T \leq M^{\varepsilon n}$ such that, for every $\alpha \in A \setminus T$,

$$D_1 \cdot \log M \leq \lambda(\alpha) \leq D_2 \cdot \log M$$

holds.

3. For the subset $T$ in (2) and for every $\alpha \in A \setminus T$, the equality $\alpha O_K + Wa = a$ holds.

In the three conditions above, (1) corresponds to Theorem 7.4 in the proof of Theorem 2.8 in Section 7. (2) and (3) correspond to Lemma 7.8.

To formulate the infinitary version of the $(\rho, M, v, S)$-condition, dependence between $M$ and $\rho$ is of importance. However, on the data $(D_1, D_2, \varepsilon)$, the only requirement is that they
exist without depending on \( M \); we do not care the exact values of them. For this reason, in Definition 8.2, we divide the seven data into two classes, \((\rho, M, \nu, S)\) and \((D_1, D_2, \epsilon)\), and use the terminology of ‘the \((\rho, M, \nu, S)\)-condition with parameters \((D_1, D_2, \epsilon)\).’ Note also that \( \nu \) and \( S \) are given data.

**Definition 8.3** (The family \( S_{\psi_{\log}}(a) \)). Under Setting 8.1, we define a family \( S_{\psi_{\log}}(a) \) of subsets of \( a \) as follows. For \( A \subseteq a \), we declare that \( A \in S_{\psi_{\log}}(a) \) if for every standard shape \( S \subseteq a \), there exist \( D_1, D_2 > 0 \) and \( \epsilon \in (0,1)_{\mathbb{R}} \) such that the following holds true: for every \( \rho > 0 \), there exists \( M(\rho) = M(\rho, S) \in \mathbb{R} \) such that, for every \( M \geq M(\rho) \), \( A \cap a(\nu, M) \) satisfies the \((\rho, M, \nu, S)\)-condition with parameters \((D_1, D_2, \epsilon)\).

In the symbol ‘\( S_{\psi_{\log}}(a) \)’ above, ‘\( S \)’, ‘\( \psi \)’ and ‘\( \log \)’, respectively, stand for subset, pseudo-random, and having the sparsity of order \( 1/\log \); here, we will show in Lemma 8.5 (2) that the family \( S_{\psi_{\log}}(a) \) is closed under taking subsets. The condition of \( A \in S_{\psi_{\log}}(a) \) is formulated for a fixed \( \mathbb{Z} \)-basis \( \nu \); however, it may be easily seen that this condition does not depend on the choice of \( \nu \).

The condition ‘\( b\mathcal{O}_K + Wa = a' \) on \( b \in a \), which appears in condition (1) and (3) is equivalent to saying that \( b \) is prime to \( W \) when \( a = \mathcal{O}_K \). In view of the following lemma, the condition above may be seen as a natural generalization of the coprime condition to the case of general \( a \).

**Lemma 8.4.** Let \( a \in \text{Ideals}_K \) and let \( W \in \mathbb{N} \). Then the image of the set \( \{ b \in a : b\mathcal{O}_K + Wa = a \} \) under the natural projection \( a \to a/Wa \) has cardinality \( \varphi_K(W) \).

**Proof.** Apply Lemma 3.12 with \( b = W\mathcal{O}_K \); this yields an isomorphism \( a/Wa \cong \mathcal{O}_K/W\mathcal{O}_K \) as \( \mathcal{O}_K \)-modules. An element \( \gamma \in \mathcal{O}_K/W\mathcal{O}_K \) belongs to \( (\mathcal{O}_K/W\mathcal{O}_K)^\times \) if and only if it generates \( \mathcal{O}_K/W\mathcal{O}_K \) as an \( \mathcal{O}_K \)-module. For \( b \in a \), the equality \( b\mathcal{O}_K + Wa = a \) holds if and only if \( \overline{b} \) generates \( a/Wa \) as an \( \mathcal{O}_K \)-module, where \( \overline{b} \) is the image of \( b \) under \( a \to a/Wa \). Combination of these observations ends the proof.

**Lemma 8.5** (Hereditry to subsets). The following hold true.

1. If \( A \subseteq a(\nu, M) \) satisfies the \((\rho, M, \nu, S)\)-condition with parameters \((D_1, D_2, \epsilon)\), and \( A_1 \subseteq A \), then \( A_1 \) satisfies the \((\rho, M, \nu, S)\)-condition with parameters \((D_1, D_2, \epsilon)\).
2. If \( A \in S_{\psi_{\log}}(a) \) and \( A_1 \subseteq A \), then \( A_1 \in S_{\psi_{\log}}(a) \).

**Proof.** First we will prove (1). For \( A_1 \), we employ \( W \) and \( \lambda \) exactly the same as those for \( A \). Let \( T \) be an exceptional set for \( A \), meaning that \( T \) satisfies conditions (2) and (3). Then \( T_1 := T \cap A_1 \) is an exceptional set for \( A_1 \). Hence (1) holds. Item (2) immediately follows from (1).

The following theorem provides a motivating example of a member of the family \( S_{\psi_{\log}}(\mathcal{O}_K) \).

**Theorem 8.6.** The subset \( \mathcal{P}_K \) of prime elements of a number field \( K \) satisfies that \( \mathcal{P}_K \in S_{\psi_{\log}}(\mathcal{O}_K) \).
Furthermore, for every \( \alpha \) is sufficiently large depending on \( r \) (3) work without any change. More precisely, the following two statements hold true: if \( M \) to show that this \( T \) does the job, first recall the proof of Lemma 7.8. The proofs of (2) and (3) work without any change. More precisely, the following two statements hold true: if \( M \) is sufficiently large depending on \( \rho \) and \( S \), then the following holds true: for every \( b \in \mathcal{O}_K \) prime to \( W \), the function \( \bar{\lambda}_b := \frac{\varepsilon_{K}(W)}{W} (\lambda \circ \text{Aff}_{W,b}) \) is a \((\rho, M/W, S)\)-pseudorandom measure. By (7.6), we have \( W \leq M^{\frac{3}{4}} \).

Finally, we will bound \#T from above; this argument is similar to the proof of Lemma 7.8(1), but we need an extra argument because we do not restrict ourselves inside an \( \mathcal{O}_K^\times \)-fundamental domain. Proposition 3.20 implies that if \( M \) is sufficiently large depending on \( r \), then the number of non-zero ideals of \( \mathcal{O}_K \) whose ideal norms are at most \( R \) does not exceed \( 2\kappa R \). In particular, this bound holds for the number of non-zero principal ideals with the same condition. Consider the map \( \alpha \mapsto \alpha \mathcal{O}_K \), which sends a non-zero element to a non-zero principal ideal. The key here is Lemma 4.14(2): for each non-zero principal ideal of \( \mathcal{O}_K \), the number of \( \alpha \in \mathcal{O}_K(\omega, M) \) which is sent to this ideal by the map above is at most \( \Xi' \cdot (\log M)^{n-1} \). Here \( \Xi' = \Xi'(\omega) > 0 \) is the constant appearing in Lemma 4.14(2). Indeed, notice that \( r_1 + r_2 \leq n \), where \( r_1 \) and \( r_2 \) are as in Setting 4.1.

Therefore, we have that
\[
\#T \leq \Xi' \cdot (\log M)^{n-1} \cdot (2\kappa R).
\]

If \( M \) is sufficiently large depending on \( \omega \), then \( R \leq \frac{1}{2\pi \Xi} \cdot \frac{M^{\frac{1}{n}}}{(\log M)^{n-1}} \) holds. In this case, we conclude that
\[
\#T \leq M^{\frac{1}{n}} \leq M^{\frac{3}{2n}}.
\]

For a given \( \rho > 0 \), consider the case where \( M \) is sufficiently large depending on \( \rho, \omega \) and \( S \); we write this situation as \( M \geq M_{\mathcal{P}_K, S\Psi_{\log}}(\rho, \omega, S) \) for future use. To summarize our proof, we have showed that \( \mathcal{P}_K \cap \mathcal{O}_K(\omega, M) \) satisfies the \((\rho, M, \omega, S)\)-condition with parameters
\[
(D_1, D_2, \varepsilon) = \left( \frac{\kappa}{17(r + 1)2^r \cdot c \chi}, \frac{\kappa}{17(r + 1)2^r \cdot c \chi}, \frac{3}{4} \right).
\]

It ends our proof.

As in the proof above, in the case where \( A \) is not inside an \( \mathcal{O}_K^\times \)-fundamental domain, then the map \( A \ni \alpha \mapsto \alpha \mathcal{O}_K \in \text{Ideals}_K \) is not injective in general. Then, we need to take into account the contribution of the action of the group of units in order to transfer ideal countings to element countings. To treat this, Lemma 4.14 is a key tool, as we have seen in the deduction of (8.2) in the above proof.
8.2 Axiomatization for constellation theorems of type 1

In this subsection, we establish axiomatizations for constellation theorems of type 1 with the aid of the \((\rho, M, v, S)\)-condition and \(S\Psi_{\log}(a)\) introduced in Subsection 8.1. Here exhibit the two statements: one is the finitary version and the other is the infinitary version. Recall the definition of \(N_S(A)\) from Definition 2.3 (2).

**Theorem 8.7.** Assume Setting \([8.1]\) Let \(\delta > 0, D_1, D_2 > 0, \varepsilon \in (0,1)\). Then there exist \(\rho = \rho_1(D_1, v, \delta, S) > 0\) and \(M_1 = M_1(D_1, D_2, \varepsilon, v, \delta, S) \in \mathbb{N}\) such that the following holds true. Assume that \(M \in \mathbb{N}\) with \(M \geq M_1\) and \(A \subseteq a(v, M)\) satisfies the following two conditions:

(i) the cardinality \(#A\) satisfies

\[ #A \geq \delta \cdot \frac{M^n}{\log M}, \tag{8.4} \]

(ii) \(A\) satisfies the \((\rho, M, v, S)\)-condition with parameters \((D_1, D_2, \varepsilon)\).

Then \(A\) contains an \(S\)-constellation. Furthermore, let \(W\) be as in the \((\rho, M, v, S)\)-condition. Then there exists \(\gamma = \gamma_1(D_1, D_2, v, \delta, S) > 0\) such that

\[ N_S(A) \geq \gamma \cdot \left( \frac{M}{W} \right)^{n+1} (\log M)^{-(r+1)} \tag{8.5} \]

holds.

**Theorem 8.8.** Assume Setting \([8.1]\) Assume that a subset \(A \subseteq a\) satisfies the following two conditions:

(i) the inequality

\[ \limsup_{M \to \infty} \frac{#(A \cap a(v, M))}{M^n(\log M)^{-1}} > 0 \tag{8.6} \]

holds,

(ii) \(A \in S\Psi_{\log}(a)\).

Then for every finite subset \(S \subseteq a\), there exists an \(S\)-constellation in \(A\).

In Theorem \([8.7]\) the first condition is that on countings, and the second condition is a condition which inherits to subsets; recall Lemma \([8.5]\) The same holds true for the two conditions in Theorem \([8.8]\). The existence of a constellation no way inherits to subsets. Nevertheless, in the proof of constellation theorems, we can decompose our criteria into the following two parts: conditions on mere countings, and conditions related to pseudorandomness, which inherit to subsets. In this manner, we may have a clear description of the proofs. For instance, Theorem \([8.8]\) yields the following relative Szemerédi-type theorem. To state it, we extend the definition of the relative asymptotic density in Definition \([2.9]\) (2) in the following manner.
Definition 8.9. Let $Z$ be a free $\mathbb{Z}$-module $\mathbb{Z}$ of finite rank and $\mathbf{v}$ a $\mathbb{Z}$-basis. For a non-empty set $X \subseteq Z$ and a subset $A \subseteq X$, define the relative upper asymptotic density of $A$ with respect to $X$ measured by $\| \cdot \|_{\infty, \mathbf{v}}$ as

$$d_{X, \mathbf{v}}(A) := \limsup_{M \to \infty} \frac{\#(A \cap Z(\mathbf{v}, M))}{\#(X \cap Z(\mathbf{v}, M))}.$$ 

The relative lower asymptotic density of $A$ with respect to $X$ measured by $\| \cdot \|_{\infty, \mathbf{v}}$ is also defined as

$$d_{X, \mathbf{v}}(A) := \liminf_{M \to \infty} \frac{\#(A \cap Z(\mathbf{v}, M))}{\#(X \cap Z(\mathbf{v}, M))}.$$ 

Corollary 8.10. Assume Setting 8.1. Assume that a subset $A \subseteq a$ satisfies the following two conditions:

(i) the inequality

$$\liminf_{M \to \infty} \frac{\#(A \cap a(\mathbf{v}, M))}{M^n(\log M)^{-1}} > 0 \quad (8.7)$$

holds,

(ii) $A \in S_{\Psi_{\log}(a)}$.

Then for every subset $A' \subseteq A$ with $d_{A, \mathbf{v}}(A') > 0$, the following holds: for every finite subset $S$, $A'$ contains an $S$-constellation.

Proof of “Theorem 8.8 $\implies$ Corollary 8.10”. Suppose $A' \subseteq A$ and $d_{A, \mathbf{v}}(A') > 0$. By Lemma 8.5 (ii), we have $A' \in S_{\Psi_{\log}(a)}$. The set $A'$ satisfies (8.6) with $A$ replaced by $A'$. Therefore, we can apply Theorem 8.7 with replacing $A$ by $A'$.

Theorem 8.8 is deduced from Theorem 8.7 in the following manner.

Proof of “Theorem 8.7 $\implies$ Theorem 8.8”. Let $A \subseteq a$ be a subset fulfilling the two conditions in Theorem 8.8. Take an arbitrary standard shape $S \subseteq a$. Since $A \in S_{\Psi_{\log}(a)}$, we can take parameters $(D_1, D_2, \varepsilon)$ associated with $S$. Set $\delta > 0$ as the left-hand side of (8.6): if the left-hand side is $+\infty$, then set $\delta = 2$. By Theorem 8.7, there exist $\rho = \rho(D_1, \mathbf{v}, \delta/2, S) > 0$ and $M_1 = M_1(D_1, D_2, \varepsilon, \mathbf{v}, \delta/2, S) \in \mathbb{N}$. Then since $A \in S_{\Psi_{\log}(a)}$, there exist $M(\rho, \mathbf{v}, S)$ as in Definition 8.3 and a positive integer $M$ at least $M_1$ such that the following hold true: we have

$$\#(A \cap a(\mathbf{v}, M)) \geq \frac{\delta}{2} \cdot \frac{M^n}{\log M},$$

and $A \cap a(\mathbf{v}, M)$ satisfies the $(\rho, M, \mathbf{v}, S)$-condition with parameters $(D_1, D_2, \varepsilon)$. Therefore, Theorem 8.7 applies to $A \cap a(\mathbf{v}, M)$, and we can find an $S$-constellation in $A$. As $S$ is arbitrarily taken, this ends our proof.

It remains to prove Theorem 8.7. The following proof is motivated by the proofs of Proposition 7.9 and Theorem 7.10.
Proof of Theorem 8.7. Let $S$, $\delta$, $D_1$, $D_2$ and $\varepsilon$ be as in the statement. Let $M$ be a real parameter; we will take it sufficiently large. Take an arbitrary $\rho > 0$.

Let $A \subseteq a(v, M)$ be a set which satisfies (8.4) and which fulfills the $(\rho, M, v, S)$-condition with parameters $(D_1, D_2, \varepsilon)$; take $W \leq M^\varepsilon$, $\lambda: a \to \mathbb{R}_{\geq 0}$ as above and $T \subseteq A$ associated to $A$. Trim $A$ as $A' := A \setminus T$. First, we count $A'$ from below. For a sufficiently large $M$ depending on $\varepsilon$ and $\delta$, we have

$$\#T \leq M^{\varepsilon n} \leq \frac{\delta}{2} \cdot \frac{M^n}{\log M}.$$ 

Hence by (8.4) the inequality

$$\#A' \geq \frac{\delta}{2} \cdot \frac{M^n}{\log M}$$

holds.

In what follows, we will verify that Theorem 5.4 applies to $A'$, provided that $M$ is sufficiently large. By the $(\rho, M, v, S)$-condition (3) and by Lemma 8.4, the cardinality of the image of $A'$ under the natural projection $a \to a/Wa$ is at most $\varphi_K(W)$. The pigeonhole principle tells us that there exists $b \in a/Wa$ such that

$$\#(A' \cap b) \geq \frac{1}{\varphi_K(W)} \cdot \#A'.$$

Here we regard $b$ as a subset of $a$. Combine this with (8.8), and obtain that

$$\#(A' \cap b) \geq \frac{1}{2\varphi_K(W)} \cdot \frac{M^n}{\log M}.$$ 

Set a positive integer $N$ from $M$ and $W$ by $N := \ceil{\frac{M}{W}}$. Since $W \leq M^\varepsilon$, we have

$$M^{1-\varepsilon} \leq N \leq \frac{2M}{W}.$$ 

Choose a representative $b \in \tilde{b}$ in such a way that $\|b\|_{\infty,v} < W$. Since $A' \cap \tilde{b} \neq \emptyset$, we have $bO_K + Wa = a$ by the $(\rho, M, v, S)$-condition (3). By the definition of $N$ and by the triangle inequality, we have

$$\text{Aff}_{W,b}(a(v, N)) \supseteq a(v, M) \cap (Wa + b) \supseteq A' \cap \tilde{b}.$$ 

This implies that $B := \text{Aff}_{W,b}^{-1}(A' \cap \tilde{b})$ is a subset of $a(v, N)$. For this $B$, by (8.9), we have that

$$\#B \geq \frac{1}{2\varphi_K(W)} \cdot \frac{M^n}{\log M}.$$ 

Define $\tilde{\lambda}: a \to \mathbb{R}_{\geq 0}$ by $\tilde{\lambda} := \frac{\varphi_K(W)}{W^n}(\lambda \circ \text{Aff}_{W,b})$. By the $(\rho, M, v, S)$-condition (1), this $\tilde{\lambda}$ is a $(\rho, N, S)$-pseudorandom measure. Furthermore, by the estimate from below in the
$(\rho, M, v, S)$-condition \cite{2} and by (8.11) and (8.10), we have the following estimate of the weighted density:

$$
\mathbb{E}(1_B \cdot \lambda | a(v, N)) \geq \left( \frac{1}{2\varphi_K(W)} \right) \delta \frac{M^n}{\log M} \cdot \left( \frac{\varphi_K(W)}{W^n} D_1 \cdot \log M \right) \cdot (2N + 1)^{-n}
$$

\begin{equation}
\geq \frac{D_1}{2} \cdot \left( \frac{M}{3WN} \right)^n \geq \frac{D_1}{2} \cdot 6^n \cdot \delta;
\end{equation}

it ensures the weighted density condition in the relative multidimensional Szemerédi theorem. On the smallness condition, we employ (8.10) and the estimate from above in the $(\rho, M, v, S)$-condition \cite{2}. Then, we have that

$$
\frac{1}{N} \cdot \mathbb{E}(1_B \cdot \lambda^{r+1} | a(v, N)) \leq D_2^{r+1} \cdot \frac{(\log M)^{r+1}}{M^{1-\varepsilon}},
$$

where $r := \#S - 1$.

Finally, we specify $\rho > 0$ and $M_1$ so as to activate Theorem 5.4. We set $\rho = \rho_1(D_1, v, \delta, S) := \rho_{\text{RMS}}(v, \frac{D_1}{26^n} \delta, S)$. Also, set $\gamma'_1 = \gamma'_1(D_1, v, \delta, S) > 0$ as $\gamma'_1 := \gamma_{\text{RMS}}(v, \frac{D_1}{26^n} \delta, S)$. The arguments in the current proof up to this point work for a sufficiently large $M$ depending on $\varepsilon$ and $\delta$; if necessary, we replace $M$ with a larger number depending on $D_1$, $D_2$, $\varepsilon$, $v$, $\delta$ and $S$ in such a way that

$$
D_2^{r+1} \cdot (\log M)^{r+1} \leq \gamma'_1 \cdot M^{1-\varepsilon}
$$

holds true. Set $M_1$ as the smallest positive integer which satisfies the inequality above.

Then, we may appeal to the relative multidimensional Szemerédi Theorem (Theorem 5.4); indeed, by (8.12) and (8.13), if $M \geq M_1$, then it applies to $B \subseteq a(v, N)$. Therefore, there exists an $S$-constellation in $B$. Since $\text{Aff}_{W,b}(B) \subseteq A' \subseteq A$, we can find an $S$-constellation in $A$.

Finally, we make an estimate of $\mathcal{K}_S(A)$. By Theorem 5.5 and the estimate from above in the $(\rho, M, v, S)$-condition \cite{2}, we have that

$$
\frac{1}{N(2N + 1)^n} \cdot \mathcal{K}_S(B) \cdot (D_2 \log M)^{r+1} \geq \gamma'_1.
$$

Hence, by setting $\gamma_1 = \gamma_1(D_1, D_2, S, \delta, v)$ as $\gamma_1 := 2^nD_2^{-(r+1)}\gamma'_1$, we obtain that

$$
\mathcal{K}_S(B) \geq \gamma_1 \cdot N^{n+1}(\log M)^{-r+1} \geq \gamma_1 \cdot \left( \frac{M}{W} \right)^{n+1} (\log M)^{-(r+1)}.
$$

Since $\mathcal{K}_S(B) \leq \mathcal{K}_S(A') \leq \mathcal{K}_S(A)$, this ends our proof.

\[\square\]

**Remark 8.11.** The estimate from above in the $(\rho, M, v, S)$-condition \cite{2} is stated as the order of $\log M$. On the existence part of Theorem 8.7, we may relax this order; for instance, under $W \leq M^{\varepsilon}$, we can take the order of $o_{M \to \infty}(M^{\varepsilon+1})$. However, if we raise the order of this estimate from above, then the estimate of $\mathcal{K}_S(A)$ in Theorem 8.7 becomes worse. Examples appearing in the present paper have the estimate from above in the $(\rho, M, v, S)$-condition \cite{2} with the order of $\log M$; see for instance Theorem 8.6.
In the last part of this subsection, we will prove Theorem 8.13 below as an application of Theorem 8.7. For the proof, we employ the following counting from below.

**Proposition 8.12.** Let \( \omega \) be an integral basis of \( K \). Then there exist \( C_{P_{K,1}}(\omega) > 0 \) and a positive integer \( M_{P_{K,1}}(\omega) \) such that for every \( M \geq M_{P_{K,1}}(\omega) \), the inequality

\[
\#(P_K \cap O_K(\omega, M)) \geq C_{P_{K,1}}(\omega) \cdot \frac{M^n}{\log M}
\]  

holds. In particular, for \( a = O_K \), the set \( A = P_K \) fulfills the two conditions \([i], \[ii]\) of Corollary 8.10.

**Proof.** First we will show (8.14). Take an NL-compatible \( O_K \times K \)-fundamental domain \( D \); such a \( D \) exists by Proposition 4.11. Proposition 7.7 provides a constant \( \tilde{C} = \tilde{C}(\omega, D) > 0 \) depending on \( \omega \) and \( D \) such that for sufficiently large \( M \), the inequality

\[
\#(P_K \cap D \cap O_K(\omega, M)) \geq \tilde{C} \cdot M^n
\]

holds. Then we obtain (8.14) by observing that \( P_K \cap D \subseteq P_K \). The rest of the statement of Proposition 8.12 now immediately follows from (8.14) and Theorem 8.6.

Theorem 8.13 is a type 1 version of Theorem A, that means, we do not go into the point whether an \( S \)-constellation admits an associate pair. We will present the full proof of Theorem A in the latter part of the present section; for this, we will develop axiomatizations for constellation theorems of type 2. Note that, by Proposition 8.12, Corollary 8.10 implies the infinitary version of Theorem 8.13. For the reader’s convenience, we sketch the proof of Theorem 8.13 itself.

**Theorem 8.13.** Let \( K \) be a number field of degree \( n \), and \( \omega \) an integral basis of \( K \). Let \( S \subseteq O_K \) be a standard shape. Let \( \delta > 0 \). Then the following hold:

1. There exists a positive integer \( M_{PES,1} = M_{PES,1}(\omega, \delta, S) \) depending only on \( \omega \), \( \delta \) and \( S \) such that the following holds true: if \( M \geq M_{PES,1} \) and if a subset \( A \) of \( P_K \cap O_K(\omega, M) \) satisfies

\[
\#A \geq \delta \cdot \#(P_K \cap O_K(\omega, M)),
\]

then there exists an \( S \)-constellation in \( A \).

2. There exist a constant \( \gamma = \gamma_{PES,1}(\omega, \delta, S) > 0 \) and \( M_{PES,1} = M_{PES,1}(\omega, \delta, S) \) depending only on \( \omega \), \( \delta \) and \( S \) such that the following holds true: if \( M \geq M_{PES,1} \) and if a subset \( A \) of \( P_K \cap O_K(\omega, M) \) satisfies (8.15), then

\[
\mathcal{N}_S(A) \geq \gamma \cdot M^{n+1} \log M)^{-(\#S+a_{M \rightarrow \infty, n}(1))}
\]

holds.
Proof. First, we will prove (1). Set \( f \) as in Setting 7.2. Set \( D := \kappa \cdot (17(r + 1)2^r \cdot c_\chi)^{-1} \). 
Set \( \rho := \rho_l(D, \omega, \delta \cdot C_{\mathcal{P},1}(\omega), S) \) and
\[
M_{\mathcal{P},1} := \max \{ M_{\mathcal{P},1}(\omega), M_{\mathcal{P},s \Psi_{\log}}(\rho, \omega, S), M_l(D, D, 3/4, \omega, \delta \cdot C_{\mathcal{P},1}(\omega), S) \}. \tag{8.16}
\]
Here, \( M_{\mathcal{P},s \Psi_{\log}}(\rho, \omega, S) \) is defined in the proof of Theorem 8.6. Then, for \( M \geq M_{\mathcal{P},1} \) and for \( A \subseteq \mathcal{P}_K \cap \mathcal{O}_K(\omega, M) \) with \( \#A \geq \delta \cdot \#(\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)) \), Proposition 8.12 implies that \( \#A \geq \delta \cdot C_{\mathcal{P},1}(\omega) \cdot M^n \log M \).

Hence by Lemma 8.5 (1), the proof of Theorem 8.6 implies that \( A \) satisfies the \((\rho, M, \omega, S)\)-condition with parameters \((D, D, 3/4, \omega, \delta \cdot C_{\mathcal{P},1}(\omega), S)\). Therefore, Theorem 8.7 applies to \( A \), and we can find an \( S \)-constellation in \( A \).

Finally, to prove (2), in this case, set \( f(t) = \frac{1}{2} \log^{\alpha_3} t \) in Setting 7.2. Then, for this \( f \), define \( M_{\mathcal{F},I} \) by (8.16), and let
\[
\gamma_{\mathcal{F},I}(\omega, \delta, S) := \gamma_I(D, D, \omega, \delta \cdot C_{\mathcal{P},1}(\omega), S).
\]
where \( \gamma_I \) is as in Theorem 8.7. Suppose \( M \geq M_{\mathcal{F},1} \). Then, using the parameter \( W \) as in the definition of the \((\rho, M, \omega, S)\)-condition, we have (8.5). In the current setting, by (7.3), we have \( W \leq \log^{\alpha_2} M \). Therefore, we obtain the desired estimate of \( \mathcal{N}_S(A) \).

8.3 Counting prime elements from above

In Subsection 8.4, we will upgrade Theorem 8.13 to its type 2 version, Theorem A. The key to this upgrading is a counting of prime elements from above. In this subsection, as a prototype of this counting, we will make an estimate of \( \#(\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)) \) from above; see also Remark 8.16.

Proposition 8.14. Let \( \omega \) be an integral basis of \( K \). Then there exist a constant \( C_{\mathcal{P},1}(\omega) > 0 \) and a positive integer \( M_{\mathcal{P},1}(\omega) \) such that for every \( M \geq M_{\mathcal{P},1}(\omega) \), the inequality

\[ \#(\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)) \leq C_{\mathcal{P},1}(\omega) \cdot \frac{M^n}{\log M} \]

holds true.

The following lemma will be employed in the proof of Proposition 8.14. Recall the definition of the logarithmic integral \( \text{Li} \) from (3.9).

Lemma 8.15. For every \( k \in \mathbb{Z}_{\geq 0} \), there exists a constant \( C_{\text{Li}}(k) > 0 \) such that for every \( L, \eta \in \mathbb{R}_{\geq 2} \), the inequalities
\[
\int_2^L \frac{1}{\log t} \left\{ \log \left( \frac{\eta L}{t} \right) \right\}^k dt \leq C_{\text{Li}}(k) \cdot (\log \eta)^k \cdot \frac{L}{\log L} \tag{8.17}
\]
and
\[ \int_2^L \frac{1}{\log t} \left\{ \log \left( \frac{L}{t} \right) \right\}^k dt \leq C_{\text{Li}}(k) \cdot \frac{L}{\log L} \] (8.18)
hold true.

Proof. First, we will prove (8.17) by induction on \( k \). For \( k = 0 \), this follows from (3.9). Now we proceed to the induction step. We will reduce the assertion for \( k \geq 1 \) to that for \( k - 1 \).

