Cubic Forms as Sum of Cubes of Linear Forms

Leonhard Summerer

Institut für Mathematik, University of Vienna,
Strudlhofgasse 4, A-1090 Vienna, Austria

Communicated by R. F. Tichy

Received February 2, 1998

The topic of investigation is cubic forms $F$ over $\mathbb{Z}$ in $n$ variables that are representable as a sum $L_1^3 + L_2^3$ of two cubes of linear forms with algebraic coefficients. If $Z_2(n, X)$ denotes the number of such forms $F$, the main result, stated as Theorem 1.3, gives its order of magnitude as $Z_2(n, X) \approx X^{2n/3}$, with the implied constants depending on $n$ only. The gist of our method consists of the analysis of the $p$-adic conditions for the coefficients of the linear forms $L_1$ and $L_2$ which stem from the fact that $F$ is defined over $\mathbb{Z}$. This leads to results concerning local lattices and their connection to global lattices that seem of interest even beyond the treated problem, and which are therefore stated with some more generality in Theorems 4.1 and 4.8. The combination of a fact from the Geometry of Numbers with the above then leads to the main theorem. Even though these steps are applied to changes of variables leading to the special diagonal form $X_1^3 + X_2^3$, they may be applicable to more general situations, the final goal being the treatment of forms that can be transformed into an arbitrary given form $f(X, Y)$ by a suitable linear, algebraic change of variables. Another, probably difficult generalisation consists in increasing the number of variables to deal with forms $X_1^3 + \cdots + X_k^3$ for $k \geq 3$.

1. SUMS OF 2 CUBES OF LINEAR FORMS WITH ALGEBRAIC COEFFICIENTS

1.1. Notations and Problem Setting. As usual we denote by

- $\mathbb{C}$ the complex number field,
- $\mathbb{Q}$ the rational number field,
- $\mathbb{Z}$ the rational integers,
- $K$ an algebraic number field,
- $\mathcal{O}_K$ its ring of integers.

With $F$ we denote cubic forms in $n$ variables with coefficients from one of the rings mentioned above, whereas $L$ is reserved for linear forms. If
$X = (X_1, \ldots, X_n)$ is the $n$-tuple of variables and $q_{ik}$, $1 \leq i \leq j \leq k \leq n$ are the coefficients of $F$, we have:

$$F(X) = \sum_{1 \leq i \leq j \leq k \leq n} q_{ik} X_i X_j X_k.$$ 

We write

$$L(X) = \sum_{1 \leq i \leq n} a_i X_i \quad \text{or briefly} \quad L(X) = aX,$$

where $a = (a_1, \ldots, a_n)$ denotes the coefficient vector.

We first want to examine cubic forms over $\mathbb{C}$ so that we stipulate $q_{ik} \in \mathbb{C}$. The simplest kind of a cubic form is probably one where only the coefficients $q_{ii}$ ($1 \leq i \leq n$) are different from 0, so that

$$F(X) = \sum_{1 \leq i \leq n} q_{ii} X_i^3,$$

and we call such $F$ a diagonal form. One may ask which forms can be transformed into a diagonal form after a suitable linear change of variables. This leads in a natural way to representations of cubic forms as sums of cubes of linear forms, i.e.

$$F(X) = \sum_{i=1}^{r} \lambda_i L_i(X)^3,$$

where $\lambda_i \in \mathbb{C}$ and $r$ denotes the number of summands. For a given form $F$ the above representation is far from being unique, even the number of summands can vary. We therefore need:

**Definition 1.1.** Let $F$ be a cubic form over $\mathbb{C}$ in $n$ variables. The smallest $r$ for which there exists a representation as above with complex $\lambda_i$ and linear forms $L_i$ with complex coefficients, is called the rank of the form $F$.

In the case of cubic forms over $\mathbb{Z}$, we may ask about the frequency of forms of rank $r$.

**Definition 1.2.** Let $Z_r(n, X)$ be the number of cubic forms $F$ in $n$ variables, $F(X) = \sum_{1 \leq i \leq j \leq k} q_{ik} X_i X_j X_k$ with $q_{ik} \in \mathbb{Z}$, $|q_{ik}| \leq X$ and rank $r$.

The aim of our investigation is to give an estimate for the order of magnitude of the first non-trivial quantity $Z_r(n, X)$, that is $Z_1(n, X)$. As the reader may easily check,

$$Z_1(n, X) \asymp X^{n/3} \quad \text{for} \quad n \geq 4.$$
whereas for \( n = 3 \) resp. \( n = 2 \) we only obtain

\[
Z_1(3, X) = X \log X \quad \text{resp.} \quad Z_1(2, X) = X.
\]

The main result of the paper is contained in the following

**Theorem 1.3.** For \( n \geq 10 \) we have:

\[
Z_2(n, X) \sim X^{2n/3}
\]

with the constants in \( \sim \) depending on \( n \) only.

1.2. **Representations of Cubic forms of Rank 2.** The crucial fact and thus the base for all further investigation is contained in

**Proposition 1.4.** Let \( F \) be a cubic form over \( \mathbb{C} \) of rank 2. If

\[
F(X) = L_1(X)^3 + L_2(X)^3 = M_1(X)^3 + M_2(X)^3,
\]

then either we have (1):

\[
L_1 = M_1 \quad \text{and} \quad L_2 = M_2,
\]

so that \( L_1 = \zeta M_1 \) and \( L_2 = \zeta M_2 \) with cube roots of unity \( \zeta, \zeta', \) or (2):

\[
L_1 = M_2 \quad \text{and} \quad L_2 = M_1,
\]

so that \( L_1 = \zeta M_2 \) and \( L_2 = \zeta M_1 \) with cube roots of unity \( \zeta, \zeta'. \)

**Proof.** Since \( L_1, L_2 \) are linearly independent, \( \text{grad} \ F = 0 \) precisely on the space \( L_1 = L_2 = 0 \), which is therefore determined by \( F \), and is thus the same as the space \( M_1 = M_2 = 0 \). Therefore \( L_1 = \alpha_1 M_1 + \alpha_2 M_2 \) and \( L_2 = \beta_1 M_1 + \beta_2 M_2 \) and we obtain:

\[
\alpha_1^2 + \alpha_2^2 = \beta_1^2 + \beta_2^2 = 1,
\]

\[
\alpha_1 \alpha_2 + \beta_1 \beta_2 = \alpha_1 \beta_2 + \beta_1 \alpha_2 = 0.
\]

If we had \( \alpha_1 \alpha_2 \neq 0 \), then \( \beta_1 \beta_2 \neq 0 \) and \( (\alpha_1/\beta_1)^3 = -(\beta_2/\alpha_2)^3 = -(\alpha_1/\beta_1)^4 \) by the second equation, so that \((\alpha_1/\beta_1)^3 = -1\), which contradicts the first one.

If \( \alpha_1 = 0 \), then \( \beta_2 = 0 \), \( \beta_1 = 0 \), and we get \( \alpha_1^3 = \beta_2^3 = 1 \), hence (1). If \( \alpha_1 = 0 \), we get \( \beta_1 \neq 0 \), \( \beta_2 = 0 \), further \( \alpha_2^3 = \beta_1^3 = 1 \), hence (2).

This allows us to give a criterion to decide whether a cubic form in the representation \( F = L_1^3 + L_2^3 \) has rank 1 or rank 2.
Corollary 1.5. Let $F(X) = L_1(X)^3 + L_2(X)^3 = \lambda_1(a_1X)^3 + \lambda_2(a_2X)^3$ be a cubic form of rank $\leq 2$. Then $F$ has rank 1 if and only if $L_1$ and $L_2$ respectively to the forms in question found in Corollary 1.6.

The uniqueness of the representation of cubic forms of rank 2 implies the existence of representations over certain number fields for rational forms. Let $K$ be the field generated by the quotients $a_i/a_j$, $(1 \leq i, j \leq n; a_j \neq 0)$.

Corollary 1.6. The field $K$ depends only on the form $F$. It is either the rational field or a quadratic number field. When $K$ is rational, also the quotients $a_i'/a_j'$ are rational; when $K$ is quadratic, then $a_i'/a_j' (1 \leq i, j \leq n; a_j' \neq 0)$ is the conjugate of $a_i/a_j$ in $K$.

There exist representations $F(X) = \lambda(\sum a_iX_i)^3 + \lambda'(\sum a'_iX_i)^3$ where $a_1, ..., a_n, a_1', ..., a_n'$, $\lambda, \lambda'$ are in $K$ and if $K$ is quadratic, the pairs $\lambda, \lambda'$ respectively $a_i, a_i'$ $(i = 1, ..., n)$ are pairs of conjugates.

Proof. By Proposition 1.4 the pair of points $(a_1', \cdot \cdot \cdot : a_n)$ and $(a_1, \cdot \cdot \cdot : a_n')$ in $(n - 1)$-dimensional projective space is uniquely determined by the form $F$. Every automorphism either leaves these two points fixed (i.e., leaves the quotients $a_i/a_j$ (with $a_j \neq 0$) and $a_i'/a_j'$ (with $a_j' \neq 0$) fixed), or interchanges these two points (i.e., interchanges $a_i/a_j$ and $a_i'/a_j'$). If every automorphism is of the first kind, then $K = \mathbb{Q}$ and all the quotients $a_i/a_j$ and $a_i'/a_j'$ (when defined) lie in $\mathbb{Q}$. If there is an automorphism of the second kind, then $K$ is quadratic and $a_i/a_j$ and $a_i'/a_j'$ are conjugates in $K$.

There are representations of $F$ with $(a_1, ..., a_n)$ and $(a_1', ..., a_n')$ in $K^n$ and these vectors are not proportional. Hence if $K = \mathbb{Q}$, every automorphism maps $\lambda(\sum a_iX_i)^3, \lambda'(\sum a'_iX_i)^3$ into themselves, and therefore $\lambda, \lambda' \in \mathbb{Q}$. If $K$ is quadratic, an automorphism may also interchange the two summands of $F$. Since the coefficients of the two appearing linear forms are respective conjugates in $K$, the same must hold for $\lambda, \lambda'$.

We now want to give a name to the special kind of representations respectively to the forms in question found in Corollary 1.6.

Definition 1.7. We call a cubic form over $\mathbb{Q}$ of rank 2 which has a representation of the shape

$$F(X) = \lambda(\sum a_iX_i)^3 + \lambda'(\sum a'_iX_i)^3$$

with $\lambda, \lambda', a_i, a_i' \in \mathbb{Q}$, $i = 1, ..., n$ representable over $\mathbb{Q}$.

Otherwise by Corollary 1.6 there exists a uniquely determined quadratic number field $\mathbb{Q}(\sqrt{d})$ in which $\lambda, \lambda', a_i, a_i' (i = 1, ..., n)$ lie and are conjugates respectively. We then call $\mathbb{Q}(\sqrt{d})$ the representation field of $F$. 


With these observations made, it is now clear that we may restrict ourselves to forms representable over \( \mathbb{Q} \) or with a quadratic representation field when dealing with forms counted in \( \mathbb{Z}_2(n, X) \).

1.3. The Estimate of \( Z_3(n, X) \). As a consequence of these results, we first split \( Z_3(n, X) \) into the quantities \( Z_3(d, n, X) \), which refer to the possible representation fields of the forms in question. We therefore need:

**Definition 1.8.** Let \( Z_3(d, n, X) \) be the number of cubic forms counted by \( Z_3(n, X) \) that are representable over \( \mathbb{Q}(\sqrt{-d}) \) for some squarefree \( d \neq 0 \).

In the case \( d = 1 \), by definition we set \( \mathbb{Q}(\sqrt{-d}) := \mathbb{Q} \) and for \( d = 0, 1 \) as usual the quadratic number field defined by \( d \).

With these notations the uniqueness of the number field associated to each form yields:

\[
Z_3(n, X) = \sum_{d \neq 0 \text{ sq-free}} Z_3(d, n, X)
\]

and in view toward the estimate of \( Z_3(n, X) \) we may first count all forms with representation field \( \mathbb{Q}(\sqrt{-d}) \) for fixed \( d \), and then sum over all such number fields in question.

The estimate of \( Z_3(d, n, X) \) is the subject of the second theorem of the paper, namely:

**Theorem 1.9.** Let \( n \geq 7 \) and \( h = h(d) \) the class number of the quadratic number field \( \mathbb{Q}(\sqrt{d}) \). Then there exists an absolute constant \( C > 0 \) with

\[
Z_3(d, n, X) \ll X^{2\omega(d)/3} h(d) C^{\omega(d)} d^{-n/6},
\]

where \( \omega(d) \) denotes the number of distinct prime factors of \( d \), and the implied constant in \( \ll \) depends only on \( n \) and not on \( d \).

Since the proof of this theorem will only be given at the end of the paper, let us use the rest of this section to show how Theorem 1.3 can be deduced from Theorem 1.9. To be able to sum over all involved number fields, i.e. the quadratic fields \( \mathbb{Q}(\sqrt{d}) \) and \( \mathbb{Q} \), we need a well known estimate for the class number of quadratic number fields:

**Proposition 1.10.** Let \( \mathbb{Q}(\sqrt{d}) \) be a quadratic number field with class number \( h(d) \). Then for all \( \varepsilon > 0 \):

\[
h(d) \ll |d|^{1/2 + \varepsilon}.
\]
Moreover, if \( d < 0 \), we have \( h(d) \sim \sqrt{|d|} \), and the exponent \( 1/2 \) cannot be improved.

**Proof.** This is an immediate consequence of Dirichlets class number formula (see e.g., [SSRL], p. 91, Theorem 8).

This enables us to achieve the goal of determining the order of magnitude of \( Z_2(n, X) \) if we allow an additional assumption concerning the number \( n \) of variables of the forms in question.

**Deduction (of Theorem 1.3).** Theorem 1.9 yields for \( n \geq 7 \):

\[
Z_2(n, X) = \sum_{d \neq 0 \text{ sq-free}} Z_2(d, n, X) \\
\ll \sum_{d \neq 0 \text{ sq-free}} x^{2n/3} h(d) C^{\omega(d)} |d|^{-n/6}
\]

\[
= x^{2n/3} \sum_{d \neq 0 \text{ sq-free}} h(d) C^{\omega(d)} |d|^{-n/6}.
\]

Proposition 1.10 then gives \( h(d) \ll |d|^{1/2 + \varepsilon} \) for \( \varepsilon > 0 \) and it is clear that \( C^{\omega(d)} \ll d^\delta \) for \( \delta > 0 \). Neglecting the condition \( d \) square free we find:

\[
Z_2(n, X) \ll x^{2n/3} \sum_{d=1}^\infty d^{1/2 - n/6 + \varepsilon}.
\]

Now \( d^{1/2 - n/6 + \varepsilon} \leq d^{-7/6 + \varepsilon} \) for \( n \geq 10 \), which implies

\[
\sum_{d=1}^\infty d^{1/2 - n/6 + \varepsilon} \leq \sum_{d=1}^\infty d^{-1 + \delta} \ll 1
\]

for any \( \delta = \varepsilon - 1/6 < 0 \), and we finally obtain:

\[
Z_2(n, X) \ll x^{2n/3}.
\]

To round up our discussion of \( Z_2(n, X) \), it remains to give a lower bound for this quantity. This turns out to be trivial since every pair of non collinear vectors \( ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) \in \mathbb{Z}^n \times \mathbb{Z}^n \) with \( |a_i|, |b_i| \leq c(n) X^{1/3} \) determines a form of the requested shape via

\[
F(\mathbf{X}) = \left( \sum a_i X_i \right)^3 + \left( \sum b_i X_i \right)^3.
\]
The estimate

\[ Z_2(n, X) \gg X^{2n/3} \]

follows immediately.

1.4. The Strategy for the Estimate of \( Z_2(d, n, X) \). Within a given number field, the representation of a given form \( F \) as \( F(X) = \lambda(\sum a_iX_i)^3 + \lambda'(\sum a'_iX_i)^3 \) with \( \lambda, \lambda', a_i, a'_i \in \mathbb{Q}(\sqrt{d}) \) for \( i = 1, \ldots, n \), which are supposed to be conjugates for \( d \neq 1 \), is far from being unique.

Our next task is therefore to choose a canonical representation, that is, to determine canonically a pair \((\lambda, \lambda')\) among all such pairs that may appear in any representation of \( F \). To do so, we need:

**Definition 1.11.** Let \( F \) be a cubic form counted by \( Z_2(d, n, X) \) in the representation of Definition 1.7. Then we call \((\lambda, \lambda')\) the leading coefficient pair of \( F \) in this representation, and we identify \((\lambda, \lambda')\) with \((\lambda', \lambda)\). In the case \( d = 1 \) we get in this way a pair of rational numbers and for \( d \neq 1 \) a pair of conjugate numbers from the given quadratic number field.