By integration by parts, we have that
\[ \int_2^L \frac{1}{\log t} \left\{ \log \left( \frac{\eta L}{t} \right) \right\}^k dt = \text{Li}(L) \cdot (\log \eta)^k + k \cdot \int_2^L \frac{\text{Li}(t)}{t} \left\{ \log \left( \frac{\eta L}{t} \right) \right\}^{k-1} dt. \]

By noting that \((\log \eta)^k \geq (\log 2)(\log \eta)^{k-1}\), we can make the desired reduction; recall also (3.9). Therefore, (8.17) holds.

Next we will prove (8.18). Apply (8.17) with \( \eta = e > 2 \), and obtain
\[ \int_2^L \frac{1}{\log t} \left\{ \log \left( \frac{eL}{t} \right) \right\}^k dt \leq C_{\text{Li}}(k) \cdot \frac{L}{\log L}. \]
Since \( \int_2^L \frac{1}{\log t} \left\{ \log \left( \frac{\eta L}{t} \right) \right\}^k dt \geq \int_2^L \frac{1}{\log t} \left\{ \log \left( \frac{L}{t} \right) \right\}^k dt \), we conclude (8.18). \( \square \)

Proof of Proposition 8.14. Let \( r_1 \) and \( r_2 \) be the numbers, respectively, of real embeddings and of imaginary embeddings. Let \( k := r_1 + r_2 - 1 \). Take the constant \( \Xi = \Xi(\omega) > 0 \) as in Lemma 4.14 (1) in such a way that \( C' \leq \Xi \), where \( C' = C'(\omega) \) is as in (NLC). In particular, for every \( \pi \in \mathcal{P}_K \cap \mathcal{O}_K(\omega, M) \), we have \( N(\pi) \in [2, \Xi M^n] \cap \mathbb{Z} \). For each \( t \in \mathbb{Z}_{\geq 2} \), set
\[ p_K(t) := \# \{ p \in |\text{Spec}(\mathcal{O}_K)|^{\text{PI}} : N(p) = t \}, \]
and for every \( L \in \mathbb{R}_{\geq 2} \), define
\[ P_K(L) := \sum_{t \in [2, L]\cap \mathbb{Z}} p_K(t). \]

By Landau’s prime ideal theorem (Theorem 3.21), there exists \( C_{\text{Lan}} = C_{\text{Lan}}(K) > 0 \) such that for every \( L \in \mathbb{R}_{\geq 2} \),
\[ P_K(L) \leq C_{\text{Lan}} \cdot \frac{L}{\log L} \] (8.19)
holds true; this rough estimate suffices for the present proof. If \( k = 0 \), in other words, if \( \#(\mathcal{O}_K^\text{K}) < \infty \), then (8.19) already provides the desired estimate. In what follows, we treat the case where \( k \geq 1 \).

Focus on the map \( \mathcal{P}_K \cap \mathcal{O}_K(\omega, M) \ni \pi \mapsto \pi \mathcal{O}_K \in |\text{Spec}(\mathcal{O}_K)|^{\text{PI}} \). By considering the multiplicities of this map, we derive the following inequality from Lemma 4.14 (1):
\[ \#(\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)) \leq \Xi \cdot \sum_{t \in [2, \Xi M^n] \cap \mathbb{Z}} p_K(t) \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^k. \]
By Abel’s summation formula (see [HW08, Theorem 421]), this implies that
\[
\#(P_K \cap \mathcal{O}_K(\omega, M)) \leq k \Xi \cdot \int_{2}^{\Xi M^n} \frac{P_K(t)}{t} \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^{k-1} dt.
\]

Recall (8.19), and apply (8.18) with \( k \) replaced by \( k - 1 \) and with \( L = \Xi M^n \). Then, we obtain the desired estimate for the case of \( k \geq 1 \). It completes our proof.

**Remark 8.16.** Proposition 8.12 together with Proposition 8.14 asserts that
\[
0 < \lim_{M \to \infty} \inf \frac{\#(P_K \cap \mathcal{O}_K(\omega, M))}{M^n(\log M)^{-1}} \quad \text{and} \quad \lim_{M \to \infty} \sup \frac{\#(P_K \cap \mathcal{O}_K(\omega, M))}{M^n(\log M)^{-1}} < \infty
\]
for a fixed \( \omega \). If we appeal to Mitsui’s generalized prime number theorem [Mit56], then we can deduce that \( \liminf \) and \( \limsup \), in fact, coincide in the inequalities above. See [KRE20, Theorem 2, 3] for the details of this deduction. However, as we mentioned at the beginning of this section, in the present paper we do not need this precise piece of information on the multiplicative constants associated with the main term. Indeed, the following two are the keys to our counting arguments: the strict positivity of \( \liminf \), and the order inequality (8.19) derived from Theorem 8.21. For instance, conditions (i) and (ii) in Corollary 8.22 exactly correspond to these two points.

### 8.4 Reduction to the case of fixing a fundamental domain

By examining the proof and the estimate of Proposition 8.14 we are able to reduce the setting of Theorem A to that of fixing an \( \mathcal{O}_K \)-fundamental domain. We explain this reduction in the present subsection. Furthermore, in this manner, we present our axiomatization for constellation theorems of type 2; recall that those mean theorems that ensure the existence of constellations without associate pairs. Recall also that for \( a \in \text{Ideals}_K \), we have introduced the equivalence relation, of being associate, on \( a \setminus \{0\} \) induced by the action \( \mathcal{O}_K^\times \curvearrowright a \setminus \{0\} \) by multiplication. The key theorem for this axiomatization is Theorem 8.19, the axiomatizations for type 2 in this subsection are presented in Theorem 8.20 (finitary version) and Theorem 8.21 (infinitary version). With the aid of them, Theorem A and Theorem 1.4 will be established.

**Lemma 8.17.** Assume Setting 8.1. Let \( \Omega > 0 \) and \( M \in \mathbb{R}_{\geq 1} \). Assume that \( A \subseteq a(\upsilon, M) \setminus \{0\} \) satisfies
\[
\#(A \setminus \mathcal{O}_K(\Omega M^n)) \geq \frac{1}{2} \cdot \#A.
\]

Then there exist a constant \( c_{\Omega, \upsilon} \in (0, 1]_{\mathbb{R}} \), depending only on \( \Omega, \upsilon \), and a subset \( A_0 \subseteq A \setminus \mathcal{O}_K(\Omega M^n) \) such that the following hold true:

1. \( \#A_0 \geq c_{\Omega, \upsilon} \cdot \#A \),
2. the subset \( A_0 \) admits no associate pairs.
Proof. Let \( k := r_1 + r_2 - 1 \) be the rank of \( \overline{O}_K^r \). Take \( \Xi = \Xi(v) > 0 \) as in Corollary 4.16 (1). Then, for every \( \alpha \in a(v, M) \setminus \{0\} \cup O_K(\Omega M^n) \), there exist at most \( \Xi \cdot \left\{ \log \left( \frac{\Xi}{\Omega} \right) \right\}^k \) elements in \( a(v, M) \setminus \{0\} \) which are associate to \( \alpha \). Set

\[
c_{\Omega, v} := \frac{1}{2\Xi} \cdot \left\{ \log \left( \frac{\Xi}{\Omega} \right) \right\}^{-k}.
\]

Consider the quotient set of \( A \setminus O_K(\Omega M^n) \) by the equivalence relation of being associate. Take a complete system of representatives for this, and write \( A_0 \) for it. Then, under (8.20), we have (1) with the constant \( c_{\Omega, v} \) as defined above. By construction of \( A_0 \), (2) also holds. We remark that Lemma 8.17 (2) may be rephrased as follows: there exists a fundamental domain \( D \) for the action \( O_K \rtimes a \{0\} \) such that \( A_0 \subseteq A \cap D \) holds. Also (1) asserts that the counting in \( A \) is comparable to that in \( A_0 \), as long as \( \Omega \) is fixed. Hence, in order to reduce the general case of \( A \) to that of fixing a fundamental domain, it suffices to find \( \Omega > 0 \) for \( A \) in a certain controlled way.

The following proposition provides a criterion on \( A \) for which such a controlled constant \( \Omega > 0 \) exists.

**Proposition 8.18.** Assume Setting 8.1. Let \( \delta > 0 \) and \( \Delta > 0 \). Then, there exist a constant \( \Omega = \Omega_{\text{red}}(v, \delta, \Delta) > 0 \) and a positive integer \( M_{\text{red}} = M_{\text{red}}(v, \delta, \Delta) \) such that for all \( M \geq M_{\text{red}} \), the following holds true: if \( A \subseteq a(v, M) \setminus \{0\} \) satisfies that

\[
\text{for all } L \in \mathbb{R}_{\geq 2}, \quad \# \{ \alpha O_K \in \text{Ideals}_K : \alpha \in A \cap O_K(L) \} \leq \Delta \cdot \frac{L}{\log L}, \tag{8.21}
\]

then we have

\[
\#(A \cap O_K(\Omega M^n)) \leq \delta \cdot \frac{M^n}{\log M}. \tag{8.22}
\]

Note that in the counting in (8.21), we count ideals instead of the elements themselves.

**Proof.** Let \( k := r_1 + r_2 - 1 \) be the rank of \( \overline{O}_K^r \). For \( k = 0 \), we can set

\[
\Omega := \frac{\delta n}{2 \# \mu(K) \cdot \Delta}.
\]

Indeed, (8.21) directly ensures (8.22); note that for a sufficiently large \( M \) depending on \( \delta, \Delta \) and \( K \), we have \( \Omega M^n \geq M^{n/2} \).

Hence, in what follows, we focus on the case of \( k \geq 1 \); in particular, we have \( n \geq 2 \) in this case. We will generalize the argument of the proof of Proposition 8.14 in the following manner. For each \( t \in \mathbb{N} \), define \( h_A(t) := \# \{ \alpha O_K \in \text{Ideals}_K : \alpha \in A, \ N(\alpha) = t \} \), and for each \( L \in \mathbb{R}_{\geq 1} \), set \( H_A(L) := \sum_{t \in [1, L] \cap \mathbb{Z}} h_A(t) \). Then, assumption (8.21) is equivalent to saying that

\[
\text{for all } L \in \mathbb{R}_{\geq 2}, \quad H_A(L) \leq \Delta \cdot \frac{L}{\log L}. \tag{8.23}
\]
Take a constant \( \Xi = \Xi(v) \) as in Corollary 4.16 (1) with \( \Xi \geq 2 \). Take a parameter \( \theta \in (0,1) \); we will indicate its value later. Then, Corollary 4.16 (1) implies that

\[
#(A \cap \mathcal{O}_K(\theta M^n)) \leq \Xi \cdot \sum_{t \in [1,\theta M^n] \cap \mathbb{Z}} h_A(t) \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^k
\]

\[
\leq \Xi \cdot \left( \{ \log(\Xi M^n) \}^k + \sum_{t \in [2,\theta M^n] \cap \mathbb{Z}} h_A(t) \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^k \right). \quad (8.24)
\]

Indeed, note that \( h_A(1) \leq 1 \). Since \( \{ \log(\Xi M^n) \}^k \), as a function of \( M \), has a smaller order than \( M^n / \log M \), we have that for a sufficiently large \( M \) depending on \( v \),

\[
\Xi \cdot \{ \log(\Xi M^n) \}^k \leq \frac{1}{2} \delta \cdot \frac{M^n}{\log M}. \quad (8.25)
\]

In what follows, we will make estimates of \( \sum_{t \in [2,\theta M^n] \cap \mathbb{Z}} h_A(t) \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^k \) appearing in (8.24).

By Abel’s summation formula, we have that

\[
\sum_{t \in [2,\theta M^n] \cap \mathbb{Z}} h_A(t) \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^k
\]

\[
\leq H_A(\theta M^n) \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^k + k \cdot \int_{2}^{\theta M^n} \frac{H_A(t)}{t} \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^{k-1} dt.
\]

By assumption (8.23), the value \( \sum_{t \in [2,\theta M^n] \cap \mathbb{Z}} h_A(t) \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^k \) does not exceed the following:

\[
\Delta \cdot \frac{\theta M^n}{\log(\theta M^n)} \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^k + k \Delta \cdot \int_{2}^{\theta M^n} \frac{1}{\log t} \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^{k-1} dt.
\]

The second term is estimated as follows: apply (8.17) with \( k \) replaced by \( k - 1 \) and with \( \eta = \Xi / \theta \) and \( L = \theta M^n \). Then, with the constant \( C = k C_{\text{Li}}(k - 1) \), we have that

\[
k \Delta \cdot \int_{2}^{\theta M^n} \frac{1}{\log t} \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^{k-1} dt \leq C \Delta \cdot \frac{\theta M^n}{\log(\theta M^n)} \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^{k-1}.
\]

Hence, if \( M \geq 1/\theta \), then we obtain that

\[
\sum_{t \in [2,\theta M^n] \cap \mathbb{Z}} h_A(t) \left\{ \log \left( \frac{\Xi M^n}{t} \right) \right\}^k
\]

\[
\leq \frac{\theta \Delta}{n} \left( \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^k + C \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^{k-1} \right) \cdot \frac{M^n}{\log M}
\]

\[
\leq \frac{\theta \Delta}{n - 1} \left( \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^k + C \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^{k-1} \right) \cdot \frac{M^n}{\log M}.
\]
There exists a real number $\theta \in (0, 1]$, depending on $\delta$, $\Delta$ and $\nu$, such that

$$\frac{\theta \Delta}{n-1} \left( \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^k + C \left\{ \log \left( \frac{\Xi}{\theta} \right) \right\}^{k-1} \right) \leq \frac{\delta}{2\Xi};$$

we take such a small $\theta$, and write $\Omega$ for it. Take $M_{\text{red}} \in \mathbb{N}$ such that $M_{\text{red}} \geq 1/\Omega$ and that for all $M \geq M_{\text{red}}$, (8.25) holds. Then, by (8.24) and the arguments after this, we conclude that for every $M \geq M_{\text{red}},$

$$\#(A \cap \mathcal{O}_K(\Omega M^n)) \leq \frac{1}{2} \delta + \frac{1}{2} \delta = \delta;$$

this is the desired estimate. It completes our proof.

Proposition 8.18 together with Lemma 8.17 derives the following theorem.

**Theorem 8.19** (Reduction to the case of fixing a fundamental domain). Assume Setting 8.1. Let $\delta > 0$ and $\Delta > 0$. Then there exist $\delta' = \delta'_{\text{red}}(\nu, \delta, \Delta) > 0$, $\Omega' = \Omega'_{\text{red}}(\nu, \delta, \Delta) > 0$ and $M'_{\text{red}} = M'_{\text{red}}(\nu, \delta, \Delta) \in \mathbb{N}$ such that for every $M \geq M'_{\text{red}}$, the following holds true. Let $A \subseteq a(\nu, M) \setminus \{0\}$ be a set that satisfies (8.4) and (8.21). Then, there exist a fundamental domain $D$ for $O_K^\times \curvearrowright (a \setminus \{0\})$ and a subset $A_0 \subseteq D$ such that

$$
\#A_0 \geq \delta' \cdot \frac{M^n}{\log M}
$$

and

$$
A_0 \subseteq A \setminus \mathcal{O}_K(\Omega' M^n)
$$

hold true.

**Proof.** Take $\Omega' = \Omega'_{\text{red}}(\nu, \delta, \Delta) := \Omega_{\text{red}}(\nu, \delta/2, \Delta)$ and $M'_{\text{red}}(\nu, \delta, \Delta) := M_{\text{red}}(\nu, \delta/2, \Delta)$. Let $A \subseteq a(\nu, M) \setminus \{0\}$ be the set in the assertion of the theorem. Then, by assumption (8.21), Proposition 8.18 implies that

$$
\#(A \cap \mathcal{O}_K(\Omega' M^n)) \leq \frac{\delta}{2} \cdot \frac{M^n}{\log M}.
$$

By combining this with assumption (8.4), we have that

$$
\#(A \setminus \mathcal{O}_K(\Omega' M^n)) \geq \frac{1}{2} \cdot \#A.
$$

Therefore, we can apply Lemma 8.17. This provides a subset $A_0 \subseteq A \setminus \mathcal{O}_K(\Omega' M^n)$ with $\#A_0 \geq c_{\Omega'} \cdot \#A$ such that $A_0$ admits no associate pairs. This $A_0$ satisfies (8.27). Finally, to ensure (8.26), take an arbitrary fundamental domain $D$ for the $O_K^\times$-action in such a way that $A_0 \subseteq D$ holds. Then, set $\delta' := c_{\Omega', \nu} \cdot \delta$. \qed
Theorem 8.19 enables us to upgrade axiomatizations for type 1 to those for type 2 in the following manner. Recall here that we have three axiomatizations for type 1: Theorem 8.7, Theorem 8.8 and Corollary 8.10.

**Theorem 8.20.** Assume Setting 8.1. Let $S \subseteq \mathfrak{a}$ be a standard shape. Let $\delta > 0$, $\Delta > 0$, $D_1, D_2 > 0$, and $\varepsilon \in (0, 1)_{\mathbb{R}}$. Then, there exist a positive real number $\rho = \rho_{II}(D_1, v, \delta, \Delta, S) > 0$ and a positive integer $M_{II} = M_{II}(D_1, D_2, \varepsilon, v, \delta, \Delta, S) \in \mathbb{N}$ such that the following holds true. Assume that $M \geq M_{II}$ and a set $A \subseteq \mathfrak{a}(v, M) \setminus \{0\}$ fulfill the following three conditions:

(i) the inequality

\[ \# A \geq \delta \cdot \frac{M^n}{\log M} \]

holds,

(ii) for every $L \in \mathbb{R}_{\geq 2}$,

\[ \# \{\alpha \mathcal{O}_K \in \text{Ideals}_K : \alpha \in A \cap \mathcal{O}_K(L)\} \leq \Delta \cdot \frac{L}{\log L} \]

holds,

(iii) $A$ satisfies the $(\rho, M, v, S)$-condition with parameters $(D_1, D_2, \varepsilon)$.

Then, there exists an $S$-constellation without associate pairs in $A$. Furthermore, if $W$ is the integer appearing in the $(\rho, M, v, S)$-condition, then there exists $\gamma = \gamma_{II}(D_1, D_2, v, \delta, \Delta, S) > 0$ such that

\[ \mathcal{N}^3_S(A) \geq \gamma \cdot \left( \frac{M}{W} \right)^{n+1} (\log M)^{-1} \]

holds true.

**Theorem 8.21.** Assume Setting 8.1. Assume that $A \subseteq \mathfrak{a} \setminus \{0\}$ fulfills the following three conditions:

(i) the inequality

\[ \limsup_{M \to \infty} \frac{\#(A \cap \mathfrak{a}(v, M))}{M^n (\log M)^{-1}} > 0 \]

holds,

(ii) there exists $\Delta > 0$ such that for every $L \in \mathbb{R}_{\geq 2}$,

\[ \# \{\alpha \mathcal{O}_K \in \text{Ideals}_K : \alpha \in A \cap \mathcal{O}_K(L)\} \leq \Delta \cdot \frac{L}{\log L} \]

holds,

(iii) $A \in S\Psi_{\log}(\mathfrak{a})$. 
Then, for every finite subset \( S \subseteq \mathfrak{a} \), there exists an \( S \)-constellation with no associate pairs in \( A \).

**Corollary 8.22.** Assume Setting \( 8.1 \). Assume that \( A \subseteq \mathfrak{a} \setminus \{0\} \) fulfills the following three conditions:

(i) the inequality
\[
\liminf_{M \to \infty} \frac{\#(A \cap \mathfrak{a}(v, M))}{M^n (\log M)^{-1}} > 0
\]
holds,

(ii) condition (ii) in Theorem \( 8.21 \) is satisfied,

(iii) \( A \in S_{\log} \mathfrak{a} \).

Then, for every \( A' \subseteq A \) with \( \mathcal{D}_{A,v}(A') > 0 \), the following holds true: for every finite subset \( S \subseteq \mathfrak{a} \), there exists an \( S \)-constellation with no associate pairs in \( A' \).

**Remark 8.23.** In the statement of Theorem \( 8.21 \) (ii) implies that the limit superior in (i) is finite. To verify this, run an argument similar to that of the proof of Proposition \( 8.14 \); examine also the proof of Proposition \( 8.18 \).

**Proofs of Theorem 8.20. Theorem 8.21 and Corollary 8.22.** First, we will prove Theorem \( 8.20 \). Set
\[
\rho_\Pi(D_1, v, \delta, \Delta, S) := \rho_1(D_1, v, \delta', S),
\]
\[
M_\Pi(D_1, D_2, \varepsilon, v, \delta, \Delta, S) := M_1(D_1, D_2, \varepsilon, v, \delta', S),
\]
\[
\gamma_\Pi(D_1, D_2, v, \delta, \Delta, S) := \gamma_1(D_1, D_2, v, \delta', S);
\]
here \( \delta' = \delta'_{\text{red}}(v, \delta, \Delta) \) is the one as in Theorem \( 8.19 \). Consider a set \( A \) that fulfills the three conditions of Theorem \( 8.20 \). By assumptions (i) and (iii), Theorem \( 8.19 \) applies. Hence, there exist a fundamental domain \( \mathcal{D} \) for the \( \mathcal{O}_K \times \mathbb{K} \)-action and a set \( A_0 \subseteq \mathcal{D} \) such that \( (8.26) \) holds. Then, by Lemma \( 8.5 \) (i), \( A_0 \) satisfies the \( (\rho, M, v, S) \)-condition with parameters \( (D_1, D_2, \varepsilon) \).

Therefore, we can apply Theorem \( 8.7 \) to this \( A_0 \) and \( \delta' \), thus proving Theorem \( 8.20 \). Here, recall that since \( A_0 \subseteq \mathcal{D} \), we have \( \mathcal{N}_S(A_0) = \mathcal{N}_S(A_0) \).

In a similar manner to the deduction of Theorem \( 8.8 \) from Theorem \( 8.7 \), we can deduce Theorem \( 8.21 \) from Theorem \( 8.20 \). We can also derive Corollary \( 8.22 \) from Theorem \( 8.21 \) in a way similar to the deduction of Corollary \( 8.10 \) from Theorem \( 8.8 \). Here, observe that assumption (ii) in Corollary \( 8.22 \) on \( A \) inherits to subsets.

**Proposition 8.24.** For a number field \( K \), \( \mathcal{P}_K \subseteq \mathcal{O}_K \setminus \{0\} \) satisfies the three conditions in Corollary \( 8.22 \).

**Proof.** We have already proved in Proposition \( 8.12 \) that \( \mathcal{P}_K \) satisfies assumptions (i) and (iii). By Landau’s prime ideal theorem (Theorem \( 3.21 \)), \( \mathcal{P}_K \) satisfies assumption (ii) as well.
Now we are ready to complete the proofs of Theorem A and Theorem 1.4.

Proofs of Theorem A and Theorem 1.4. Theorem 1.4 immediately follows from Proposition 8.24 and Corollary 8.22. Recall that we have showed Theorem 8.13 from Proposition 8.12 and Theorem 8.8. In a manner similar to this, Theorem A can be established from Proposition 8.24 and Theorem 8.20.

In the last part of this subsection, we will prove the following theorem; it may be regarded as the infinitary version of Theorem 8.19.

**Theorem 8.25** (Reduction to the case of fixing a fundamental domain, infinitary version). Assume Setting 8.1. Assume that $A \subseteq a \setminus \{0\}$ satisfies condition (ii) of Theorem 8.21. Then the following hold true.

1. Assume that $A$ satisfies condition (i) of Theorem 8.21. Then there exists an NL-compatible fundamental domain $D = D(A, v)$ for the action $O_K \curvearrowright (a \setminus \{0\})$ such that
   \[ \limsup_{M \to \infty} \frac{(A \cap D \cap a(v, M))}{M^n (\log M)^{-1}} > 0 \quad (8.28) \]

2. Assume that $A$ satisfies condition (i) in Corollary 8.22. Then there exists an NL-compatible fundamental domain $D' = D'(A, v)$ for the action $O_K \curvearrowright (a \setminus \{0\})$ such that
   \[ \liminf_{M \to \infty} \frac{(A \cap D' \cap a(v, M))}{M^n (\log M)^{-1}} > 0 \quad (8.29) \]

Note that the notion of the NL-compatibility is defined for subsets of $O_K$; in particular, it is defined for a subset of $a$. Also recall that for a fixed integral basis $\omega$ of $K$, the restriction of $\| \cdot \|_{\infty, \omega}$ on $a$ is bi-Lipschitz equivalent to $\| \cdot \|_{\infty, v}$.

Proof. There exists a constant $C' > 0$ depending only on $v$ such that for every $\alpha \in a \setminus \{0\}$, $N(\alpha) \leq C'\|\alpha\|^n_{\infty, v}$ holds. Indeed, this can be verified in a similar manner to the proof of Lemma 4.8. We fix such $C' > 0$ in the present proof.

First, we will prove (1). Since condition (i) in Theorem 8.21 is fulfilled, there exist a strictly increasing positive real sequence $(M_l)_{l \in \mathbb{N}}$ with $\lim_{l \to \infty} M_l = \infty$ and $\delta > 0$ such that for every $l \in \mathbb{N}$, the inequality
   \[ \frac{(A \cap a(v, M_l))}{M_l^n (\log M_l)^{-1}} \geq \delta \]
holds. Take constants $\delta' = \delta'_{\text{red}}(v, \delta, \Delta) > 0$, $\Omega' = \Omega'_{\text{red}}(v, \delta, \Delta) > 0$ and $M'_{\text{red}} = M'_{\text{red}}(v, \delta, \Delta) \in \mathbb{R}_{>0}$ as in Theorem 8.19 associated with $\delta$ and with $\Delta$ appearing in condition (iii) of Theorem 8.21. By passing to a subsequence of $(M_l)_{l \in \mathbb{N}}$ if necessary, we may assume that $M_1 \geq M'_{\text{red}}$ and that for every $l \in \mathbb{N}$, the inequality
   \[ M_{l+1} \geq \left( \frac{C'}{\Omega'} \right)^{\frac{1}{n}} M_l \quad (8.30) \]
holds. Note that (8.30) implies that
\[ \Omega' M_1^n < C' M_2^n \leq \Omega' M_2^n \leq C' M_3^n \leq \Omega' M_3^n \leq \cdots. \] (8.31)

Let \( l \in \mathbb{N} \). Apply Theorem 8.19 to \( A \cap a(\nu, M_l) \); then we can find \( A^{(l)}_0 \subseteq A \cap a(\nu, M_l) \) which admits no associate pairs such that
\[ \#A^{(l)}_0 \geq \delta' \cdot \frac{M_l^n}{\log M_l} \] (8.32)
and that for every \( \alpha \in A^{(l)}_0 \), the inequality
\[ \Omega' M_l^n < \mathcal{N}(\alpha) \leq C' M_l^n \] (8.33)
holds. Thus, we obtain a family of sets \( (A^{(l)}_0)_{l \in \mathbb{N}} \). Set
\[ A_0 := \bigcup_{l \in \mathbb{N}} A^{(l)}_0. \] (8.34)

Here, we can show that the union in the right-hand side of (8.34) is indeed a disjoint union in the following manner: by (8.33) and (8.31), for distinct \( l_1, l_2 \in \mathbb{N} \), the intersection of \( \mathcal{N}(A^{(l_1)}_0) \) and \( \mathcal{N}(A^{(l_2)}_0) \) is empty. This argument, furthermore, implies that \( A_0 \) admits no associate pairs. By (8.33), \( A_0 \) is NL-compatible; recall the remark after the statement of Theorem 8.25. Take an NL-compatible \( \mathcal{O}_K^\times \)-fundamental domain \( D_0 \subseteq \mathcal{O}_K \setminus \{0\} \) with the aid of Proposition 4.11. Set \( D_1 := (D_0 \cap a) \setminus (\mathcal{O}_K^\times \cdot A_0) \) and \( D := A_0 \cup D_1 \). Then since \( A_0 \) does not admit an associate pair, by construction of \( D \), this \( D \) is a fundamental domain for the action \( \mathcal{O}_K^\times \rhd a \setminus \{0\} \). Moreover, \( D \) is NL-compatible: indeed, it is the union of two NL-compatible sets \( A_0 \) and \( D_1 \). By (8.32) and (8.34), we have (8.28). Therefore, we have proved (1).

Secondly, we will show (2). By condition (i) in Corollary 8.22, there exists \( \delta > 0 \) such that for every sufficiently large \( M \), the inequality
\[ \frac{\#(A \cap a(\nu, M))}{M^n \log M} \geq \delta \] (8.35)
holds. Take constants \( \delta' = \delta'_{\text{red}}(\nu, \delta, \Delta) > 0 \), \( \Omega' = \Omega'_{\text{red}}(\nu, \delta, \Delta) > 0 \) and \( M'_0 = M'_{\text{red}}(\nu, \delta, \Delta) \in \mathbb{R}_{>0} \) as in Theorem 8.19 associated with this \( \delta \) and \( \Delta \) appearing in condition (iii) of Theorem 8.21. By replacing \( M'_0 \) with a bigger number if necessary, we may assume that for every \( M \geq M'_0 \), (8.35) holds. Now, define a sequence \( (M_l)_{l \in \mathbb{N}} \) inductively as follows: set \( M_1 := M'_0 \) and for each \( l \in \mathbb{N} \), set
\[ M_{l+1} := \left( \frac{C'}{\Omega'} \right) \frac{1}{M_l}. \] (8.36)

Note that (8.31) holds by construction.