As already noticed, the leading coefficient pair is not uniquely determined for a given form, but we can show:

**Lemma 1.12.** Let \( F \) be counted by \( Z_2(d, n, X) \). Then there exists a representation of \( F \) in the sense of Corollary 1.5 with integer leading coefficient pair, that is \((\lambda, \lambda') \in \mathbb{Z}^2 \) for \( d = 1 \) and \((\lambda, \lambda') \in \mathbb{O}_d^2 \) for \( d \neq 1 \).

Moreover we have: two leading coefficient pairs of a given form may only differ by a cube in the respective representation field in each component.

**Proof.** By Corollary 1.6 there exists a representation of \( F \) given by \( F(X) = \lambda(\sum a_iX_i)^3 + \lambda'(\sum a'_iX_i)^3 \). We may multiply \( \lambda, \lambda' \) by \( x^3, x'^3 \) respectively, and divide \( a_i, a'_i \) by \( x, x' \) respectively. For suitable \( x \), both \( x^3\lambda \) and \( x'^3\lambda' \) will be in \( \mathbb{O}_d \).

The rest follows from Corollary 1.6 and the comparison of the coefficients of two representations of the same form.

Lemma 1.12 leads us straight to the question of finding a system of representatives for \( \mathbb{Q}(\sqrt{d})^*/(\mathbb{Q}(\sqrt{d})^*)^3 \) to show the possibility of choosing canonically one leading coefficient pair (i.e. one representation) for a form counted in \( Z_2(d, n, X) \). This makes it necessary to pass to prime ideals \((\lambda)\), since \( \mathbb{O}_d \) need not be a factorial ring and so does not guarantee unique prime decomposition. However, the unique prime ideal decomposition will enable us to single out a canonical representation.
Let therefore \( h = h(d) \) be the class number of \( \mathbb{Q}(\sqrt{d}) \) and \( \mathcal{A}_j, \ldots, \mathcal{A}_h \) the distinct ideal classes. We then choose from each class an integer prime ideal \( \mathfrak{p}_i \in \mathcal{A}_j \) that is relatively prime to \( 6d \) such that \( \mathcal{A}_j \neq \mathcal{A}_i \) yields

\[
\mathcal{A}_j = \mathcal{A}_i^{-1} \Rightarrow \mathfrak{p}_j = \mathfrak{p}_i^*.
\]

This choice is possible, for in each class one can find a prime ideal that is relatively prime to a given one (see e.g. [N], p. 22, Exercise 5). Once such a \( \mathfrak{p}_i \) is chosen for \( \mathcal{A}_i \), the conjugate \( \mathfrak{p}_i^* \) obviously lies in \( \mathcal{A}_i^{-1} \) and satisfies all requirements as well.

With the use of this terminology and the choice of \( \mathfrak{p}_i, (1 \leq i \leq h) \) we now need a series of lemmas to construct the desired system of representatives.

**Lemma 1.3.** If \( A \) denotes the ideal group of \( \mathbb{Q}(\sqrt{d}) \) and \( H \) the group of principal ideals \( \neq 0 \), then the ideals \( \mathfrak{p}_i^3a, i = 1, \ldots, h \) with integral and cubefree \( a \# A \) build up a system of representatives of \( AH^3 \).

**Proof.** Let \( b \in A \) be arbitrarily given. It may be written uniquely as \( a_0^3a \) with \( a \in A \) a cubefree integral ideal. Choosing the representative \( \mathfrak{p}_i \) of the class \( \mathcal{A}_i \) in which \( a_0 \) lies, we find \( a_0\mathfrak{p}_i^{-1} \in H \) and so \( a_0^3\mathfrak{p}_i^{-3} \in H^3 \). This implies (note that \( b = \mathfrak{p}_i^3a_0\mathfrak{p}_i^{-3}a_0^3 \)) immediately \( b \in \mathfrak{p}_i^3aH^3 \).

In the construction, \( a \) is uniquely determined as being the integer cubefree part of \( b \) and this determines the class of \( \mathfrak{p}_i^3 \) and in turn \( \mathfrak{p}_i \). This concludes the proof of the statements since \( b \in A \) was arbitrary.

**Lemma 1.14.** The ideals \( \mathfrak{p}_i^3a, i = 1, \ldots, n \) with integral and cubefree \( a \in A \) in \( \langle \mathfrak{p}_i^3 \rangle^{-1} \) build up a system of representatives of \( H/H^3 \).

**Proof.** This follows from the preceding lemma, since \( \mathfrak{p}_i^3aH^3 \subset H \) implies \( \mathfrak{p}_i^3a \in H \), that is \( a \in \langle \mathfrak{p}_i^3 \rangle^{-1} \).

We now have to investigate the group of units modulo their cubes to be able to transfer the information of the previous lemmas concerning principal ideals to elements of the quadratic numberfield in question, since the change from ideals to elements always involves the appearance of units.

**Lemma 1.15.** If \( E \) denotes the group of units in \( \mathbb{Q}(\sqrt{d}) \), we have \( |E/E^3| = w \), where \( w = 1 \) or \( w = 3 \). Consequently there exists a system of representatives \( \{e_j\} \mid 1 \leq j \leq w \} \) of \( E/E^3 \).

**Proof.** First assume that \( d \leq 0 \). By Dirichlets Unit Theorem \( E \) is a finite abelian group of order 2, 4 or 6, which yields \( E \cong \mathbb{Z}_2 \), \( \mathbb{Z}_4 \) or \( \mathbb{Z}_6 \).

In \( \mathbb{Z}_2 \) and \( \mathbb{Z}_4 \) every element is a multiple of 3 and consequently every unit in \( E \) is a cube, so \( |E/E^3| = 1 \). For \( E \cong \mathbb{Z}_6 \) we have \( |E/E^3| = 3 \).
Now assume $d \geq 0$. Dirichlet’s Unit Theorem then states $E \cong \mathbb{Z}_2 \times \mathbb{Z}$ which gives again $|E/E^3| = 3$.

Summarising all the acquired information, we obtain a system of representatives of $\mathbb{Q}(\sqrt{d})^*/(\mathbb{Q}(\sqrt{d})^*)^3$ in the following way:

**Proposition 1.16.** Let $\pi_{aw}$ be elements in $\mathcal{O}_d$ satisfying $(\pi_{aw}) = \varphi^3 a$, $1 \leq i \leq h$ with integral and cubefree $a \in \langle \varphi^3 \rangle^{-1} \subseteq A$ and $e_j$, $1 \leq j \leq w$ units that build up a system of representatives for $E/E^3$.

Then the set $\{e_j \pi_{aw} | 1 \leq j \leq w, 1 \leq i \leq h, a as above\}$ contains a system of representatives $\Pi$ for $\mathbb{Q}(\sqrt{d})^*/(\mathbb{Q}(\sqrt{d})^*)^3$.

**Proof.** The mapping $\pi \mapsto (\pi)$, $\mathbb{Q}(\sqrt{d})^* \rightarrow H$ is surjective and for given $a \in H$ and $\pi_1, \pi_2 \in \mathbb{Q}(\sqrt{d})^*$ with $(\pi_1) = a = (\pi_2)$ we have $\pi_1 = e \pi_2$ for an $e \in E$. So $\mathbb{Q}(\sqrt{d})^* \leq E \times H$ and it follows that:

$$\mathbb{Q}(\sqrt{d})^*/(\mathbb{Q}(\sqrt{d})^*)^3 \leq (E \times H)/(E \times H)^3 \cong E/E^3 \times H/H^3,$$

and the products of the respective systems for $E/E^3$ and $H/H^3$ contain the required system of representatives as stated.

Proposition 1.16 enables us to choose a canonical representation whose leading coefficient pair lies in the just constructed system of representatives for each form counted in $Z_3(d, n, X)$. This pair is then uniquely determined since by Lemma 1.12 two leading coefficient pairs of one form only differ by a cube in the given representation field. We write this fact as $(\lambda, \lambda') \in \Pi_d$, where $\Pi_d$ is the subset of $\Pi \times \Pi$ for which $\lambda$ and $\lambda'$ are conjugate in the case $d \neq 1$.

**Definition 1.17.** We define $Z_3(\lambda, \lambda', d, n, X)$ to be the number of cubic forms counted in $Z_3(d, n, X)$ which have leading coefficient pair $(\lambda, \lambda')$.

The current state of knowledge then yields:

$$Z_3(d, n, X) = \sum_{(\lambda, \lambda') \in \Pi_d} Z_3(\lambda, \lambda', d, n, X)$$

This determines the strategy to adopt to estimate the quantity $Z_3(d, n, X)$: the first step consists in evaluating $Z_3(\lambda, \lambda', d, X)$ for fixed $d \neq 0$ squarefree and given $(\lambda, \lambda') \in \Pi_d$. Special attention has to be paid to the dependence of all the constants on $(\lambda, \lambda')$ and on $d$, in view of a later summation over these parameters.
2. SOME BASIC INEQUALITIES

2.1. The Special Role of \( F(x, y) = x^2 + y^3 \). In this section we deal with those \((a, a') \in \mathbb{Q}((\sqrt{d}))^2 \) (where in the case \( d \neq 1 \) the \( a_i \) and \( a'_i \) are conjugates over \( \mathbb{Q}((\sqrt{d})) \)) that ensure that for a fixed \( \lambda, \lambda' \in \mathbb{F}_d \) the cubic form \( F(X) = \lambda(aX)^3 + \lambda'(a'X)^3 \) is counted in \( \mathbb{Z}_2(\lambda, \lambda', d, n, X) \).

Denoting by \( q_{ijk} \) the coefficients of \( F \), that is

\[
F(X) = \sum_{1 \leq i < j < k \leq n} q_{ijk}X_iX_jX_k,
\]

a comparison with the representation of \( F \) as \( \lambda(aX)^3 + \lambda'(a'X)^3 \) yields the following system \( \{1), (2), (3)\} \) of equations:

\[
\begin{align*}
(1) & \quad \lambda a_i^3 + \lambda a_i^6 = q_{ii} \\
(2) & \quad 3\lambda a_i^3a_j + 3\lambda' a_i^6a_j = q_{ij} \quad (i < j) \\
(3) & \quad 6\lambda a_i a_j a_k + 6\lambda' a_i^6 a_j a_k = q_{ijk} \quad (i < j < k)
\end{align*}
\]

where the \( n \) equations of type (1) correspond to the coefficients of \( F \) with 3 identical subscripts, the ones of type (2) to those with 2 identical subscripts and the ones of type (3) to those with 3 different subscripts.

When looking at the left side of the above equations, it seems quite natural to consider the cubic form \( F \) in the variables \( \zeta = (\zeta, \zeta') \) which is defined by \( F(\zeta, \zeta') := \lambda \zeta^3 + \lambda' \zeta'^3 \).

On one hand with \( F(X) = \lambda(\sum a_iX_i)^3 + \lambda'(\sum a'_iX_i)^3 \) and the notation \( \gamma_i := (a_i, a'_i) \) we have

\[
F(X) = F\left( \sum a_iX_i, \sum a'_iX_i \right) = \mathcal{F}\left( \sum X_i\gamma_i \right)
\]

and any given form counted in \( \mathbb{Z}_2(n, X) \) can be represented in this way using \( F \).

On the other hand \( \{1), (2), (3)\} \) give the following representations for the coefficients of \( F \):

\[
\begin{align*}
q_{ii} &= \mathcal{F}(\gamma_i) \\
q_{ij} &= (1/2)(\mathcal{F}(\gamma_i + \gamma_j) - \mathcal{F}(\gamma_i - \gamma_j)) - \mathcal{F}(\gamma_i) \\
q_{ijk} &= (1/4)(\mathcal{F}(\gamma_i + \gamma_j + \gamma_k) - (\gamma_i + \gamma_j - \gamma_k) \\
& \quad - \mathcal{F}(\gamma_i - \gamma_j + \gamma_k) + \mathcal{F}(\gamma_i - \gamma_j - \gamma_k))
\end{align*}
\]

as can be checked quite easily, and all three equations from \( \{1), (2), (3)\} \) for the form \( F \) may as well be expressed in terms of linear combinations of \( F \)'s.
The arguments of $F$ are then exactly one, two or three of the $n$ variables $a_1, \ldots, a_n$ and we introduce the simplifying notation: let $e_i \in \{0, 1, -1\}$ for $i := 1, \ldots, n$ and $\sum_{i=1}^n |e_i| \leq 3$ as well as $F(\sum e_i a_i) = F(\sum e_i a_i, a'_i)$.

This allows us to use a collective notation for all expressions $F(a_1)$. $F(a \pm a_k)$ and $F(a, a \pm a_k)$ that show up in the equations for the coefficients.

After these technical remarks, we now want to use the conditions $|q_{ijk}| \leq X$ and $q_{ijk} \in \mathbb{Z}$ for the coefficients of $F$ to estimate the number of $(a, a') \leq Q$ that gives a form with integer coefficients bounded by $X$ with the help of the system \{(1), (2), (3)\}.

The condition $|q_{ijk}| \leq X$ yields as a consequence of \{(1), (2), (3)\} the system \{(1), (2), (3)\} of inequalities given by:

\[
\begin{align*}
(1) & \quad |\lambda a_i^3 + \lambda' a_i^3| \leq X \\
(2) & \quad |3\lambda a_i^2 a_j + 3\lambda' a_i^2 a_j| \leq X \\
(3) & \quad |6\lambda a_i a_j a_k + 6\lambda' a_i a_j a_k| \leq X
\end{align*}
\]

The condition $q_{ijk} \in \mathbb{Z}$ is equivalent with $|q_{ijk}| \leq 1 \forall p \in \mathbb{P}$ and yields for each prime $p$ a system \{(1), (2), (3)\} of inequalities given by:

\[
\begin{align*}
(1) & \quad |\lambda a_i^3 + \lambda' a_i^3| \leq 1 \\
(2) & \quad |3\lambda a_i^2 a_j + 3\lambda' a_i^2 a_j| \leq 1 \\
(3) & \quad |6\lambda a_i a_j a_k + 6\lambda' a_i a_j a_k| \leq 1
\end{align*}
\]

The next step is to examine what these inequalities imply for the expressions $F(\sum e_i a_i)$. With the notations of this section we get:

**Lemma 2.1.**
Moreover for \( p = 2 \):  
\[ |F(a_i + a_j) - F(a_i - a_j)|_2 \leq 1/2 \quad \text{and} \quad |F(a_i + a_j + a_k) - F(a_i + a_j - a_k) + F(a_i - a_j - a_k)|_2 \leq 1/4. \]

Proof. For the first two statements, the system \( \{(1), (2), (3)\} \) allows us to write the expressions \( F(\sum \epsilon_i a_i) \) as linear combinations of the coefficients of \( F \) as follows:

\[
F(a_i) = q_{ii}
\]

\[
F(a_i + a_j) = q_{ii} + q_{jj} + q_{ij} + q_{ij}
\]

\[
F(a_i + a_j + a_k) = q_{ii} + q_{jj} + q_{jk} + q_{jk} + q_{ij} + q_{kk}
\]

\[+ q_{ij} + q_{jk} + q_{kk} + q_{kk}.
\]

The restrictions on the coefficients then complete the proof of the archimedean part of the statement since sign permutations do not affect the triangle inequality and since we have one, four or ten summands respectively that are bounded by \( X \) in absolute value. Analogously we find \( |F(\sum \epsilon_i a_i)|_p \leq 1 \) for \( p \in \mathbb{P} \) using the strong triangle inequality.

The supplement for \( p = 2 \) follows by substitution of the linear combinations of \( F \)’s by the coefficients \( q_{jk} \):

\[
F(a_i + a_j) - F(a_i - a_j) = 2q_{jj} + 2q_{ij}
\]

and

\[
F(a_i + a_j + a_k) - F(a_i + a_j - a_k) - F(a_i - a_j + a_k) + F(a_i - a_j - a_k) = 4q_{jk}.
\]

2.2. The Decomposition of \( F \) into Linear Factors. To estimate the number of solutions of the systems \( \{(1), (2), (3)\}_\infty \) and \( \{(1), (2), (3)\}_p \) for \( p \in \mathbb{P} \), it is profitable to decompose \( F \) into linear factors since products of linear terms are easier to handle than sums of cubes. It is easily seen that

\[
\lambda \xi^3 + \lambda' \xi'^3 = (\lambda^{1/3} \xi + \lambda'^{1/3} \xi')(\xi^{1/3} \xi + \xi'^{1/3} \xi')(\xi^{2/3} \xi + \zeta \xi^{1/3} \xi')
\]

\[= L_1(\xi, \xi') L_2(\xi, \xi') L_3(\xi, \xi'), \]

where \( \lambda^{1/3}, \xi^{2/3}, \zeta \xi^{1/3} \) denote the third roots of \( \lambda \) and \( \xi^2 + \xi + 1 = 0 \) yields

\[
L_1(\xi, \xi') + L_2(\xi, \xi') + L_3(\xi, \xi') = 0.
\]

We now set \( K = \mathbb{Q}(\sqrt{d}, \xi, \xi^{1/3}, \lambda^{1/3}). \) Since \( \lambda, \lambda' \) lie in \( \mathbb{Q}(\sqrt{d}) \), we obtain

\[
[K : \mathbb{Q}] \leq 2 \times 2 \times 3 \times 3 = 36.
\]

Using this decomposition in linear factors, the inequalities \((1)^n \) and \((1)^p \) for \( i = 1, \ldots, n \), and \( p \in \mathbb{P} \) can be stated as follows:
\[ |\lambda a_i^3 + \lambda a_i^4| \leq X \Leftrightarrow |L_1(a_i) L_2(a_i) L_3(a_i)| \leq X, \]
\[ |\lambda a_i^4 + \lambda a_i^5|_p \leq 1 \Leftrightarrow |L_1(a_i) L_2(a_i) L_3(a_i)|_p \leq 1 \quad p \in \mathbb{P}. \]

Since the coefficients of the linear forms now lie in the field $K$, an extension of the valuations $| |$ and $| |_p$ becomes necessary.

To do so, just a little algebraic number theory comes in: if $K$ denotes an algebraic number field, then above each place of $\mathbb{Q}$ (= equivalence class of valuations) lie finitely many places of $K$, which each define such an equivalence class of $K$. Selecting one representant per class, one obtains a countable infinite set denoted by $M(K)$. Let $M_0(K)$ be reserved for those valuations lying above the usual one in $\mathbb{Q}$ and $M_p(K)$ for those lying above the $p$-adic absolute values, that is, the non-archimedean ones.

If for $v \in M(K)$ we abbreviate $L_i^j := L_j(a_i)$ with $j = 1, 2, 3$ and $i = 1, \ldots, n$, we get:

\[ |L_1^i|_v, |L_2^j|_v, |L_3^k|_v \leq X \quad \text{for} \quad v \in M_0(K), \]
\[ |L_1^i|_v, |L_2^j|_v, |L_3^k|_v \leq 1 \quad \text{for} \quad v \in M_p(K). \]

**Proposition 2.2.** With the introduced notations one has:

\[ \max_i |L_1^i|_v, \max_j |L_2^j|_v, \max_k |L_3^k|_v \leq \left\{ \begin{array}{ll} 45X & \text{if} \; v \mid \infty, \\ 1 & \text{if} \; v \mid p, \; p \in \mathbb{P}. \end{array} \right. \]

**Proof.** We first define:

\[ \max_i |L_1^i|_v := |L_1^i|_v, \]
\[ \max_j |L_2^j|_v := |L_2^j|_v, \]
\[ \max_k |L_3^k|_v := |L_3^k|_v. \]

and distinguish 3 cases.

1. $i_0 = j_0 = k_0$. Then the statement follows immediately from Lemma 2.1, putting $e_i = 1, e_j = 0$ for $i \neq i_0$, which implies

\[ |L_1^i|_v, |L_2^j|_v, |L_3^k|_v \leq \left\{ \begin{array}{ll} X & \text{if} \; v \mid \infty, \\ 1 & \text{if} \; v \mid p, \; p \in \mathbb{P}. \end{array} \right. \]

2. $i_0 = j_0 \neq k_0$. We have

\[ 2L_1^k L_2^k L_3^k = \overline{f}(a_k + a_k) - \overline{f}(a_k - a_k) - 2\overline{f}(a_k) \]
\[ - 2L_1^k L_2^k L_3^k - 2L_1^k L_2^k L_3^k, \]
and this gives
\[ |2L^j v L^L v | \leq |F(a_h + a_k) - F(a_h - a_k)| + |2F(a_h)| + |2L^j v L^L v |\]
\[ + |2L^j v L^L v | + |2L^j v L^L v | \]
for \( v \), \( \infty \),
\[ |2L^j v L^L v | \leq \max \{ |F(a_h + a_k) - F(a_h - a_k)|, |2F(a_h)| \}
\[ + |2L^j v L^L v |, |2L^j v L^L v | \}
for \( v \), \( M(K) \). The definition of \( i_0 \) and \( k_0 \) yields
\[ |L^j v | \leq |L^j v | \text{ and } |L^j v | \leq |L^j v | \]
and the last two terms are \( \leq |L^j v L^L v | \), in both inequalities, that is \( \leq 2X \)
for \( v \), \( \infty \) and \( \leq 1 \) for \( v | p, p \neq 2 \), respectively \( \leq 1/2 \) for \( v | 2 \).
By Lemma 2.1 we obtain
\[ |L^j v | \leq \begin{cases} 7X & \text{if } v \not| \infty, \\ 1 & \text{if } v | p. \end{cases} \]

(3) \( i_0 \not= j_0 \not= k_0 \not= i_0 \). We have
\[ 4L^j v L^L v L^j v = F(a_h + a_h + a_k) - F(a_h + a_h - a_k) - F(a_h - a_h + a_k) \]
\[ + F(a_h - a_h - a_k) - 4L^j v L^L v L^j v - 4L^j v L^L v L^j v \]
\[ - 4L^j v L^L v L^j v - 4L^j v L^L v L^j v - 4L^j v L^L v L^j v \]
and this gives
\[ |4L^j v L^L v L^j v | \leq |F(a_h + a_h + a_k)| + |F(a_h + a_h - a_k)|
\[ + |F(a_h - a_h + a_k)| + |F(a_h - a_h - a_k)| \]
\[ + |4L^j v L^L v L^j v | + |4L^j v L^L v L^j v | + |4L^j v L^L v L^j v | \]
\[ + |4L^j v L^L v L^j v | \]
for \( v \), \( \infty \),
\[ |4L^j v L^L v L^j v | \leq \max \{ |F(a_h + a_h + a_k) - F(a_h + a_h - a_k) \]
\[ - F(a_h - a_h + a_k) + F(a_h - a_h - a_k)|, \]
\[ + 4L^j v L^L v L^j v |, |4L^j v L^L v L^j v |, |4L^j v L^L v L^j v |, \]
\[ + 4L^j v L^L v L^j v | \}
for \( v \mid p \). The estimate of the \( f \)-terms is evident by Lemma 2.1, when for \( p \mid 2 \) the extra result is taken in account. The remaining 5 terms can be treated by case 2), as we will show with \( L_i^3 L_j^3 L_k^3 \) for example.

We use

\[
|L_i^3 L_j^3 L_k^3|_v \leq |L_i^3 L_j^3 L_k^3|_v \quad \text{if} \quad |L_i^3|_v \gg |L_j^3|_v,
\]

\[
|L_i^3 L_j^3 L_k^3|_v \leq |L_i^3 L_j^3 L_k^3|_v \quad \text{if} \quad |L_j^3|_v \gg |L_k^3|_v.
\]

If none of these two situations occurs, we must have

\[
|L_i^3 L_j^3 L_k^3|_v \leq |L_j^3 L_k^3 L_i^3|_v.
\]

and (1) can be applied.

Suppose w.l.o.g. that \( |L_i^3|_v \gg |L_j^3|_v \), then (2) implies:

\[
2L_i^3 L_j^3 L_k^3 = \& (a_i + a_j) - \& (a_j - a_k) - 2\& (a_k) + 2L_i^3 L_j^3 + 2L_i^3 L_k^3.
\]

The \( f \)-terms are estimated as usually and in view of \( |L_j^3|_v \leq |L_j^3|_v \) by the definition of \( f_0 \) and \( |L_j^3|_v \leq |L_j^3|_v \), by assumption, the estimate from (2) is applicable in this case also.

Altogether, for \( v \mid \infty \) the 4 \( f \)-terms are bounded by \( 10X \) and the remaining 5 ones by \( 4 \ast 7X \) to give

\[
|4L_i^3 L_j^3 L_k^3|_v \leq 4 \ast 10X + 5 \ast 4 \ast 7X = 180X,
\]

which implies \( |L_i^3 L_j^3 L_k^3|_v \leq 45X \) for \( v \mid \infty \). For \( p \mid 2 \), \( p \neq 2 \), all terms are bounded by 1 and the maximum is thus \( \leq 1 \); in the case \( v \mid 2 \) a factor \( 1/4 \) appears in each term, which cancels on both sides to give \( |L_i^3 L_j^3 L_k^3|_v \leq 1 \) for \( v \mid p \), \( p \in \mathbb{P} \), as desired.

This answers the question of the estimate of \( |L_i^3|_v \), \( |L_j^3|_v \), \( |L_k^3|_v \) for arbitrary \( 1 \leq i, j, k \leq n \), since even the product of the maxima of the absolute values of the arising linear forms is bounded absolutely.

2.3. The Switch to Rational Variables. Since \( a_i, a'_i \) are conjugates in \( \mathbb{Q}(\sqrt{d}) \) when \( d \neq 1 \), we have

\[
a_i = A_i + B_i \sqrt{d} \quad \text{and} \quad a'_i = A_i - B_i \sqrt{d}
\]

with rational \( A_i \) and \( B_i \). This also makes sense for \( d = 1 \). The reader should be aware of the fact that integer \( a_i, a'_i \) do not always imply \( (A_i, B_i) \in \mathbb{Z}^2 \), but this does not matter for the following.
Defining $\tilde{F}(a_i, b_i) := F(a_i, a'_i)$, the decomposition of $F$ implies a similar one for $\tilde{F}$, namely:

$$\tilde{F}(a_i, b_i) = \tilde{L}_s(A_i, B_i) \tilde{L}_s(A_i, B_i) \tilde{L}_s(A_i, B_i),$$

where $\tilde{L}_j(A_i, B_i) = L_j(a_i, a'_i) = L_j^s + L_j^r$ and:

$$\tilde{L}_1^r = (\lambda^{1/3} + \lambda^{1/3}) A_i + (\lambda^{1/3} - \lambda^{1/3}) \sqrt{d} B_i,$$

$$\tilde{L}_2^r = (\zeta \lambda^{1/3} + \zeta^2 \lambda^{1/3}) A_i + (\zeta \lambda^{1/3} - \zeta^2 \lambda^{1/3}) \sqrt{d} B_i,$$

$$\tilde{L}_3^r = (\zeta^2 \lambda^{1/3} + \zeta \lambda^{1/3}) A_i + (\zeta^2 \lambda^{1/3} - \zeta \lambda^{1/3}) \sqrt{d} B_i.$$

The results of the preceding section give

$$|L_1|, |L_2|, |L_3| \leq X \quad \text{and} \quad |\tilde{L}_1|, |\tilde{L}_2|, |\tilde{L}_3| \leq 45X \quad \forall \ |\infty.$$

$$|\tilde{L}_1|, |\tilde{L}_2| \leq 1 \quad \text{and} \quad |\tilde{L}_3| \leq 1 \quad \forall \ |\in P.$$

This is a system of inequalities in the variables $(A_i, B_i)_{i=1,...,n}$ whose number of solutions has to be estimated.

Since the methods involved for $\forall \ |\infty$ and $\forall \ |p$ are somewhat different, it seems wise to treat the two systems separately for a while. Doing so, we are facing two separate problems, an archimedean and a non-archimedean one, which nevertheless show some remarkable parallels.

To keep notations simple, instead of writing $\tilde{L}$ we use $L$ for variables $(A_i, B_i) \in \mathbb{Q}^2$. For $(A_i, B_i)_{i=1,...,n}$ we shortly write $(A, B)$.

3. THE ARCHIMEDEAN PROBLEM

3.1. The Domains $S_d(X)$ and $S(X)$. In this chapter we want to study rational solutions $(A_i, B_i)$ of $|L_1|, |L_2|, |L_3| \leq X$ for $\forall \ |\infty$ and $(A_i, B_i)_{i=1,...,n}$ of the mixed inequality $|L_1|, |L_2|, |L_3| \leq 45X$ for $\forall \ |\infty$. We will need the following domains $S_d(X)$ and $S(X)$:

**Definition 3.1.** Let $S_d(X) \subset \mathbb{R}^2$ be the domain defined by an inequality of type (1)$_n^d$:

$$S_d(X) = \{(A, B) \in \mathbb{R}^2 : F(A, B) \leq X\}.$$ 

By $S(X)$ we denote the domain in $\mathbb{R}^{2n}$ defined by the system $\{(1), (2), (3)\}_n^\infty$:

$$S(X) = \{(A, B) \in \mathbb{R}^{2n} : (A, B) \text{ satisfies } \{(1), (2), (3)\}_n^\infty\}.$$ 

This leads to the observation $S(X) \subset S_d(X)^n$ since in the definition of $S(X)$ all inequalities of type (1)$_n^m$ have to be satisfied as necessary for
S\(_0(X)\) and the additional constraints of type \((2)^m, (3)^m\) can only make the domain in question smaller.

Let us start with \(S\(_0(X)\)\) whose shape is determined mainly by the decomposition of \(F(A, B)\) in \(L_1L_2L_3\). Since for fixed \((A, B)\) the expression \(F(A, B) = \lambda a^3 + \lambda' a^3\) appears as a coefficient of \(F\), we have \(F(A, B) \in \mathbb{Q}[A, B]\), which implies that either all three factors \(L_j, 1 \leq j \leq 3\) of the decomposition of \(F\) are real or one is real and the other two are complex conjugates.

Let first all three linear forms be real. Then \(S\(_0(X)\)\) is an unbounded domain in \(\mathbb{R}^2\) with three asymptotes corresponding to the solutions \((A, B)\) of \(L_j(A, B) = 0\). Our next goal is to prove the existence of a covering of this domain by convex sets that are symmetric with respect to the origin and whose role should become evident soon.

**Lemma 3.2.** Let all three linear forms in the decomposition \(F = L_1L_2L_3\) be real, that is \(S\(_0(X)\)\) has 3 asymptotes. Then three series of convex polygons \(P_m, Q_m, R_m, (m = 1, 2, \ldots)\) defined by the inequalities

\[
\begin{align*}
|P_m| &\leq 2\left(2m + 3\right)^{1/3} \\
|Q_m| &\leq 2m + 3 \\
|R_m| &\leq 2m + 3 \\
|L_1| &\leq 2m + 3 \\
|L_2| &\leq 2m + 3 \\
|L_3| &\leq 2m + 3 \\
|L_4| &\leq 2m + 3 \\
|L_5| &\leq 2m + 3 \\
|L_6| &\leq 2m + 3 \\
\end{align*}
\]

cover the whole domain \(S\(_0(X)\)\).

**Proof.** First choose \(m \in \mathbb{N}\) such that for some \((A, B) \in S\(_0(X)\)\):

\[
2^{-2m + 1} \leq \min_{j \in \{1, 2, 3\}} |L_j(A, B)| \leq 2^{-2m + 3} X^{1/3}.
\]

Then \(m \geq 1\) since \(|L_1L_2L_3| \leq X\), which implies that not all three absolute values can be \(\geq 2X^{1/3}\). All hypotheses being symmetric in \(j = 1, 2, 3\) we may assume without loss of generality \(|L_1| \leq |L_2| \leq |L_3|\). In turn:

\[
|L_1L_2L_3| \leq X \Rightarrow |L_2L_3| \leq 2m \Rightarrow |L_2| \leq 2m X^{1/3},
\]

and \(L_1 + L_2 + L_3 \equiv 0\) yields:

\[
|L_3| \leq |L_1| + |L_2| \Rightarrow |L_3| \leq 2^{-2m + 3} X^{1/3} + 2m X^{1/3} \leq 2m X^{1/3}.
\]

Consequently we have:

\[
|L_1| \leq 2^{-2m + 3} X^{1/3} \quad \text{and} \quad |L_2| \leq 2m X^{1/3} \quad \text{and} \quad |L_3| \leq 2m X^{1/3},
\]
which means \((A, B) \in P_m\). All other cases are completely analogous and lead to \((A, B) \in Q_m\) respectively \((A, B) \in R_m\), so that \(S_0(X) \subset \bigcup_{m=1}^{\infty} (P_m \cup Q_m \cup R_m)\).

Now let two of the linear forms in the decomposition \(F = L_1 L_2 L_3\) be complex conjugates. Then \(S_0(X) \subset \mathbb{R}^3\) turns out to be an unbounded domain with one asymptote corresponding to the solutions \((A, B)\) of the equation \(L_j(A, B) = 0\) where \(j \in \{1, 2, 3\}\) is the subscript of the real factor \(L_j\). Again we look for a covering of \(S_0(X)\) by convex, symmetric about the origin sets.

**Lemma 3.3.** In the decomposition \(F = L_1 L_2 L_3\) let w.l.o.g. \(L_1\) be real and \(L_2\) the complex conjugate of \(L_3\), so that \(S_0(X)\) has one asymptote. Then the sequence of convex sets \(P_m, m \in \mathbb{N}\), defined by the inequalities

\[
\langle P_m \rangle \\
|L_1| \leq 2^{-2m + 3} X^{1/3} \\
|L_2 L_3| \leq 2^{2m + 6} X^{2/3}
\]

covers the domain \(S_0(X)\).