From this sequence \( (M_l)_{l \in \mathbb{N}} \), construct \( (A^{(l)}_0)_{l \in \mathbb{N}} \) and an NL-compatible fundamental domain \( D' \) for \( \mathcal{O}_K^\times \rhd a \setminus \{0\} \) in the same manner as in the proof of (1). What remains to verify
is that $D'$ fulfills (8.29). Take an arbitrary $M \geq M_0'$. Then by (8.36), there exists $l \in \mathbb{N}$ such that
\[ M_l \leq M < \left( \frac{C'}{\Omega'} \right)^{\frac{1}{n}} M_l \] (8.37)
holds. For this $l \in \mathbb{N}$, we note that $A \cap D' \cap a(v, M) \supseteq A_0^{(l)}$. Hence by (8.35), the definition of $\delta'$ and (8.37), we conclude that
\[ \frac{\#(A \cap D' \cap a(v, M))}{M^n (\log M)^{-1}} \geq \left( \frac{M_l}{M} \right)^n \frac{\log M}{\log M_l} \cdot \delta' \geq \frac{\Omega'}{C'} \cdot \delta', \]
thus proving (8.29). It completes our proof. \hfill \Box

Here we state the reduction theorem again, which was mentioned as Theorem 2.11 in Section 2.

**Corollary 8.26 (Theorem 2.11 restated).** Let $K$ be a number field and $\omega$ an integral basis. Assume that $A \subseteq \mathcal{P}_K$ satisfies $\overline{d}_{\mathcal{P}_K, \omega}(A) > 0$. Then there exists an NL-compatible $O_K^\times$-fundamental domain $D = D(A, \omega)$ such that
\[ \overline{d}_{\mathcal{P}_K \cap D, \omega}(A \cap D) > 0 \]
holds.

**Proof.** Recall the countings of prime elements, both from above and below, from Proposition 7.7 and Proposition 8.14. Then, apply Theorem 8.25 (1) to $A$. \hfill \Box

**Remark 8.27.** In the present paper, we have established Theorem 1.4 and Corollary 2.10. The former treats the setting without fixing a fundamental domain, and the latter does that of fixing a fundamental domain. In this remark, we explain the ways of reducing one setting to the other setting, in both directions. Let $D$ be an NL-compatible $O_K^\times$-fundamental domain. Then by Propositions 7.7 and 8.14, for every $A \subseteq \mathcal{P}_K \cap D$ with $\overline{d}_{\mathcal{P}_K \cap D, \omega}(A) > 0$, we have $\overline{d}_{\mathcal{P}_K, \omega}(A) > 0$. Thus, the setting of Corollary 2.10 may be reduced to that of Theorem 1.4. Conversely, Corollary 8.26 enables us to reduce the setting of Theorem 1.4 to that of Corollary 2.10.

In a argument similar to the one above, by switching from infinite to finitary versions, we have the following: in Theorem A and Theorem 2.8 we may reduce one setting to the other, in both directions.

### 9 Szemerédi-type theorems for short intervals

The main goal of this section is to prove the finitary version of the Szemerédi-type theorem for short intervals in prime elements of number fields (Theorem B). For the rational field $\mathbb{Q}$, a stronger form of the Green–Tao theorem for short intervals is proved; see Theorem 9.3 and Theorem 9.4.
In Subsection 9.2, we first prove a stronger form of the Green–Tao theorem for short intervals, and later in Subsection 9.5, Theorem B will be established. A notable difference between the proof of Theorem B and that of Theorem 9.3, which arises when \([K: \mathbb{Q}] \geq 2\), is overcome by sophisticated use of the pigeonhole principle. This technique is commonly used in combinatorics; we call this the slide trick, and present it in Subsection 9.3. In Subsection 9.6, we prove Theorem 9.20 as an application of our constellation theorems for short intervals; Theorem 9.20 plays a key role in Section 10.

9.1 Statements of the theorems for short intervals

Setting 9.1. Let \(K\) be a number field of degree \(n\). Let \(\omega\) be an integral basis of \(K\).

Recall from Definition 2.5 that the \(\ell_\infty\)-interval \(O_K(\omega, x, M)\) for \(x \in O_K\) and \(M \in \mathbb{R}_{\geq 0}\) is defined as
\[
O_K(\omega, x, M) := \{ \alpha \in O_K : \|\alpha - x\|_{\ell_\infty, \omega} \leq M \}.
\]

We say this \(O_K(\omega, x, M)\) is a ‘short interval’ if \(M\) is sufficiently small compared to \(\|x\|_{\ell\infty, \omega}\).

Our concern in this section is to prove the existence of a constellation in short intervals in the sense above. Informally speaking, this amounts to proving the following statements (I) and (II). Note that, it is possible to formulate Szemerédi-type theorems after suitable modifications. We state, however, as constellation theorems for the set \(P_K\) for brevity. Let \(f: \mathbb{R}_{>0} \to \mathbb{R}_{\geq 0}\) be a monotonically non-decreasing function which diverges to infinity slower than the identity function \(t \mapsto t\).

(I) For every finite set \(S \subseteq O_K\), there exists a sequence \((y_l)_{l \in \mathbb{N}}\) in \(O_K\) with \(\|y_l\|_{\ell_\infty, \omega} \to \infty\) such that, for each \(l \in \mathbb{N}\), there exists an \(S\)-constellation in \(P_K \cap O_K(\omega, y_l, f(\|y_l\|_{\ell_\infty, \omega}))\).

(II) For every finite set \(S \subseteq O_K\), there exists \(M \in \mathbb{R}_{\geq 0}\) such that, for each \(x \in O_K\) with \(\|x\|_{\ell_\infty, \omega} \geq M\), there exists an \(S\)-constellation in \(P_K \cap O_K(\omega, x, f(\|x\|_{\ell_\infty, \omega}))\).

We refer to (II) the strong form for short intervals, because the assertion (II) implies (I).

For the case \(K = \mathbb{Q}\), we prove the strong form (II), as follows.

**Theorem 9.2** (The Green–Tao theorem for short intervals: strong version). Let \(a \in (0, 1)\), and assume that there exists \(\delta > 0\) such that, for a sufficiently large \(M > 0\),
\[
\#(P \cap [M, M + M^a]) \geq \delta \cdot \frac{M^a}{\log M}
\]
holds. Then we have the following, where \(k\) is an integer with \(k \geq 3\).

1. There exists \(M_{\text{GTSI}} = M_{\text{GTSI}}(a, \delta, k) \in \mathbb{N}\) depending only on \(a, \delta\) and \(k\) such that, for every \(M \in \mathbb{R}\) with \(M \geq M_{\text{GTSI}}\), \(P \cap [M, M + M^a]\) contains an arithmetic progression of length \(k\).
(2) There exist $\gamma = \gamma_{\text{GTSI}}^\chi(a, \delta, k) > 0$ and $M_{\text{GTSI}}^\chi = M_{\text{GTSI}}^\chi(a, \delta, k) \in \mathbb{N}$ depending only on $a, \delta$ and $k$ such that, for every $M \in \mathbb{R}$ with $M \geq M_{\text{GTSI}}^\chi$,

$$\mathcal{A}_k^\chi(\mathcal{P} \cap [M, M + M^a]) \geq \gamma \cdot M^{2a}(\log M)^{-(k+o_M \to \infty(1))}$$

holds. Here, for a finite subset $X \subseteq \mathbb{Z}$, $\mathcal{A}_k^\chi(X)$ denotes the number of arithmetic progressions (as sets) of length $k$ in $X$.

We prove Theorem 9.2 in Subsection 9.2. As for the possible values of $a$ in (9.1), that is, ‘prime number theorem in short intervals,’ a number of results are known; see [BHP01] and references therein. Among those, we mention the celebrated result of Baker–Harman–Pintz.

**Theorem 9.3** ([BHP01, p.562]). For sufficiently large real numbers $M$, we have

$$\#(\mathcal{P} \cap [M, M + M^{0.525}]) \geq \frac{9}{100} \cdot \frac{M^{0.525}}{\log M}.$$  

This theorem implies the following unconditional result:

**Theorem 9.4.** The assertions (1) and (2) of Theorem 9.2 hold for $a = 0.525$ and $\delta = 0.09$.

The strong form for short version, that is, the assertion of Theorem 9.2 makes sense only for real numbers $a$ satisfying (9.1). This requires deep results in the theory of distribution of primes. Under the Riemann hypothesis, we can ensure (9.1) for the range $a > 0.5$.

For a general number field $K$, we are content with the assertion (1), which is weaker than the strong form (2). While no results are needed from the theory of distribution of primes, we need an additional argument beyond those done in Section 8, namely, the slide trick.

**Theorem 9.5** (Theorem B, restated). Let $K$ be a number field and $\omega$ an integral basis of $K$. Let $\delta$ be a positive real number and $S$ a finite subset of $\mathcal{O}_K$. Take a real number $a$ with $0 < a < 1$. Then the following hold.

(1) There exists a positive integer $M_{\text{PESSI}} = M_{\text{PESSI}}(\omega, \delta, S, a)$ depending only on $\omega, \delta, S$ and $a$ such that the following holds: if $M \geq M_{\text{PESSI}}$ and a subset $A$ of $\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)$ satisfies

$$\#A \geq \delta \cdot \#(\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)), \quad (9.2)$$

then there exists $x \in A$ with

$$\frac{M}{\log^{a^2} M} \leq \|x\|_{\infty, \omega} \leq M \quad (9.3)$$

such that $A \cap \mathcal{O}_K(\omega, x, \|x\|_{\infty, \omega}^a)$ contains an $S$-constellation without associate pairs. Here, $\log^{a^2}$ means $\log \log$.

(2) If $S$ is a standard shape, then there exist a constant $\gamma_{\text{PESSI}}^\chi = \gamma_{\text{PESSI}}^\chi(\omega, \delta, S, a) > 0$ and a positive integer $M_{\text{PESSI}}^\chi = M_{\text{PESSI}}^\chi(\omega, \delta, S, a)$ depending only on $\omega, \delta, S$ and $a$ such that the following holds: if $M \geq M_{\text{PESSI}}^\chi$ and a subset $A$ of $\mathcal{P}_K \cap \mathcal{O}_K(\omega, M)$ satisfies (9.2), then there exists $x \in A$ with (9.3), which satisfies

$$\mathcal{A}_S^\chi(A \cap \mathcal{O}_K(\omega, x, \|x\|_{\infty, \omega}^a)) \geq \gamma \cdot M^{a(n+1)}(\log M)^{-(\#S + o_M \to \infty(1))}.$$
The following corollary is an infinitary version of Theorem $\square$ (= Theorem 9.5).

**Corollary 9.6.** Let $K$ be a number field, and let $\omega$ be an integral basis of $K$. If a subset $A \subseteq \mathcal{P}_K$ satisfies $\overline{d}_{\mathcal{P}_K\omega}(A) > 0$, then there exists a sequence $(y_l)_{l \in \mathbb{N}}$ in $A$ satisfying the following: for every $a \in (0,1)_{\mathbb{R}}$ and every finite set $S \subseteq A$, there exists a finite subset $L \subseteq \mathbb{N}$ such that for all $l \in \mathbb{N} \setminus L$, the set $A \cap \mathcal{O}_K(\omega, y_l, \|y_l\|_\infty^a, \omega)$ contains an $S$-constellation consisting of pairwise non-associate elements.

The proofs of Theorem 9.5 and of Corollary 9.6 will be presented in Subsection 9.5.

**Remark 9.7.** The statement of the form (I) for the case $K = \mathbb{Q}$ in terms of upper density can be found in [TZ08, Remark 2.4], as follows. Let $k$ be an integer with $k \geq 3$. If $A \subseteq \mathcal{P}$ satisfies $\overline{d}_\mathcal{P}(A) > 0$, then for every $a > 0$, there is a sequence of real numbers $(M_l)_{l \in \mathbb{N}}$ tending to $\infty$ such that, $A \cap [M, M + Ma]_{\mathbb{R}}$ contains an arithmetic progression of length $k$.

9.2 Strong form for the case $K = \mathbb{Q}$

In this subsection, we prove Theorem 9.2 which is the strong form for short version for the case $K = \mathbb{Q}$, along the lines of the axiomatization given in Section 8.

**Proposition 9.8.** Let $a \in (0,1)_{\mathbb{R}}$, and let $S_k = \{0,1, \ldots, k-1\}$, where $k$ is an integer with $k \geq 3$. Then, there exist $D_1, D_2 > 0$ and $\varepsilon \in (0,1)_{\mathbb{R}}$ such that the following statements hold. For every $\rho > 0$, there exists $M_{SI,\psi_{log}}(\rho) = M_{SI,\psi_{log}}(\rho, k, a) \in \mathbb{N}$ such that for every $M \geq M_{SI,\psi_{log}}(\rho)$, the following hold: there exist $W \in \mathbb{N}$ with $W \leq Ma$ and a function $\lambda: \mathbb{Z} \to \mathbb{R}_{\geq 0}$ such that the following (1), (2) and (3) are fulfilled.

1. For every $b \in \mathbb{Z}$ relatively prime to $W$, the function $\tilde{\lambda}_b := \frac{\varphi(W)}{W}(\text{Aff}_{W,b} \circ \lambda)$ is a $(\rho, \frac{Ma}{W}, S_k)$-pseudorandom measure. Here $\varphi = \varphi_{\mathbb{Q}}$ is Euler’s totient function.

2. For every $q \in \mathcal{P} \cap [M, M + Ma]_{\mathbb{R}}$,

$$D_1 \log M \leq \lambda(q) \leq D_2 \log M$$

holds.

3. Every $q \in \mathcal{P} \cap [M, M + Ma]_{\mathbb{R}}$ is relatively prime to $W$.

Notice that conclusions (1), (2) and (3) are slightly different from conditions (1), (2) and (3) of Definition 8.2. First, the inequality for $W$ is now $W \leq Ma$ instead of $W \leq M^\varepsilon$; secondly, the width of the interval for the pseudorandomness is $Ma/W$ instead of $M/W$; and finally, there is no exceptional set $T$ in (2) or (3). The first two differences come from the fact that the width of the interval $[M, M + Ma]_{\mathbb{R}}$ is $Ma$; the absence of $T$ means that we may take $T = \emptyset$. 
Proof. We proceed as in the proof of Theorem 8.6 for the case $K = \mathbb{Q}$, with some modifications. Let $R = M^{\frac{a}{17k \cdot 2^{k-1}}}$, $f$ be a function defined for sufficiently large real numbers such that $\lim_{t \to +\infty} f(t) = +\infty$ and $f(t) \leq \frac{a}{2} \log t$ hold. Define $\chi$ and $M_f$ as in Setting 7.2 and suppose $M \geq M_f$. Since $f$ and $\chi$ can be taken arbitrarily, we will not consider dependency on them. Let $w := f(M) = \prod_{p \leq M} p$. Define $\lambda$ as in Setting 7.2 under this setting.

In our case, $\kappa = \kappa_\mathbb{Q} = 1$. We now verify the assertions. First, by (7.3) and the assumption on $f$, we have $W \leq M^{a(\log 2)} \leq M^{\frac{a}{4}}$. This also implies $R > M^{\frac{a}{4}}$. It follows from the proof of Theorem 7.4 that, for every $\rho > 0$, if $M$ is sufficiently large depending on $\rho, k$ and $a$, then $\tilde{\lambda}_b$ defined by (1) is a $(\rho, M, S_k)$-pseudorandom measure. As for (2), by the definition of $\lambda$ and $R < M$, we have, for $q \in \mathcal{P} \cap [M, M + Ma]$, $\lambda(q) = 1$ holds. Since $w < M$, we also have (3). Therefore, with

$$\lambda(q) = \frac{1}{c_x} \log R = \frac{a}{17k \cdot 2^{k-1}c_x} \cdot \log M$$

holds. Since $w < M$, we also have (3). Therefore, with

$$(D_1, D_2, \varepsilon) = \left( \frac{a}{17k \cdot 2^{k-1}c_x}, \frac{a}{17k \cdot 2^{k-1}c_x}, \frac{3}{4} \right),$$

the assertions hold.

Proof of Theorem 9.2. Let $S_k := \{0, 1, \ldots, k - 1\} \subseteq \mathbb{Z}$. Despite that this set $S_k$ is not a standard shape, it meets all the requirements in Definition 2.3 except ‘$S = \bar{S}$.’ We will prove the theorem along the same lines of Theorem 8.7 using Proposition 9.8. Let $a \in (0, 1)_R$, and define $D_1, D_2, \varepsilon$ by (9.4). We will take $M$ sufficiently large as needed, and take $W$ accordingly as Proposition 9.8. Let

$$X_M := \mathcal{P} \cap [M, M + Ma] = \mathbb{Z}.$$ 

By assumption, there exists $\delta > 0$ such that (9.1) holds. If $M$ is taken to be sufficiently large depending on $a$ and $\delta$, then

$$\#X_M \geq \delta \cdot \frac{Ma}{\log M}$$

holds. The pigeonhole principle using Proposition 9.8 (3) implies that, there exists $\bar{b} \in (\mathbb{Z}/W) \times$ such that

$$\#(X_M \cap \bar{b}) \geq \frac{1}{\varphi(W)} \delta \cdot \frac{Ma}{\log M}$$

(9.5) holds. Setting $N := \lceil \frac{Ma}{W} \rceil$ and noting $W \leq M^{\varphi(a)}$, we find

$$M^{(1-\varepsilon)a} \leq N \leq \frac{2Ma}{W}.$$ 

(9.6)
Choose a representative \( b \in \overline{b} \) in such a way that \( b \) is maximal subject to \( b \leq M \). Then by
the triangle inequality, \( \text{Aff}_{W,b}([-N,N]) \supseteq X_M \cap \overline{b} \) holds. Setting \( B := \text{Aff}^{-1}_{W,b}(X_M \cap \overline{b}) \), we
have \( B \subseteq [-N,N] \), and by (9.5),
\[
\#B \geq \frac{1}{\varphi(W)} \delta \cdot \frac{M^a}{\log M}
\] (9.7)
holds.

Define a function \( \tilde{\lambda} : \mathbb{Z} \to \mathbb{R}_{\geq 0} \) by \( \tilde{\lambda} := \frac{\varphi(W)}{W}(\lambda \circ \text{Aff}_{W,b}) \). Then by Proposition 9.8 (1), for \( M \geq M_{\text{ST,\text{log}}} (\rho, k, a) \), \( \tilde{\lambda} \) is a \((\rho, N, S_k)\)-pseudorandom measure, where \( \rho \) is to be determined. By Proposition 9.8 (2), (9.6) and (9.7), we have
\[
\mathbb{E}(1_B \cdot \tilde{\lambda} \mid [-N,N]) \geq D_1 \cdot \delta \cdot \frac{M^a}{W} \geq D_1 \cdot \frac{1}{6} \cdot \delta
\]
and
\[
\frac{1}{N} \cdot \mathbb{E}(1_B \cdot \tilde{\lambda}^k \mid [-N,N]) \leq D_2^k \cdot \frac{(\log M)^k}{M^{(1-\varepsilon)a}}.
\]

Now we define \( \rho := \rho_{\text{RMS}}(\omega, \frac{D_1}{6} \delta, S_k) \) and \( \gamma := \gamma_{\text{RMS}}(\omega, \frac{D_1}{6} \delta, S_k) \), where \( \omega = (\omega) \), \( \omega = 1 \).

Choose \( M_{\text{GTSI}} \) in such a way that \( M \geq M_{\text{GTSI}} \) satisfies all the previous arguments, and that \( D_2^k \cdot (\log M)^k \leq \gamma \cdot M^{(1-\varepsilon)a} \) holds. Then for \( M \geq M_{\text{GTSI}} \), we can apply the relative
Szemerédi theorem \((n = 1 \text{ in Theorem 5.4})\) to \( B \subseteq [-N,N] \). It follows that \( B \) contains an \( S_k \)-constellation. Applying the transformation \( \text{Aff}_{W,b} \), we obtain an \( S_k \)-constellation in \( X_M = \mathcal{P} \cap [M, M + M^a] \).

Finally, we prove (2). Theorem 5.15 and Proposition 9.8 (2) imply
\[
\frac{1}{4N(2N+1)} \cdot (\mathcal{N}_{\text{Sk}}(B) + \mathcal{N}_{-\text{Sk}}(B)) \cdot (D_2 \log M)^k \geq \frac{\gamma}{2}.
\]
Since \( \mathcal{N}_{\text{Sk}}(B) + \mathcal{N}_{-\text{Sk}}(B) = 2 \mathcal{N}_k(B) \), we have
\[
\mathcal{N}_k(X_M) \geq \mathcal{N}_k(B) \geq 2D_2^{-k} \gamma \cdot \left( \frac{M^a}{W} \right)^2 (\log M)^{-k}.
\]
Let \( \gamma_{\text{GTSI}} := 2D_2^{-k} \gamma \), and define a function \( f \) in the proof of Proposition 9.8 by \( f(M) = \frac{1}{2} \log^{o^2} M \). Then, since \( W \leq \log^{o^2} M \), we obtain the desired estimate for \( \mathcal{N}_k(X_M) \). We remark that we need to take \( M_{\text{GTSI}} \) greater than \( M_{\text{GTSI}} \), as mentioned in Remark 7.12.

9.3 Slide trick

In this subsection, we present a technique necessary in proving constellation theorems of the form (1). More precisely, we first describe the difficulty which arises when \([K : \mathbb{Q}] \geq 2\), and then present the technique called a slide trick to overcome this difficulty.
Note that the natural density version of the Chebotarev density theorem (Theorem 3.22) provides an estimate of the number of prime elements in the domain of the form $O_K(\omega, [M_1, M'_1])$. Here, we define, for a free $\mathbb{Z}$-module $\mathcal{Z}$, its $\mathbb{Z}$-basis $\omega$, and $M_1, M'_1 \in \mathbb{R}_{\geq 0}$ with $M_1 \leq M'_1$:

$$\mathcal{Z}(\omega, [M_1, M'_1]) := \{\alpha \in \mathcal{Z} : \|\alpha\|_{\infty, \omega} \in [M_1, M'_1]_{\mathbb{R}}\}.$$  

We suppose that $M'_1$ is reasonably close to $M_1$. If $n = 1$, that is, if $K = \mathbb{Q}$, then with respect to its basis $\omega = (\omega)$, where $\omega = 1$, we have

$$O_\mathbb{Q}(\omega, [M_1, M'_1]) = ([-M'_1, -M_1]_{\mathbb{R}} \cap \mathbb{Z}) \cup ([M_1, M'_1]_{\mathbb{R}} \cap \mathbb{Z}).$$

Since $\mathcal{P}_\mathbb{Q} = \mathcal{P} \cup (-\mathcal{P})$, this amounts to considering the single interval $[M_1, M'_1]_{\mathbb{R}} \cap \mathbb{Z}$. If $n \geq 2$, then there is a significant difference between $O_K(\omega, [M_1, M'_1])$ and a short interval $O_K(\omega, x, M)$. The former is an $n$-dimensional cube with a smaller $n$-dimensional cube removed, while the latter is just a small $n$-dimensional cube. In order to apply the relative multidimensional Szemerédi theorem (Theorem 5.4), it is necessary to transfer the estimate in the former to the latter. This is an extra step which arises when $n \geq 2$. The transfer is possible if we can guarantee the density of prime elements is large in the latter, provided that the density of prime elements is large in the former. This assertion can be proved using the pigeonhole principle, which we formulate explicitly as the slide trick. In the setting of Szemerédi-type theorems of finitary version, the slide trick can be thought of taking a better representative $b \in \tilde{b}$ of $\tilde{b} \in (O_K/WO_K)^{\times}$ in the proof; retaking a representative is nothing but ‘sliding’ it by an element of $WO_K$, hence the name. We remark that this argument already appeared in the proof of Theorem 9.2 when a representative $b \in \tilde{b}$ was chosen. The reason why the slide trick is useful in our application is that the assertion of the Goldston–Yıldırım type asymptotic formula (Theorem 6.2) is strong enough that $b \in O_K$ can be arbitrary as long as $bO_K + WO_K = O_K$.

We now describe the slide trick. This can be formulated in the following general setting. Let $n \in \mathbb{N}$. Suppose that the additive group $\mathbb{Z}^n$ acts on a non-empty set $\mathbb{L}$ and that this action is simply transitive. This means that, for all $l, l' \in \mathbb{L}$, there exists a unique $z \in \mathbb{Z}^n$ such that $l' = z \cdot l$. In this case, for a non-empty subset $P$ of $\mathbb{L}$, the set of the form $z \cdot P$, where $z \in \mathbb{Z}^n$, is called a translate of $P$. The following is the fundamental lemma for the slide trick.

**Lemma 9.9.** Let $n \in \mathbb{N}$, and let $\mathbb{Z}^n \curvearrowright \mathbb{L}$ be a simply transitive action. Let $P, X \subseteq \mathbb{L}$ be finite non-empty sets, and let $\mathcal{Q}$ be the family of all translates $Q$ of $P$ satisfying $Q \cap X \neq \emptyset$. Then there exists $Q_X \in \mathcal{Q}$ such that

$$\frac{\#(Q_X \cap X)}{\#Q_X} \geq \frac{\#X}{\#\mathcal{Q}}$$

holds.

**Proof.** Since the action is simply transitive, the number of $Q \in \mathcal{Q}$ containing a given $x \in X$ is exactly $\#P$. This implies

$$\sum_{Q \in \mathcal{Q}} \#(Q \cap X) = \#\{(x, Q) \in X \times \mathcal{Q} \mid x \in Q\} = \sum_{x \in X} \#\{Q \in \mathcal{Q} \mid x \in Q\} = \#X \cdot \#P,$$
and hence
\[ E \left( \frac{\#(Q \cap X)}{\#Q} \bigg| Q \in \mathcal{Q} \right) = \frac{1}{\# \mathcal{Q}} \sum_{Q \in \mathcal{Q}} \frac{\#(Q \cap X)}{\#Q} = \frac{1}{(\# \mathcal{Q}) \cdot (\#P)} \sum_{Q \in \mathcal{Q}} \#(Q \cap X) = \frac{\#X}{\# \mathcal{Q}}. \]

The result then follows by the pigeonhole principle.

**Remark 9.10.** The above lemma can be generalized as follows. Let \( f : \mathbb{L} \to \mathbb{R}_{\geq 0} \) be a function which is 0 on \( \mathbb{L} \setminus X \). Then there exists a translate \( Q_f \) of \( P \) such that
\[ E (f | Q_f) \geq \frac{\#X}{\# \mathcal{Q}} \cdot E (f | X) \]
holds. Lemma 9.9 is exactly the case where \( f = 1_X \).

If the subset \( P \subseteq \mathbb{L} \) tiles \( \mathbb{L} \), that is, if there exists a subset \( Z \subseteq \mathbb{Z}^n \) such that \( \mathbb{L} = \bigcup_{z \in Z} z \cdot P \), then an analogous statement as Lemma 9.9 can be proved more directly. Lemma 9.9 is used in the proof of Theorem B with \( P \) being an \( n \)-dimensional cube, and this falls in the above situation. We have, however, stated Lemma 9.9 as a more general statement.

### 9.4 Axiomatization for short intervals

In this subsection and the next, we use Setting 8.1. In a manner similar to the argument in Section 8, we present axiomatizations of both finitary and infinitary versions, for constellation theorems of the form (I) for short intervals. We present our axiomatizations only for type 2, that is, for constellations without associate pairs; it is, however, possible to deduce the assertion of type 2 from that of type 1.

**Definition 9.11** \(((\rho, M, \nu, S, a)-\text{condition})\). Let \( a \in (0, 1)_\mathbb{R} \), and let \( S \subseteq a \) be a standard shape. Let \( \rho > 0 \), \( D_1, D_2 > 0 \), \( \varepsilon \in (0, 1)_\mathbb{R} \) and let \( M \in \mathbb{R}_{\geq 1} \). A subset \( A \subseteq a \) is said to satisfy the \((\rho, M, \nu, S, a)-\text{condition with parameters} \ (D_1, D_2, \varepsilon)\), if \( A \subseteq a(\nu, M) \), and if there exist \( W \in \mathbb{N} \) with \( W \leq M^{\varepsilon a} \) and \( \lambda : a \to \mathbb{R}_{\geq 0} \) such that the following conditions hold.

1. For every \( b \in a \) satisfying \( bO_K + W a = a \), the mapping \( \beta \mapsto \varphi_K(W)^{\frac{\nu(a, \lambda(\beta), W)}}{W^a}(\lambda \circ \text{Aff}_{W, b})(\beta) \) on \( a \) is a \((\rho, \frac{M^a}{W \log^{\varepsilon a} M}, S)\)-pseudorandom measure.

2. There exists \( T \subseteq A \) with \( \#T \leq M^{\varepsilon a} \) such that, for every \( \alpha \in A \setminus T \),
\[ D_1 \cdot \log M \leq \lambda(\alpha) \leq D_2 \cdot \log M \]
holds.