**Proof.** First choose \(m \in \mathbb{N}\) such that for some \((A, B) \in S_0(X)\):

\[
2^{-2m + 1} X^{1/3} \leq |L_1| \leq 2^{-2m + 3} X^{1/3}.
\]

(This is the analogous procedure as in Lemma 3.2; the choice of \(L_1\) as the real linear form doesn’t involve any loss of generality.) Then \(m \geq 1\) since \(|L_1 L_2 L_3| = |L_1 L_2 L_2| = |L_1| |L_2|^2 \leq X\). If we had \(|L_1| \geq 2X^{1/3}\), this would imply \(|L_2| = |L_3| \leq (1/\sqrt{2}) X^{1/3}\) and \(L_1 + L_2 + L_3 = 0\) would give \(|L_1| \leq |L_2| + |L_3| = (2/\sqrt{2}) X^{1/3} \leq 2X^{1/3}\), a contradiction to the hypothesis. \(|L_1| \geq 2^{-2m + 1} X^{1/3}\), in view of \(|L_1 L_2 L_3| \leq X\), immediately yields \(|L_2 L_3| \leq 2^{2m - 1} X^{2/3} \leq 2^{2m + 6} X^{2/3}\), which means \((A, B) \in P_m\). Since \((A, B)\) was arbitrary in \(S_0(X)\), we finally get \(S_0(X) \subset \bigcup_{m=1}^{\infty} P_m\).

So far we didn’t use the inequalities \((2)^{\alpha}, (3)^{\alpha}\) and the resulting inequality \(|L_1|, |L_2|, |L_3| \leq 45X\).

3.2. \(S(X)\) and the Repartition of Rational Solutions of \(\{(1), (2), (3)\}_X\). Our aim is to show that points in \(S(X)\) have all their \(n\) components \((A_j, B_j)\) concentrated respectively along one asymptote of \(S_0(X)\) that does not depend on \(i\) in such a way that there exists a covering set from Lemma 3.2 resp. Lemma 3.3 that contains all those \(n\) components. So not only we would have

\[
S(X) \subset S_0(X)^n = \left( \bigcup_{m=1}^{\infty} (P_m \cup Q_m \cup R_m) \right)^n,
\]
but even
\[ S(X) \subseteq \bigcup_{m=1}^{\infty} (P_m^* \cup Q_m^* \cup R_m^*), \]
where \( Q_m \) and \( R_m \) appear only in the case of three asymptotes.

**Proposition 3.4.** Let all 3 factors in the decomposition of \( \mathbb{V} \) be real. If \((A, B) = (A_i, B_i), i=1, \ldots, n \in \mathbb{Q}^2 \) lies in \( S(X) \), then there exists an \( m \geq 1 \), such that all \( n \) components \( (A_i, B_i) \) of \((A, B)\) lie in \( P_m \) (resp. \( Q_m, R_m \)).

**Proof.** When \((A, B) \in S(X)\) we first choose \( m \geq 1 \) such that
\[ 2^{-m+1}X^{1/3} \leq \min\{|L_1^b|, |L_2^b|, |L_3^b|\} \leq 2^{-2m+3}X^{1/3}. \]
As usual \(|L_i^b|\) denotes the maximum of the \(|L_i^b|\) for \( i = 1, \ldots, n \), etc. Once again, w.l.o.g. we assume that \(|L_1^b|\) is this minimum and also \(|L_2^b| \leq |L_3^b|\).

By Proposition 2.2:
\[ |L_1^b| |L_2^b| |L_3^b| \leq 45X, \]
and we get:
\[ |L_j^b| |L_k^b| \leq 45 + 2^{2m-1}X^{2/3} \]
\[ \Rightarrow |L_j^b| \leq \sqrt{45 + 2^{2m-1}X^{2/3}} \leq 5 + 2^mX^{1/3}, \]
which leads to:
\[ |L_k^b| \leq |L_j^b| + |L_j^b| \leq 2^{-2m+3}X^{1/3} + 5 + 2^mX^{1/3}. \]
So we find \( \forall i, j, k: \)
\[ |L_1^b| \leq 2^{-2m+3}X^{1/3} \text{ and } |L_2^b| \leq 2^{-2m+3}X^{1/3} \text{ and } |L_3^b| \leq 2^{-2m+3}X^{1/3}. \]
This means precisely that each \((A_i, B_i), i = 1, \ldots, n \) lies in \( P_m \) since the required inequalities are even satisfied for the maxima of the absolute values of the corresponding \( L_j^b \), \( j = 1, 2, 3 \). If instead of \(|L_1^b|\) one of the other maxima is minimal, all \((A_i, B_i)\) lie in \( Q_m \) resp. \( R_m \).

An analogous result is also for the case that \( S_0(X) \) has only one asymptote:

**Proposition 3.5.** Let only one of the factors in the decomposition of \( \mathbb{V} \) be real. If \((A, B) = (A_i, B_i), i=1, \ldots, n \in \mathbb{Q}^2 \) lies in \( S(X) \), then there exists an \( m \geq 1 \), such that all \( n \) components \( (A_i, B_i) \) of \((A, B)\) lie in \( P_m \).
Proof. Let again $L_1$ be the real linear form and $(A, B) \in S(X)$. We choose $m \geq 1$ such that:

$$2^{-2m + 1}X^{1/3} \leq |L_1^2| \leq 2^{-2m + 3}X^{1/3}.$$ 

By Proposition 2.2:

$$|L_1^2| |L_2^1| |L_3^0| \leq 45X.$$ 

We get

$$|L_1^2| \max_j |L_j^1 L_j^3| \leq 45X \Rightarrow |L_j^1 L_j^3| \leq 45 \ast 2^{2m - 1}X^{2/3} \leq 2^{2m + 6}X^{2/3}$$

for all $j$, since $\max_j |L_j^1 L_j^3| \leq |L_j^2| |L_j^3|$. We find $\forall i, j$:

$$|L_i^1| \leq 2^{-2m + 3}X^{1/3} \quad \text{and} \quad |L_j^1 L_j^3| \leq 2^{2m + 6}X^{2/3}.$$ 

This means precisely that each $(A_i, B_i)$ for $i = 1, ..., n$ lies in $P_m$, since all requirements are satisfied even for the maxima of the absolute values of $L_i^1$ and $L_j^1 L_j^3$.

3.3. The Archimedean Bound. Such a bound consists in the estimate of the volumes of the introduced domains. But it is not the volume $V(S(X))$ of the domain of solutions of the system $\{ (1), (2), (3) \}$ that turns out to be of interest, it is the 2-dimensional pieces that matter. So we focus mainly on $V(P_m)$ (resp. $V(Q_m)$, $V(R_m)$), the reason being that the sets $P_m$, $Q_m$, $R_m$ are convex and symmetric with respect to the origin, which makes them accessible to lattice point methods. We are only interested in a sufficiently good bound depending explicitly on $m$, $\delta$, $\lambda'$ and $d$; let us treat the case of $P_m$ as an example easily applicable to $Q_m$, $R_m$ also.

Lemma 3.6. For $m \geq 1$ we have

$$V(P_m) \ll 2^{-m}d^{-1/2}(\delta \lambda')^{-1/3}X^{2/3},$$

where the constant in $\ll$ depends on $n$ only and moreover,

$$V(S_d(X)) \ll d^{-1/2}(\delta \lambda')^{-1/3}X^{2/3}.$$ 

Proof. To shorten the exposition, we first want to combine the cases of one and three asymptotes distinguished in the previous section. The corresponding volumes of the $P_m$ are certainly smaller than the ones of the domains defined by

$$|L_1| \leq 2^{-2m + 3}X^{1/3} \quad \text{and} \quad |L_2 L_3| \leq 2^{2m + 6}X^{2/3},$$
where we again assume that $|L_1| = \min\{|L_1|, |L_2|, |L_3|\}$, since for the case of three asymptotes we trivially have:

$$|L_2| \leq 2^{m+3}X^{1/3} \quad \text{and} \quad |L_3| \leq 2^{m+3}X^{1/3} \Rightarrow |L_2L_3| \leq 2^{2m+6}X^{2/3}.$$  

The system of equations to analyse then is (with $\lambda^{1/3}$ being the real third root of $\lambda$ and $i \in \{1, \ldots, n\}$):

$$|\lambda^{1/3}a_i + \lambda'^{1/3}a'_i| \leq 2^{-2m+3}X^{1/3}$$

$$|\lambda^{2/3}a_i^2 + \lambda'^{2/3}a'_i^2 - (\lambda^{1/3}a_ia'_i)| \leq 2^{2m+6}X^{2/3}$$

when $(A_i, B_i)$ is transformed back to $(a_i, a'_i)$, where in the case $d = 1$ the numbers $a_i, a'_i$ are independent rationals, whereas they are conjugates over $\mathbb{Q}(\sqrt{d})$ for $d \neq 1$. The arising determinant of this transformation is $2 \sqrt{d}$.

The transformation

$$\lambda^{1/3}a_i \mapsto \alpha_i \quad \text{and} \quad \lambda'^{1/3}a'_i \mapsto \alpha'_i$$

whose determinant is given by $(\lambda \lambda')^{1/3}$ reduces the above system to

$$|\alpha_i + \alpha'_i| \leq 2^{-2m+3}X^{1/3}$$

$$|\alpha_i^2 + \alpha'_i^2 - \alpha_i\alpha'_i| \leq 2^{2m+6}X^{2/3}$$

with $(\alpha_i, \alpha'_i) \in \mathbb{Q}^2$ for $d = 1$ and $\alpha_i$ conjugate to $\alpha'_i$ over $\mathbb{Q}(\sqrt{d})$ for $d \neq 1$. In both cases the substitution

$$\alpha_i = S_i + T_i \sqrt{d} \quad \text{and} \quad \alpha'_i = S_i - T_i \sqrt{d}$$

whose determinant is $1/(2 \sqrt{d})$ leads to

$$|2S_i| \leq 2^{-2m+3}X^{1/3}$$

$$|S_i^2 + 3dT_i^2| \leq 2^{2m+6}X^{2/3}$$

with independent rational variables $S_i$ and $T_i$. This leads to

$$|S_i| \ll 2^{-2m}X^{1/3} \quad \text{and} \quad |T_i| \ll 2^{m}d^{-1/2}X^{1/3},$$

and considering the determinants of all intermediate changes of variables we obtain:

$$V(P_m) \ll (\lambda \lambda')^{-1/3} \left(2^{-2m}X^{1/3} \right) \left(2^{m}d^{-1/2}X^{1/3} \right)$$

$$\ll 2^{-m}d^{-1/2}X^{2/3}.$$
An analogous estimate leads to the same result for \( V(Q_m) \) and \( V(R_m) \):

\[
S_0(X) \subset \bigcup_{m=1}^{\infty} (P_m \cup Q_m \cup R_m)
\]

then yields immediately:

\[
V(S_0(X)) \ll \sum_{m=1}^{\infty} 2^{-m}d^{-1/2}(\lambda \cdot \gamma)^{-1/3} X^{2/3} = d^{-1/2}(\lambda \cdot \gamma)^{-1/3} X^{2/3},
\]

and \( S(X) \subset S_0(X) \) gives the stated bound for the \( n \)-dimensional domain.

### 4. THE NON-ARCHIMEDEAN PROBLEM

In the first part of this chapter, we shall work on the non-archimedean inequalities obtained in Chapter 2 for fixed \( p \not\in \mathcal{P} \), whereas in the second part the results will be combined and completed for all \( p \in \mathcal{P} \).

#### Results for Fixed \( p \)

4.1. The Discrete \( \mathbb{Z}_p \)-Module \( A_0(p) \). In this first part of Chapter 4, let \( p \) denote a fixed, given prime. Our first task is to analyse the inequalities

\[
|L_i|_v \leq 1 \quad \text{for } v \mid p \text{ and } i \in \{1, \ldots, n\}
\]

which were resulting from (1). Corresponding to the three possibilities to choose the minimum among \( |L_i|_v, |L_j|_v, |L_k|_v \), we are led to three cases for given \( i \) whose treatment is completely identical, so that we may assume \( |L_1|_v \) to be that minimum.

Some simple facts concerning \( |L_j|_v \) (\( j = 1, 2, 3 \)) from algebraic number theory: the linear forms \( L_j \) have rational variables \((A_i, B_i)\) and coefficients from the algebraic number field \( K \) (see Chapter 2, Section 2), satisfying

\[
[K: \mathbb{Q}] \leq 36.
\]

The value group of \( | \cdot |_v \) is thus a subset of \( \mathbb{R}^+ \), and we find:

\[
|L_1|_v, |L_2|_v, |L_3|_v \leq 1 \Rightarrow |L_1|_v \leq p^3, |L_2|_v \leq p^3, |L_3|_v \leq p^3
\]

for \( z_1, z_2, z_3 \in (1/36) \mathbb{Z} \) with \( z_1 + z_2 + z_3 \leq 0 \) and \( z_1 = \min_{j \in \{1, 2, 3\}} z_j \).

Because of \( L_1 + L_2 + L_3 \equiv 0 \) this reduces to

\[
|L_1|_v \leq p^{-2z},
|L_2|_v \leq p^{z_3},
|L_3|_v \leq p^{z_3}
\]

for a \( z \in (1/36) \mathbb{N}_0 \), since the maximum of the three absolute values must appear at least twice. The third inequality is thus a consequence of the previous ones, reducing the system to

\[
|L_1|_v \leq p^{-2z},
|L_2|_v \leq p^{z_3}.
\]
What can be said about rational solutions \((A_i, B_i)\) in \(\mathbb{Q}^2\) of this system? We shall study this question in a slightly more general context with \((A_i, B_i) \in \mathbb{Q}_p^2\), where \(\mathbb{Q}_p\) denotes the \(p\)-adic field. For every continuation \(v\) of \(p\) to an algebraic number field \(K_v\), let \(K_v\) denote its completion with respect to \(v\).

**Remark.** If \(A, B\) are rank \(r\) submodules of a free \(\mathbb{Z}_p\)-module \(N\) of rank \(r\), we define the “index” of \(B\) in \(A\) by \([A : B] := [M : B] / [M : A]\), where \(M\) is a module in \(N\) containing both \(A, B\). This “index” is well defined, since it is independent of the choice of \(M\) under the given restrictions.

**Theorem 4.1.** Let \(p \notin \mathcal{P}\) and \(K\) be an algebraic number field. For each \(v \mid p\), let \(A_v\) be a non-singular \(m \times m\) matrix with entries from \(K_v\).

Then the \(x = (x_1, ..., x_m) \in \mathbb{Q}_p^m\) satisfying \(|\alpha_v x|_v \leq 1\) for \(v \mid p\) lie in a discrete \(\mathbb{Z}_p\)-module \(A_0(p)\) of \(\mathbb{Q}_p^m\) of rank \(m\). Moreover

\[A_0(p) \subset \mathbb{A}_0(p) \subset \overline{A}_0(p)\]

where \(A_0(p)\) denotes the module defined by \(|x|_v \leq |\alpha_v|^{-1}_v\) for all \(v \mid p\) and \(\mathbb{A}_0(p)\) is defined by \(|x|_v \leq |\alpha_v^{-1}|_v\) for all \(v \mid p\).

For the “index” of \(A_0(p)\) in \(\mathbb{Z}_p^m\) we have:

\[[\mathbb{Z}_p^m : A_0(p)] \succ \max_{v \mid p} \{|\det \alpha_v|_v\}_p,\]

where \(\{\alpha\}_v := \min\{p^\epsilon : g \in \mathbb{Z}_p, p^\epsilon \succ A\}\) and \(|\alpha_v|_v\) denotes the maximum norm of the entries of \(\alpha_v\).

**Proof.** By assumption all \(x \in A_0(p)\) satisfy the condition \(|\alpha_v x|_v \leq 1\) for \(v \mid p\) with a non-singular matrix \(\alpha_v\) from \(K_v^m\). We may thus consider \(\alpha_v^{-1}\) and find:

\[|x|_v = |\alpha_v^{-1} \cdot x|_v \leq |\alpha_v^{-1}|_v \cdot |\alpha_v x|_v \leq |\alpha_v^{-1}|_v\]

which implies \(x \in \overline{A}_0(p)\). The points \(x \in A_0(p)\) satisfy \(|x| \leq |\alpha_v|^{-1}_v\) for all \(v \mid p\), and we get:

\[|\alpha_v x|_v \leq |\alpha_v^\epsilon|_v \cdot |\alpha_v|_v \cdot |\alpha_v^{-1}|_v = 1\]

which implies \(x \in A_0(p)\). Now \(A_0(p)\) and \(\overline{A}_0(p)\) are obviously free, discrete \(\mathbb{Z}_p\)-modules of rank \(m\), hence the same holds for \(A_0(p)\).

The above observations lead to the existence of \(a_1^p, ..., a_m^p\) in \(\mathbb{Q}_p^m\) with

\[A_0(p) = a_1^p \mathbb{Z}_p + \cdots + a_m^p \mathbb{Z}_p.\]
Combining $a_1^r, \ldots, a_m^r$ to a matrix $A_p$, we obtain

$$[Z_m^p : A_p(p)] = |\det A_p|_p^{-1}.$$ 

Now all the $a_i^r$, $(1 \leq i \leq n)$ lie in $A_0(p)$, implying $|\alpha_i a_i^r|_v \leq 1$ for $i = 1, \ldots, n$ and $v | p$ resp. $|\alpha_i A_p|_v \leq 1$ for $v | p$. The ultrametric triangle inequality yields:

$$|\det \alpha_i A_p|_v \leq 1$$

for $v | p$.

$$|\det A_p|_v |\det \alpha_i|_v \leq 1$$

for $v | p$.

$$|\det A_p|_v^{-1} \geq |\det \alpha_i|_v$$

for $v | p$.

But $A_p$ consists of vectors $a_i^r \in \mathbb{Q}_p^m$, so that $|\det A_p|_v = |\det A_p|_p$ for all $v | p$. Consequently we may choose the $v | p$ for the above estimate that yields the strongest restriction to get

$$[Z_m^p : A_0(p)] = |\det A_p|_p^{-1} \geq \max_{v | p} |\det \alpha_i|_v.$$

Note that the exponents of $p$ in $|\det A_p|_p$ are allowed to take only integer values and we obtain

$$[Z_m^p : A_0(p)] \geq \max_{v | p} |\det \alpha_i|_v,$$

as stated.

The following definitions and observations will turn out to be useful. Let us start with the computation of the determinant of the matrix $L_{1, 2}$ whose entries are the coefficients of $L_1$ and $L_2$. We have

$$L_{1, 2} = \begin{pmatrix}
    \lambda^{1/3} + \lambda^{1/3} & (\lambda^{1/3} - \lambda^{1/3}) \sqrt{d} \\
    (\zeta \lambda^{1/3} + \zeta^2 \lambda^{1/3}) & (\zeta \lambda^{1/3} - \zeta^2 \lambda^{1/3}) \sqrt{d}
\end{pmatrix}
$$

$$= \begin{pmatrix}
    \lambda^{1/3} & \lambda^{1/3} \\
    \zeta \lambda^{1/3} & \zeta^2 \lambda^{1/3}
\end{pmatrix}
$$

as the reader may easily check using the expressions for $L_1$ and $L_2$ in terms of the variables $a_i$ and $a_i^r$, hence

$$\det L_{1, 2} = (\zeta^2 (\lambda \lambda')^{1/3} - \zeta (\lambda \lambda')^{1/3}) (-2 \sqrt{d}) = -2 \zeta (\lambda - 1) \sqrt{d} (\lambda \lambda')^{1/3}.$$
Definition 4.2. Let $L_{j,k}$ be the matrix whose entries are the coefficients of $L_j$ and $L_k$, $(j \neq k \in \{1, 2, 3\})$. We define:

$$A_0 := \det L_{j,k} = -2(\zeta - 1) \sqrt{d}(\lambda \lambda')^{1/3}$$

and this quantity depends only on the order of $j$ and $k$, however

$$A := A_0^6 = 2^3 \lambda^3 d(\lambda \lambda')^3 \in \mathbb{Q} \text{ for every possible choice of } j, k$$

$$|A_0|_v = |A_0|^1_6 = |A|^1_6 = |A|^1_p$$

depends only on $p$, not on $v|p$.

Definition 4.3. For the given system of inequalities

$$|L_{1j}|_v \leq p^{-2v}$$

$$|L_{1k}|_v \leq p^{v_0}$$

with $z_v \in (1/36) \cap \mathbb{Q}_p$ we define $z_p := \max_{v|p} z_v$, which yields an additional quantity depending on $p$ only that can be associated to the pair $(A, B) \in \mathbb{Q}_p^2$. We generalize this by:

$$(A, B) \in \mathbb{Q}_p^2 \to z_p(A, B) .$$

To each pair of $p$-adic numbers $(A, B)$ with $|L_1(A, B) L_2(A, B) L_3(A, B)|_v \leq 1$ we associate the quantity $z_p \in (1/36) \cap \mathbb{Q}_p$ defined by

$$p^v := \max_{v|p} \max_{k \in \{1, 2, 3\}} |L_k(A, B)|_v .$$

Because of $L_1 + L_2 + L_3 \equiv 0$ and the maximality of $z_p$, we see that $z_p$ is the greatest rational for which

$$\min_{j \neq k \in \{1, 2, 3\}} |L_j(A, B)|_v \leq p^{-2z_p}$$

$$|L_k(A, B)|_v = p^{z_p}$$

holds for $j \neq k \in \{1, 2, 3\}$ and some $v|p$.

Now we are in position to apply Theorem 4.1 with

$$Ax := \begin{pmatrix} p^{-2v} & 0 \\ 0 & p^v \end{pmatrix} L_{1,2}$$

to obtain:
Corollary 4.4. For given \( z_p \) the pairs \( (A, B) \in \mathbb{Q}_p^2 \) of \( p \)-adic numbers satisfying \( z_p(A, B) = z_p \) lie in the union of 3 discrete \( \mathbb{Z}_p \)-modules \( A_j(p) \), \( A_0(p) \) and \( A_3(p) \) of \( \mathbb{Q}_p^2 \) with

\[
\left[ Z^2 : A_j(p) \right] \geq \left\{ |A|^{1/6} p^{5/6} \right\}_p
\]

for \( j = 1, 2, 3 \).

Proof. By assumption \( z_p(A, B) = z_p \) and therefore for some \( j \neq k \in \{1, 2, 3\} \) and \( v \mid p \) we have:

\[
|L_j(A, B)|_v \leq p^{-2e_v} \\
|L_k(A, B)|_v \leq p^{e_v}
\]

with \( z_p = \max_{v \mid p} z_v \).

For each of the 3 possible choices of \( L_j \) as “minimal” linear form for \( (A, B) \), we may apply Theorem 4.1 with \( m = 2 \) and \( \mathcal{A}_e \) as indicated above. Then as required, \( \mathcal{A}_e \) is non-singular with

\[
|\det \mathcal{A}_e|_v = p^{5/6} |A|^{1/6}_p
\]

Hence

\[
\max_{v \mid p} |\det \mathcal{A}_e|_v = p^{5/6} |A|^{1/6}_p
\]

by assumption and for each case (3 in total since for given \( j \) the choice of \( k \) in the underlying system of inequalities is arbitrary) we obtain a discrete \( \mathbb{Z}_p \)-module \( A_j(p) \) satisfying:

\[
\left[ Z^2 : A_j(p) \right] \geq \left\{ |A|^{1/6} p^{5/6} \right\}_p,
\]

as shown in Theorem 4.1 in general.

4.2. \( A(p) \) and the \( p \)-adic Solutions of \( \{(1), (2), (3)\}_p \). Whereas the previous section dealt with pairs \( (A, B) \in \mathbb{Q}_p^2 \) for which \( |L_1|_v, |L_2|_v, |L_3|_v \leq 1 \) for \( v \mid p \), we now want to use the mixed inequality \( |L_1|_v, |L_2|_v, |L_3|_v \leq 1 \) for \( v \mid p \) to determine \( n \)-tuples \( (A, B) = (A_i, B_i)_{i=1, \ldots, n} \in \mathbb{Q}_p^2 \times \mathbb{Q}_p^2 \) that are solutions of \( \{(1), (2), (3)\} \).

To do this, we start by generalizing the mapping

\[
(A, B) \in \mathbb{Q}_p^2 \to z_p(A, B)
\]

introduced in Definition 4.3 to \( n \)-tuples \( (A, B) \in \mathbb{Q}_p^{2n} \) in the following way:

\[
z_p(A, B) := \max_{1 \leq i \leq n} z_p(A_i, B_i) \quad \text{if} \quad (A, B) = (A_i, B_i)_{i=1, \ldots, n}.
\]
Moreover, let $A(p) := A_0(p)^\ast$ and also $A'(p) := A_0'(p)^\ast$ for $j = 1, 2, 3$ denote the $n$-fold cartesian products of the $\mathbb{Z}_p$-modules in $\mathbb{Q}_p^2$ that appear in Theorem 4.1 and Corollary 4.4. Thus $A'(p)$ becomes a discrete $\mathbb{Z}_p$-module in $\mathbb{Q}_p^{2n}$.

**Corollary 4.5.** For given $z_\rho$ the $n$-tuples $(A, B)$ of pairs $(A_i, B_i), i = 1, \ldots, n \in \mathbb{Q}_p^2$ with $z_\rho(A, B) = z_\rho$ lie in the union of $3$ discrete $\mathbb{Z}_p$-modules $A'(p)$, $A'(p)^\ast$ and $A'(p)$ of $\mathbb{Q}_p^{2n}$, that satisfy $A'(p) = A_0'(p)^\ast$.

**Proof.** By assumption $z_\rho(A, B) = z_\rho$ and we pick one of those $1 \leq i \leq n$, for which $z_\rho(A_i, B_i) = z_\rho$. For this $i$ we have

$$|L_i(A, B)|_{v_\rho} = p^{-2\rho}$$
$$|L_i(A, B)|_{v_\rho} = p^{\rho}$$
$$|L_i(A, B)|_{v_\rho} = p^{\rho}$$

for some $v_\rho = v_\rho(p) \mid p$ and a suitable permutation $(j, k, l)$ of $(1, 2, 3)$.

An application of Corollary 4.4 implies that the $(A_i, B_i)$ in question lie in the union of three discrete $\mathbb{Z}_p$-modules $A_j'(p)$, $j = 1, 2, 3$ of $\mathbb{Q}_p^2$.

We claim: if $(A_i, B_i)$ lays in some $A_j'(p)$, then all remaining components $(A, B)$ of $(A, B)$ also lay in the same $A_j'(p)$. Let $(A_k, B_k) \neq (A_i, B_i)$ be given. Then:

$$|L_k^i|_{v_\rho} = |L_k^i(A, B)|_{v_\rho} \leq p^{\rho}$$

by definition of $z_\rho$ as maximal coefficient that appears.

But we also have $|L_k^i|_{v_\rho} \leq p^{-2\rho}$; since Proposition 2.2 said

$$|L_k^i|_{v_\rho} \leq 1.$$
thus corresponds to the estimate
\[
\left[ Z^2_p : A(p) \right] \geq \left\{ |\mathcal{A}|^{1/6} \right\}_p \geq |\mathcal{A}|^{1/6} p^{5/6}.
\]

Furthermore, points from \( S(X) \) in the archimedean part are already contained in the union of the \( P^n_m \) (resp. \( Q^n_m, R^n_m \)), those in \( A(p) \) in turn already lie in \( \bigcup_p A(p)^n \).

Before we go further to combine the acquired information for all \( p \in \mathbb{P} \) to conclude the non-archimedean part of the problem, we shall examine the index \( \left[ Z^2_p : A(p) \right] \) a little closer. Due to the presence of \( \{ \} \_p \), a phenomenon occurs that we did not encounter in the archimedean part; it is precisely this difference that will be crucial since it will make possible the summation over \( (\ell, \ell') \in \Pi_d \) and \( d \neq 0 \) squarefree later on.

4.3. The Role of \( \Pi_d \) for the Estimate of the Index of \( A_d(p) \). The estimate
\[
\left[ Z^2_p : A(p) \right] \geq \left\{ |\mathcal{A}|^{1/6} \right\}_p
\]
for \( j = 1, 2, 3 \) is obtained from the general result in Theorem 4.1 by plugging in the parameters in our particular situation. A closer analysis of the quantity \( \mathcal{A} = 2^{6d^2}d\ell^2(\ell')^2 \), combined with the fact \( A_d(p) \leq A_d(p) \), should allow a slight modification of this estimate.

For the convenience of the reader, let us recall the definition of \( \Pi_d \). By the construction of this system of representatives, all of its elements are of the form \( a \mathfrak{p}_j, \) where the only prime ideal that might appear as a cube in the decomposition of \( (\mathfrak{p}_j) = \mathfrak{p}_j^3 \mathfrak{a}_j^3 \), combined with the fact \( A_d(p) \leq A_d(p) \), should allow a slight modification of this estimate.

For any given leading coefficient pair \( (\ell, \ell') \) we have by construction of \( \Pi_d \) for \( d = 1 \):
\[
\ell = \mathfrak{p}_1^i a \quad \text{and} \quad \ell' = \mathfrak{p}_1^i b
\]
and for \( d \neq 1 \):
\[
\ell = \mathfrak{p}_1^i a \quad \text{and} \quad \ell' = \mathfrak{p}_1^i a'
\]
for some \( 1 \leq i \leq h. \) This determines uniquely the rational prime that lies below the prime ideals \( \mathfrak{p}_j \) and \( \mathfrak{p}_j' \) of the ideal classes containing the cubic parts of \( \ell \) and \( \ell' \). We may thus give the

**Definition 4.6.** Let \( p_1, \ldots, p_h, h' \leq h \) be the primes in \( \mathbb{Q} \) that lie below the \( h \) prime ideals \( \mathfrak{p}_1, \ldots, \mathfrak{p}_h \) that were chosen as representatives of the \( h \) ideal classes of \( \mathbb{Q}((\sqrt{d}) \) for the construction of \( \Pi_d \).
By assumption \( p_1, \ldots, p_k \) are relatively prime to 2, 3 and \( d \) and for given \((\lambda, \lambda')\) we denote by \( p_0 \in \{ p_1, \ldots, p_k \} \) the prime lying below the representative of the ideal class \( \mathcal{A}_0 \) containing the cubic part of \( \lambda \) (and also \( \lambda' \) since \( p_0, \varphi' \) lie above the same prime \( p \)).

Set \( P_1 := \{2, 3, p_0\} \).

**Proposition 4.7.** In the case \( p \nmid A \), \( p \notin P_1 \) the estimate for the index of \( A_2(p) \) in \( \mathbb{Z}_p^2 \) from Corollary 4.4 can be replaced by

\[
[\mathbb{Z}_p^2 : A_2(p)] \geq |A_1^{1/6} p^{\max(1/6, z_p)}|
\]

**Proof.** Since trivially \( \{ |A_1|^{1/6} p^{s}\} \geq |A_1|^{1/6} p^{s} \) by the definition of \( \{ \} \), the statement of the proposition is surely true for \( z_p \geq 1/6 \).

Now assume \( z_p < 1/6 \) as well as \( p \nmid \mathcal{A} \) and \( p \notin P_1 \).

If \( p' \mid A \) (i.e. \( p' \) is the greatest power of \( p \) dividing \( A \)) with \( s \neq 0(6) \), then \( |A_1|^{1/6} \notin \{ p' : v \in \mathbb{Z} \} \) and the presence of \( \{ \} \) makes us gain at least \( p^{1/6} \), which leads to

\[
\{ |A_1|^{1/6} p^{s}\} \geq |A_1|^{1/6} p^{1/6}.
\]

We are thus left with the case \( p' \mid A \) for some \( s \equiv 0(6) \). We claim \( s = 6 \). Obviously \( s > 0 \) since \( p \nmid A \). If we had \( p^{12} \mid A \), then \( A = 2^{6} 3^{6} (\lambda \lambda')^{2} \) would imply in the case \( p \mid \mathcal{A} \) the existence of some \( p' \mid \mathcal{A} \) (\( \lambda \lambda' \) and \( \lambda' \) squarefree) Altogether this would yield the existence of \( \pi \mid (p) \) with \( \pi^3 \mid (\lambda') \), a contradiction to \( p \notin P_1 \).

We are thus left with the case \( s = 6 \), that is, \( p^{6} \mid A \).

In this situation we will show that \( (A, B) \in \mathbb{Z}_p^2 \). Thus \( A_2(p) \in \mathbb{Z}_p^2 \) and

\[
[\mathbb{Z}_p^2 : A(p)] \geq 1 = |A_1|^{1/6} p > |A_1|^{1/6} p^{1/6},
\]

since \( z_p < 1/6 \), which will prove the assertion.