3. For the subset \( T \) in (2) and \( \alpha \in A \setminus T \), \( \alpha O_K + W a = a \) holds.

The difference of Definition 9.11 from Definition 8.2 is that the appearance of \( a \) in the exponent for the upper bound on \( W \), and the lower bound on the width of the interval for the pseudorandom condition in (1) is changed from \( \frac{M}{W} \) to \( \frac{M^a}{W \log^{\varepsilon a} M} \). The reason for the change
in the numerator from $M$ to $M^a$ is similar to the situation in Proposition 9.8, the width of the interval is $M^a$ instead of $M$. The factor $\log^{\sigma} M$ in the denominator is introduced for the removal of a small $n$-dimensional cube from a larger one in the pigeonhole principle. The role of the exponent $a$ in the upper bound on the size of an exceptional set $T$ in (2) and (3) is a minor issue. It is placed so as to force the containment of the set $S\Psi_{log}(a)$ in $S\Psi_{log}(a)$; the former will be defined in Definition 9.12. The removal of an exceptional set $T$ is necessary even in the weak form of the short interval version. Indeed, it cannot be avoided unless $O_K^\times$ is finite; see the proof of Theorem 9.14. This is in contrast to Proposition 9.8, where no exceptional set was needed.

**Definition 9.12** (The family $S\Psi_{log}^SI(a)$). We define a family $S\Psi_{log}^SI(a)$ of subsets of $a$ as follows: we declare $A \in S\Psi_{log}^SI(a)$ if and only if, for every $a \in (0,1)_\mathbb{R}$ and for every standard shape $S \subseteq a$, there exist $D_1, D_2 > 0$ and $\varepsilon \in (0,1)_\mathbb{R}$ such that the following holds: for every $\rho > 0$, there exists $M(\rho) = M(\rho, v, S, a) \in \mathbb{R}_{\geq 0}$ such that, for all $M \geq M(\rho)$, $A \cap a(v, M)$ satisfies the $(\rho, M, v, S, a)$-condition with parameters $(D_1, D_2, \varepsilon)$.

We chose to attach symbols ‘SI’ in $S\Psi_{log}^SI(a)$ to signify ‘short interval.’

**Lemma 9.13.** The following statements hold.

1. If $A \subseteq a$ satisfies the $(\rho, M, v, S, a)$-condition with parameters $(D_1, D_2, \varepsilon)$, then so do its subsets.

2. If $A \in S\Psi_{log}^SI(a)$, $A_1 \subseteq A$, then $A_1 \in S\Psi_{log}^SI(a)$.

3. $S\Psi_{log}^SI(a) \subseteq S\Psi_{log}(a)$.

**Proof.** Items (1) and (2) can be proved in a manner similar to that of Lemma 8.5.

We prove (3). Let $A \in S\Psi_{log}^SI(a)$. Let $S \subseteq a$ be a standard shape, and fix $a \in (0,1)_\mathbb{R}$ arbitrarily. Then there exist $D_1, D_2 > 0$ and $\varepsilon \in (0,1)_\mathbb{R}$ as described in Definition 9.12. Let $\rho > 0$, and let $M > 0$ be a real number satisfying $M^{1/a} \geq M(\rho, v, S, a)$. Since $A \in S\Psi_{log}^SI(a)$, the set $A \cap a(v, M^{1/a})$ satisfies the $(\rho, M^{1/a}, v, S, a)$-condition with parameters $(D_1, D_2, \varepsilon)$. It follows from (1) that $A \cap a(v, M)$ satisfies the $(\rho, M^{1/a}, v, S, a)$-condition with parameters $(D_1, D_2, \varepsilon)$. By Definition 9.11, this means that there exist $W \in \mathbb{N}$ with $W \leq M^{\varepsilon}$ and $\lambda: a \rightarrow \mathbb{R}_{\geq 0}$ such that the conditions (1)-(3) of Definition 9.11 hold. If we take $M$ large enough such that $\log^{\sigma}(M^{1/a}) \geq 1$ holds, then we see that $A \cap a(v, M)$ satisfies the $(\rho, M, v, S)$-condition with parameters $(D_1/a, D_2/a, \varepsilon)$. Therefore, $A \in S\Psi_{log}(a)$.

**Theorem 9.14.** $P_K \in S\Psi_{log}^SI(O_K)$.

**Proof.** The proof proceeds along the same lines of that of Proposition 9.8 except the treatment of an exceptional set, and also along the same lines of that of Theorem 8.6 except that we need to take into consideration the parameter $a$. Let $a \in (0,1)_\mathbb{R}$ be arbitrary. In the proof of Theorem 8.6, we replace the function $f$ by another non-negative function $f$ defined for sufficiently large real numbers satisfying $\lim_{t \rightarrow +\infty} f(t) = +\infty$ and $f(t) \leq \frac{\sigma}{2} \log t$. For this new function $f$, we define $w$ and $R$ by (7.1), and $R$ by $R := M^{\frac{1}{\min(\sigma + 1, \sigma)}}$. Then we have
\[ W \leq M^a \log^2 M < M^{\frac{3}{4}a}. \] Moreover, if \( M \) is sufficiently large depending on \( a \), then \( R^{4(r+1)2^r+1} \leq \frac{M^n}{W \log^{2a} M} \) holds. Thus, if we define \( \lambda: \mathcal{O}_K \to \mathbb{R}_{\geq 0} \) by (7.4), then Definition 9.11(1) is satisfied, by the same reasoning as in the proof of Theorem 8.6.

Define an exceptional set \( T \subseteq \mathcal{P}_K \cap \mathcal{O}_K(\omega, M) \) by \( T := \mathcal{P}_K \cap \mathcal{O}_K(\omega, M) \cap \mathcal{O}_K(R) \). As in the proof of Lemma 7.8, if \( M \) is sufficiently large depending on \( r, K \) and \( a \), then every \( \alpha \in \mathcal{P}_K \setminus T \) is prime to \( W \), and \( \lambda(\alpha) = \kappa^a \frac{\alpha}{17(r+1)2^r \cdot c_\chi} \) · \( \log^{\omega M} M \) holds. Moreover, if \( M \) is sufficiently large depending on \( \omega \) and \( a \), then by (8.2), we obtain \( \#T \leq M^{a \frac{\alpha}{2}} \). We write this situation as \( M \geq M_{P_K \cdot S_{\mathcal{O}_K}(\rho, \omega, S, a)} \) for future use. Therefore, the parameters for the \((\rho, M, \omega, S, a)\)-condition can be taken as \( (D_1, D_2, \epsilon) = \left( \frac{\kappa^a}{17(r+1)2^r \cdot c_\chi}, \frac{\kappa^a}{17(r+1)2^r \cdot c_\chi}, \frac{3}{4} \right) \).

This implies \( \mathcal{P}_K \in S_{\mathcal{O}_K}(\omega, M) \).

The following two theorems are the short interval versions of Theorem 8.20 and Theorem 8.21, respectively. Recall Definition 2.5.

**Theorem 9.15.** We use Setting 8.1. Let \( a \in (0, 1)_\mathbb{R} \), and let \( S \subseteq a \) be a standard shape. Let \( \delta, \Delta, D_1, D_2 > 0 \) and \( \varepsilon \in (0, 1)_\mathbb{R} \). Then there exist \( \rho = \rho_{SI}(D_1, v, \delta, \Delta, S) > 0 \) and \( M_{SI} = M_{SI}(D_1, D_2, \varepsilon, v, \delta, \Delta, S, a) \in \mathbb{N} \) such that the following holds. Assume an integer \( M \geq M_{SI} \) and a set \( A \subseteq a(v, M) \setminus \{0\} \) satisfy the following three conditions:

(i) the inequality
\[ \#A \geq \delta \cdot \frac{M^n}{\log M} \]
holds,

(ii) for every \( L \in \mathbb{R}_{\geq 2} \),
\[ \#\{\alpha \mathcal{O}_K \in \text{Ideals}_K: \alpha \in A \cap \mathcal{O}_K(L)\} \leq \Delta \cdot \frac{L}{\log L} \]
holds,

(iii) the set \( A \) satisfies the \((\rho, M, v, S, a)\)-condition with parameters \((D_1, D_2, \varepsilon)\).

Then there exists \( x \in A \) satisfying
\[ \frac{M}{\log^{2a} M} \leq \|x\|_{\infty, v} \leq M \] (9.9)
such that \( A \cap a(v, M, x, \|x\|_{\infty, v}) \) contains an \( S \)-constellation without associate pairs. Moreover, taking \( W \) in the \((\rho, M, v, S, a)\)-condition, there exists \( \gamma = \gamma_{SI}(D_1, D_2, v, \delta, \Delta, S) > 0 \) such that the above \( x \in A \) can be taken in such a way that
\[ M^a \leq W^{(r+1)(\log M)^{-(r+1)}} \] holds.
**Theorem 9.16.** We use Setting 8.1. Assume that a subset $A \subseteq a \setminus \{0\}$ satisfies the following three conditions:

(i) the inequality

$$\limsup_{M \to \infty} \frac{\#(A \cap a(v, M))}{M^n(\log M)^{-1}} > 0$$

holds,

(ii) there exists $\Delta > 0$ such that for every $L \in \mathbb{R}_{\geq 2}$,

$$\# \{ \alpha \mathcal{O}_K \in \text{Ideals}_K : \alpha \in A \cap \mathcal{O}_K(L) \} \leq \Delta \cdot \frac{L}{\log L}$$

(9.10)

holds,

(iii) $A \in S_{\Psi}^{S_{\text{SI}}} (a)$.

Then, there exists a sequence $(y_l)_{l \in \mathbb{N}}$ in $A$ satisfying the following: for every $a \in (0,1)_\mathbb{R}$ and every finite set $S \subseteq a$, there exists a finite subset $L \subseteq \mathbb{N}$ such that for all $l \in \mathbb{N} \setminus L$, $A \cap a(v, y_l, \|y_l\|_{\infty, v})$ contains an $S$-constellation consisting of pairwise non-associate elements.

We prove Theorem 9.15 in Subsection 9.5 and then deduce Theorem 9.16 from Theorem 9.15.

We obtain the following corollary from Theorem 9.16 and Lemma 9.13.

**Corollary 9.17.** We use Setting 8.1. Assume that a subset $A \subseteq a \setminus \{0\}$ satisfies the following three conditions:

(i) the inequality

$$\liminf_{M \to \infty} \frac{\#(A \cap a(v, M))}{M^n(\log M)^{-1}} > 0$$

holds,

(ii) condition (ii) of Theorem 9.16 is satisfied,

(iii) $A \in S_{\Psi}^{S_{\text{SI}}} (a)$.

Then for every $A' \subseteq A$ satisfying $d_{A,v}(A') > 0$, there exists a sequence $(y_l)_{l \in \mathbb{N}}$ in $A'$ satisfying the following: for every $a \in (0,1)_\mathbb{R}$ and every finite set $S \subseteq a$, there exists a finite subset $L \subseteq \mathbb{N}$ such that for all $l \in \mathbb{N} \setminus L$, $A' \cap a(v, y_l, \|y_l\|_{\infty, v})$ contains an $S$-constellation consisting of pairwise non-associate elements.

**Proof of Theorem 9.16 $\implies$ Corollary 9.17.** This is analogous to the deduction of Corollary 8.22 from Theorem 8.21.

We note that the sequence $(y_l)_{l \in \mathbb{N}}$ can be found independent of the choice of $a$ and $S$ in Theorem 9.16 and Corollary 9.17.
9.5 Proof of Theorems 9.15 and 9.16

In this subsection, we prove Theorem 9.15 and Theorem 9.16, and using these theorems, we prove Theorem 9.5 and Corollary 9.6

Let $n \in \mathbb{N}$. Define the $\ell_\infty$-metric $\| \cdot \|_\infty$ on $\mathbb{Z}^n$ by the standard basis. For $M_1, M_2 \in \mathbb{R}$ with $0 \leq M_1 \leq M_2$, let $\mathbb{Z}^n([M_1, M_2]) := \{ x \in \mathbb{Z}^n : \|x\|_\infty \in [M_1, M_2]\}.$

**Lemma 9.18.** Let $M_0, M$ and $a \in (0, 1)_\mathbb{R}$ be real numbers with $0 < M_0 \leq M$. Then, for every $A \subseteq \mathbb{Z}^n([M_0, M])$, there exists $M_1 \in [M_0, M]_\mathbb{R}$ such that

$$\#(A \cap \mathbb{Z}^n([M_1, M_1 + M_1^a])) \geq \frac{1}{2^n} \frac{(M_1 + M_1^a)^n - M_1^n}{M^n} \cdot \#A$$

**Proof.** We define a finite sequence $m_1, m_2, \ldots$ of real numbers as follows. We first set $m_0 := M_0$. Assuming $m_i$ has been defined, we stop constructing the sequence if $m_i \geq M$, and otherwise define $m_{i+1} := m_i + m_i^a$. This process terminates because we continue to have $m_{i+1} \geq m_i + M_0^a$. Let $m_l$ be the last term of this sequence. Then there exists $l_A \in [0, l - 1]$ such that

$$\#(A \cap \mathbb{Z}^n([m_{lA}, m_{lA+1}])) \geq \frac{1}{2^n} \frac{m_{lA+1}^n - m_{lA}^n}{M^n} \cdot \#A$$

holds. Indeed, otherwise, taking the summation from $i = 0$ to $l - 1$ gives

$$\#A < \frac{1}{2^n} \frac{m_l^n - m_0^n}{M^n} \cdot \#A \leq \frac{1}{2^n} \frac{(M + M^a)^n - M_0^n}{M^n} \cdot \#A \leq \#A,$$

which is a contradiction. The desired inequality holds by setting $M_1 := m_{lA}$. \hfill \Box

**Proof of Theorem 9.15** Let $a, \delta, \Delta, D_1, D_2, \varepsilon$ be as in the statement of the theorem. We let $M$ be a sufficiently large real number, to be determined exactly later. We also take $\rho > 0$ arbitrarily at this point. Let $A \subseteq a(v, M) \setminus \{0\}$ be a subset satisfying the conditions [1], [2] and [3] of the theorem. Thus we can take an integer $W \leq M^\varepsilon a$, a function $\lambda : a \to \mathbb{R}_{\geq 0}$, and an exceptional set $T \subseteq A$ as in these conditions. Recall that, for real numbers $M_1$ and $M_2$ satisfying $0 \leq M_1 \leq M_2$, the set $a(v, [M_1, M_2])$ is defined in (9.8) by setting $Z = a$. We define a real number $M_b$ by

$$M_b := \frac{2M}{\log^{\varepsilon^2} M}. \quad (9.11)$$

Take $M'_\text{red}(v, \delta, \Delta) \in \mathbb{N}$, $\delta' = \delta'_\text{red}(v, \delta, \Delta) > 0$ and $\Omega' = \Omega'_\text{red}(v, \delta, \Delta) > 0$ as in Theorem 8.19. Now assume that $M \geq M'_\text{red}(v, \delta, \Delta) > 0$ as in Theorem 8.19. Then we can apply Theorem 8.19 to the set $A$. This implies that there exist a fundamental domain $D$ for the action $\mathcal{O}_K^2 \curvearrowleft a \setminus \{0\}$ and a subset $A_0 \subseteq A \cap D$ such that

$$\#A_0 \geq \delta' \cdot \frac{M^n}{\log M} \quad (9.12)$$

holds. In addition (8.27) holds, that is, for $\alpha \in A_0$, we have $N(\alpha) > \Omega'M^n$. Therefore, if $M$ is sufficiently large depending on $v, \delta$ and $\Delta$, then Lemma 4.8 implies

$$A_0 \subseteq a(v, [M_b, M]) \quad (9.13)$$
Let \( A'_0 := A_0 \setminus T \). If \( M \) is sufficiently large depending on \( \varepsilon, \nu, \delta, \Delta \) and \( a \), it follows from the upper bound \( \#T \leq M^{\varepsilon a} \) and (9.12) that

\[
\#A'_0 \geq \frac{1}{2} \delta' \cdot \frac{M^n}{\log M} \tag{9.14}
\]

holds. Under the isometry \( (a, \| \cdot \|_\infty, \nu) \simeq (\mathbb{Z}^N, \| \cdot \|_\infty) \), we may regard \( A'_0 \) as a subset of \( \mathbb{Z}^n([M_0, M]) \) by (9.13). We can thus apply Lemma 9.18 by setting \( \nu = M_0, A = A'_0 \). This, together with (9.14), implies that there exists \( M^\nu \in [M_0, M] \) such that

\[
\#A''_0 \geq \frac{1}{2^{n+1}} \delta' \cdot \frac{(M_2 + M_2^a)^n - M_2^n}{\log M} \tag{9.15}
\]

holds, where \( A''_0 := A'_0 \cap a(\nu, [M_2, M_2 + M_2^a]) \).

Next we apply Lemma 8.4 to \( A''_0 \), noting that condition (3) holds by the \((\rho, M, \nu, S, a)\)-condition. By (9.15), we see that there exists \( b \in a/Wa \) such that

\[
\|(A''_0 \cap b) \| \geq \frac{1}{2^{n+1}} \varphi_K(W) \cdot \frac{(M_2 + M_2^a)^n - M_2^n}{\log M} \tag{9.16}
\]

holds. Note that the set \( A''_0 \cap b \) is not located inside an \( n \)-dimensional cube with a small diameter for which the relative multidimensional Szemerédi theorem applies.

We will determine the center \( x \in A \) of a short interval by suitably choosing a representative \( b \in \tilde{b} \) using the slide trick, in such a way that we can apply the relative multidimensional Szemerédi theorem. Let \( N := 2 \left\lceil \frac{M^a}{3W} \right\rceil \). Since \( W \leq M^{\varepsilon a} \) and \( M_0 \leq M \), for a sufficiently large \( M \) depending on \( \varepsilon \) and \( a \), we have

\[
\frac{M^n}{W \log^{2n} M} \leq N \leq \frac{M^n}{3W}. \tag{9.17}
\]

Observe that the additive group \( a \simeq \mathbb{Z}^n \) acts simply transitively on \( \tilde{b} \) by \( \beta \cdot x := x + W \beta \). Fix an arbitrary \( b_0 \in \tilde{b} \). We aim to apply Lemma 9.9 by setting \( P = Wa(\nu, N/2) + b_0 \) and \( X = A''_0 \cap \tilde{b} \). The size of the set \( Q \) in Lemma 9.9 for this setting can be estimated by considering the location of the ‘upper left’ corner of \( Wa(\nu, N/2) + b \), a translate of \( P \), as follows.

\[
\#Q \leq \left( \frac{2M_2 + 2M_2^a + WN + 1}{W} + 1 \right)^n - \left( \frac{2M_2 - WN - 1}{W} \right)^n \\
\leq \left( \frac{(2M_2 + 3M_2^a)^n - (2M_2 - M_2^a)^n}{W^n} \right).
\]

We use the following general inequalities: for \( t, t' \geq 0 \) with \( t'/t \) small enough depending on \( n \),

\[
t^n + nt^{-1} t' \leq (t + t')^n \leq t^n + 2nt^{-1} t'.
\]
Therefore, Bernoulli’s inequality implies \((t - t')^n \geq t^n - nt^{n-1}t'\). Since \(a \in (0,1)_R\), for a sufficiently large \(M\) depending on \(a\) and \(n\), we have
\[
(2M_t^3 + 3M_t^a)^n - (2M_t^3 - M_t^a)^n \leq 2^{n+2}(M_t^3 + M_t^a)^n - M_t^n.
\]
Therefore,
\[
\#Q \leq \frac{2^{n+2}}{W^n} \cdot ((M_t^3 + M_t^a)^n - M_t^n). \tag{9.18}
\]
It follows from Lemma 9.9, (9.16) and (9.18) that there exists a representative \(b \in \mathcal{B}\) such that the following holds:
\[
\#(A_0'' \cap \text{Aff}_{W,b}(a(v, N/2))) \geq \frac{W^n}{\varphi_K(W)} \cdot \frac{1}{2^{2n+3}} \cdot \delta' \cdot (N + 1)^n. \tag{9.19}
\]
We fix such a representative \(b\). Since \(A_0'' \cap \text{Aff}_{W,b}(a(v, N/2)) \neq \emptyset\), we can choose \(x \in A_0'' \cap \text{Aff}_{W,b}(a(v, N/2))\), which will also be fixed for the rest of the proof. Note, in particular, that \(x \in A\). By (9.13), we have \(\|b\|_{\infty,v} - WN/2 \leq \|x\|_{\infty,v} \leq M\) and \(\|b\|_{\infty,v} \geq M - WN/2\). Thus, if \(M\) is sufficiently large depending on \(a\), we see that (9.9) holds.

We now define \(\tilde{\lambda} := \frac{\varphi_K(W)}{W^n}(\lambda \circ \text{Aff}_{W,x})\) and \(B := \text{Aff}_{W,x}^{-1}(A_0'') \cap a(v, N)\). By (9.17) and the assumption on \(\lambda\), the function \(\tilde{\lambda}\) is a \((\rho, N, S)\)-pseudorandom measure. By (9.17), we have \(WN \leq \frac{M_a}{3}\). Since \(x \in A_0''\), we have \(\|x\|_{\infty,v} \geq M_t\). Thus \(3WN \leq \|x\|_{\infty,v}^a\) holds. In particular,
\[
A_0'' \cap \text{Aff}_{W,b}(a(v, N/2)) \subseteq A_0'' \cap \text{Aff}_{W,x}(a(v, N)) \subseteq A_0'' \cap a(v, x, \|x\|_{\infty,v}^a) \tag{9.20}
\]
holds. It follows from the first containment in (9.20) and (9.19) that
\[
\#B \geq \frac{W^n}{\varphi_K(W)} \cdot \frac{1}{2^{2n+3}} \cdot \delta' \cdot (N + 1)^n \tag{9.21}
\]
holds. We now treat the weighted density and smallness conditions. By (9.21) and the lower bound in (2) in the \((\rho, M, v, S, a)\)-condition, we obtain
\[
\mathbb{E}(1_B \cdot \tilde{\lambda} | a(v, N)) \geq \frac{D_1}{2^{3n+3}} \cdot \delta'. \tag{9.22}
\]
By (9.17) and \(W \leq M^\varphi\), if \(M\) is sufficiently large depending on \(\varepsilon\) and \(a\), then \(N \geq M^{\frac{1-\varepsilon}{\varphi}}\) holds. This, together with the upper bound in (2) in the \((\rho, M, v, S, a)\)-condition, we obtain
\[
\frac{1}{N} \cdot \mathbb{E}(1_B \cdot \tilde{\lambda}^{r+1} | a(v, N)) \leq D_2^{r+1} \cdot \frac{(\log M)^{r+1}}{M^{\frac{1-\varepsilon}{\varphi}}}, \tag{9.23}
\]
where $r := \#S - 1$.

We next define $\rho$ and $M_{\text{SI}}$. First, we define $\rho := \rho_{\text{RMS}}(v, \frac{D_2^\delta}{2n+1}, S)$. Before defining $M_{\text{SI}}$, we need some preparations. Let $\gamma'_S := \gamma_{\text{RMS}}(v, \frac{D_2^\delta}{2n+1}, S)$. Note that $M$ has been assumed to be sufficiently large up to this point. We further make $M$ large enough in such a way that $D_2^{\gamma_1 + 1} \cdot (\log M)^{\gamma_1 + 1} \leq \gamma'_S \cdot M^{\frac{1}{2n+1}}$ holds, and we set $M_{\text{SI}}$ to be the smallest positive integer such that all these requirements hold for as long as $M \geq M_{\text{SI}}$. Then by (9.22) and (9.23), Theorem 5.4 can be applied to $B \subseteq a(v, N)$ under the hypothesis $M \geq M_{\text{SI}}$. It follows that there exists an $S$-constellation in $B$. Applying $\text{Aff}_{W, x}$, this leads to the existence of an $S$-constellation in $A_0^\rho \cap \text{Aff}_{W, x}(a(v, N))$. Since $A_0^\rho \subseteq D$, such an $S$-constellation contains no associate pairs. By the second containment in (9.20), this implies the existence of an $S$-constellation in $A \cap a(v, x, \|x\|_{\infty, \rho})$ without associate pairs.

Finally, we estimate the number of $S$-constellations. Since $N(B) \leq N_s^2(A \cap a(v, x, \|x\|_{\infty, \rho}))$, it suffices to give a lower bound on $N_s(B)$. By Theorem 5.5 and condition (2) in the $(\rho, M, v, S, a)$-condition, we obtain

$$\frac{1}{N(2N + 1)^n} \cdot N(B) \cdot (D_2 \log M)^{r_1 + 1} \geq \gamma'_S.$$ 

Thus, by setting $\gamma'_{\text{SI}} := 2^n D_2^{r_1} \gamma'_S$, we see from (9.17) that

$$N(B) \geq \gamma_{\text{SI}} \cdot N^{n+1}(\log M)^{-r_1} \geq \gamma_{\text{SI}} \cdot \left(\frac{M^n}{W \log^2 M}\right)^{n+1}(\log M)^{-r_1}$$

holds. This provides the desired estimate.

Proof of Theorem 9.16 By (i), there exist $\delta > 0$ and an increasing sequence $(M_l)_{l \in \mathbb{N}}$ of real numbers with $\lim_{l \to \infty} M_l = \infty$ such that, for all $l \in \mathbb{N},$

$$\#(A \cap a(v, M_l)) \geq \delta \cdot \frac{M_l^n}{\log M_l}$$

holds. By (ii), there exists $\Delta > 0$ such that (9.10) holds.

Fix $a \in (0, 1)_{\mathbb{R}}$ and a standard shape $S \subseteq a$. By (iii), we can choose $D_1, D_2 > 0$ and $\varepsilon \in (0, 1)_{\mathbb{R}}$ such that the property described in Definition 9.12 holds. Then take $\rho > 0$ and $M_{\text{SI}} \in \mathbb{N}$ such that the conclusion of Theorem 9.15 holds. In order to apply this conclusion, choose $l \in \mathbb{N}$ in such a way that $M_l \geq \max\{M_{\text{SI}}, M_{A, S, \psi_{\log}}(\rho, v, S, a)\}$ and set $A' := A \cap a(v, M_l)$. Then by (9.24),

$$\#A' \geq \delta \cdot \frac{M_l^n}{\log M_l}$$

holds. This implies that condition (ii) of Theorem 9.15 is fulfilled with $(A, M)$ replaced by $(A', M_l)$. Since (9.10) is valid even if $A$ is replaced by $A'$, condition (ii) of Theorem 9.15 is fulfilled with $A$ replaced by $A'$. Finally, since $M_l \geq M_{A, S, \psi_{\log}}(\rho, v, S, a)$, $A'$ satisfies the $(\rho, M_l, v, S, a)$-condition with parameters $(D_1, D_2, \varepsilon)$. This implies that condition (iii) of
Theorem [9.15] is fulfilled with \((A, M)\) replaced by \((A', M_l)\). Thus, by Theorem [9.15] there exists \(x(\alpha, S) \in A'\) such that \(A' \cap \alpha(v, x(\alpha, S), \|x(\alpha, S)|\|_{\infty, v})\) contains an \(S\)-constellation without associate pairs.

In order to complete the proof of the theorem, we employ the diagonal argument. Fix a decreasing sequence \((a_i)_{i \in \mathbb{N}}\) in \((0, 1)_\mathbb{R}\) with \(\lim a_i = 0\). Since \(a\) is countable, we can take a sequence \(S_1 \subseteq S_2 \subseteq \cdots\) of standard shapes in \(a\) such that \(\bigcup_{i \in \mathbb{N}} S_i = a\). Applying the above argument to \((a_i, S_i)\) for each \(l \in \mathbb{N}\), we find a sequence \((y_i)_{i \in \mathbb{N}}\) of elements in \(A'\) such that \(A' \cap a(v, y_i, \|y_i\|_{\infty, v})\) contains an \(S_l\)-constellation without associate pairs. It remains to show that the sequence \((y_i)_{i \in \mathbb{N}}\) satisfies the desired property. Indeed, let \(a \in (0, 1)_\mathbb{R}\) and a standard shape \(S \subseteq a\) be arbitrary. Then there the set \(L := \{l \in \mathbb{N} : a < a_l \text{ or } S \not\subseteq S_l\}\) is finite. Then for all \(l \in \mathbb{N} \setminus L\), we have \(a \geq a_l\) and \(S \subseteq S_l\). Since \(A' \cap a(v, y_i, \|y_i\|_{\infty, v})\) contains an \(S_l\)-constellation without associate pairs, we see that \(A \cap a(v, y_i, \|y_i\|_{\infty, v})\) contains an \(S\)-constellation without associate pairs.

We have completed the necessary axiomatization. The proofs of Theorem [9.5] and Corollary [9.6] are now within reach.

**Proposition 9.19.** For a number field \(K\), the set \(\mathcal{P}_K\) satisfies all the assumptions of Corollary [9.17].

**Proof.** By Proposition [8.12], condition [i] holds. By Theorem [3.21], condition [ii] holds. Finally, by Theorem [9.14], condition [iii] holds.