We have \( |\mathcal{A}| \leq 1 \), and since the dimension \( m = 2 \), this gives

\[
|x|_p \leq |\mathcal{A}|_p \leq |\det \mathcal{A}|_p^{-1}.
\]

But we also have

\[
|\det \mathcal{A}|_p = p^{12} |\det L_{1,2}|_p = p^{12} |A_1|^{1/6} = p^{12} > 0
\]

and

\[
|\mathcal{A}|_p = p^{12} |L_{1,2}|_p.
\]

Now \( p^6 \mid A \) yields \( p^6 \mid (\lambda \lambda')^2 \), hence \( p^3 \mid \lambda \lambda' \). When \( d = 1 \), we have (after possible relabeling of \( \lambda, \lambda' \)) that \( p^3 \not\mid \lambda' \) (since \( \lambda, \lambda' \) are cubefree). When \( d \neq 1 \), then \( p \) cannot ramify in \( \mathcal{Q}(\sqrt{d}) \), since \( p \nmid d, p \neq 2 \). If \( p \) were inert, \( (p) = \pi \), the same power of \( p \) would divide \( \lambda, \lambda' \), contradicting \( p^3 \not\mid \lambda \lambda' \).
Hence \( p \) splits, \((p) = \pi \pi'\), and (after possible relabeling of \( \lambda, \lambda' \), \( \pi \pi' | (\lambda), \pi \pi' | (\lambda') \)). In each case, every valuation \( v | p \) has

\[
|\lambda|_v \leq p^{-1} \quad \text{and} \quad |\lambda'|_v \leq p^{-1}.
\]

The entries of \( L_{1,2} \) are linear combinations of \( \lambda^{1/3}, \lambda'^{1/3} \) with integral coefficients, and hence \( |L_{1,2}|_v \leq p^{-1/3} \). In combination with the estimates above this yields \( |A'|_v \leq p^{3 \lambda - 1/3} \), hence \( |x|_v \leq p^{ \lambda + 2/3} < p \) since \( z_p < 1/3 \), and since \( |x|_v \) is an integral power of \( p \), finally \( |x|_v \leq 1 \).

Let \( Q \) be the set of primes \( p \) having \( p | A \) or \( p \in P_1 \). The primes \( p \notin Q \) then satisfy \( p | A \) and \( p \notin P_1 \).

**Results for all Primes \( p \in \mathbb{P} \)**

4.4. The Lattice \( A_0 \) as Intersection of the \( A_0(p) \). In this section the results concerning the solutions of \( |L'_1|_v |L'_2|_v |L'_3|_v \leq 1 \) for a fixed prime \( p \) shall be combined for all \( p \in \mathbb{P} \).

Let \( I_m \) denote the \( m \)-dimensional unit-matrix and for any \( m \times m \) matrix \( A \) with entries from an algebraic number field \( K \) we say \( A \equiv I_m \mod v \) if the equivalence

\[
|A|x_v \leq 1 \iff |I_m x_v|_v \leq |x_v|_v \leq 1, \quad 1 \leq i \leq n
\]

holds for all \( x \in K^m \).

**Theorem 4.8.** Let \( K \) be an algebraic number field and suppose that for every \( v \in M(K) \) we are given a non-singular \( m \times m \) Matrix \( A \) with entries from \( K \), such that \( A \equiv I_m \mod v \) for almost all \( v \in M(K) \). For \( p \in \mathbb{P} \) let \( A_0(p) \) be the discrete \( \mathbb{Z}_p \)-module of \( \mathbb{Q}_p^m \) of Theorem 4.1 consisting of \( y = (y_1, ..., y_m) \in \mathbb{Q}_p^m \) that satisfy \( |A|y_v \leq 1 \) for all \( v | p \).

Then the \( x = (x_1, ..., x_m) \in \mathbb{Q}^m \) satisfying \( |A|x_v \leq 1 \) for every \( v \in M(K) \) lie in the lattice \( A_0 \) in \( \mathbb{R}^m \) that is the intersection of the rational points of the modules \( A_0(p) \):

\[
A_0 = \bigcap_{p \in \mathbb{P}} (\mathbb{Q}^m \cap A_0(p)).
\]

Moreover we have

\[
\det A_0 = \prod_{p \in \mathbb{P}} \left[ \mathbb{Z}_p^m : A_0(p) \right] \geq \prod_{p \in \mathbb{P}} \left\{ \max_{v | p} |\det A|_v \right\}_p.
\]
Proof. For fixed \( p \) the matrices \( \mathcal{A}_v \) with \( v \mid p \) fall under the conditions of Theorem 4.1. It is shown there that the \( y \in \mathbb{Q}^m_p \) satisfying \( |\mathcal{A}_v y|_v \leq 1 \) for \( v \mid p \) lie in a discrete \( \mathbb{Z}_p \)-module \( A_d(p) \) of \( \mathbb{Q}^m_p \), for whose index we have:

\[
[\mathbb{Z}_p^m : A_d(p)] \geq \max_{v \mid p} |\det \mathcal{A}_v|_v.
\]

The rational solutions \( x \) of \( |A_v x|_v \leq 1 \) for \( v \mid p \) lie in \( \mathbb{Q}^m_{\mathbb{Z}_p} \) for given \( p \), consequently the rational solutions \( x \) of \( |A_v x|_v \leq 1 \) for \( v \in M_d(K) \) lie in \( \bigcap_{v \in \mathbb{P}} (\mathbb{Q}^m \cap A_d(p)) \).

Conversely, if \( x \in \mathbb{Q}^m \) lies in this intersection, we get \( |A_v x|_v \leq 1 \) for \( v \in M_d(K) \) by definition of \( A_d(p) \), and the first statement of the theorem is proved.

We claim: \( 4_0 : = \mathbb{Z}_p : (\mathbb{Q}^m \cap A_d(p)) \) is a lattice in \( \mathbb{Q}^m_{\mathbb{Z}_p} \). Obviously \( 4_0 \) is a subgroup of \( \mathbb{Q}^m \), since it is the intersection of such and it only remains to show that \( 4_0 \) is discrete in \( \mathbb{Q}^m \). By Theorem 4.1 every \( x \in A_0 \subset A_d(p) \) satisfies

\[
|x|_v \leq |\mathcal{A}_v^{-1}|_v
\]

for \( v \mid p \), so for every \( p \) there exists some \( s(p) \in \mathbb{Z} \) with \( |x|_p \leq p^{s(p)} \) and consequently \( |x_i|_p \leq p^{s(p)} \) for all components \( x_i \) of \( x \). Since \( \mathcal{A}_v = I_m \mod v \) for almost all \( v \), we may choose \( s(p) = 0 \) for almost all \( p \in \mathbb{P} \), and the product formula yields:

\[
|x_i| = \prod_{p \in \mathbb{P}} |x_i|_p^{-1} \geq \prod_{p \in \mathbb{P}} p^{-s(p)}.
\]

All components of \( x \in A_0 \) are thus bounded from below so that \( A_0 \) is indeed discrete, and therefore a lattice.

To prove the statement involving the determinant of \( A(p) \), it will suffice to show that

\[
[\mathbb{Z}_p^m : (\mathbb{Q}^m \cap A_d(p))] = [\mathbb{Z}_p^m : A_d(p)].
\]

For then this number is a power of \( p \), so that

\[
\det A_0 = \prod_p [\mathbb{Z}_p^m : (\mathbb{Q}^m \cap A_d(p))] = \prod_p [\mathbb{Z}_p^m : A_d(p)].
\]

In order to prove this next to last equality, it will suffice to show that \( A_d(p) \) has a basis in \( \mathbb{Q}^m \), so that \( A_d(p) \) and \( \mathbb{Q}^m \cap A_d(p) \) have the same basis \( a_1, \ldots, a_m \), and their "index" in \( \mathbb{Z}_p^m \) respectively in \( \mathbb{Z}^m \) equals

\[
|\det(a_1, \ldots, a_m)| = |\det(a_1, \ldots, a_m)|_p^{-1}.
\]
There is a power $p'$ with $p'Z^m_p \subset A_d(p)$. Given a basis $b_1, ..., b_m$ of $A_d(p)$, pick $a_1, ..., a_m$ in $Q^m$ with

$$a_i = b_i \quad \text{for } i = 1, ..., m.$$ 

The lattice $\mathcal{A}_d(p)$ in $Z^m_p$ with basis $a_1, ..., a_m$ clearly satisfies $\mathcal{A}_d(p) \subset A_d(p)$, and $A_d(p) \subset \mathcal{A}_d(p) + p^{j+1}Z^m_p$. Suppose $A_d(p) \subset \mathcal{A}_d(p) + p^jZ^m_p$ where $j \geq t+1$. Then

$$p^jZ^m_p = p^{j-t}p^iZ^m_p \subset p^{j-t}A_d(p) \subset \mathcal{A}_d(p) + p^{j-t+1}Z^m_p = \mathcal{A}_d(p) + p^{j+1}Z^m_p,$$

so that $A_d(p) \subset \mathcal{A}_d(p) + p^{j+1}Z^m_p$. Hence $A_d(p)$ lies in the intersection of $\mathcal{A}_d(p) + p^jZ^m_p$ ($j = t+1, t+2, ...$), which is $\mathcal{A}_d(p)$; and indeed $A_d(p) = \mathcal{A}_d(p)$ and everything is proved.

Following the strategy of the first part of this chapter, we shall now apply the results of Theorem 4.8 to our given problem.

To do so, we first generalize Definition 4.3 to all $p \in P$ by extending the correspondence  

$$(A, B) \in Q^2_p \to \nu_p(A, B)$$

for fixed $p$ to all $p \in P$ and get:

$$(A, B) \in Q^2 \to (\nu_1(A, B), ..., \nu_p(A, B), ...) := \nu(A, B),$$

where to every pair of rational numbers we associate a sequence $(\nu_p)_{p \in P}$ whose $p$th term is just the quantity $\nu_p$ from Definition 4.3. As the reader may easily check:

- $\nu(A, B) \in ((1/36) \mathbb{N}_0)^P$,
- $\nu(A, B)$ has only finitely many components different from 0.

We denote by $r(\nu) := r(\nu(A, B))$ the number of components $\nu_p(A, B)$ of $\nu(A, B)$ that are different from 0.

With these notations in place, we shall apply Theorem 4.8 with $m = 2$ and

$$A_c := \begin{pmatrix} p^{2-\nu} & 0 \\ 0 & p^{\nu} \end{pmatrix} L_{1,2}.$$
Corollary 4.9. For given \( z \) the pairs \( (A, B) \in \mathbb{Q}^2 \) of rational numbers satisfying \( z A, B = z = (z_p)_{p \in \mathbb{P}} \) lie in the union of \( 3^{(x)} \) lattices \( A^*_j \) in \( \mathbb{R}^2 \) for which we have (for \( 1 \leq j \leq 3^{(x)} \)):

\[
\det A^*_j \geq \prod_{p \in \mathbb{P}} \{ |A|_{p}^{1/6} p^{5/6} \}_{p}.
\]

Proof. By assumption \( z A, B = z = (z_p)_{p \in \mathbb{P}} \) and \( z_p(A, B) = 0 \) for almost all \( p \in \mathbb{P} \). Thus for almost all \( p \in \mathbb{P} \):

\[
|L_j(A, B)|_1 \leq 1 \quad \text{for } v \mid p \quad \text{and } j = 1, 2, 3
\]

and any choice of two of the three linear forms leads to the same restrictions on \( (A, B) \). For the remaining \( r(z) \) values of \( p \) the definition of \( z_p \) yields, for some \( j \neq k \in \{1, 2, 3\} \) and \( v \mid p \):

\[
|L_j(A, B)|_1 \leq p^{-2e},
\]

\[
|L_k(A, B)|_1 \leq p^{5}
\]

with \( z_p = \max_{1 \leq j \leq 3} |z_j|_1 \neq 0 \).

For fixed \( p \) there are again 3 possible choices for \( L_j \) as minimal linear form for \( (A, B) \) and consequently, for the \( r(z) \) primes where such a selection is relevant, we obtain \( 3^{(x)} \) cases to which Theorem 4.8 may be applied with the already mentioned parameters, since for \( v \in M_0(K) \) the matrix \( \alpha_{v} \) is non-singular and \( z_p = 0 \) for almost all \( p \) guarantees that \( \alpha_{v} \equiv I_m \mod v \) for almost all \( v \). (at least those \( v \mid p \) for which \( |L_{1, 2}|_1 \leq 1 \) and \( \det L_{1, 2} \leq 1 \) in addition to \( z_p = 0 \).)

We get \( \max_{v \mid p} |\det \alpha_{v}|_1 = p^5 |A|_{p}^{1/6} \) for \( p \in \mathbb{P} \), where this last expression is 1 if \( \alpha_{v} \equiv I_m \mod v \) for all \( v \mid p \) for fixed \( p \). Each of the \( 3^{(x)} \) possible cases gives a lattice \( A^*_j \), \( (j = 1, ..., 3^{(x)} \) in \( \mathbb{R}^2 \) for which

\[
\det A^*_j \geq \prod_{p \in \mathbb{P}} \{ |A|_{p}^{1/6} p^{5/6} \}_{p}.
\]

4.5. \( A \) and Rational Solutions of \( \{1, (2), (3)\}_{p \in \mathbb{P}} \). Our next task is to extend the information contained in \( |L_1|_1, |L_2|_1, |L_3|_1 \leq 1 \) for \( v \mid p \) which lead to the discrete \( \mathbb{Z}_p \)-modules \( A(p) \) to the whole set of primes.

We therefore generalize the introduced correspondence

\( (A, B) \in \mathbb{Q}^2 \rightarrow z(A, B) \)

to \( n \)-tuples \( (A, B) \in \mathbb{Q}^n \times \mathbb{Q}^n \) in the following way:

\[
z(A, B) := (z_1(A, B), ..., z_p(A, B), ...) = (z_p(A, B))_{p \in \mathbb{P}},
\]
in analogy to the extension of Definition 4.3 to \( n \)-tuples of \( p \)-adic numbers. This definition of \( r(x) \) is immediately applicable to \( r(z(A, B)) \) with \( r(z(A, B)) = r(z(A, B)) \) for \( 1 \leq i \leq n \).

We set \( A := A(p)^n \) and \( A_j := (A_j^*)^n \) for \( j = 1, \ldots, 3^{(e)} \) the \( n \)-dimensional cartesian products of the lattices from Corollary 4.9. This makes \( A_j \) the product lattice of one two-dimensional lattice \( A_j^* \) and we can show:

**Corollary 4.10.** For given \( z \) the \( n \)-tuples \((A_i, B_i)_{i=1, \ldots, n}\) in \( \mathbb{Q}^2 \) with \( z(A, B) = z \) lie in the union of \( 3^{(e)} \) lattices \( A_j \), \( 1 \leq j \leq 3^{(e)}, \) of \( \mathbb{R}^{2n} \), each of which satisfies \( A_j = (A_j^*)^n \) for one of the lattices \( A_j^* \) from Corollary 4.9.

**Proof.** Of course the pairs \((A, B) \in \mathbb{Q}^{2n} \subseteq \mathbb{Q}_p^{2n} \) fall under the hypotheses of Corollary 4.5 for fixed \( p \) with \( z_p(A, B) = z \). Thus for \( z_p \neq 0 \), \((A, B) \) lies in one of 3 discrete \( \mathbb{Z}_p \)-modules \( A^j(p), j = 1, 2, 3 \) of \( \mathbb{Q}_p^{2n} \), and for \( z_p = 0 \) the point \((A, B) \in \mathbb{Z}_p^{2n} \) is arbitrary.

Consequently \((A, B) \) lies in one of \( 3^{(e)} \) lattices \( V_j \) of \( \mathbb{Q}^{2n} \), that arise as the intersection of the rational points from \( A^j(p) \). But the \( A^j(p) \) are exactly the products of the discrete \( \mathbb{Z}_p \)-modules \( A^j(p) \) of \( \mathbb{Q}_p^{2n} \) and by Corollary 4.9 the pairs \((A, B) \) of rational numbers in these lattices lie in the union of \( 3^{(e)} \) lattices \( A^*_j \) of \( \mathbb{R}^{2n} \). These being just the components \((A_i, B_i) \) of \((A, B) \), we find that \( V_j \) is the product of the lattices \( A^*_j \) which was defined \( A_j \) and we are done.

At this level we may pursue the comparison with the archimedean part of the problem with the observation that in the correspondence between \( V(P_m) \) and the determinants of the obtained lattices \( A(p)^j \) the factor \( 2^{-\epsilon_p} |A|^{-1/6} \) is the analogue of \( \prod_{p \neq P} \{ |A_p|^{1/6} p^{\nu} \} \) resp. \( \prod_{p \neq P} |A_p|^{1/6} p^{\nu} \).

The role of \( 2^{-\epsilon_p} \) and \( p^{\nu} \) was already mentioned, both will disappear in the summation over the respective parameters and we are left with \( |A|^{-1/6} \) as counterpart to \( \prod_{p \neq P} |A_p|^{1/6} \) — the exact analogy of archimedean and non-archimedean valuations in accordance with the product formula.

### 4.6. The Non-archimedean Bound

Such a bound consists in the final estimate for the determinants of the involved lattices. Once again we focus on the two-dimensional lattices \( A^*_j \) since these, as the domains \( P_m \) (resp. \( Q_m, R_m \)), lie in \( \mathbb{R}^2 \) and represent the ingredients for the more complicated \( A_j \) in \( \mathbb{R}^{2n} \).

To achieve this step, it remains to take care of the special shape of the \((\lambda, \lambda') \in \Pi_d \) which was begun in Proposition 4.7 and combine this result with Corollary 4.10.