**Proof of Theorem 9.5.** We may assume without loss of generality that \(S\) is a standard shape. Fix a function \(\chi\) and define \(c_\chi\) as in Setting [7.2]. Recall \(\kappa\) from Theorem [3.19]. Let \(r := \#S - 1\) and \(D := \kappa a \cdot (17r + 1)2^n \cdot c_\chi^{-1}\). By Proposition [8.12], there exist \(C_{\mathcal{P}_K,1}(\omega) > 0\) and \(M_{\mathcal{P}_K,1}(\omega) \in \mathbb{N}\) such that, for every \(M \geq M_{\mathcal{P}_K,1}(\omega)\), inequality (8.14) holds. Recall \(\rho_{\mathcal{S}l}\) from Theorem [9.15] to define

\[
\rho := \rho_{\mathcal{S}l}(D, \omega, \delta \cdot C_{\mathcal{P}_K,1}(\omega), C_{\text{lan}}, S),
\]

where \(C_{\text{lan}}\) is given in (8.19). By Theorem [9.14], we have \(\mathcal{P}_K \in S_{\mathcal{S}l}(\mathcal{O}_K)\). Recall \(M_{\mathcal{P}_K, S_{\mathcal{S}l}}\) from the proof of Theorem [9.14] and \(M_{\mathcal{S}l}\) from Theorem [9.15] to define

\[
M_{\text{Pessi}} := \max\{M_{\mathcal{P}_K,1}(\omega), M_{\mathcal{P}_K, S_{\mathcal{S}l}}(\rho, \omega, S, a),
M_{\mathcal{S}l}(D, D, 3/4, \omega, \delta \cdot C_{\mathcal{P}_K,1}(\omega), C_{\text{lan}}, S, a)\}. \quad (9.25)
\]

Suppose \(M \geq M_{\text{Pessi}}\) and a subset \(A \subseteq \mathcal{P}_K \cap \mathcal{O}_K(\omega, M)\) satisfies (9.2). Since \(M \geq M_{\mathcal{P}_K,1}(\omega)\), we can combine (8.14) with assumption (9.2) to obtain

\[
\#A \geq \delta \cdot C_{\mathcal{P}_K,1}(\omega) \cdot \frac{M^n}{\log M}. \quad (9.26)
\]

It follows from the proof of Theorem [9.14] that \(\mathcal{P}_K\) satisfies \((\rho, M, \omega, S, a)\)-condition with parameters \((D, D, 3/4)\). By Lemma [9.13], \(A\) also satisfies \((\rho, M, \omega, S, a)\)-condition with parameters \((D, D, 3/4)\).
Thus, we can apply Theorem 9.15 with $\Delta = C_{\text{Lan}}$, $D_1 = D_2 = D$ and $\varepsilon = 3/4$ to conclude that there exists $x \in A$ such that $A \cap \mathcal{O}_K(\omega, x, \|x\|_{\infty, \omega})$ contains an $S$-constellation without associate pairs. This proves (1).

As for (2), taking the function $f$ in the proof of Theorem 9.14 as $f = \frac{1}{2} \log^3 t$, let

$$\gamma_{\text{PESSI}}' := \gamma_{\text{SI}}(D, D, \omega, \delta \cdot C_{\mathcal{P}K,1}(\omega), C_{\text{Lan}}, S),$$

and define $M_{\text{PESSI}}'$ by (9.25) for this $f$. Then the parameter $W$ in the $(\rho, M, \omega, S, a)$-condition can be assumed to satisfy $W \leq \log^2 M$, and $x \in A$ can be taken in such a way that $N^*_{\mathcal{S}}(A \cap \mathcal{O}_K(\omega, x, \|x\|_{\infty, \omega})) \geq \gamma_{\text{PESSI}}' \cdot \left( \frac{M^a}{W \log^2 M} \right)^{n+1} (\log M)^{-(r+1)}$ holds, provided $M \geq M_{\text{PESSI}}$. As in the proof of Theorem 7.11 this yields the desired estimate. \hfill $\square$

Proof of Corollary 9.6. Immediate from Corollary 9.17 and Proposition 9.19. \hfill $\square$

9.6 Constellations whose norms are close

In this subsection, we exhibit one application of our constellation theorems for short intervals. For simplicity, we only state the infinitary version.

**Theorem 9.20.** We use Setting 8.1. Assume that a subset $A \subseteq a \setminus \{0\}$ satisfies the three conditions in Theorem 9.16. Then, there exists a sequence $(\mathcal{I}_l)_{l \in \mathbb{N}}$ of pairwise disjoint finite subsets in $A$ with no associate pairs satisfying the following. For every $a \in (0, 1) \mathbb{R}$, every finite set $S \subseteq a$ and every $\eta > 0$, there exists a finite subset $L \subseteq \mathbb{N}$ such that for all $l \in \mathbb{N} \setminus L$, the following hold true.

1. The set $\mathcal{I}_l$ contains an $S$-constellation.

2. For every $\alpha_1, \alpha_2 \in \mathcal{I}_l$,

$$\frac{N(\alpha_2)}{N(\alpha_1)} \leq 1 + \eta \cdot (\min\{N(\alpha) : \alpha \in \mathcal{I}_l\})^{\frac{a-1}{n}}$$

holds.

We remark that in (2), the exponent $(a - 1)/n$ cannot be improved to any constant less than $-1/n$ in general; see the discussion in Remark 10.2.

**Proof.** Let $\sigma_1, \ldots, \sigma_{\tau_1}, \sigma_{\tau_1+1}, \ldots, \sigma_{\tau_1+2r_2}$ be the embeddings of $K$ into $\mathbb{C}$. Recall that there exists a constant $D' = D'_{\mathbf{v}} > 0$, depending only on $\mathbf{v}$, such that for every $\alpha \in a$ and for each $i \in [n]$, we have $|\sigma_i(\alpha)| \leq D'\|\alpha\|_{\infty, \mathbf{v}}$; see Lemma 4.8. Take an arbitrary $\delta > 0$ which is strictly smaller than the limit superior appearing in condition (i) of Theorem 9.16. Take $\Delta > 0$ as in condition (ii) of Theorem 9.16. From $\delta$ and $\Delta$, set $\Omega' = C_{\text{red}}'(\mathbf{v}, \delta, \Delta) > 0$ as in Theorem 8.19.
Consider a sequence \(((a_l, S_l, \eta_l))_{l \in \mathbb{N}}\), where \((a_l)_{l \in \mathbb{N}}\) is a decreasing sequence in \((0, 1)_\mathbb{R}\) with \(\lim_{l \to \infty} a_l = 0\) and \((\eta_l)_{l \in \mathbb{N}}\) is a decreasing sequence of positive reals with \(\lim_{l \to \infty} \eta_l = 0\). The sequence \((S_n)_{n \in \mathbb{N}}\) comes from a filtration \(S_1 \subseteq S_2 \subseteq \cdots\) of standard shapes of \(a\) with \(\bigcup_{l \in \mathbb{N}} S_l = a\).

Apply the proof of Theorem 9.13 to this setting. Then, we obtain a strictly increasing sequence \((M_l)_{l \in \mathbb{N}}\) in \(\mathbb{R}_{\geq 1}\) with \(\lim_{l \to \infty} M_l = \infty\), a sequence \((y_l)_{l \in \mathbb{N}}\) in \(A\), and a sequence of sets \((A''_l(M_l))_{l \in \mathbb{N}}\) such that for every \(l \in \mathbb{N}\), the following conditions are fulfilled:

(a) \(A''_l(M_l) \subseteq A \cap a(v, M_l) \cap a(v, y_l, \frac{n}{2} \|y_l\|^2_{\infty,v})\),

(b) for every \(\alpha \in A''_l(M_l)\), \(N(\alpha) \geq \Omega l^a\),

(c) \(A''_l(M_l)\) admits no associate pairs, and it contains an \(S_l\)-constellation.

Indeed, for (a), consider \((a_l/2)_{l \in \mathbb{N}}\) instead of \((a_l)_{l \in \mathbb{N}}\), and take sufficiently large \(M_l\) to obtain the \(\eta_l\)-factor. Moreover, we can take in such a way that \((A''_l(M_l))_{l \in \mathbb{N}}\) is pairwise disjoint.

Now, for each \(l \in \mathbb{N}\), we set \(T_l := A''_l(M_l)\). What remains is to verify (2). Fix \(l \in \mathbb{N}\), and take \(\alpha \in T_l\). It then follows from (b) and Lemma 3.5 that there exists a constant \(D' = D'_l\), depending only on \(v\), such that for each \(i \in [n]\),

\[
|\sigma_i(\alpha)| \geq D'\Omega l^a. 
\]

Now take \(\alpha_1, \alpha_2 \in T_l\). Then, since \(\|\alpha_1 - \alpha_2\|_{\infty,v} \leq \eta_l M_l^{a_l}\) by (a), we have that for each \(i \in [n]\),

\[
|\sigma_i(\alpha_1) - \sigma_i(\alpha_2)| \leq \eta_l D M_l^{a_l}. 
\]

By combining Lemma 3.5, (9.27) and (9.28), we have that

\[
\frac{N(\alpha_2)}{N(\alpha_1)} \leq \prod_{i \in [n]} \left(1 + \frac{|\sigma_i(\alpha_1) - \sigma_i(\alpha_2)|}{|\sigma_i(\alpha_1)|}\right) \leq \left(1 + \frac{\eta_l D}{D'\Omega} \cdot M_l^{a_l - 1}\right)^n.
\]

By (b), for every \(a \in (0, 1)\) and \(\eta > 0\), if \(l\) is sufficiently large depending on \(v, A, a\) and \(\eta\) then we have that for all \(\alpha_1, \alpha_2 \in T_l\),

\[
\frac{N(\alpha_2)}{N(\alpha_1)} \leq 1 + \eta \cdot \left(\min_{\alpha \in T_l} N(\alpha)\right)^\frac{a_l - 1}{n}.
\]

Hence we confirm (2), and the proof completes.

\[\square\]

## 10 Constellations in ideals and quadratic forms

The goal of the present section is to establish the following theorem on binary quadratic forms. This is a refinement of Theorem [C] condition (b2) in [3] is the additional part. For a binary quadratic form \(F: \mathbb{Z}^2 \to \mathbb{Z}; F(x, y) := ax^2 + bxy + cz^2\) with integral coefficients, recall that \(F\) is primitive if \(\gcd(a, b, c) = 1\), and that \(D_F\) denotes the discriminant \(b^2 - 4ac\). We say that \(F\) is non-degenerate if \(D_F\) is not a perfect square. If \(D_F\) is a perfect square, then \(F\) decomposes into the product of two linear polynomials in the polynomial ring \(\mathbb{Z}[x, y]\); such a form can take prime values only if one of the two factors is equal to \pm 1, and hence it is not of our interest. Recall also Definition 8.9.
Theorem 10.1 (A refined version of Theorem C). Let $F(x, y) := ax^2 + bxy + cz^2 \in \mathbb{Z}[x, y]$ be a non-degenerate primitive quadratic form. Assume that $a > 0$. Let $u$ be the standard basis of $\mathbb{Z}^2$.

(1) Let $A \subseteq F^{-1}(\mathcal{P})$ be a set with $d_{F^{-1}(\mathcal{P}), u}(A) > 0$. Then, for a finite set $S \subseteq \mathbb{Z}^2$, there exists an $S$-constellation in $A$.

(2) Assume that $D_F > 0$. Let $A \subseteq F^{-1}(\mathcal{P})$ be a set with $d_{F^{-1}(\mathcal{P}), u}(A) > 0$. Then, for a finite set $S \subseteq \mathbb{Z}^2$, there exists an $S$-constellation in $A$.

(3) In both (1) and (2), the following furthermore holds true for $A$: there exists a sequence of pairwise disjoint finite subsets $(\mathcal{T}_l)_{l \in \mathbb{N}}$ of $A$ which fulfills the following two conditions.

(a) For every $l \in \mathbb{N}$, $F \mid_{\mathcal{T}_l} : \mathcal{T}_l \to \mathcal{P}_Q$ is injective.

(b) For every $\theta \in (0, 1)_\mathbb{R}$, for every finite subset $S \subseteq \mathbb{Z}^2$ and for every $\eta > 0$, there exists a finite subset $L \subseteq \mathbb{N}$ such that for every $l \in \mathbb{N} \setminus L$, the following hold:

\[
|p_2| \leq 1 + \eta \cdot \left( \min \{|p| : p \in F(\mathcal{T}_l)\} \right)^{\frac{\theta - 1}{2}}
\]

holds.

Remark 10.2. The exponent $\frac{\theta - 1}{2}$ in condition (b2) in Theorem 10.1 (3) can not be improved to any constant less than $-\frac{1}{2}$ in general. Indeed, consider the case where $F(x, y) = x^2 + y^2$ and $S = \{(0, 0), (1, 0), (0, 1)\}$. Note that if $|x| \geq |y|$ and if $0 < d < |x|$, then

\[
\left| \frac{F(x+d, y)}{F(x, y)} - 1 \right| \geq \frac{|d|}{2} \cdot (F(x, y))^{-\frac{1}{2}}.
\]

We exhibit key theorems to the proof of Theorem 10.1 in Subsection 10.1 there, we provide the organization of the present section.

10.1 Strategy for the proof of Theorem 10.1

In this subsection, we describe the strategy for the proof of Theorem 10.1. The first key to the proof is the following correspondence between primitive quadratic forms and invertible fractional ideals of orders. This is a classical result due to Gauss and Dirichlet. In the present paper, we exhibit a proof of Theorem 10.3 in the appendix for the convenience of the reader; see Theorem A.5. See also [Bha04, Subsections 3.2 and 3.3].

Theorem 10.3. Let $F(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ be a primitive and non-degenerate binary quadratic form. Then there exist an order $\mathcal{O}$ in $K := \mathbb{Q}(\sqrt{D_F})$, an invertible fractional
ideal \( \mathfrak{c} \) of \( \mathcal{O} \), a basis \((\gamma_1, \gamma_2)\) of \( \mathfrak{c} \) as a \( \mathbb{Z} \)-module, and a signature \( \epsilon_{\mathfrak{c}} \in \{\pm 1\} \) such that the following identity holds:

\[
F(x, y) = \epsilon_{\mathfrak{c}} \cdot \frac{N_{K/Q}(\gamma_1 x + \gamma_2 y)}{N(\mathfrak{c})} \quad \text{for all } (x, y) \in \mathbb{Z}^2. \tag{10.1}
\]

We will present the definitions of orders and invertible fractional ideals in Subsection 10.2 for an invertible ideal \( \mathfrak{c} \) of an order \( \mathcal{O} \), the definition of the ideal norm \( N(\mathfrak{c}) \) of \( \mathfrak{c} \) will be provided in Subsection 10.3. Throughout this section, we use the symbols \( \mathfrak{c} \) and \( \mathfrak{d} \) for invertible fractional ideals of an order, and \( \mathfrak{a} \) and \( \mathfrak{b} \) for non-zero fractional ideals of the ring of integers, which is also called the maximal order.

Inspired by Theorem 10.3, we define the following subsets of fractional ideals of \( \mathcal{O}_K \) and \( \mathcal{O} \), which may be regarded as counterparts of the set \( \mathcal{P}_K \) of prime elements in the proof of Theorem 10.1. Indeed, if \( \mathfrak{a} = \mathcal{O}_K \), then the set \( \mathcal{P}_{\mathcal{O}_K} \) coincides with \( \mathcal{P}_K \).

**Definition 10.4.** Let \( K \) be a number field, and \( \mathcal{O}_K \) the ring of integers of \( K \). Let \( \mathcal{O} \) be an order in \( K \).

1. Let \( \mathfrak{a} \) be a non-zero fractional ideal of \( \mathcal{O}_K \). Define the set \( \mathcal{P}_\mathfrak{a} \subseteq \mathfrak{a} \) by

\[
\mathcal{P}_\mathfrak{a} := \{ \alpha \in \mathfrak{a} : \text{the ideal } \alpha \mathfrak{a}^{-1} \subseteq \mathcal{O}_K \text{ is a prime ideal} \}.
\]

2. Let \( \mathfrak{c} \) be an invertible fractional ideal of \( \mathcal{O} \). Define the set \( \mathcal{P}_\mathfrak{c} \subseteq \mathfrak{c} \) by \( \mathcal{P}_\mathfrak{c} := \mathcal{P}_{\mathcal{O}_K} \cap \mathfrak{c} \).

With this definitions, we will establish the following theorem. Finally, we will derive Theorem 10.1 from Theorem 10.5.

**Theorem 10.5.** Let \( K \) be a number field of degree \( n \) and \( \mathcal{O} \) an order in \( K \). Let \( \mathfrak{c} \) be an invertible fractional ideal of \( \mathcal{O} \) and \( \mathfrak{w} \) be a \( \mathbb{Z} \)-basis of \( \mathfrak{c} \). Let \( \mathcal{P}_\mathfrak{c} \subseteq \mathfrak{c} \) be the set defined in Definition 10.4 (2). Assume that \( A \subseteq \mathcal{P}_\mathfrak{c} \) satisfies that \( \mathcal{I}_{\mathcal{P}_\mathfrak{c}, \mathfrak{w}}(A) > 0 \). Then there exists a sequence of pairwise disjoint finite subsets \((\mathcal{I}_l)_{l \in \mathbb{N}}\) of \( A \) such that the following holds: for every \( \theta \in (0, 1) \), for every finite subset \( S \subseteq \mathfrak{c} \), and for every \( \eta > 0 \), there exists a finite subset \( L \subseteq \mathbb{N} \) such that for every \( l \in \mathbb{N} \setminus L \), the following hold.

1. \( \mathcal{I}_l \) contains an \( S \)-constellation,
2. for every \( \alpha_1, \alpha_2 \in \mathcal{I}_l \),

\[
\frac{|N_{K/Q}(\alpha_2)|}{|N_{K/Q}(\alpha_1)|} \leq 1 + \eta \cdot \left( \min\{|N_{K/Q}(\alpha)| : \alpha \in \mathcal{I}_l\} \right)^{\theta - 1} \frac{1}{n}
\]

holds.

Theorem 10.5 in fact, can derive a result for the norm forms associated with the triple \((\mathcal{O}, \mathfrak{c}, \mathfrak{w})\) of an order \( \mathcal{O} \) in a number field of an arbitrary degree \( n \), an invertible fractional ideal \( \mathfrak{c} \) of \( \mathcal{O} \), and a basis \( \mathfrak{w} = (\gamma_1, \gamma_2, \ldots, \gamma_n) \) of \( \mathfrak{c} \); see Setting 10.35 for the definition. We will state the precise statement in Theorem 10.36. Elsholtz and Frei [EF19] have studied prime numbers
represented by norm forms. The novel point of our work is that we study combinatorics for the set of tuples \((x_1, x_2, \ldots, x_n)\) with respect to which the norm form represents primes. For this purpose, we need to establish our constellation theorem, Theorem 10.5.

In Subsections 10.2 and 10.3, we recall some definitions needed for the proofs of Theorems 10.5 and 10.1. Theorem 10.21 is the goal in these two subsections. In Subsection 10.4, we prove that \(\mathcal{P}_a \subseteq S\psi_{\log}(a)\) for every \(a \in \text{Ideals}_K\) with the aid of Theorem 6.33. In Subsection 10.5, we count certain subsets of \(\mathcal{P}_e\) by employing a version of the Chebotarev density theorem (Theorem 10.27). We prove Theorem 10.5 in Subsection 10.6. Finally, in Subsection 10.7, we establish Theorem 10.1, thus proving Theorem C as well.

**10.2 Preliminaries on invertible ideals of orders**

Here we review generalities of invertible fractional ideals of orders.

For a number field \(K\) of degree \(n\), an order \(\mathcal{O}\) in \(K\) is a subring of \(\text{O}_K\) such that \(\mathcal{O}\) is isomorphic to \(\mathbb{Z}^n\) as a \(\mathbb{Z}\)-module. In particular, \(\text{O}_K\) itself is an example of an order in \(K\); it is called the maximal order. One example of a non-maximal order is \(\mathbb{Z}[\sqrt{5}]\), where \(K = \mathbb{Q}(\sqrt{5})\). For this \(K\), the maximal order \(\mathcal{O}_K\) is \(\mathbb{Z}[(1 + \sqrt{5})/2]\). Orders in number fields are examples of 1-dimensional Noetherian integral domains; see for instance [Neu99, Chapter I, Proposition 12.2]. Recall that an (always associative commutative unital) ring is said to be Noetherian if every non-empty set of its ideals has a maximal element with respect to the inclusion relation. For a ring, the condition that it is a 1-dimensional integral domain is equivalent to saying that its only prime ideals are the zero ideal and the non-zero maximal ideals and that there exists at least one non-zero maximal ideal.

**Lemma 10.6.** Let \(\mathcal{O}\) be a 1-dimensional Noetherian integral domain. For every non-zero ideal \(\mathfrak{d} \subseteq \mathcal{O}\), there exist finitely many maximal ideals \(p_1, \ldots, p_s\), not necessarily distinct, such that \(p_1 \cdots p_s \subseteq \mathfrak{d}\) holds.

**Proof.** Let \(\Phi\) be the set of non-zero ideals which do not satisfy the claimed property. By way of contradiction, suppose \(\Phi\) is non-empty. Then by the Noetherian assumption, it has a maximal element. We write \(\mathfrak{d}\) for it. Note that \(\mathfrak{d}\) is not equal to \(\mathcal{O}\) or a maximal ideal because they trivially satisfy the claimed condition. Since \(\mathcal{O}\) is a 1-dimensional integral domain, it follows that \(\mathfrak{d}\) is not a prime ideal. Hence there exist elements \(a, b \in \mathcal{O} \setminus \mathfrak{d}\) with \(ab \in \mathfrak{d}\). The two ideals \(a\mathcal{O} + \mathfrak{d}\) and \(b\mathcal{O} + \mathfrak{d}\) are strictly larger than \(\mathfrak{d}\). By the maximality of \(\mathfrak{d}\), they do not belong to \(\Phi\). By the definition of \(\Phi\), there exist maximal ideals \(p_1, \ldots, p_r, p_{r+1}, \ldots, p_s\) such that \(p_1 \cdots p_r \subseteq a\mathcal{O} + \mathfrak{d}\) and that \(p_{r+1} \cdots p_s \subseteq b\mathcal{O} + \mathfrak{d}\). Take the product of the two inclusions above. The right-hand side of the product is contained in \(\mathfrak{d}\) by the relation \(ab \in \mathfrak{d}\). Hence we obtain \(p_1 \cdots p_s \subseteq \mathfrak{d}\). This contradicts \(\mathfrak{d} \notin \Phi\), and we conclude that \(\Phi\) is empty.

Also recall the following general fact.

**Lemma 10.7.** Let \(p\) and \(q\) be maximal ideals in a given ring. If there exists a positive integer \(e > 0\) such that \(p^e \subseteq q\) holds, then we have \(p = q\).
Proof. Since \( q \) is in particular a prime ideal, from the given inclusion we have \( p \subseteq q \). Then by the fact that \( p \) is maximal, we obtain the equality \( p = q \).

Now we recall the definition of invertible fractional ideals of an order.

**Definition 10.8.** Let \( K \) be a number field, and \( \mathcal{O} \) an order in \( K \). A non-zero \( \mathcal{O} \)-submodule \( c \) of \( K \) is called an invertible fractional ideal of \( \mathcal{O} \) if there exists a non-zero \( \mathcal{O} \)-submodule \( d \) of \( K \) such that \( cd = \mathcal{O} \). Here, the left-hand side is defined to be the \( \mathcal{O} \)-submodule of \( K \) generated by the set \( \{ cd : c \in c, \ d \in d \} \). Such a \( d \) is uniquely determined by \( c \), and is called the inverse fractional ideal of \( c \). It is written as \( c^{-1} \). If moreover \( c \subseteq \mathcal{O} \) holds, then we say that \( c \) is an invertible ideal of \( \mathcal{O} \).

By [Neu99, Chapter I, Proposition 3.8], every non-zero fractional ideal \( a \) of \( \mathcal{O}_K \) is invertible; see the discussion before Theorem 3.3. Lemma 10.9 (1) justifies the term ‘invertible fractional ideal.’

**Lemma 10.9.** Let \( K \) be a number field, \( \mathcal{O} \) an order in \( K \). Let \( c \) be an invertible fractional ideal of \( \mathcal{O} \).

1. The \( \mathcal{O} \)-submodule \( c \) is a finitely generated \( \mathcal{O} \)-module.

2. Let \( p \) be a maximal ideal. Then there exists an element \( c \in c \) such that for every ideal \( d \) containing a power \( p^e \) of \( p \), where \( e \in \mathbb{N} \), the multiplication map \( \mathcal{O} \ni x \mapsto cx \in c \) induces a bijection

\[
\mathcal{O}/d \cong c/cd.
\]

Proof. By \( c \cdot c^{-1} = \mathcal{O} \), there exist elements \( c_1, \ldots, c_r \in c \) and \( d_1, \ldots, d_r \in c^{-1} \) such that we have

\[
c_1d_1 + \cdots + c_rd_r = 1. \tag{10.3}
\]

Multiply this by an arbitrary \( c \in c \) to get \( c_1(d_1c) + \cdots + c_r(d_rc) = c \). Since we have \( d_ic \in \mathcal{O} \) for all \( i \in [r] \), this shows that \( c \) is generated by the elements \( c_1, \ldots, c_r \). This proves (1).

To show (2), in (10.3) note that for all \( i \in [r] \), \( c_id_i \in \mathcal{O} \) holds. It follows that there exists \( i \in [r] \) such that \( c_id_i \in \mathcal{O} \setminus p \). Fix such \( i \). We claim that \( c := c_i \) is an element with the desired property. To prove this claim, first observe the following equality of ideals of \( \mathcal{O} \): \( cc^{-1} + d = \mathcal{O} \). Indeed, suppose that it is not the case. Then, there must exist a maximal ideal \( q \) of \( \mathcal{O} \) containing the left-hand side. Since \( cd_i \in cc^{-1} \) is not contained in \( p \), we have that \( q \neq p \). However, by Lemma 10.7 \( p \) is the only maximal ideal that can contain \( d \), a contradiction. Thus we obtain \( cc^{-1} + d = \mathcal{O} \). By multiplying this by \( c \), we have \( c\mathcal{O} + cd = c \) as an equality of submodules of \( c \). This is equivalent to saying that the map (10.2) is surjective.

For the injectivity, apply [3.2] to \( cc^{-1} + d = \mathcal{O} \), and obtain that \( cc^{-1} \cap d = cc^{-1} \cdot d \). Since \( c \) is an invertible fractional ideal, we have that \( c\mathcal{O} \cap cd = cd \). This implies that if an element of the form \( cd \) with \( d \in \mathcal{O} \) belongs to \( cd \), then \( d \) is necessarily in \( d \). It is equivalent to the injectivity of the map (10.2).
Proposition 10.10. Let $K$ be a number field, and $\mathcal{O}$ an order in $K$. Let $\mathfrak{c}$ be an invertible fractional ideal of $\mathcal{O}$ and $\mathfrak{d} \subseteq \mathcal{O}$ a non-zero ideal. Then the $\mathcal{O}$-module $\mathfrak{c}/\mathfrak{c}\mathfrak{d}$ is isomorphic to $\mathcal{O}/\mathfrak{d}$. In particular, it is generated by a single element.

Proof. Recall that $\mathcal{O}$ is a 1-dimensional Noetherian integral domain. By Lemma 10.6, there exist distinct maximal ideals $p_1, \ldots, p_s$ of $\mathcal{O}$ and an exponent $e \geq 0$ such that $(p_1 \cdots p_s)^e \subseteq \mathfrak{d}$ holds. For each $i \in [s]$, set $\mathfrak{d}_i := \mathfrak{d} + p_i^e$. By Lemma 10.7, the ideals $\mathfrak{d}_i$, $i \in [s]$, are mutually coprime. Then by (3.2) we have $igcap_{i \in [s]} \mathfrak{d}_i = \prod_{i \in [s]} \mathfrak{d}_i$. Since $(p_1 \cdots p_s)^e \subseteq \mathfrak{d}$, this is contained in $\mathfrak{d}$. We trivially have $\mathfrak{d} \subseteq \bigcap_{i \in [s]} \mathfrak{d}_i$. Therefore, $\mathfrak{d} = \prod_{i \in [s]} \mathfrak{d}_i$ holds. Hence by (3.4), we have an isomorphism of $\mathcal{O}$-modules $\mathfrak{c}/\mathfrak{c}\mathfrak{d} \simeq \prod_{i \in [s]} \mathfrak{c}/\mathfrak{c}\mathfrak{d}_i$. By Lemma 10.9, for each $i \in [s]$, the $i$-th factor on the right-hand side is isomorphic to $\mathcal{O}/\mathfrak{d}_i$. Finally, the product $\prod_{i \in [s]} \mathcal{O}/\mathfrak{d}_i$ is isomorphic to $\mathcal{O}/\mathfrak{d}$ by (3.3).

Proposition 10.10 in particular implies Lemma 3.12, which has been employed in Section 8 in axiomatizations for constellation theorems.

Corollary 10.11. Let $K$ be a number field, and $\mathcal{O}$ an order in $K$. Let $\mathfrak{c}$ be an invertible fractional ideal of $\mathcal{O}$, and $f \in \mathcal{O}\setminus\{0\}$. Then there exists an element $x \in K^\times$ such that $x\mathfrak{c} + f\mathcal{O} = \mathcal{O}$ holds as an equality of $\mathcal{O}$-submodules of $K$. That means, the submodule $x\mathfrak{c}$ is contained in $\mathcal{O}$ and coprime with the given element $f$.