**Corollary 4.11.** For given \( z \) the \( n \)-tuples \((A_i, B_i)_{i=1, \ldots, n}\) in \( \mathbb{Q}^2 \) with \( z(A, B) = z \) lie in the union of \( 3^{(e)} \) lattices \( A_j \) of \( \mathbb{R}^{2n} \), each of which
being the cartesian product of one two-dimensional lattice \( A_j^* \) from Corollary 4.10. For the determinant of these two-dimensional lattices we have:

\[
\det A_j^* \geq \prod_{p \in \mathbb{Q}_1} \left\{ |A|^{1/6} p^{5/2} \right\}_p \prod_{p \notin \mathbb{Q}_1} |A|^{1/6} p^{\max(1/6, z_p)}.
\]

**Proof.** By Corollary 4.10 we have \( A_j = (A_j^*)^n \), \( 1 \leq j \leq 3^{(x)} \) for one of the lattices \( A_j^* \) from Corollary 4.9 whose determinant satisfied the estimate

\[
\det A_j^* \geq \prod_{p \in \mathbb{P}} \left\{ |A|^{1/6} p^{5/2} \right\}_p.
\]

Combining this fact with the result of Proposition 4.7, for the primes \( p | A \) and \( p \notin \mathbb{P}_1 \), that is \( p \in \mathbb{Q}_1 \), the factor \( \left\{ |A|^{1/6} p^{5/2} \right\}_p \) may be replaced by \( |A|^{1/6} p^{\max(1/6, z_p)} \) which leads to the desired estimate for \( \det A_j^* \).

5. THE SYNTHESIS OF BOTH PROBLEMS

5.1. A Result from the Geometry of Numbers. The last two chapters carried the archimedean resp. the non-archimedean part of the problem of analysing forms counted by \( \mathbb{Z}_2(n, X) \) as far as this was possible separately. Now we need a result to combine both of them, in the sense that it establishes a relation between points in the lattices \( A_j, \ 1 \leq j \leq 3^{(x)} \) and those in the domain \( S(X) \).

As it was mentioned several times, the best context for this purpose is the two-dimensional level, i.e. the convex, central symmetric sets \( P_m \) (resp. \( Q_m, R_m \)) with \( m \in \mathbb{N} \) as well as the lattices \( A_j^*, \ 1 \leq j \leq 3^{(x)} \) with \( z = (z_p)_{p \in \mathbb{P}} \in ((1/36)^N_0)^{\mathbb{P}} \). We will use

**Proposition 5.1.** Let \( A \) denote a lattice in \( \mathbb{R}^2 \) and \( K \) a convex set in \( \mathbb{R}^2 \) that is symmetric with respect to the origin and has the volume \( V(K) \).

Then the number of \( n \)-tuples \( (g_1, ..., g_n) \) with \( g_i \in A \cap K \) for \( i = 1, ..., n \) for which \( g_1, ..., g_n \) span \( \mathbb{R}^2 \) is \( \ll (V(K)/\det A)^n \) with the implied constant depending on \( n \) only.

**Proof.** We refer to a result of John asserting that convex, central symmetric sets are very well described by ellipsoids. In particular, if \( K \subset \mathbb{R}^2 \) is bounded, symmetric with respect to the origin and convex, then there exists an ellipse \( E \), also symmetric with respect to the origin, with \( E \subset K < \sqrt{2} E \). (see [G-L], p. 13, Theorem 8). Thus it suffices to prove the statement of the proposition for the ellipses in question. In this case a linear transformation reduces \( K \) to the unit ball \( S \subset \mathbb{R}^2 \). In fact, if \( A \) is the
linear transformation for which \( K = AS \) (\( A \) is non-singular of course) and \( A^d \) the lattice obtained by application of \( A^{-1} \), we find:

\[
\det A^d = |\det A^{-1}| \det A = |\det A|^{-1} \det A,
\]

and this yields:

\[
\frac{V(K)}{\det A} = \frac{V(AS)}{\det A} = \frac{|\det A| V(S)}{|\det A| \det A^d} = \frac{V(S)}{\det A^d},
\]

which makes the statement invariant under invertible linear transformations.

So assume now \( K = S \), the two-dimensional unit ball. In this situation the estimate follows from a corollary of Davenport’s Theorem given by W. Schmidt in [Sch], p. 8, Lemma 3. He shows that under the same assumptions as here and \( N \) denoting the number of \( n \)-tuples \((g_1, \ldots, g_n)\) to estimate, one even has:

\[
N = \left( \frac{V(K)}{\det A} \right)^n + O(\lambda_1^{-1} |\det A|^{-1-n}),
\]

where \( \lambda_1 \) denotes the first minimum of \( A \). This immediately proves the weaker statement needed in this context since the second minimum \( \lambda_2 \ll V(K) \) to assure that not all \( g_i \) are collinear.

Let us try now to apply Proposition 5.1 to the present situation. For the parameters \( m = z_w \in \mathbb{N} \) and \( z = (z)_{p \in P} \in ((1/36) \mathbb{N})^P \) we define, for the 3 possible covering sets \( P, Q \) and \( R \) and the \( 3^{(4)} \) lattices \( A_j^* \):

- let \( A(z) \) denote one of the lattices \( A_j^* \), \((1 \leq j \leq 3^{(4)}) \) containing the points \((A, B)\) for which \( z(A, B) = z \).
- let \( P(z_w) \) denote one of the covering sets of \( S_0(X) \) for which \((A, B)\) lies in \( P_{z_w} \) (resp. \( Q_{z_w}, R_{z_w} \)).

**Corollary 5.2.** The number of \( n \)-tuples \((A, B)\) of pairs \((A_i, B_i)\) of pairs \((A_1, B_1), \ldots, (A_n, B_n)\) span \( \mathbb{R}^2 \) and which lie in the intersection of \( P(z_w) \) with \( A(z) \) is

\[
\ll \left( \prod_{\rho \in P_1} p_{\rho}^{2 \lambda_1^{-1}} \prod_{\rho \in Q_1, Q_1} p_{\rho}^{2 \lambda_1^{-1}} \prod_{\rho \in Q_1, Q_1} p_{\rho}^{\max(1/6, \lambda_1)} \right)^n.
\]

**Proof.** The \( n \)-tuples \((A, B)\) of pairs \((A_i, B_i)\) in \( A(z) \) satisfy \( z(A, B) = z \) and Corollary 4.11 yields:

\[
\det A(z) \geq \left( \prod_{\rho \in Q_1} \frac{|A|^{1/6} p_{\rho}^{\lambda_1}}{p_{\rho}^{\max(1/6, \lambda_1)}} \right) \left( \prod_{\rho \in Q_1} \frac{|A|^{1/6} p_{\rho}^{\lambda_1}}{p_{\rho}^{\max(1/6, \lambda_1)}} \right).
\]
\( P(z_{\infty}) \) is convex and symmetric with respect to the origin in \( \mathbb{R}^2 \) with

\[
V(P(z_{\infty})) \ll 2^{-z_{\infty}} |A|_{z_{\infty}}^{-1/6} X^{2/3}
\]

and thus, together with the lattice \( A(z) \), falls under the hypotheses of Proposition 5.1.

Note that this result restricts to \( n \)-tuples \((A, B)\) whose components span \( \mathbb{R}^2 \) as demanded in the formulation of this corollary. With

\[
(V(K))/|\text{det } A|^n = X^{2n/3} \left( 2^{-z_{\infty}} \prod_{p \in Q_1} |A|_p^{1/6} p^{v_p} \prod_{p \notin Q_1} |A|_p^{1/6} p^{\max(1/6, z_p)} \right)^{-n},
\]

an application of the product formula yields (note \( \prod_{p \in P, \cup \infty} |A|_p^{1/6} = 1 \) and \( |A|_p = 1 \) for \( p \in Q_1 \backslash P_1 \)):

\[
(V(K))/|\text{det } A|^n = X^{2n/3} \left( 2^{-z_{\infty}} \prod_{p \in P_1} p^{v_p} \prod_{p \in Q_1} p^{\max(1/6, z_p)} \right)^{-n},
\]

as desired.

With the help of the results of the previous chapters concerning the way \( S(X) \) is built up with \( P(z_{\infty}) \), \((z_{\infty} \in \mathbb{N}) \) and \( A_j \), with \( A_j \), \((j = 1, ..., 3^{n_{\infty}}, z \in \{1/36, n_{\infty}\}) \), Corollary 5.2 shall be used to get information about points \((A, B)\) in \( S(X) \) that lie in the union of the lattices \( A_j \) for some \( j \) and some \( z \).

5.2. The Sum over \( z_{\infty} \) and \((z_p)_{p \in P} \). Let us first consider all the possibilities for \( P(z_{\infty}) \) and \( A(z) \) for given \( z_{\infty} \) resp. \( z \). There are 3 (for \( P, Q, R \) resp, \( 3^{n_{\infty}} \) for \( A_j \)) options for every two-dimensional partial problem and these bounds immediately carry over to the \( n \)-dimensional problems because of Propositions 3.4, 3.5 (for \( P(z_{\infty}) \)) and Corollary 4.10 (for \( A(z) \)).

**Corollary 5.3.** The number of \( n \)-tuples \((A, B) = (A_i, B_i)_{i=1, ..., n} \) of pairs \((A_i, B_i) \in \mathbb{Q}^2 \), for which \((A_1, B_1), ..., (A_n, B_n) \) span \( \mathbb{R}^2 \) and which lie in the intersection of one of the three sets \( P(z_{\infty}) \) with one of the \( 3^{n_{\infty}} \) lattices \( A(z) \) is

\[
\ll X^{2/3} \left( 2 \prod_{p \in P_1} p^{v_p} \prod_{p \in Q_1} p^{\max(1/6, z_p)} \right)^{-1}.
\]

**Proof.** By Propositions 3.4, 3.5 there are exactly 3 options for the choice of the sets \( P(z_{\infty}) \) in which the components \((A_i, B_i)\) of \((A, B)\) can lie if \( z_{\infty} \) is given and the choice of one of these covering sets \( P(z_{\infty}) \) for any
component already implies that all other components lie in the same \( P(z_\infty) \).

By Corollary 4.10 there are exactly \( 3^r \) possible choices for the lattice \( A_j^* \) in which the components \((A_i, B_i)\) of \((A, B)\) can lie if \( z \) is given and the choice of one of these two-dimensional lattices for any component already implies that all other components lie in the same lattice. Thus there are again \( 3^r \) possible lattices \( A_j = (A_j^*)^* \) in \( \mathbb{R}^{2n} \) for \((A, B)\). The combination of these two observations with the result of Corollary 5.2 finally concludes the proof.

The main step to accomplish now consists in the summation over all possible \( z_\infty \) and \( z \) that may appear. As already mentioned, this means \( z_\infty \in \mathbb{N} \) and \( z = (z_p)_{p \in \mathbb{P}} \) with \( z_p = 0 \) for almost all \( p \). The summation over \( z_\infty \) is straightforward since \( \sum_{z_\infty \in \mathbb{N}} 2^{-z_\infty} \ll 1 \); for the one over \( z \) we need:

**Lemma 5.4.**

\[
\prod_{p \neq P_1} p^{n_{p}} \prod_{p \neq Q_1} \{ p^{n_{p}} \} \prod_{p \neq Q_1} p^{n_{max}(1/6, z_p)} = 2^{n_2} 3^{n_3} p_0^{n_{p_0}} \prod_{p \neq 2, 3, p_0} p^{n_{max}(1/6, z_p)}
\]

and the constants in the following estimates are absolute and hence independent of \( A \) and \( Q_1 \):

\[
1 + \sum_{s=1}^{\infty} 3 p^{-n/36} = 1 + \frac{3 p^{-n/36}}{1 - p^{-n/36}} \ll 1,
\]

\[
\prod_{p \neq P_1} \left( 1 + \sum_{s=1}^{\infty} 3 p^{s(1-1/36)} \right) = \prod_{p \neq P_1} \left( 1 + \frac{108 p^{-n}}{1 - p^{-n}} \right) \ll 1,
\]

\[
\prod_{p \neq Q_1} \left( \sum_{s=0}^{\infty} 3 p^{-n_{max}(1/6, s/36)} \right) = \prod_{p \neq Q_1} \left( 18 p^{-n} + \frac{3 p^{-n/6}}{1 - p^{-n/36}} \right) \ll \prod_{p \neq Q_1} c_0 p^{-n/6}
\]

for some \( c_0 \in \mathbb{N} \), \( c_0 > 18 + 3\left(1 - 2^{-1/18}\right) \).

**Proof.** By Definition 10 we have \( P_1 = \{2, 3, p_0\} \) and therefore

\[
\prod_{p \neq P_1} p^{n_p} = 2^{n_2} 3^{n_3} p_0^{n_{p_0}}.
\]
For all primes \( p \) that don’t divide \( \mathcal{A} \), only integer powers of \( p \) may appear and the definition of \( \{ \}_p \) yields

\[
\prod_{p \in \mathcal{Q} \setminus \mathcal{P}_1} \{ p^n \} = \prod_{p \in \mathcal{Q} \setminus \mathcal{P}_1} p^{-[\varepsilon_{1,p} - s_{1,p}]}.
\]

For all divisors of \( \mathcal{A} \) not contained in \( \mathcal{P}_1 \) we use directly the expression obtained in Proposition 4.7.

The estimates of the mentioned products are as follows:

\[
1 + \sum_{s=1}^{\infty} 3p^{-n_{36}} = 1 + 3 \sum_{s=1}^{\infty} p^{-n_{36}},
\]

and evaluation of the geometric series leads to \( 1 + (3p^{-n_{36}}/1 - p^{-n_{36}}) \) which is bounded independently of \( p \).

\[
\prod_{p \mid \mathcal{A}} \left( 1 + \sum_{s=1}^{\infty} 3p^{-x/s_{36}} \right) = \prod_{p \mid \mathcal{A}} \left( 1 + 36 \sum_{s \equiv n \mod 36} p^{-x/s_{36}} \right)
\]

\[
= \prod_{p \mid \mathcal{A}} \left( 1 + \frac{108p^{-n}}{1 - p^{-n}} \right).
\]

This expression may only increase if we omit the condition \( p \mid \mathcal{A} \). Writing \( o(n) \) for the number of distinct prime factors of \( n \) we find

\[
\prod_{p} \left( 1 + \frac{108p^{-n}}{1 - p^{-n}} \right) \leq \prod_{p} (1 + 2 \cdot 108p^{-n})
\]

\[
\ll \sum_{s \in \mathbb{N}} 216o(s)s^{-n}
\]

\[
\ll 1 \quad \text{for} \quad n \geq 2,
\]

if we use the well known estimate \( o(s) \ll \log s (\log \log s)^{-1} \) from analytic number theory to obtain \( 216o(s) \ll s^\varepsilon \) for \( \varepsilon > 0 \).

\[
\prod_{p \notin \mathcal{Q}_1} \left( \sum_{s=0}^{\infty} 3p^{-n \max(1/s, s/36)} \right) = \prod_{p \notin \mathcal{Q}_1} \left( \sum_{s=0}^{5} 3p^{-n/s} + \sum_{s=6}^{\infty} 3p^{-n/36} \right)
\]

\[
= \prod_{p \notin \mathcal{Q}_1} \left( 18p^{-n/8} + \sum_{s=6}^{\infty} 3p^{-n/36} \right)
\]

\[
= \prod_{p \notin \mathcal{Q}_1} \left( 18p^{-n/8} + \frac{3p^{-n/36}}{1 - p^{-n/36}} \right)
\]
is obtained by evaluating the geometric series. With
\[
\frac{3p^{-n/6}}{1 - p^{-n/36}} = 3p^{-n/6}(1 - p^{-n/36})^{-1} \leq 3p^{-n/36}(1 - 2^{-1/18})^{-1}
\]
this yields:
\[
\prod_{p \not\equiv Q_1} \left( \sum_{r=0}^{5} 3p^{-r/36} + \sum_{r=6}^{\infty} 3p^{-r/36} \right) \leq \prod_{p \not\equiv Q_1} c_0 p^{-n/6},
\]
as desired.

The above calculations will turn out to be useful in the next proposition to modify the bound from Corollary 5.3.