Proof. Apply Proposition 10.10 to $\mathfrak{c}^{-1}$ and $\mathfrak{d} = f\mathcal{O}$ to find an element $x \in \mathfrak{c}^{-1}\setminus\{0\}$ such that $x\mathcal{O} + fc^{-1} = c^{-1}$. By multiplying this by $\mathfrak{c}$, we obtain the desired equality.

10.3 Ideal norms of invertible fractional ideals

The goal of this subsection is to prove Theorem 10.21, which enables us to reduce the setting of an invertible fractional ideal of an order to a non-zero (integral) ideal of a maximal order (ring of integers). First, we recall the notion of the norm of invertible fractional ideals in the context of number fields, and then we provide a proof of Proposition 10.18 for the convenience of the reader.

Throughout this subsection, we assume the following setting:

Setting 10.12. Let $K$ be a number field of degree $n$, and $\mathcal{O}$ an order in $K$. Let $f$ be a positive integer satisfying $f\mathcal{O}_K \subseteq \mathcal{O}$.

Recall from Remark 3.6 that for $\alpha \in \mathcal{O}_K$, the element norm $N_{K/\mathbb{Q}}(\alpha)$ is defined as

$$N_{K/\mathbb{Q}}(\alpha) := \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_{r_1+2r_2}(\alpha) \in \mathbb{Z}.$$ 

Here, $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ are the embeddings of $K$ into $\mathbb{C}$.

Definition 10.13. Let $\mathfrak{c}$ be an invertible fractional ideal of $\mathcal{O}$.

(1) If $\mathfrak{c} \subseteq \mathcal{O}$, we define its ideal norm by $N(\mathfrak{c}) := \#(\mathcal{O}/\mathfrak{c})$. 
(2) We define the ideal norm of $c$ in the following manner: choose an element $d \in \mathcal{O} \setminus \{0\}$ such that $dc \subseteq \mathcal{O}$, and set
\[ N(c) := \frac{N(dc)}{N(d\mathcal{O})}. \] (10.4)

Note that in (1), the quotient group $\mathcal{O}/c$ is finite because both $\mathcal{O}$ and $c$ are free abelian groups of rank $n$. Also, when $\mathcal{O} = \mathcal{O}_K$, (1) is consistent with the definition of the ideal norm in Section 3. In (2), such an element $d$ exists by Lemma 10.9 (1). Moreover, well-definedness of (10.4) will be verified in Proposition 10.16.

**Remark 10.14.** An invertible fractional ideal $c$ of $\mathcal{O}$ can be an $\mathcal{O}'$-module for several different orders $\mathcal{O}'$. Nevertheless, the absence of the ring $\mathcal{O}$ from the symbol $N(c)$ is justified as follows.

Under the assumption that $c$ is an invertible fractional ideal of $\mathcal{O}$, the ring $\mathcal{O}$ can be recovered from $c \subseteq K$ as $\mathcal{O} = \{ x \in K \mid xc \subseteq c \}$.

**Lemma 10.15.** Let $c \subseteq K$ be a subgroup isomorphic to $\mathbb{Z}^n$ and $x \in \mathcal{O}_K \setminus \{0\}$. Assume that $xc \subseteq c$ as subsets of $K$. Then we have $\#(c/xc) = |N_{K/\mathbb{Q}}(x)|$.

**Proof.** Choose an arbitrary $\mathbb{Z}$-basis $w$ for $c$ and let $X$ be the matrix representing the map $c \ni c \mapsto xc \in c$ with respect to $w$. Then, we have $\#(c/xc) = |\det(X)|$. Recall that the norm $N_{K/\mathbb{Q}}(x)$ equals the determinant of the $\mathbb{Q}$-linear endomorphism $K \ni y \mapsto xy \in K$. Since $w$ may be seen as a $\mathbb{Q}$-basis of $K$, the result follows.

**Proposition 10.16.** Let $c$ be an invertible fractional ideal of $\mathcal{O}$.

(1) Assume that $c \subseteq \mathcal{O}$, and let $d \in \mathcal{O} \setminus \{0\}$. Then we have
\[ N(dc) = |N_{K/\mathbb{Q}}(d)| \cdot N(c). \] (10.5)

(2) The ideal norm of $c$ in (10.4) is independent of the choice of $d$. Moreover (10.5) holds for all invertible fractional ideals $c$ and all $d \in K^\times$.

**Proof.** First, we prove (1). By the filtration $dc \subseteq c \subseteq \mathcal{O}$, we have
\[ \#(c/dc) = \#(c) \cdot \#(c/dc). \]

By Lemma 10.15, we have $\#(c/dc) = |N_{K/\mathbb{Q}}(d)|$. Therefore, we obtain the desired formula (10.5).

For (2), let $c, d \in \mathcal{O} \setminus \{0\}$ be two elements with $\mathcal{O}c \subseteq \mathcal{O}$ and $dc \subseteq \mathcal{O}$. By (1), we have that
\[ N(cdc) = |N_{K/\mathbb{Q}}(c)|N(dc) = |N_{K/\mathbb{Q}}(d)|N(c). \]

From this, we obtain that $N(dc)/|N_{K/\mathbb{Q}}(d)| = N(c)/|N_{K/\mathbb{Q}}(c)|$. It ensures that Definition 10.13 (2) is well-defined. Equality (10.5) for the general case follows in a similar manner by repeated application of (1).

The following lemma describes a relationship between the ideal norm of an ideal of $\mathcal{O}$ and that of an ideal of $\mathcal{O}_K$.

**Lemma 10.17.** Let $c \subseteq \mathcal{O}$ be an invertible ideal satisfying $c + f\mathcal{O} = \mathcal{O}$. Then we have $N(c) = N(c\mathcal{O}_K)$. 


Proof. Consider the following commutative diagram

\[
\begin{array}{ccccccc}
0 & \rightarrow & \mathfrak{c} & \rightarrow & \mathcal{O} & \rightarrow & \mathcal{O}/\mathfrak{c} & \rightarrow & 0 \\
& & \downarrow & & \downarrow v & & \downarrow & & \\
0 & \rightarrow & \mathfrak{c}\mathcal{O}_K & \rightarrow & \mathcal{O}_K & \rightarrow & \mathcal{O}_K/\mathfrak{c}\mathcal{O}_K & \rightarrow & 0
\end{array}
\]

with exact rows. By the assumption $\mathfrak{c} + f\mathcal{O} = \mathcal{O}$, the integer $f$ is invertible in the rings $\mathcal{O}/\mathfrak{c}$ and $\mathcal{O}_K/\mathfrak{c}\mathcal{O}_K$. By definition, $f$ acts as zero on the quotient groups $\mathfrak{c}\mathcal{O}_K/\mathfrak{c}$ and $\mathcal{O}_K/\mathcal{O}$. Hence, by the snake lemma, we conclude that on the kernel and cokernel of the vertical map $v$, the integer $f$ acts as zero and invertibly at the same time. Therefore, $\ker(v)$ and $\coker(v)$ are both zero; in other words, $v$ is bijective. In particular, we obtain that

\[
N(\mathfrak{c}) = #(\mathcal{O}/\mathfrak{c}) = #(\mathcal{O}_K/\mathfrak{c}\mathcal{O}_K) = N(\mathfrak{c}\mathcal{O}_K),
\]

as desired. \hfill \Box

**Proposition 10.18.** Let $\mathfrak{c}$ be an invertible fractional ideal of $\mathcal{O}$. Then we have $N(\mathfrak{c}) = N(\mathfrak{c}\mathcal{O}_K)$.

Proof. By Corollary 10.11, there exists an element $x \in K^\times$ such that $x\mathfrak{c} + f\mathcal{O} = \mathcal{O}$ holds. By Lemma 10.17, we have $N(x\mathfrak{c}) = N(x\mathfrak{c}\mathcal{O}_K)$. By Proposition 10.16, this then implies that $|N_{K/Q}(x)|N(\mathfrak{c}) = |N_{K/Q}(x)|N(\mathfrak{c}\mathcal{O}_K)$. Hence, $N(\mathfrak{c}) = N(\mathfrak{c}\mathcal{O}_K)$. \hfill \Box

The following reduction theorem (Theorem 10.21) plays a key role in the proof of Theorem 10.3, as well as in the deduction of Theorem 10.1 from Theorem 10.5. Recall the definitions of $\mathcal{P}_a$ and $\mathcal{P}_c$ from Definition 10.4. To prove the reduction theorem, we employ the concept of signature. We recall the definition and a basic fact. Let $\text{Hom}(K, \mathbb{R})$ be the set of real embeddings of $K$, and $r_1 := \# \text{Hom}(K, \mathbb{R})$.

**Definition 10.19.** Let the signature $\text{sgn}(\xi)$ of an element $\xi \in K^\times$ be the tuple

\[
\text{sgn}(\xi) := \left( \text{sgn}(\sigma(\xi)) \right)_{\sigma \in \text{Hom}(K, \mathbb{R})} \in \{ \pm 1 \}^{\text{Hom}(K, \mathbb{R})}
\]

of signatures $\pm 1$ indexed by $\text{Hom}(K, \mathbb{R})$.

**Lemma 10.20.** For every signature $s \in \{ \pm 1 \}^{\text{Hom}(K, \mathbb{R})}$ and for every class $\tau \in \mathcal{O}_K/f\mathcal{O}_K$, there exists an element of $\mathcal{O}_K$ whose signature is $s$ and whose residue class is $\tau$.

If $r_1 = 0$, then we do not impose any condition on signatures.

Proof. Take a complete set of representatives $\mathcal{F}$ of $\mathcal{O}_K/f\mathcal{O}_K$ by addition. Consider the vector space $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^2$, which is isomorphic to $\mathbb{R}^n$ as a real vector space. Fix an arbitrary real vector norm $\| \cdot \|$ on $K \otimes_{\mathbb{Q}} \mathbb{R}$. Recall that each embedding $\sigma$ of $K$ into $\mathbb{R}$ or $\mathbb{C}$ extends to a $\mathbb{R}$-linear map $\sigma_\mathbb{R}$ from $K \otimes_{\mathbb{Q}} \mathbb{R}$; see Subsection 4.1. In particular, for each $x \in K \otimes_{\mathbb{Q}} \mathbb{R}$ with $N_{\mathbb{R}}(x) \neq 0$, we can define its signature $\text{sgn}_\mathbb{R}(x) \in \{ \pm 1 \}^{\text{Hom}(K, \mathbb{R})}$ by $\text{sgn}_\mathbb{R}(x) := \left( \text{sgn}(\sigma_\mathbb{R}(x)) \right)_{\sigma \in \text{Hom}(K, \mathbb{R})}$. For each $s \in \{ \pm 1 \}^{\text{Hom}(K, \mathbb{R})}$, consider $V := \{ x \in K \otimes_{\mathbb{Q}} \mathbb{R} :$
\( N_R(x) \neq 0, \, \text{sgn}_R(x) = s \}. \) Then, Lemma 4.3 implies that \( V \) is a non-empty open subset of \( K \otimes \mathbb{Q} R \); in addition, it is closed under multiplication of positive reals. Hence, we can take an open ball \( B \) inside \( V \) in \( \| \cdot \| \). Let \( R_1 := \sup \{ \inf \{ \| x - \alpha \| : \alpha \in fO_K \} : x \in K \otimes \mathbb{Q} R \} < \infty \). Let \( R_2 < \infty \) be the diameter of \( F \). Take \( t > 0 \) in such a way that the radius of \( tB \) is more than \( R_1 + R_2 \). Then, we conclude that there exists \( \alpha \in fO_K \) such that \( F + \alpha \subseteq tB \subseteq V \). This ensures the assertion.

\textbf{Theorem 10.21 (Reduction to ideals in maximal orders).} Assume Setting 10.12. Let \( \mathfrak{c} \) be an invertible fractional ideal of \( O \). Then there exists \( \xi \in K^\times \) such that the following three hold true. Here, we define \( a := \xi \mathfrak{c}O_K \).

1. The set \( \xi \mathfrak{c} \) is an ideal of \( O \), and it is coprime with \( f \).
2. The ideal \( a \) is coprime with \( f \).
3. The multiplication map \( \alpha \mapsto \xi \alpha \) in \( K \) induces injective maps from \( \mathfrak{c} \) to \( a \) and from \( \mathcal{P}_\mathfrak{c} \) to \( \mathcal{P}_a \).
4. For every \( \alpha \in \mathfrak{c} \), we have
   \[ \frac{N_{K/\mathbb{Q}}(\alpha)}{N(\mathfrak{c})} = \frac{N_{K/\mathbb{Q}}(\xi \alpha)}{N(a)}. \]

Note that (2) is implied by (1). Nevertheless, we explicitly state (2) because this property of \( a \) is frequently employed in the present section.

**Proof.** Apply Corollary 10.11 to \( \mathfrak{c} \) and \( f \). Then, we obtain \( \xi_0 \in K^\times \) such that \( \xi_0 \mathfrak{c} + fO = O \). Now, we divide the proof into the following two cases.

First, we treat the case of \( r_1 > 0 \). We define \( \xi \in K^\times \) from \( \xi_0 \) as follows. If \( N_{K/\mathbb{Q}}(\xi_0) > 0 \), then set \( \alpha := 1 \). Otherwise, we employ Lemma 10.20. Since \( r_1 > 0 \), we can find \( \alpha \in O_K \) which is congruent to 1 modulo \( f \) such that \( N_{K/\mathbb{Q}}(\alpha) < 0 \). Then, set \( \xi := \alpha \xi_0 \). Note that \( N_{K/\mathbb{Q}}(\xi) > 0 \). Since \( \alpha \in O_K \), Corollary 10.11 implies that \( \xi \mathfrak{c} \) is an ideal of \( O \). Since \( \xi_0 \mathfrak{c} + fO = O \) and \( \alpha \equiv 1 \mod f \), we have (1). Item (1) immediately implies (2). Next, we verify (3). First, by definition, we have \( \mathcal{P}_\mathfrak{c} \subseteq \mathcal{P}_{\xi \mathfrak{c}O_K} \). Then, observe that the multiplication map \( \alpha \mapsto \xi \alpha \) induces a bijection from \( \mathcal{P}_{\xi \mathfrak{c}O_K} \) to \( \mathcal{P}_a \). Indeed, for every \( \alpha \in \mathfrak{c} \), we have \( \alpha(\xi \mathfrak{c}O_K)^{-1} = (\xi \alpha)(\xi \mathfrak{c}O_K)^{-1} \). Hence, (3) holds. To prove (4), first observe that \( N(\mathfrak{c}) = N(\xi \mathfrak{c}O_K) \) by Proposition 10.16. Then, (4) follows from Proposition 10.16 (2). Here, recall that \( N_{K/\mathbb{Q}}(\xi) > 0 \).

Secondly, we deal with the case of \( r_1 = 0 \). In this case, we have \( N_{K/\mathbb{Q}}(\xi_0) > 0 \). Hence we can take \( \xi := \xi_0 \). Then, the argument above works. \( \square \)

Theorem 10.21 explains the reason why in Theorem 6.33 and in our axiomatizations in Sections 8 and 9, we only consider a non-zero ideal \( a \) of \( O_K \), instead of treating a general invertible fractional ideal \( \mathfrak{c} \) of an order \( O \).
10.4 ‘Prime elements’ in ideals and subpseudorandom condition

Let $K$ be a number field and $a$ be a non-zero fractional ideal of $K$. In Definition 10.4 [1], we define $\mathcal{P}_a$, which serves as the set of ‘prime elements’ in the proof of Theorem 10.1; see also Theorem 10.3. The following is the goal of this subsection.

**Theorem 10.22.** Let $K$ be a number field of degree $n$ and $a \in \text{Ideals}_K$. Then $\mathcal{P}_a$ is a member of $S\Psi_{\log}^\text{SI}(a)$.

The key to the proof is the Goldston–Yıldırım type asymptotic formula for ideals, stated in Theorem 6.33. Since we use the symbol $a$ for the coefficient of $F(x, y) = ax^2 + bxy + cz^2$, we use the symbol $\theta$ for the ‘parameter $a \in (0, 1)_{\mathbb{R}}$’ in the proof.

**Proof.** Fix a $C^\infty$-function $\chi: \mathbb{R} \to [0, 1]$ with $\chi(0) = 1$ and $\text{supp}(\chi) \subseteq [-1, 1]_{\mathbb{R}}$. Let $\theta \in (0, 1)_{\mathbb{R}}$ be arbitrary.

Now we fix a parameter $M \in \mathbb{R}_{>0}$. Let $w := \frac{\theta}{2} \log M$ and $W := \prod_{p \in \mathcal{P}_{\leq w}} p$. Fix a standard shape $S \subseteq a$ and set $r := \#S - 1$. Set $R$ by $R := M^{17(r+1)^2}$. Then we have $W \leq M^{\theta \log 2} < M^{\frac{1}{10}}$. Moreover, if $M$ is sufficiently large depending on $\theta$, then $R^{4(r+1)^2+1} \leq \frac{M^\theta}{W \log^2 M}$ holds. Define $\lambda: a \to \mathbb{R}_{\geq 0}$ as follows: for $\alpha \in a$,

$$\lambda(\alpha) := \frac{\kappa}{c_\chi \log R} \cdot \left(\Lambda_{R, \chi}^a(\alpha)\right)^2.$$

Here $\kappa$ is the constant appearing in Theorem 3.19 and $c_\chi := \int_0^\infty \chi^2(x)dx$; recall the definition of $\Lambda_{R, \chi}^a$ from (6.33). Then, by appealing to Theorem 6.33, we can prove that for every $\rho > 0$, if $M$ is sufficiently large depending on $\rho, S$ and $\theta$, then the following holds: for every $b \in a$ with $b\mathcal{O}_K + Wa = a$, the function $\beta \mapsto \frac{\varphi(W)}{W^n}(\lambda \circ \text{Aff}_{W, b})(\beta)$ on $a$ is a $\left(\rho, \frac{M^\theta}{W \log^2 M}, S\right)$-pseudorandom measure. Indeed, imitate the proofs of Theorems 7.4 and 8.6 in the current setting.

Let $v$ be a $\mathbb{Z}$-basis of $a$. Define an exceptional set $T \subseteq \mathcal{P}_a \cap a(v, M)$ by $T := \mathcal{P}_a \cap a(v, M) \cap \mathcal{O}_K(N(a) \cdot R)$. We claim that if $M$ is sufficiently large depending on $r, n$ and $\theta$, then every $\alpha \in \mathcal{P}_a \setminus T$ satisfies that $\alpha\mathcal{O}_K + Wa = a$. Indeed, since $\alpha \in \mathcal{P}_a$, there exists a prime ideal $p_\alpha$ such that $\alpha\mathcal{O}_K = p_\alpha a$. If $M$ is sufficiently large depending on $r, n$ and $\theta$, then the inequality $N(p_\alpha) > R$ implies that $p_\alpha$ is prime to $W$. Hence, $\alpha\mathcal{O}_K + Wa = a$ in this case. This argument in addition shows that for every $\alpha \in \mathcal{P}_a \setminus T$, we have $\lambda(\alpha) = \frac{\kappa}{17(r+1)2^r \cdot c_\chi} \cdot \log M$. Moreover, if $M$ is sufficiently large depending on $v$ and $\theta$, then by (8.2), we obtain $\#T \leq M_\theta^{\varphi}$.

Therefore, with

$$(D_1, D_2, \varepsilon) = \left(\frac{\kappa \theta}{17(r+1)2^r \cdot c_\chi}, \frac{\kappa \theta}{17(r+1)2^r \cdot c_\chi}, \frac{3}{4}\right),$$

we conclude the following: for every standard shape $S \subseteq a$ and for every $\rho > 0$, if $M$ is sufficiently large depending on $\rho, v, S$ and $\theta$, then $\mathcal{P}_a \cap a(v, M)$ satisfies the $(\rho, M, v, S, \theta)$-condition with parameters $(D_1, D_2, \varepsilon)$. Hence, $\mathcal{P}_a \in S\Psi_{\log}^\text{SI}(a)$. \qed
10.5 Counting by the Chebotarev density theorem

In order to establish Theorem 10.5, we will apply Theorem 9.20 to the set $A$; recall also the reduction theorem (Theorem 10.21). Since we have proved Theorem 10.22 in Subsection 10.4, what remains is to verify conditions (i) and (ii) in Theorem 8.21. As we will argue in Subsection 10.6, condition (ii) can be confirmed by Landau’s prime ideal theorem. Thus, the main task to apply Theorem 9.20 is the verification of condition (i). In this subsection, we will perform this counting argument, with the aid of a finer version of the Chebotarev density theorem (Theorem 10.27) than we have been using. See Theorems 10.31 and 10.34 for the statements of our countings. Two main differences between the counting argument in this section and that in previous sections are the following: first, we have additional data, such as $a$, $O$ and $c$. Secondly, when applying Theorem 10.3 in order to establish Theorem 10.1, we need to count elements with signs. Note that for every $\alpha \in O_K \setminus \{0\}$, we have $N(\alpha O_K) = |N_{K/Q}(\alpha)|$: to count elements with signs, the mere counting of ideals does not suffice, and extra data are required.

We utilize the following setting in this subsection, except in Theorem 10.34.

Setting 10.23. Let $K$ be a number field of degree $n$. Let $a$ be a non-zero ideal of $O_K$, and $f \in \mathbb{N}$. Assume that $a$ is prime to $f$. Let $O$ be an order in $K$, and $c$ be an invertible fractional ideal of $O$. Let $r_1 := \#\text{Hom}(K, \mathbb{R})$. Let $\varphi_K$ be the totient function of $K$ (Definition 3.8).

In what follows, if $r_1 = 0$, equivalently, if $\text{Hom}(K, \mathbb{R}) = \emptyset$, then we do not impose any condition on signatures.

First, we treat the case of $P_a$; then we proceed to the case of $P_c$, where an order shows up. We collect some terminology appearing in Theorem 10.27 and recall some basic facts and definitions to state the Chebotarev density theorem. Recall that for $f \in \mathbb{N}$, a non-zero fractional ideal $a$ of $O_K$ is said to be coprime with $f$, or prime to $f$, if the prime ideal decompositions (Theorem 3.3) of $a$ and $f$ share no prime factors.

For $\xi \in K^\times$ and $\alpha \in O_K$, we write $\xi \equiv \alpha \pmod{f}$ if there exist $x \in fO_K$ and $y \in O_K \setminus \{0\}$ with $y$ prime to $f$ such that $\xi = \alpha + \frac{x}{y}$.

Definition 10.24. (1) We denote by $I^f_K$ the commutative group of fractional ideals of $O_K$ coprime with $f$.

(2) Let $K^\times_{f+}$ be the subgroup of elements of $K^\times$ which are congruent to 1 modulo $f$ and totally positive. Namely, set

$$K^\times_{f+} := \left\{ \xi = 1 + \frac{x}{y} \in K : \begin{array}{l} x \in fO_K, \ y \in O_K \setminus \{0\} \text{ prime to } f, \\ \text{sgn}(\xi) = (+1, \ldots, +1) \end{array} \right\}.$$

Then the map $\xi \mapsto \xi O_K$ gives rise to a homomorphism from $K^\times_{f+}$ to $I^f_K$.

(3) We define the ideal class group $\text{Cl}^f_K$ with modulus $f$ as the cokernel of the homomorphism from $K^\times_{f+}$ to $I^f_K$ above. We define $h_f$ as the order of $\text{Cl}^f_K$. 

(4) Let $\mathcal{O}_{K,f+}^\times$ be the subgroup of $\mathcal{O}_K^\times$ consisting of the elements which are congruent to 1 modulo $f$ and which are totally positive.

In [3], it is well known that $h_f$ is finite; for instance, see [Neu99, Chapter VI, Proposition 1.8 and Proposition 1.9]. In Definition 10.24 we followed the signature convention of [Neu99] and [Hei67]. The group $\mathcal{O}_{K,f+}^\times$ is the kernel of a natural homomorphism $\mathcal{O}_K^\times \to (\mathcal{O}_K/f\mathcal{O}_K)^\times \times \{\pm 1\}^{\text{Hom}(K,R)}$. Since $(\mathcal{O}_K/f\mathcal{O}_K)^\times \times \{\pm 1\}^{\text{Hom}(K,R)}$ is a finite group, we have that $\text{rank}(\mathcal{O}_{K,f+}) = \text{rank}(\mathcal{O}_K^\times)$.

Note that under Setting 10.23 the ideal $\mathfrak{a}$ is assumed to be coprime with $f$. For $\tau \in \mathcal{O}_K/f\mathcal{O}_K$, recall that we regard $\tau$ as a subset of $\mathcal{O}_K$.

**Definition 10.25.** Given $\tau \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ and a signature $s \in \{\pm 1\}^{\text{Hom}(K,R)}$, we define the set $|\text{Spec}(\mathcal{O}_K)|_{\mathfrak{a},\tau,s}$ of prime ideals by

$$|\text{Spec}(\mathcal{O}_K)|_{\mathfrak{a},\tau,s} := \{ \mathfrak{p} \in |\text{Spec}(\mathcal{O}_K)| : \mathfrak{p}\mathfrak{a} = \alpha\mathcal{O}_K \text{ for some } \alpha \in \tau \text{ with sgn}(\alpha) = s \}.$$ 

We will state the version of the Chebotarev density theorem which we will employ in our present counting arguments. This can be deduced from the version appearing in [Hei67, Theorem 4]. In what follows, we explain the deduction. Let $\tau \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ and $s \in \{\pm 1\}^{\text{Hom}(K,R)}$. Fix an element $\xi_0 \in K^\times$ with signature $s$ such that $\xi_0 \in \tau$; the existence of $\xi_0$ is ensured by Lemma 10.26. Since $\mathfrak{a}$ is prime to $f$, we can consider the class $[\mathfrak{a}]$ of $\mathfrak{a}$ in the ideal class group $\text{Cl}_K^f$.

**Lemma 10.26.** In the setting above, we have

$$|\text{Spec}(\mathcal{O}_K)|_{\mathfrak{a},\tau,s} = \{ \mathfrak{p} \in |\text{Spec}(\mathcal{O}_K)| : [\mathfrak{p}] = -[\mathfrak{a}] + [\xi_0\mathcal{O}_K] \text{ in } \text{Cl}_K^f \}.$$ 

**Proof.** Let $\mathfrak{p} \in |\text{Spec}(\mathcal{O}_K)|_{\mathfrak{a},\tau,s}$. That means, there exists $\alpha \in \tau$ with sgn$(\alpha) = s$ such that $\mathfrak{p}\mathfrak{a} = \alpha\mathcal{O}_K$. Then $\xi := \alpha/\xi_0 \in K^\times$ satisfies that $\xi \equiv 1 \text{ (mod } f) \text{ and sgn}(\xi) = (+1, \ldots, +1)$. Therefore we conclude that $[\alpha\mathcal{O}_K] = [\xi_0\mathcal{O}_K]$ in $\text{Cl}_K^f$, thus proving that $\mathfrak{p}$ satisfies $[\mathfrak{p}] = -[\mathfrak{a}] + [\xi_0\mathcal{O}_K]$.

Conversely, suppose that $\mathfrak{p}$ satisfies $[\mathfrak{p}] + [\mathfrak{a}] = [\xi_0\mathcal{O}_K]$. Then by the definition of $\text{Cl}_K^f$, there exists a totally positive $\eta \in K^\times$ with $\eta \equiv 1 \text{ (mod } f)$ such that $\mathfrak{p}\mathfrak{a} = \xi_0\eta\mathcal{O}_K$. Now $\alpha := \xi_0\eta$ satisfies that $\alpha \in \tau$ and that sgn$(\alpha) = s$. Moreover, since $\mathfrak{p}$ and $\mathfrak{a}$ are subsets of $\mathcal{O}_K$, we have $\alpha\mathcal{O}_K \subseteq \mathcal{O}_K$. Therefore, we conclude that $\alpha \in \mathcal{O}_K \setminus \{0\}$, as desired.

A version of the Chebotarev density theorem, stated in [Hei67, Theorem 4], asserts that for every $\mu \in \text{Cl}_K^f$, the set $\{ \mathfrak{p} \in |\text{Spec}(\mathcal{O}_K)| : [\mathfrak{p}] = \mu \text{ in } \text{Cl}_K^f \}$ has relative natural asymptotic density $\frac{1}{h_f}$ with respect to $|\text{Spec}(\mathcal{O}_K)|$ measured by the ideal norm. Thus, by Lemma 10.26, we can deduce the following version of the Chebotarev density theorem.

**Theorem 10.27.** (A version of the Chebotarev density theorem, see [Hei67, Theorem 4]). Under Setting 10.23 let $\tau \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ and $s \in \{\pm 1\}^{\text{Hom}(K,R)}$. Then, we have that

$$\# \{ \mathfrak{p} \in |\text{Spec}(\mathcal{O}_K)|_{\mathfrak{a},\tau,s} : N(\mathfrak{p}) \leq L \} = (1 + o_{L \to \infty,f,a}(1)) \cdot \frac{1}{h_f} \cdot \frac{L}{\log L}.$$
Now we turn this counting of prime ideals into that of elements. First, we treat the case of $P_a$.

**Definition 10.28.** For every $\tau \in \mathcal{O}_K/f\mathcal{O}_K$ and every $s \in \{\pm 1\}^{\text{Hom}(K,\mathbb{R})}$, define a subset $P_{a;\tau,s}$ of $P_a$ as the set of $\alpha \in P_a$ with signature $s$ such that $\alpha \in \tau$.

**Lemma 10.29.** Let $\mathcal{D}' \subseteq a \setminus \{0\}$ be a fundamental domain for the action $\mathcal{O}_K^{\times,f} \curvearrowright a \setminus \{0\}$ by multiplication.

1. The set $P_a$ can be partitioned as $P_a = \bigsqcup_{(\tau,s)} P_{a;\tau,s}$. Here $(\tau,s)$ runs over $(\mathcal{O}_K/f\mathcal{O}_K) \times \{\pm 1\}^{\text{Hom}(K,\mathbb{R})}$.

2. For each $(\tau,s) \in (\mathcal{O}_K/f\mathcal{O}_K) \times \{\pm 1\}^{\text{Hom}(K,\mathbb{R})}$, the $\mathcal{O}_K^{\times,f}$-action by multiplication leaves $P_{a;\tau,s}$ invariant. If $\tau \in \mathcal{O}_K/f\mathcal{O}_K$ is not invertible, then $\#(P_{a;\tau,s}/\mathcal{O}_K^{\times,f}) < \infty$. Here $P_{a;\tau,s}/\mathcal{O}_K^{\times,f}$ means the quotient set by the $\mathcal{O}_K^{\times,f}$-action.

3. If $\tau \in (\mathcal{O}_K/f\mathcal{O}_K)^{\times}$, the following map gives rise to a bijective correspondence:

$$|\text{Spec}(\mathcal{O}_K)|_{a;\tau,s} \simeq P_{a;\tau,s} \cap \mathcal{D}'.$$  \hspace{1cm} (10.6)

Here, a prime ideal $p \in |\text{Spec}(\mathcal{O}_K)|_{a;\tau,s}$ is sent to a unique element $\alpha \in \mathcal{D}'$ which satisfies the following three conditions: $p\alpha = \alpha \mathcal{O}_K$, $\alpha \in \tau$, and $\text{sgn}(\alpha) = s$.

**Proof.** Item [1] is trivial. Next we prove [2]. For the former assertion, observe that the $\mathcal{O}_K^{\times,f}$-action changes neither the modulo $f$ residue class nor the signature of elements of $\mathcal{O}_K$. For the latter assertion, suppose that $\tau \notin (\mathcal{O}_K/f\mathcal{O}_K)^{\times}$. Take an element $\alpha$ of $P_{a;\tau,s}$. Then, $\alpha$ is not prime to $f$. Since $a$ is prime to $f$, the prime ideal $p = \alpha a^{-1}$ is not coprime with $f$. Therefore, $p$ divides $f$. In general, given $a$ and $p$, the cardinality of $\{\alpha \in \mathcal{O}_K : ap = \alpha \mathcal{O}_K\}/\mathcal{O}_K^{\times}$ is either 0 or 1. Since $\mathcal{O}_K^{\times,f}$ is a finite index subgroup of $\mathcal{O}_K^{\times}$, the latter assertion holds.

Finally, we prove [3]. For a given $p \in |\text{Spec}(\mathcal{O}_K)|_{a;\tau,s}$, by the very definition of $|\text{Spec}(\mathcal{O}_K)|_{a;\tau,s}$, there exists $\alpha \in \mathcal{O}_K \setminus \{0\}$ which fulfills the three conditions in the statement. Such an element $\alpha$ is automatically in $P_{a;\tau,s}$ by its definition. What remains is to show that this $\alpha$ is unique modulo the $\mathcal{O}_K^{\times,f}$-action. Take two elements $\alpha_1$ and $\alpha_2$ with the three conditions. Since they define the same ideal, we have that $\xi := \alpha_1/\alpha_2 \in \mathcal{O}_K^{\times}$. Since $\alpha_1, \alpha_2 \in \tau$ and they have signature $s$, in addition have that $\xi \equiv 1 \pmod{f}$ and that $\xi$ is totally positive. Here, recall that we assume $\tau \in (\mathcal{O}_K/f\mathcal{O}_K)^{\times}$. Therefore $\xi \in \mathcal{O}_K^{\times,f}$, as desired. Conversely, suppose that we are given $\alpha \in P_{a;\tau,s}$. By Definition 10.4, $p := \alpha a^{-1}$ is a prime ideal. By Definition 10.25, $p$ belongs to $|\text{Spec}(\mathcal{O}_K)|_{a;\tau,s}$. Thus, we obtain a map $\alpha \mapsto p$. Since both maps are constructed from the relation $ap = \alpha \mathcal{O}_K$, it is clear that they are inverse to each other.

**Corollary 10.30.** Assume Setting 10.23. Let $\mathcal{D}'$ be a fundamental domain for the action $\mathcal{O}_K^{\times,f} \curvearrowright a \setminus \{0\}$. Let $s \in \{\pm 1\}^{\text{Hom}(K,\mathbb{R})}$. 
(1) If $\tau \notin (\mathcal{O}_K/f\mathcal{O}_K)^\times$, then the relative asymptotic density of $\mathcal{P}_{a,\tau,s} \cap \mathcal{D}'$ with respect to $\mathcal{P}_a \cap \mathcal{D}'$ measured by the ideal norm equals 0. That means,
\[
\lim_{L \to \infty} \frac{\#(\mathcal{P}_{a,\tau,s} \cap \mathcal{D}' \cap \mathcal{O}_K(L))}{\#(\mathcal{P}_a \cap \mathcal{D}' \cap \mathcal{O}_K(L))} = 0.
\]

(2) If $\tau \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$, then
\[
\lim_{L \to \infty} \frac{\#(\mathcal{P}_{a,\tau,s} \cap \mathcal{D}' \cap \mathcal{O}_K(L))}{\#(\mathcal{P}_a \cap \mathcal{D}' \cap \mathcal{O}_K(L))} = \frac{1}{2^r \varphi_K(f)}.
\]

Proof. Both items follow from Theorem 10.27 and Lemma 10.29: the factors $2^r$ and $\varphi_K(f)$ come from the numbers of possible choices, respectively, of $s$ and $\tau$.

Finally, we have the following counting from below of $\mathcal{P}_a$.

**Theorem 10.31.** Assume Setting 10.23. Let $\tau \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ and $s \in \{\pm 1\}^\text{Hom(K,R)}$. Then, for every $\mathbb{Z}$-basis $\mathbf{v}$ of $a$, we have that
\[
\liminf_{M \to \infty} \frac{\#(\mathcal{P}_{a,\tau,s} \cap a(\mathbf{v}, M))}{M^n (\log M)^{-1}} > 0.
\]

For the proof, recall that the NL-compatibility is defined for a subset of $\mathcal{O}_K \setminus \{0\}$, in particular, for a subset of $a \setminus \{0\}$. Recall also for an integral basis $\omega$ of $K$, the restriction of $\|\cdot\|_{\infty,\omega}$ on $a$ is bi-Lipschitz equivalent to $\|\cdot\|_{\infty,\mathbf{v}}$.

Proof. Fix a $\mathbb{Z}$-basis $\mathbf{v}$ of $a$. First, we claim that there exists an NL-compatible fundamental domain for the action $\mathcal{O}^\times_{K,f+} \curvearrowleft a \setminus \{0\}$. Indeed, by Proposition 4.11 we can take an NL-compatible $\mathcal{O}^\times_K$-fundamental domain $\mathcal{D} \subseteq \mathcal{O}_K \setminus \{0\}$. Since $\mathcal{O}^\times_{K,f+}$ has a finite index in $\mathcal{O}^\times_K$, by considering the union of finitely many translates of $\mathcal{D}$, we have an NL-compatible fundamental domain $\mathcal{D} \subseteq \mathcal{O}_K \setminus \{0\}$ for the action $\mathcal{O}^\times_{K,f+} \curvearrowleft \mathcal{O}_K \setminus \{0\}$. Finally, set $\mathcal{D}' := a \cap \mathcal{D}$; then this $\mathcal{D}'$ is an NL-compatible fundamental domain for $\mathcal{O}^\times_{K,f+} \curvearrowleft a \setminus \{0\}$.

Now the assertion follows from Corollary 10.30 (2) and the NL-compatibility of $\mathcal{D}'$; the deduction goes along the same line as one in the proof of Proposition 8.12.

In the rest of the current subsection, we treat the case of $\mathcal{P}_c$; recall from Setting 10.23 that $c$ is an invertible ideal of an order $\mathcal{O}$.

**Lemma 10.32.** Under Setting 10.23, assume furthermore that $f\mathcal{O}_K \subseteq \mathcal{O}$. Then the following diagram
\[
\begin{array}{ccc}
\mathcal{O} & \to & \mathcal{O}/f\mathcal{O}_K \\
\cap & & \cap \\
\mathcal{O}_K & \to & \mathcal{O}_K/f\mathcal{O}_K
\end{array}
\]
is Cartesian. That means, elements of $c\mathcal{O}_K$ whose image in $c\mathcal{O}_K/fc\mathcal{O}_K$ is contained in $c/fc\mathcal{O}_K$ lie in $c$. 
Proof. The inclusion $f \cO_K \subseteq \cO = \c$ implies the assertion.

Lemma 10.33. Let $\d \subseteq \O$ be an ideal coprime with $f$. Assume that $f \cO_K \subseteq \O$. Then in the following diagram induced by the inclusion maps,

$$
\begin{array}{ccc}
\d/f\d\O_K & \rightarrow & \O/f\cO_K \\
\downarrow & & \downarrow \\
\d\O_K/f\d\O_K & \rightarrow & \O_K/f\cO_K
\end{array}
$$

both horizontal maps are bijective.

Proof. The assumption $\d + f = \O$ implies that $\d + f \cO_K = \O$. By the second isomorphism theorem, we obtain that $\d/(\d \cap f \cO_K) \simeq \O/f \cO_K$. Since $\d$ and $f \cO_K$ are coprime, their intersection is equal to their product. This shows that the upper horizontal map of the diagram above is an isomorphism. For the lower horizontal map, we can prove that this is an isomorphism in a similar manner with the aid of $\d \O_K + f \cO_K = \O_K$.

Now we are ready to present our counting result for $\P c$. Recall our reduction theorem, Theorem 10.21.

Theorem 10.34. Let $K$ be a number field of degree $n$, and $\O$ an order in $K$. Let $\c$ be an invertible fractional ideal of $\O$. Let $f \in \N$ be such that $f \cO_K \subseteq \O$. Take $\xi \in K^\times$ and $\a \in \text{Ideals}_K$ as in Theorem 10.21. Let $\tau \in (\O/f \cO_K)^\times$ and $s \in \{\pm 1\}^{\text{Hom}(K, \R)}$. Then for every $\Z$-basis $\v$ of $\a$, we have that

$$
\liminf_{M \to \infty} \frac{\#(\xi \P c \cap \P a_{\tau,s} \cap \a(\v, M))}{M^n (\log M)^{-1}} > 0.
$$

Proof. Set $\c' := \xi c$. Note that by Theorem 10.21, $\c'$ is an ideal of $\O$ prime to $f$. Then, the following Cartesian diagram

$$
\begin{array}{ccc}
\P c' & \rightarrow & \O/f \cO_K \\
n & \cap & n \\
\P a & \rightarrow & \O_K/f \cO_K
\end{array}
$$

is obtained by Lemmas 10.32 and 10.33. Indeed, apply Lemma 10.32 with $\c$ replaced by $\c'$, and Lemma 10.33 with $\d$ replaced by $\c'$. Also, recall that $\a = \c \O_K$. Hence, for all $(\tau, s) \in (\O/f \cO_K) \times \{\pm 1\}^{\text{Hom}(K, \R)}$, we have $\P c' \cap \P a_{\tau,s} = \P a_{\tau,s}$. By definition, we have $\P c' = \xi \P c$. Since $\a$ is prime to $f$, Theorem 10.31 applies to $\a$. This ends the proof.

Note that we have $(\O/f \cO_K)^\times \neq \emptyset$ because $1 \in \O$.

10.6 Proof of Theorem 10.5

Now we are ready to establish Theorem 10.5.
Proof of Theorem 10.5. Fix $f \in \mathbb{N}$ with $fO_K \subseteq \mathcal{O}$. First, apply Theorem 10.21 to $(\mathcal{O}, f, c)$. Then we obtain $\xi \in K^*$ and $a \in \text{Ideals}_{K}$, which is coprime with $f$. Fix a $\mathbb{Z}$-basis $v$ of $a$. Let $c' := \xi c$, and $w' := \xi w$. Set $A' := \xi A$. Then, $c' \subseteq a$, and the restriction of $\| \cdot \|_{\infty,v}$ on $c'$ is bi-Lipschitz equivalent to $\| \cdot \|_{\infty,w'}$. Apply Theorem 10.34 with $\tau = 1 \mod f \in (\mathcal{O}/fO_K)^\times$. The assumption $d_{\mathcal{O},w}(A) > 0$ then implies that

$$\limsup_{M \to \infty} \frac{\#(A' \cap a(v, M))}{M^a(\log M)^{-1}} > 0.$$ 

By Theorem 10.22 and Lemma 9.13 [2], this set $A'$ is a member of $S\Psi^{\mathbb{S}}_{\log}(a)$. In what follows, we will verify that $A'$ fulfills condition (i) of Theorem 8.21. In fact, we will prove that $P_{\mathcal{O}}$ satisfies this. Let $L \in \mathbb{R}_{>2}$. Let $\beta \in P_{\mathcal{O}} \cap O_K(L)$. Then, by definition, $p_\beta := \beta a^{-1}$ is a prime ideal. Hence, $N(p_\beta) \leq L/N(a) \leq L$. Since $p_\beta$ is a prime ideal, Theorem 3.21 implies that there exists $\Delta > 0$ such that for every $L \in \mathbb{R}_{>2}$,

$$\#\{\beta O_K : \beta \in P_{\mathcal{O}} \cap O_K(L)\} \leq \Delta \cdot \frac{L}{\log L}.$$ 

Since $A' \subseteq P_{\mathcal{O}}$, we can take the same $\Delta > 0$ for $A'$.

Therefore, Theorem 9.20 applies to $A'$, and we have a sequence $(\mathcal{T}_l)_{l \in \mathbb{N}}$ of finite subsets in $A'$. Finally, via the map $A' \ni \beta \mapsto \xi^{-1} \beta \in A$, we construct a sequence $(\mathcal{T}_l)_{l \in \mathbb{N}}$ of finite subsets in $A$. Namely, for every $l \in \mathbb{N}$, set $\mathcal{T}_l := \xi^{-1} \mathcal{T}_l'$. Then, this sequence $(\mathcal{T}_l)_{l \in \mathbb{N}}$ fulfills all conditions in Theorem 10.5. Indeed, to verify (2), note that by Theorem 10.21 (4) for $\alpha \in A$,

$$N_{K/Q}(\alpha) = \frac{N(c)}{N(a)} \cdot N_{K/Q}(\xi \alpha);$$

the factor $\frac{N(c)}{N(a)}$ does not depend on $\alpha$. 

\[ \square \]

### 10.7 Proofs of Theorem C and Theorem 10.1

In this subsection, we will establish Theorem 10.1. Since Theorem 10.1 immediately implies Theorem C and Theorem 1.6, we will obtain these theorems as well. In fact, we prove the following theorem on norm forms associated with an invertible fractional ideal of an order in a number field.

**Setting 10.35.** Let $K$ be a number field of degree $n$, and $\mathcal{O}$ an order in $K$. Let $c$ be an invertible fractional ideal. Let $u$ be the standard basis of $\mathbb{Z}^n$, $w = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ be a $\mathbb{Z}$-basis of $c$, and $\iota: \mathbb{Z}^n \to c$ be the isomorphism of $\mathbb{Z}$-modules which sends $u$ to $w$. Let $F = F_{(\mathcal{O}, \mathcal{O},w)}: \mathbb{Z}^n \to \mathcal{O}$ be the norm form associated with $(\mathcal{O}, c, w)$, meaning that, for all $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$,

$$F_{(\mathcal{O}, \mathcal{O},w)}(x_1, x_2, \ldots, x_n) := \frac{N_{K/Q}(\gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n)}{N(c)}.$$ 

In other words, $F_{(\mathcal{O}, \mathcal{O},w)} = (N(c))^{-1}(N_{K/Q} \circ \iota)$. Set $r_1 := \# \text{Hom}(K, \mathbb{R})$ and $r_2$ to be the number of pairs of imaginary embeddings of $K$. 

Theorem 10.36 (Szemerédi-type theorem on prime representations of norm forms). Assume Setting 10.35. If $r_1 > 0$, then take an arbitrary $\epsilon \in \{\pm 1\}$; if $r_1 = 0$, then set $\epsilon = +1$. Let $A \subseteq F^{-1}(\epsilon P)$ be a set with $\delta_{F^{-1}(\epsilon P), u}(A) > 0$. Then, there exists a sequence of pairwise disjoint finite subsets $(T_l)_{l \in \mathbb{N}}$ of $A$ which fulfills the following two conditions.

(a) For every $l \in \mathbb{N}$, $F |_{T_l} : T_l \to \mathcal{P}_Q$ is injective.

(b) For every $\theta \in (0, 1)_\mathbb{R}$, for every finite subset $S \subseteq \mathbb{Z}^n$ and for every $\eta > 0$, there exists a finite subset $L \subseteq \mathbb{N}$ such that for every $l \in \mathbb{N} \setminus L$, the following hold:

(b1) $T_l$ contains an $S$-constellation,

(b2) for every $p_1, p_2 \in F(T_l)$,

$$\frac{|p_2|}{|p_1|} \leq 1 + \eta \cdot (\min\{|p| : p \in F(T_l)\})^{\frac{\theta - 1}{n}}$$

holds.

Remark 10.37. In Theorem 10.36, $r_1 = 0$ if and only if $K$ is totally imaginary. In this case, the norm form $F$ is positive definite. Theorem 10.36 asserts that this is the only obstruction to obtaining our constellation theorem with signature $\epsilon = -1$.

To prove Theorem 10.36, take $f \in \mathbb{N}$ with $f \mathcal{O}_K \subseteq \mathcal{O}$. Apply Theorem 10.21 to $(\mathcal{O}, f, c)$, and obtain $\xi \in K^\times$ and an ideal $a \in \text{Ideals}_K$ coprime with $f$. Recall the definition of the degree of a prime ideal from Subsection 3.3.

Definition 10.38. Assume Setting 10.35. Let $\epsilon \in \{\pm 1\}$. Let $\xi$ and $a$ be as in Theorem 10.21.

(1) Define $|\text{Spec}(\mathcal{O}_K)|^1$ as the set of prime ideals of $\mathcal{O}_K$ of degree 1.

(2) Define $\mathcal{P}_\epsilon$ as the set of $\alpha \in \mathcal{P}$ such that $N_{K/Q}(\alpha)$ has signature $\epsilon$.

(3) Define $\mathcal{P}_\epsilon^{1, \epsilon}$ by

$$\mathcal{P}_\epsilon^{1, \epsilon} := \{\alpha \in \mathcal{C} : (\xi \alpha)a^{-1} \in |\text{Spec}(\mathcal{O}_K)|^1 \text{ and } N_{K/Q}(\alpha) \text{ has signature } \epsilon\}.$$ 

Recall the isomorphism $\iota : \mathbb{Z}^n \to \mathcal{C}$ of $\mathbb{Z}$-modules from Setting 10.35.

Lemma 10.39. The map $\iota$ sends the set $F^{-1}(\epsilon P)$ bijectively to $\mathcal{P}_\epsilon^{1, \epsilon}$.

Proof. The composite map $F \circ \iota^{-1}$ is computed as:

$$\epsilon \ni \alpha \mapsto N_{K/Q}(\alpha)N(c)^{-1}.$$ 

(10.9)

This last value has signature $\text{sgn}(N_{K/Q}(\alpha))$. Also, the right-hand side of (10.9) has absolute value $N(\alpha c^{-1})$, which equals $N((\xi \alpha)c^{-1})$ by Theorem 10.21 (4). Note that for $b \in \text{Ideals}_K$, $b \in |\text{Spec}(\mathcal{O}_K)|^1$ if and only if $N(b) \in \mathcal{P}$. This ends our proof. \qed
The next lemma discusses the inclusions \( \mathcal{P}^1_{\epsilon, \xi} \subseteq \mathcal{P}^\epsilon \subseteq \mathcal{P} \) multiplied by \( \xi \). The conclusions of \( \text{Lemma 10.40} \) are equivalent to \( d_{\mathcal{P}^\epsilon, v}(\mathcal{P}^\epsilon) > 0 \) and \( d_{\mathcal{P}^1_{\epsilon, \xi}, v}(\mathcal{P}^1_{\epsilon, \xi}) = 1 \).

**Lemma 10.40.** Assume Setting \( \text{[10.35]} \). Let \( \xi \) and \( a \) be as in Theorem \( \text{[10.21]} \). Let \( v \) be a \( \mathbb{Z} \)-basis of \( a \). Let \( \epsilon \) be an arbitrary signature \( \epsilon \in \{ \pm 1 \} \) if \( r_1 > 0 \); otherwise, let \( \epsilon = +1 \). Set \( \mathcal{P}'_2 := \xi \mathcal{P}^1_{\epsilon, \xi} \), \( \mathcal{P}'_2 := \xi \mathcal{P}^\epsilon \) and \( \mathcal{P}'_3 := \xi \mathcal{P} \). Then, we have \( d_{\mathcal{P}'_2, v}(\mathcal{P}'_2) > 0 \) and \( d_{\mathcal{P}'_2, v}(\mathcal{P}'_3) = 1 \).

**Proof.** First, we prove \( d_{\mathcal{P}'_2, v}(\mathcal{P}'_2) > 0 \). If \( r_1 = 0 \), then the norm form \( F \) is positive definite. Hence we have \( \mathcal{P}'_2 = \mathcal{P}'_2 \); recall we have taken \( \epsilon = +1 \) in this case. Now we treat the remaining case of \( r_1 > 0 \). By Theorem \( \text{[10.34]} \), Cartesian diagram \( \text{(10.8)} \) states that \( \mathcal{P}'_2 \supseteq \bigcup_{(\tau, r)} \mathcal{P}_{a, \tau, r} \).

Here \( (\tau, r) \) runs over the set of pairs \( (\tau, r) \) with \( \tau \in (\mathcal{O}/f\mathcal{O}_K) \) and \( s = (s_1, s_2, \ldots, s_{r_1}) \in \{ \pm 1 \}^{\text{Hom}(\mathcal{K}, \mathbb{R})} \) satisfying \( s_1 s_2 \cdots s_{r_1} = \epsilon \). Note that this set of pairs is non-empty because \( 1 \in \mathcal{O} \) and \( r_1 > 0 \). Corollary \( \text{[10.30]} \) and Theorem \( \text{[10.31]} \) apply. Hence, in this case, we also conclude that \( d_{\mathcal{P}'_2, v}(\mathcal{P}'_2) > 0 \). See also Remark \( \text{[8.23]} \).

Secondly, we prove \( d_{\mathcal{P}'_2, v}(\mathcal{P}'_3) = 1 \). By Theorem \( \text{[10.31]} \) and the argument above, we have that

\[
\lim_{M \to \infty} \inf \frac{\#(\mathcal{P}'_2 \cap a(v, M))}{M^2 (\log M)^{-1}} > 0.
\]

We claim that

\[
\lim_{M \to \infty} \sup \frac{\#(\mathcal{P}'_2 \setminus \mathcal{P}'_1) \cap a(v, M)}{M^2 (\log M)^{-1}} = 0.
\] (10.10)

To prove this, take \( \beta \in (\mathcal{P}'_2 \setminus \mathcal{P}'_1) \cap a(v, M) \). Then, there exists \( p_\beta \in |\text{Spec}(\mathcal{O}_K)| \) such that \( \beta a^{-1} = p_\beta \). Since \( p_\beta \in |\text{Spec}(\mathcal{O}_K)| \) such that \( a_\beta \in \mathcal{P} \) and \( f_\beta \in \mathbb{N}_{\geq 2} \) such that \( N(p_\beta) = p_\beta^{f_\beta} \). Then we have

\[
p_\beta \leq \left( \frac{|N_{K/Q}(\beta)|}{N(a)} \right)^{\frac{1}{2}}.
\]

Here, if \( M \) is sufficiently large depending on \( v \), then the right-hand side of the inequality above does not exceed \( M^{(2n+1)/4} \). By Lemma \( \text{[3.15]} \) there exist at most \( n M^{(2n+1)/4} \) possibilities of \( p_\beta \). By Corollary \( \text{[4.16]} \), we conclude that

\[
\lim_{M \to \infty} \sup \frac{\#((\mathcal{P}'_2 \setminus \mathcal{P}'_1) \cap a(v, M))}{M^{2n+1} (\log M)^n} < \infty;
\]

note that \( r_1 + r_2 - 1 \leq n \). Therefore, (10.10) holds. It follows that \( d_{\mathcal{P}'_2, v}(\mathcal{P}'_3) = 1 \). \( \square \)

**Proof of Theorem 10.36.** We continue to use the same notation as in Lemma \( \text{[10.40]} \). By Lemma \( \text{[10.40]} \) we have \( d_{\mathcal{P}'_2, v}(\mathcal{P}'_3) > 0 \). By Lemma \( \text{[10.39]} \) this implies that \( d_{\mathcal{P}'_2, v}(\xi, \iota(A)) > 0 \).

By Theorem \( \text{[10.34]} \), Theorem \( \text{[8.25]} \) applies, and there exists an \( \mathcal{N} \)-compatible fundamental domain \( \mathcal{D} \) for the action \( \mathcal{O}_K^\times \curvearrowright \mathcal{a} \setminus \{ 0 \} \) such that \( d_{\mathcal{P}'_2, v}(\mathcal{D} \cap (\xi, \iota(A))) > 0 \). Define

\[
\mathcal{P}(A, \mathcal{D}) := \left\{ \frac{|N_{K/Q}(\beta)|}{N(a)} : \beta \in \mathcal{D} \cap (\xi, \iota(A)) \right\}.
\]
By Lemma 10.39, this is a subset of $\mathcal{P}$. In what follows, we will construct a set $\tilde{\mathcal{A}}'$ from $\mathcal{D} \cap (\xi \cdot \iota(A))$. For each $p \in \mathcal{P}(A, \mathcal{D})$, choose an arbitrary $\tilde{\beta}_p \in \mathcal{D} \cap (\xi \cdot \iota(A))$ satisfying

$$\|\tilde{\beta}_p\|_{\infty,v} = \min \left\{ \|\beta\|_{\infty,v} : \beta \in \mathcal{D} \cap (\xi \cdot \iota(A)), \frac{|N_{K/Q}(\beta)|}{N(a)} = p \right\}. \tag{10.11}$$

Then, define $\tilde{\mathcal{A}}'$ by $\tilde{\mathcal{A}}' := \{ \tilde{\beta}_p : p \in \mathcal{P}(A, \mathcal{D}) \}$. We claim that the map $\tilde{\mathcal{A}}' \ni \tilde{\beta} \mapsto |N_{K/Q}(\tilde{\beta})| \in \mathbb{N}$ is injective, and that

$$d_{\mathcal{D} \cap (\xi \cdot \iota(A)),v}(\tilde{\mathcal{A}}') \geq \frac{1}{n}. \tag{10.12}$$

holds true. Indeed, the former assertion holds by construction. To see the latter assertion, recall from Lemma 3.15 that for every $p \in \mathcal{P}$, the number of prime $p$-ideals in $\mathcal{O}_K$ does not exceed $n$. Hence, for every $p \in \mathcal{P}(A, \mathcal{D})$, we have

$$\#\left\{ \beta \in \mathcal{D} \cap (\xi \cdot \iota(A)) : \frac{|N_{K/Q}(\beta)|}{N(a)} = p \right\} \leq n.$$

Therefore, by (10.11), we conclude (10.12).

Set $A' := \xi^{-1}A'$; this is a subset of $\iota(A)$. We claim that $d_{\mathcal{D} \cap (\xi \cdot \iota(A)),v}(A') > 0$. Indeed, combine $d_{\mathcal{D} \cap (\xi \cdot \iota(A)),v}(\mathcal{D} \cap (\xi \cdot \iota(A))) > 0$ with (10.12). Therefore, we can apply Theorem 10.3 to this $A'$. Then, we obtain a sequence $(\mathcal{T}_l)_{l \in \mathbb{N}}$ of subsets in $A'$. Again by Lemma 10.39, the sequence $(\mathcal{T}_l)_{l \in \mathbb{N}} := (\iota^{-1}(\mathcal{T}_l))_{l \in \mathbb{N}}$ of finite subsets in $\mathbb{Z}^n$ fulfills all conditions of Theorem 10.36.

Finally, we establish Theorem 10.1. In the proof below, we do not assume Setting 10.35.