**Proposition 5.5.** The number of n-tuples \((A, B) = (A_i, B_i)_{i=1,..,n}\) of pairs \((A_i, B_i) \in \mathbb{Q}^2\) for which \((A_1, B_1), \ldots, (A_n, B_n)\) span \(\mathbb{R}^2\) and which lie in the union over \(z_\omega \in \mathbb{N}\) and \(z \in ((1/36) \mathbb{N})^p\) of the intersections of \(P(z_\omega)\) with one of the \(3^{(r)}\) lattices \(A(x)\) is
\[
\ll X^{2/3} \left( \prod_{p \not\equiv Q_1} \left( \prod_{p \not\equiv Q_1} p^{-n/6} \right) \right).
\]

**Proof.** The n-tuples \((A, B)\) in question are precisely those that are treated in Corollary 5.3 for a given \(z_\omega \in \mathbb{N}\) and \(z \in ((1/36) \mathbb{N})^p\). Thus we have to sum the number of the \((A, B)\) in this estimate over all \(z_\omega \in \mathbb{N}\) and \(z \in ((1/36) \mathbb{N})^p\). In
\[
\sum_{z_\omega \in \mathbb{N}} \sum_{z \in ((1/36) \mathbb{N})^p} 3^{(r)} 2^{-n z_\omega} \prod_{p \not\equiv P_{1}} p^{-n z_\omega} \prod_{p \not\equiv Q_1} \left\{ p^{-n z_{\omega p}} \right\} \prod_{p \not\equiv Q_1} p^{-n \max(1/6, z_{p})}
\]
we may take the sum over \(z_\omega\) and apply the first statement of the previous lemma to bound the above expression by
\[
\sum_{z \in ((1/36) \mathbb{N})^p} 3^{(r)} 2^{-n z_\omega} 3^{-n z_{p_0}} \prod_{p \not\equiv A} p^{-n z_{p_0}} \prod_{p \not\equiv Q_1} p^{-n \max(1/6, z_{p})}
\]
We shall use the identity
\[
\sum_{z \in ((1/36) \mathbb{N})^p} \prod_{p \not\equiv A} p^r(z_{p}) = \prod_{p \not\equiv A} \left( p^{r(0)} + \sum_{z_{p} \in ((1/36) \mathbb{N})^p} p^{r(z_{p})} \right)
\]
with \( v_p(z_p) \) being one of the above exponents. Considering the fact that 
\( z = (z_p)_{p \in \mathbb{P}} \) with \( z_p = 0 \) for almost all \( p \in \mathbb{P} \), the above sum can be estimated by:
\[
\left( 1 + \sum_{s=1}^{\infty} 3 \cdot 2^{-sz/36} \right) \left( 1 + \sum_{s=1}^{\infty} 3 \cdot 2^{-sz/36} \right) \left( 1 + \sum_{s=1}^{\infty} 3p^{-sz/36} \right) \times \prod_{p \nmid A} \left( 1 + \sum_{s=1}^{\infty} 3p^n \left( -s/36 \right) \right) \prod_{p \nmid Q_1} \left( \sum_{s=0}^{\infty} 3p^{-n \max(1/6, s/36)} \right).
\]

The factors in this product are precisely the ones from Lemma 5.4; except for the last one, they are all \(< <1\), so the number of \( n \)-tuples \((A, B)\) in consideration is \(< <X^{2n/3} \prod_{p \nmid Q_1} (c_0 p^{-n/6}), \) and the stated result follows easily.

5.3. The Estimate of \( \mathbb{Z}_2((\lambda, \lambda'), d, n, X) \). It remains to show that the \( n \)-tuples \((A, B)\) Proposition 5.5 deals with are already those counted in \( \mathbb{Z}_2((\lambda, \lambda'), d, n, X) \).

This requires two steps. On the one hand, the condition that \((A_i, B_i), \ i = 1, \ldots, n\) span \( \mathbb{R}^2 \) has to be interpreted differently and on the other hand, we have to pass from \( P(z_m), \ z_m \in \mathbb{N} \) and \( A(z), \ z \in ((1/36) \mathbb{N})^P \) to the domain \( S(X) \) and the lattices \( A_i \). Now Corollary 1.4 asserts that the cubic forms of rank 1 have their coefficient vectors \((a_1, \ldots, a_n)\) and \((a'_1, \ldots, a'_n)\) proportional, which means in terms of the rational variables \( A_i, B_i \) that \((A_i, B_i), i = 1, \ldots, n\) are collinear.

Thus the \( n \)-tuples \((A, B)\) treated in Proposition 5.5 are exactly those leading to forms of rank 2 as required for \( \mathbb{Z}_2((\lambda, \lambda'), d, n, X) \).

Concerning the sum over \( m = z_m \in \mathbb{N} \), by Propositions 3.4, 3.5,
\[
S(X) \subset \bigcup_{m=1}^{\infty} P^n_{z_m} \cup \bigcup_{m=1}^{\infty} Q^n_{z_m} \cup \bigcup_{m=1}^{\infty} R^n_{z_m}
\]
and the \((A, B)\) in \( S(X) \) satisfy the conditions of Proposition 5.5.

The same is true for the \( n \)-tuples \((A, B)\) with \( z(A, B) = z \) with respect to summation over \( z \in ((1/36) \mathbb{N})^P \) since each component \((A_i, B_i), i = 1, \ldots, n\) is contained in the union of the \( 3^{(n)} \) lattices \( A(z) \).

THEOREM 5.6. Let \((\lambda, \lambda') \in \Pi_d, \) and \( p_0 \) be the prime lying below the representative of the ideal class of the cubic part of \( \lambda \) as well as \( \lambda' \). Then we have for \( n \geq 2\):
\[
\mathbb{Z}_2((\lambda, \lambda'), d, n, X) \ll X^{2n/3} \left( c_{0, \Pi} \prod_{p \nmid Q_1} p^{-n/6} \right)
\]
where the constant in \( \ll \) depends on \( n \) only, in particular it is independent of \( (\lambda, \lambda') \) and \( d \).

**Proof.** Due to the previous observations, the result follows from Proposition 5.5.

5.4. A Splitting into Ideal Classes and the Proof of Theorem 1.9. We are now in a position to estimate

\[
Z_2(d, n, X) = \sum_{(\lambda, \lambda') \in \Pi_d} Z_2(\lambda, \lambda'), d, n, X,
\]
as was outlined in Chapter 1.

To do so we start by transforming the expression for \( Z_2(\lambda, \lambda'), d, n, X) \) so as to bring into evidence its dependence on \( (\lambda, \lambda') \) explicitly. The facts that \( d \) is squarefree, \( p_0 \) does not divide \( d \) and \( 2^{n/3} = 3 \) imply \( \omega(d) \leq \omega(d) + \omega(\lambda \lambda') + 2 \). Indicating the conditions \( p | \lambda \lambda', p | d \) and \( p \neq p_0 \) by \( p \in T(\lambda \lambda') \) gives:

\[
\prod_{p \in \mathcal{Q}_1} p^{-n/6} \ll d^{-n/6} \prod_{p \in T(\lambda \lambda')} p^{-n/6},
\]
and we obtain:

\[
Z_2(\lambda, \lambda'), d, n, X) \ll X^{2n/3} \sum_{p \in \mathcal{P}_0} d^{-n/6} \prod_{p \in T(\lambda \lambda')} p^{-n/6}.
\]

The next step consists in adapting the summation index \( (\lambda, \lambda') \in \Pi_d \) so as to be able to use the above estimates. We therefore split \( \Pi_d \) as the union of the sets \( \Pi_d^p, p \in \{ p_1, \ldots, p_h \} \) where \( \Pi_d^p \) contains the \( (\lambda, \lambda') \) for which \( p_i \) lies below the prime ideals \( \psi_i \) and \( \psi_i' \) of the cubic part of \( (\lambda) \) and \( (\lambda') \) to find:

\[
\sum_{(\lambda, \lambda') \in \Pi_d} Z_2(\lambda, \lambda'), d, n, X) = \sum_{i=1}^h \sum_{(\lambda, \lambda') \in \Pi_d^p} Z_2(\lambda, \lambda'), d, n, X).
\]

This splits \( Z_2(\lambda, \lambda'), d, n, X) \) into ideal classes corresponding to the cubic parts of \( (\lambda) \) and \( (\lambda') \) which is helpful since the factor \( \prod_{p \in T(\lambda \lambda')} p^{-n/6} \) depends on these cubic parts by the condition \( p \neq p_0 \).

Let us keep \( p_0 \in \{ p_1, \ldots, p_h \} \) fixed to deal with the expression

\[
\sum_{(\lambda, \lambda') \in \Pi_d^p} \epsilon_{0}(\lambda \lambda') \prod_{p \in T(\lambda \lambda')} p^{-n/6}.
\]

Note that the summand depends only on \( N := \mathcal{A}(\lambda) = \lambda \lambda' \), so we get:
Proposition 5.7. Let \((\lambda, \lambda') \in \Pi_d\) with \((\lambda) = \varphi_{\sigma}^3 a\) where \(\varphi_{\sigma} | p_0\) is some fixed prime ideal from \(\{q_1, \ldots, q_h\}\). Then we have with \(N := \mathcal{N}(\lambda) = \lambda'\): \(p_0^3 | N, \ p_0^8 | N\) for \(p \neq p_0\) and there are at most \(3^{\omega(N)}\) ideals of the form \((\lambda) = \varphi_{\sigma}^3 a\) with \(\mathcal{N}(\lambda) = N\). In particular, \(N\) contains no 8th power.

Proof. Let \((\lambda) = \varphi_{\sigma}^3 a = \varphi_{\sigma}^3 \prod \rho_i^e\) with \((\varphi, \rho, e) = 1\) be the prime decomposition of the principal ideal generated by \(\lambda\). Then \(3 \leq e_0 \leq 5\) and \(e_i \leq 2\) since \(a\) was supposed cubefree. For \(N\) this implies:

\[ p_0^3 | N, \ p_0^8 | N \quad \text{and} \quad p^5 | N \quad \text{for} \quad p \neq p_0 \]

as the reader may easily check. We subsume these conditions by a symbol \(\star\).

If \(N = \rho_0^3 \rho_1^3 \cdots \rho_r^3\) is given with the condition \(\star\), then the prime decomposition of \((\lambda)\) involves only prime ideals \(\rho_i\) that lie above the primes \(p_i, \ 1 \leq i \leq r\). This determines the exponent of \(\rho_i\) uniquely if \(p\) doesn’t split in \(\mathbb{Q}(\sqrt{d})\). If \(p\) splits into the product of two prime ideals \(p\) and \(p'\), \(\star\) only allows 3 possible choices for the exponents of \(p\) resp. \(p'\) in the decomposition of \((\lambda)\) and their sum is \(3 \leq e_0 \leq 7\) for \(p = p_0\) and \(e_i \leq 4\) for \(p = p_i \neq p_0\).

Denoting by \(\omega(N)\) once again the number of distinct prime factors of \(N\), there are at most \(3^{\omega(N)}\) different ideals \((\lambda) = \varphi_{\sigma}^3 a\) with given norm \(N\); this bound corresponds to the extremal case where all \(p | N\) split in \(\mathbb{Q}(\sqrt{d})\).

With \((\lambda, \lambda') \in \Pi_d^2\) we have \((\lambda) = \varphi_{\sigma}^3 a\) and the previous proposition implies:

\[ \sum_{(\lambda, \lambda') \in \Pi_d^2} \varphi_{\sigma}^3 a \prod_{p \in T(\lambda, \lambda')} p^{-e_0} \leq \sum_{p \in T(N)} 3^{\omega(N)} \varphi_{\sigma}^3 a \prod_{p \in T(N)} p^{-e_0}. \]

We have to examine the last expression in detail.

Proposition 5.8. Let \(M\) denote the squarefree part of \(N = \mathcal{N}(\lambda)\), \(\tau := (M, d)\) and \(L := M/\tau\). Then we have with \(c_1 := 24\sigma\):

\[ \sum \varphi_{\sigma}^3 a \prod_{p \in T(N)} p^{-e_0} \ll (c_1 + 1)^{\omega(d)} \left( \sum_{L=1}^{\infty} \varphi_{\sigma}^3 a \prod_{p \in T(L)} L^{-e_0} \right). \]

Proof. We first observe that the summand depends only on the squarefree part \(M\) of \(N\). Since \(N\) is free of 8th powers by Proposition 5.7 there are at most \(8^{\omega(M)}\) summands for given \(M\) and with \(\omega(N) = \omega(M)\) this yields:

\[ \sum \varphi_{\sigma}^3 a \prod_{p \in T(N)} p^{-e_0} \ll \sum_{M=1}^{\infty} 8^{\omega(M)} \varphi_{\sigma}^3 a \prod_{p \in T(M)} p^{-e_0}. \]
If we keep \((M, d) := \tau\) fixed, we have \(p_0 \mid \tau\) by assumption since \((p_0, d) = 1\) and we obtain:

\[
\text{for } p_0 \nmid M: \prod_{p \in \mathcal{P}(M)} p^{-\alpha_6} = (M/\tau)^{-\alpha_6} \\
\text{for } p_0 \mid M: \prod_{p \in \mathcal{P}(M)} p^{-\alpha_6} = (M/p_0\tau)^{-\alpha_6}.
\]

This implies further:

\[
\sum_{(M, d) = \tau}^{\infty} c_1^{\text{vol}(M)} \prod_{p \in \mathcal{P}(M)} p^{-\alpha_6} \\
\leq \sum_{(M, d) = \tau}^{\infty} c_1^{\text{vol}(M)}(M/\tau)^{-\alpha_6} \sum_{(M, d) = \tau}^{\infty} c_1^{\text{vol}(M)}(M/p_0\tau)^{-\alpha_6}.
\]

Substitution of \(M = p_0R\) in the latter sum yields an analogous expression to the first which leads to

\[
\sum_{(M, d) = \tau}^{\infty} c_1^{\text{vol}(M)}(M/\tau)^{-\alpha_6}.
\]

With \(M/\tau = L\) we get \(\omega(M) = \omega(L) + \omega(\tau)\), and summation over all possible \(\tau\), i.e. all divisors of \(d\), yields (if we drop the condition \(M\) sq-free):

\[
\sum_{\tau \mid d} \left( \sum_{(M, d) = \tau}^{\infty} c_1^{\text{vol}(M)}(M/\tau)^{-\alpha_6} \right) = \sum_{\tau \mid d} \left( \sum_{L = 1}^{\infty} c_1^{\text{vol}(L)}L^{-\alpha_6} \right).
\]

The number of \(\tau \mid d\) with \(\omega(\tau) = j\) is precisely \(\binom{\text{vol}(d)}{j}\), and thus we find

\[
\sum_{\tau \mid d} c_1^{\text{vol}(\tau)} = \sum_{j = 0}^{\text{vol}(d)} \left( \binom{\text{vol}(d)}{j} \right) c_1^j = (c_1 + 1)^{\text{vol}(d)}
\]

by the Binomial Theorem, which concludes the proof.

At this stage, we need the following restriction, already mentioned for forms of rank 1: the number \(n\) of variables must be chosen sufficiently large to ensure the convergence of \(\sum_{L = 1}^{\infty} c_1^{\text{vol}(L)}L^{-\alpha_6}\). This condition finally enables us to fill the last remaining gap of the proof of Theorem 1.9 already stated in Chapter 1. For the convenience of the reader we recall it here:
Theorem 5.9. Let \( n \geq 7 \) and \( h = h(d) \) the class number of the quadratic number field \( \mathbb{Q}(\sqrt{d}) \). Then there exists an absolute constant \( C > 0 \) with

\[
Z_\beta(d, n, X) \ll X^{2n/3} h(d) C^{o(d)} d^{-n/6}.
\]

The implied constant in \( \ll \) depends only on \( n \) and not on \( d \).

Proof. As already seen, we have

\[
Z_\beta(d, n, X) = \sum_{(\lambda, \lambda') \in \Pi_d} Z_\beta(\lambda, \lambda', d, n, X)
\]

\[
\ll X^{2n/3} \sum_{i=1}^{h'} \left( \sum_{(\lambda, \lambda') \in \Pi_d} c_0^{o(d)} \prod_{p \in T(\lambda, \lambda')} p^{-n/6} \right) c_0^{o(d)} d^{-n/6}
\]

\[
\ll X^{2n/3} \sum_{i=1}^{h'} (c_1 + 1)^{o(d)} \left( \sum_{L=1}^{\infty} c_1^{o(d)} L^{-n/6} \right) c_0^{o(d)} d^{-n/6}
\]

by Proposition 5.6 and Proposition 5.8. The estimate

\[
\omega(L) \ll \log L (\log \log L)^{-1} \Rightarrow c_1^{o(d)} \ll L^\varepsilon
\]

for \( \varepsilon > 0 \) then implies the convergence of \( \sum_{L=1}^{\infty} c_1^{o(d)} L^{-n/6} \) for \( n \geq 7 \).

Now the summand does not depend on the ideal class of \( \sqrt{d} \) anymore, and \( h' \ll h \) together with \( C := c_0(c_1 + 1) \) yield:

\[
Z_\beta(d, n, X) \ll X^{2n/3} h(d) C^{o(d)} d^{-n/6}.
\]

The summation over \( (\lambda, \lambda') \in \Pi_d \) was made possible since the constant in \( \ll \) was independent of \( \lambda \) and \( \lambda' \); all estimates being explicit in \( d \) we get a dependence of \( \ll \) on \( n \) only.

Acknowledgment

The author thanks Professor Wolfgang Schmidt for all his support and encouragement which have influenced this work in an extremely profitable way.

References