**Proof of Theorem 10.1** Let $F(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ be a non-degenerate and primitive binary quadratic form with $a > 0$. By Theorem 10.3, there exist an order $\mathcal{O}$ in a quadratic field $K$, an invertible fractional ideal $\mathfrak{c}$ of $\mathcal{O}$, a $\mathbb{Z}$-basis $\mathbf{w} = (\gamma_1, \gamma_2)$ of $\mathfrak{c}$ and a signature $\epsilon_{\mathfrak{c}}$ such that (10.1) holds.

If $D_F > 0$, then for each $\epsilon_0 \in \{\pm 1\}$, we can apply Theorem 10.36 with signature $\epsilon = \epsilon_0 \epsilon_{\mathfrak{c}}$. This immediately proves the assertion. If $D_F < 0$, then $a > 0$ implies that $\epsilon_{\mathfrak{c}} = +1$. Apply Theorem 10.36 with signature $\epsilon = +1$, and obtain the conclusion.

## A Binary quadratic forms and quadratic fields

The goal of this appendix is to provide a standard proof of Theorem A.5 on the correspondence of binary quadratic forms with integral coefficients and ideals in orders of quadratic fields. A part of Theorem A.5, in the form of Theorem 10.3, plays a key role for the proof of Theorem C. For the proof, we employ Proposition 10.16 more precisely, equality (10.5).

### A.1 Definitions

Recall that by a binary quadratic form with integral coefficients, we mean a map $F : \mathbb{Z}^2 \to \mathbb{Z}$ which can be written as $F(x,y) = ax^2 + bxy + cy^2$ with $a,b,c \in \mathbb{Z}$ with respect to the
standard basis of $\mathbb{Z}^2$. In this appendix, we omit writing ‘with integral coefficients.’ Note that the property that $F$ is written in the form $ax^2 + bxy + cy^2$ is preserved under a $\mathbb{Z}$-linear isomorphism $\mathbb{Z}^2 \cong \mathbb{Z}^2$, in other words, a change of basis. Hence, the following concept of equivalence is natural. Here we consider the so-called proper equivalence which respects the orientation, but we drop the adjective ‘proper.’ This is because we will never consider the improper one in this paper.

**Definition A.1.** Two binary quadratic forms $F, G: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ are said to be equivalent if there exists a $\mathbb{Z}$-linear isomorphism $\iota: \mathbb{Z}^2 \cong \mathbb{Z}^2$ preserving the orientation such that $F = G \circ \iota$, namely, the following diagram

$$
\begin{array}{ccc}
\mathbb{Z}^2 & \xrightarrow{F} & \mathbb{Z} \\
\downarrow \iota & & \downarrow \iota \\
\mathbb{Z}^2 & \xleftarrow{G} & \mathbb{Z}
\end{array}
$$

commutes.

Recall that the discriminant of a binary quadratic form $F(x, y) = ax^2 + bxy + cy^2$ is the integer $D_F := b^2 - 4ac$. Note that $D_F \equiv 0$ or 1 (mod 4) always holds. The discriminant is preserved by equivalence of binary quadratic forms. Recall also that $F$ is said to be non-degenerate if $D_F$ is not a perfect square, and that $F$ is said to be primitive if $\gcd(a, b, c) = 1$ holds.

**Definition A.2.** For an integer $D \in \mathbb{Z}$, we denote by $Q(D)$ the set of equivalence classes of non-degenerate primitive quadratic forms with discriminant $D$.

The set $Q(D)$ is empty unless $D \equiv 0$ or 1 (mod 4).

For a square-free integer $d \in \mathbb{Z} \setminus \{1\}$, let us consider the quadratic field $\mathbb{Q}(\sqrt{d})$ as a subfield of $\mathbb{C}$. We choose a square root $\sqrt{d} \in \mathbb{C}$ of $d$ in the following manner: if $d > 0$, we take $\sqrt{d}$ to be the positive real one, and if $d < 0$, the one with positive imaginary part.

**Definition A.3.** Let $d$ be a square-free integer not equal to 1 and $K$ the quadratic field $K = \mathbb{Q}(\sqrt{d})$.

1. Define the discriminant $d_K$ of $K$ by

$$
d_K := \begin{cases} 
d & \text{if } d \equiv 1 \pmod{4}, \\
4d & \text{if } d \equiv 2, 3 \pmod{4}.
\end{cases}
$$

2. Define the discriminant $D$ of an order $\mathcal{O}$ in $K$ by $D := \#(\mathcal{O}_K : \mathcal{O})^2 \cdot d_K$.

There exists a bijective correspondence between the pair of a quadratic field $K = \mathbb{Q}(\sqrt{d})$ and an order $\mathcal{O}$ in $K$, and the discriminant $D$:

$$
\left\{ (K, \mathcal{O}) : \begin{array}{l} K \text{ a quadratic field,} \\
\mathcal{O} \text{ an order in } K
\end{array} \right\} \simeq \left\{ D \in \mathbb{Z} : \begin{array}{l} D \equiv 0, 1 \pmod{4}, \\
\text{not a square}
\end{array} \right\}. \tag{A.1}
$$
It is fundamental in the proof of Theorem A.5. Hence, here we present the explicit form of the correspondence (A.1). From the left-hand side to the right-hand side is given in Definition A.3 (2). In what follows, we explain the reverse correspondence. Set \( d \) to be the square-free part of \( D \) and define

\[
K := \mathbb{Q}(\sqrt{d}), \quad \mathcal{O} := \mathbb{Z} \oplus \sqrt{\frac{D}{d_K}}\omega\mathbb{Z},
\]

where \( \omega \) is defined by

\[
\omega := \begin{cases} 
1 + \sqrt{d} & \text{if } d \equiv 1 \pmod{4}, \\
\sqrt{d} & \text{if } d \equiv 2, 3 \pmod{4}.
\end{cases}
\]

These two maps are inverse to each other from the fact that every order of \( K = \mathbb{Q}(\sqrt{d}) \) with a square-free integer not equal to 1 has the form \( \mathcal{O} = \mathbb{Z} \oplus f\omega\mathbb{Z} \) for some positive integer \( f \); see [Cox13, Lemma 7.2]; with this \( f \), we have \( \#(\mathcal{O}/\mathcal{O}) = f \) and hence \( D = f^2d_K \).

**Definition A.4.** Let \( d \) be a square-free integer not equal to 1. Let \( \mathcal{O} \) be an order of the quadratic field \( K = \mathbb{Q}(\sqrt{d}) \).

1. Define the commutative group \( \text{Cl}^{+}(\mathcal{O}) \), called the narrow class group, as follows. Let \( I_{\mathcal{O}} \) be the group of invertible fractional ideals of \( \mathcal{O} \), where the group law is given by multiplication. Then, we define \( \text{Cl}^{+}(\mathcal{O}) \) to be the cokernel of the homomorphism from \( K^{\times} \) to \( I_{\mathcal{O}} \times \{\pm 1\} \) defined by \( x \mapsto (x\mathcal{O}, \text{sgn}(N_{K/\mathbb{Q}}(x))) \).

2. Endow the 2-dimensional \( \mathbb{Q} \)-vector space \( K \) with the orientation given by the basis \((1, \sqrt{d})\). Let \( c \in I_{\mathcal{O}} \) and \( \epsilon \in \{\pm 1\} \). We say that a \( \mathbb{Z} \)-basis \((\gamma_1, \gamma_2)\) of \( c \) has signature \( \epsilon \) if the representing matrix of the inclusion map \( c \hookrightarrow K \) with respect to the bases \((\gamma_1, \gamma_2)\) and \((1, \sqrt{d})\) has determinant with signature \( \epsilon \).

**A.2 The correspondence**

The following theorem is essentially due to Gauss, Dirichlet and Dedekind, and the goal of this appendix. This specific statement is taken from [Bha04, Theorem 10]. In Theorem A.5 for a binary quadratic form \( F \) with \( D_F = D \), write \([F]\) for its equivalence class in \( Q(D) \). Similarly, for \((c, \epsilon) \in I_{\mathcal{O}} \times \{\pm 1\} \), write \([(c, \epsilon)]\) for its equivalence class in \( \text{Cl}^{+}(\mathcal{O}) \).

**Theorem A.5.** Let \( \mathcal{O} \) be an order of a quadratic field \( K \) and let \( D \) be its discriminant. Then the following maps are well-defined, and one is the inverse map to the other. In particular, they provide a bijective correspondence

\[
\text{Cl}^{+}(\mathcal{O}) \simeq Q(D).
\]

1. (From ideals to quadratic forms) For \([c, \epsilon]\) \( \in \text{Cl}^{+}(\mathcal{O}) \) with \((c, \epsilon) \in I_{\mathcal{O}} \times \{\pm 1\} \), choose a \( \mathbb{Z} \)-basis \((\gamma_1, \gamma_2)\) of \( c \) which has signature \( \epsilon \). Then, define the corresponding class \([F]\) of quadratic forms by setting

\[
F(x, y) := \frac{\text{N}_{K/\mathbb{Q}}(\gamma_1x + \gamma_2y)}{\epsilon\text{N}(c)} \quad \text{for } (x, y) \in \mathbb{Z}^2.
\]
(2) (From quadratic forms to ideals) For \([F] \in Q(D)\), consider a representative \(F\) of the form \(F(x, y) = ax^2 + bxy + cy^2\). Let \(d\) be the square-free part of \(D\), namely, \(K = \mathbb{Q}(\sqrt{d})\). Set \(\gamma := \sqrt{D/d}K\) and \(\tau := \frac{-b + \sqrt{dK}}{2} \in O_K\). Then define the corresponding element 

\[ ([c, \epsilon]) \in Cl^+(O) \] 

as follows: set

\[ c := a\mathbb{Z} \oplus \tau\mathbb{Z} \quad \text{and} \quad \epsilon := \text{sgn}(a). \]  

We will prove Theorem A.5 in Subsections A.3, A.4, and A.5. In what follows, we utilize Setting A.6. Let \(D\) be an integer not a square with \(D \equiv 0, 1 \pmod{4}\). Let \(d\) be the square-free part of \(D\) and \(K := \mathbb{Q}(\sqrt{d})\). Set \(f := \sqrt{D/d}K\) and \(O := \mathbb{Z} \oplus f\omega\mathbb{Z}\) as in (A.2).  

### A.3 Well-definedness of the correspondence \([1]\)  

In this subsection, we prove that the correspondence \([1]\) in Theorem A.5 is well-defined. By (10.5), the absolute value of the right-hand side of (A.4) equals \(N((\gamma_1x + \gamma_2y)c^{-1})\). Since \(\gamma_1x + \gamma_2y \in c\), we have \((\gamma_1x + \gamma_2y)c^{-1} \subseteq O\). Hence, for every \((x, y) \in \mathbb{Z}^2\), the value \(F(x, y)\) is an integer. This implies that \(F\) has integer coefficients.

The equivalence class of \(F(x, y)\) clearly does not depend on the auxiliary choice of the basis \((\gamma_1, \gamma_2)\). We claim that it depends only on the class of \((c, \epsilon)\) in \(Cl^+(O)\). To see this, note that for every element \(\xi \in K^\times\), the following commutative diagram

\[
\begin{array}{ccc}
\mathbb{Z}^2 & \xrightarrow{\xi} & \mathbb{Z} \\
(\gamma_1, \gamma_2) & \downarrow & \downarrow \xi \\
(\xi \gamma_1, \xi \gamma_2) & & \xi c \\
\end{array}
\]

commutes. Indeed, the commutativity of the left-hand triangle is obvious. The commutativity of the right-hand triangle follows from the fact that the norm map \(N_{K/Q}(\cdot)\) is multiplicative and from (10.5). Note that the change of the basis from \((\gamma_1, \gamma_2)\) to \((\xi \gamma_1, \xi \gamma_2)\) changes the signature by the factor \(\text{sgn}(N_{K/Q}(\xi))\), so that the lower composition map in the diagram is a quadratic form obtained from the pair \((\xi c, \text{sgn}(N_{K/Q}(\xi))\epsilon)\).

What remain to check are that the discriminant \(D\) of the quadratic form \(F(x, y)\) is equal to that of \(O\), and that \(F\) is primitive. First, we will prove that \(D_F = D\). For this, we may assume \(c \subseteq O\). Indeed, replace \(c\) with an appropriate \(\xi c\); the argument above justifies this process. By \(\zeta \mapsto \zeta\), we denote the unique non-trivial automorphism of \(K = \mathbb{Q}(\sqrt{d})\) over \(\mathbb{Q}\). Then for every \((x, y) \in \mathbb{Z}^2\), we have \(N_{K/Q}(\gamma_1 x + \gamma_2 y) = (\gamma_1 x + \gamma_2 y)(\gamma_1 \gamma_2 x + \gamma_2 \gamma_1 y)\). Hence,

\[ F(x, y) = \frac{\gamma_1 \gamma_2 x^2 + (\gamma_1 \gamma_2 + \gamma_2 \gamma_1)xy + \gamma_2 \gamma_1 y^2}{\epsilon N(c)}. \]
It then follows that $D_F = \frac{(\gamma_1 \gamma_2 - \gamma_1 \gamma_2)^2}{N(c)^2}$. The numerator is the square of $\det \begin{pmatrix} \gamma_1 & \gamma_2 \\ 1 & f\omega \end{pmatrix}$. By the assumption $c \subseteq O$, there exists a unique 2-by-2 integer matrix $T$ satisfying $\begin{pmatrix} \gamma_1 & \gamma_2 \\ 1 & f\omega \end{pmatrix} T$. It follows $\begin{pmatrix} \gamma_1 & \gamma_2 \\ 1 & f\omega \end{pmatrix}^2 = \begin{pmatrix} 1 & f\omega \\ 1 & f\omega \end{pmatrix}$. By the definition of $T$, we have $|\det(T)| = N(c)$. Hence, we obtain that

$$\det \begin{pmatrix} \gamma_1 & \gamma_2 \\ 1 & f\omega \end{pmatrix}^2 = \det \begin{pmatrix} 1 & f\omega \\ 1 & f\omega \end{pmatrix}^2 N(c)^2.$$ 

A direct calculation shows $\det \begin{pmatrix} 1 & f\omega \\ 1 & f\omega \end{pmatrix} = D$. Thus, we conclude that $D_F = D$.

Secondly, we will prove that $F(x, y)$ is primitive. By Corollary [10.11] we may assume that $c$ satisfies $c + fO = O$; in this case $N(c)$ is prime to $f$ because $f$ is invertible in the ring $O/c$. The integer $N(c)$ annihilates the abelian group $O/c$. It follows that $N(c) = N(c) \cdot 1 \in c$. Take the unique $(x, y) \in \mathbb{Z}^2$ with $\gamma_1 x + \gamma_2 y = N(c)$. For this $(x, y)$, we have $F(x, y) = \frac{N_K/O(N(c))}{cN(c)} = cN(c)$. Now suppose that $\gcd(a, b, c) \neq 1$. Take a rational prime number $p$ dividing $\gcd(a, b, c)$. Then, $p$ divides every absolute value of $F$; in particular, it divides $N(c)$. Since $N(c)$ is now prime to $f$, it follows that $p$ is prime to $f$. Note also that $p^2$ divides $b^2 - 4ac = D = f^2d_K$. This is a contradiction if $p \geq 3$. Indeed, recall the definition of $d_K$ and that $d$ is square-free. We can also draw a contradiction for the case of $p = 2$ by considering the reduction modulo 16. Therefore, $\gcd(a, b, c) = 1$, as desired.

This ends the proof of well-definedness of the correspondence (1).

### A.4 On well-definedness of the correspondence \(2\)

This subsection is devoted to the proof of well-definedness of the correspondence (2) in Theorem [A.5]. Strictly speaking, we will prove that the map $F \mapsto [(c, \epsilon)]$ from the set of all primitive binary quadratic forms $\mathbb{Z}^2 \to \mathbb{Z}$ with discriminant $D$ to $\text{Cl}^+(O)$ is well-defined, where $(c, \epsilon)$ is defined in (A.5). First, note that $a \neq 0$, since $D = b^2 - 4ac$ is not a perfect square. Hence $\text{sgn}(a)$ in (A.5) does not cause a problem. We claim that $O = \mathbb{Z} \oplus \tau \mathbb{Z}$ as an abelian group. Indeed, observe that $f\omega + \tau \equiv D_K - b \pmod{2}$ (mod $\mathbb{Z}$). From $f^2d_K = D = b^2 - 4ac$, observe also that $f d_K$ and $b$ must have the same parity. Hence, $f\omega = -\tau$ in the quotient group $O_K/\mathbb{Z}$, and we conclude that

$$O = \mathbb{Z} \oplus f\omega \mathbb{Z} = \mathbb{Z} \oplus \tau \mathbb{Z}. \quad \text{(A.6)}$$

Since $\tau^2 + b\tau + ac = 0$, the subgroup $c \subseteq O$ is in fact an ideal of $O$. We will moreover check that $c$ is an invertible ideal. Consider the conjugate $\bar{c} = a\mathbb{Z} \oplus \tau \mathbb{Z} \subseteq O$ and take the product,

$$c\bar{c} = (aO + \tau O) \cdot (aO + \tau O) = a^2O + a\tau O + a\tau O + \tau^2 O.$$ 

Since $\tau^2 + b\tau + ac = 0$, we have $\tau\bar{c} = ac$. Since $\tau + \bar{c} = -b$ and $F$ is primitive, we moreover obtain that $c\bar{c} = aO$. This shows that $c$ is invertible with the inverse $a^{-1}\bar{c}$.

The arguments above in this subsection show that the map $F \mapsto [(c, \epsilon)]$ is well-defined. To verify that the correspondence (2) is well-defined, it remains to check that the class of
(c, ϵ) in \( \text{Cl}^+(O) \) is invariant under changes of the representative \( F \) of the equivalence class \([F] \in Q(D)\). However, we postpone this proof to Subsection A.5.

### A.5 End of the proof of Theorem A.5

In Subsections A.3 and A.4, we have checked that the maps in the following diagram

\[
\begin{array}{ccc}
\{\text{primitive quadratic forms} \ F: \mathbb{Z}^2 \to \mathbb{Z} \text{ with } D_F = D\} & \xrightarrow{\text{quotient map}} & Q(D) \\
\text{Cl}^+(O) & \xrightarrow{\text{A.4}} & \text{Cl}^+(O) \quad \text{(A.4)} \\
\end{array}
\]

are all well-defined. To establish Theorem A.5, it suffices to show that the diagram is commutative, and that the horizontal map is injective. That will also establish that the map \( Q(D) \xrightarrow{\text{A.5}} \text{Cl}^+(O) \) is well defined, thus completing the arguments in Subsection A.4. In this subsection, we will prove the two assertions above.

First, we will show that the diagram (A.7) is commutative. Take a primitive binary quadratic form \( F(x, y) = ax^2 + bxy + cy^2 \) with discriminant \( D \). Let \( \tau \) and \( c \) as in Theorem A.5 (2). The basis \((a, -\tau)\) of \( c \) has signature \( \epsilon := \text{sgn}(a) \). Therefore the quadratic form associated with this pair \((c, \epsilon)\) and the basis is the map \((x, y) \mapsto N_{K/Q}(ax - \tau y) \epsilon N(c)\).

By (A.6), the denominator is \( \epsilon \cdot |a| = a \). The numerator is

\[
N_{K/Q}(ax - \tau y) = (ax - \tau y)(ax - \tau y) = a^2x^2 - a(\tau + \overline{\tau})xy + \tau \overline{\tau}y^2.
\]

By computation, we have that \( \tau + \overline{\tau} = -b \) and that \( \tau \overline{\tau} = ac \). Hence, we conclude that

\[
N_{K/Q}(ax - \tau y) = a^2x^2 + abyx + acy^2 = a \cdot F(x, y).
\]

This proves the commutativity of (A.7).

In the final part of the proof of Theorem A.5, we will show that the map \( \text{Cl}^+(O) \xrightarrow{\text{A.4}} Q(D) \) is injective. Suppose that two pairs \((c_1, \epsilon_1)\) and \((c_2, \epsilon_2)\) of invertible fractional ideals and signs give equivalent quadratic forms. Choose appropriate \( \mathbb{Z} \)-bases \((\gamma_1, \gamma_2)\) and \((\gamma_1', \gamma_2')\) respectively so that we obtain the following identity for two quadratic forms:

\[
\frac{N_{K/Q}(\gamma_1 x + \gamma_2 y)}{\epsilon_1 N(c_1)} = \frac{N_{K/Q}(\gamma_1' x + \gamma_2' y)}{\epsilon_2 N(c_2)}. \quad (A.8)
\]

Recall that for all \((x, y) \in \mathbb{Z}^2\), we have \( N_{K/Q}(\gamma_1 x + \gamma_2 y) = (\gamma_1 x + \gamma_2 y)(\overline{\gamma_1} x + \overline{\gamma_2} y) \). Similarly, \( N_{K/Q}(\gamma_1' x + \gamma_2' y) = (\gamma_1' x + \gamma_2' y)(\overline{\gamma_1'} x + \overline{\gamma_2'} y) \) holds. In each of the two equalities above, the right-hand side makes sense even for \( x, y \in K = \mathbb{Q}(\sqrt{d}) \). Set \( y = 1 \). The values of
If \( x \in K \) satisfying \((\gamma_1 x + \gamma_2)(\overline{\gamma_1} x + \overline{\gamma_2}) = 0\) are \(-\gamma_2/\gamma_1\) and \(-\overline{\gamma_1}/\overline{\gamma_2}\). A similar fact holds for \(x \mapsto (\gamma'_1 x + \gamma'_2)(\overline{\gamma'_1} x + \overline{\gamma'_2})\). From (A.8), either \(\gamma_2/\gamma_1 = \gamma'_2/\gamma'_1\) or \(\gamma_2/\gamma_1 = \overline{\gamma'_2}/\gamma'_1\) holds true. In other words, there exists \(\xi \in K^\times\) such that the following equality holds in \(K^2\):

\[(\gamma_1, \gamma_2) = \xi(\gamma'_1, \gamma'_2) \quad \text{or} \quad (\gamma_1, \gamma_2) = \xi(\overline{\gamma'_1}, \overline{\gamma'_2}). \quad \text{(A.9)}\]

In either case, if we substitute it into (A.8), we obtain that

\[
\frac{\xi \xi(\gamma'_1 x + \gamma'_2 y)(\overline{\gamma'_1} x + \overline{\gamma'_2} y)}{\epsilon_1 \mathcal{N}(c'_1)} = \frac{(\gamma'_1 x + \gamma'_2 y)(\overline{\gamma'_1} x + \overline{\gamma'_2} y)}{\epsilon_2 \mathcal{N}(c'_2)},
\]

as binary quadratic forms. Therefore, we have \(\xi \xi = \epsilon_1 \mathcal{N}(c'_1)/(\epsilon_2 \mathcal{N}(c'_2))\). In particular, \(N_{K/Q}(\xi) = \xi \xi\) has signature \(\epsilon_1/\epsilon_2\). It then follows that the basis \((\gamma'_1, \gamma'_2)\) of \(\xi c'_2\) has sign \(\epsilon_1\) and \((\overline{\gamma'_1}, \overline{\gamma'_2})\) of \(\xi \overline{c'_2}\) has signature \(-\epsilon_1\). Since the basis \((\gamma_1, \gamma_2)\) has signature \(\epsilon_1\), we conclude that in (A.9), only the first case can hold. This also implies that \(c'_1 = \xi c'_2\) as ideals. Since \(\text{sgn}(N_{K/Q}(\xi)) = \epsilon_1/\epsilon_2\), we obtain the equality \((c'_1, \epsilon_1) = (\xi c, \text{sgn}(N_{K/Q}(\xi))) \cdot (c'_2, \epsilon_2)\) in \(I_O \times \{\pm 1\}\). This proves the desired injectivity.

It completes the proof of Theorem A.5.

References

[AM16] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, economy ed., Addison-Wesley Series in Mathematics, Westview Press, Boulder, CO, 2016, For the 1969 original see [MR0242802].

[Bha04] M. Bhargava, *Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2) 159 (2004), no. 1, 217–250.

[BHP01] R. C. Baker, G. Harman, and J. Pintz, *The difference between consecutive primes. II*, Proc. London Math. Soc. (3) 83 (2001), no. 3, 532–562.

[BS20] T. F. Bloom and O. Sisask, *Breaking the logarithmic barrier in Roth’s theorem on arithmetic progressions*, preprint, arXiv:2007.03528 (2020).

[CFZ14] D. Conlon, J. Fox, and Y. Zhao, *The Green-Tao theorem: an exposition*, EMS Surv. Math. Sci. 1 (2014), no. 2, 249–282.

[CFZ15] ______, *A relative Szemerédi theorem*, Geom. Funct. Anal. 25 (2015), no. 3, 733–762.

[CMT18] B. Cook, Á. Magyar, and T. Titichetrakun, *A multidimensional Szemerédi theorem in the primes via combinatorics*, Ann. Comb. 22 (2018), no. 4, 711–768.

[Cox13] D. A. Cox, *Primes of the form \(x^2 + ny^2\)*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication.
[EF19] C. Elsholtz and C. Frei, *Arithmetic progressions in binary quadratic forms and norm forms*, Bull. Lond. Math. Soc. **51** (2019), no. 4, 595–602.

[FK78] H. Furstenberg and Y. Katznelson, *An ergodic Szemerédi theorem for commuting transformations*, J. Analyse Math. **34** (1978), 275–291 (1979).

[FZ15] J. Fox and Y. Zhao, *A short proof of the multidimensional Szemerédi theorem in the primes*, Amer. J. Math. **137** (2015), no. 4, 1139–1145.

[Gow07] W. T. Gowers, *Hypergraph regularity and the multidimensional Szemerédi theorem*, Ann. of Math. (2) **166** (2007), no. 3, 897–946.

[GT08] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547.

[Hei67] H. Heilbronn, *Zeta-functions and L-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 204–230.

[HW08] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[KMTB15] N. Kaplan, J. Marcinek, and R. Takloo-Bighash, *Distribution of orders in number fields*, Res. Math. Sci. **2** (2015), Art. 6, 57.

[KRE20] V. Kuperberg, B. Rodgers, and Roditty-Gershon E., *Sums of singular series and primes in short intervals in algebraic number fields*, preprint, arXiv:2001.09513 (2020).

[Lan53] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*, Chelsea Publishing Co., New York, 1953, 2d ed, With an appendix by Paul T. Bateman.

[Mit56] T. Mitsui, *Generalized prime number theorem*, Jpn. J. Math. **26** (1956), 1–42.

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NRS06] B. Nagle, V. Rödl, and M. Schacht, *The counting lemma for regular k-uniform hypergraphs*, Random Structures Algorithms **28** (2006), no. 2, 113–179.
[RS06] V. Rödl and J. Skokan, Applications of the regularity lemma for uniform hypergraphs, Random Structures Algorithms 28 (2006), no. 2, 180–194.

[RS07a] V. Rödl and M. Schacht, Regular partitions of hypergraphs: counting lemmas, Combin. Probab. Comput. 16 (2007), no. 6, 887–901.

[RS07b] ———, Regular partitions of hypergraphs: regularity lemmas, Combin. Probab. Comput. 16 (2007), no. 6, 833–885.

[RSTT06] V. Rödl, M. Schacht, E. Tengan, and N. Tokushige, Density theorems and extremal hypergraph problems, Israel J. Math. 152 (2006), 371–380.

[RW19] L. Rimanić and J. Wolf, Szemerédi’s theorem in the primes, Proc. Edinb. Math. Soc. (2) 62 (2019), no. 2, 443–457.

[Sol03] J. Solymosi, Note on a generalization of Roth’s theorem, Discrete and computational geometry, Algorithms Combin., vol. 25, Springer, Berlin, 2003, pp. 825–827.

[Sta67] H. M. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J. 14 (1967), 1–27.

[Tao06] T. Tao, The Gaussian primes contain arbitrarily shaped constellations, J. Anal. Math. 99 (2006), 109–176.

[TZ08] T. Tao and T. Ziegler, The primes contain arbitrarily long polynomial progressions, Acta Math. 201 (2008), no. 2, 213–305.

[TZ15] ———, A multi-dimensional Szemerédi theorem for the primes via a correspondence principle, Israel J. Math. 207 (2015), no. 1, 203–228.

[Var59] P. Varnavides, On certain sets of positive density, J. London Math. Soc. 34 (1959), 358–360.

[Wid10] M. Widmer, Counting primitive points of bounded height, Trans. Amer. Math. Soc. 362 (2010), no. 9, 4793–4829.

Mathematical Institute, Tohoku University, Sendai, 980-8578, Japan
E-mail address: kaiw@tohoku.ac.jp

Mathematical Institute, Tohoku University, Sendai, 980-8578, Japan
E-mail address: m.masato.mimura.m@tohoku.ac.jp

Graduate School of Information Sciences, Tohoku University, Sendai, 980-8579, Japan
E-mail address: munemasa@math.is.tohoku.ac.jp
Research Alliance Center for Mathematical Sciences, Tohoku University, Sendai, 980-8578, Japan
E-mail address: shinichiro.seki.b3@tohoku.ac.jp

Graduate School of Information Sciences, Tohoku University, Sendai, 980-8579, Japan
E-mail address: kiyoto.yosino.r2@dc.tohoku.ac.jp