ssdnm
środowiskowe
studia doktoranckie
z nauk matematycznych

Tomasz Lenarcik

Uniwersytet Jagielloński

An algorithm for computing the maximal order of a number filed

Praca semestralna nr 1

(semestr zimowy 2010/11)

Opiekun pracy: Zbigniew Jelonek

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

AN ALGORITHM FOR COMPUTING THE MAXIMAL ORDER OF A NUMBER FILED

TOMASZ LENARCIK

Abstract. We present an algorithm, to compute the ring of integers in a given number field. The original concept, which goes back to Zassenhaus, is slightly modified, so as to achieve the proof of Chistov's theorem. The sub-problem of finding a basis of a $\mathbb{Z}$-module, given in terms of some generating set, is addressed by means of the LLL algorithm. To deal with it systematically, we introduce the notion, and recall basic facts, from the theory of *lattices*.

Contents

1. Introduction

The main goal of this paper is to present a proof of the following Chistov's theorem (see [Ch]):

Theorem 1.1 (Chistov)**.** *Under deterministic polynomial time reductions, the problem of computing the normal closure of an order in a number field is equivalent to finding the largest square factor of a given positive integer.*

The result itself is rather pessimistic. Since no good solution is known for the problem of finding the largest square divisor of a large integer number, or equivalently, the largest square-free divisor, it seems that the maximal order of a number fields with large determinants, will remain beyond our reach (see [C]).

A good reason to compute the maximal order occurs, as soon as one wants to determine the ideal class group of a number field. The standard algorithms to do so, relies not only one the knowledge of the determinant of the field, but also involves the ring structure of the maximal order. A naive technique amounts to factorizing ideals, so as to find relations in the ideal class group (see for example [S]). However, factorizing ideals is already at least as hard, as factorizing integers, which seems to be the bottleneck of any interesting problem in computational algebraic number theory; but this is not particularly surprising, or is it?

Though, there do exists sub-exponential algorithms to compute the ideal class group of a general number field (see [C] again), they still relies on the a priori knowledge of the maximal order. It should be mentioned, at this point, that in case of quadratic fields, different techniques have been developed, usually based on Daniel Shanks' infrastructure method (see [C], [L1], [Sch], or [Sh1], [Sh2] for the original statement).

In this paper, we aim at presenting an algorithm which is a modified version of *Zassenhaus Round 2*. This modification is needed to achieve the result of Chistov. Generally speaking, this amounts to doing linear algebra over the ring $\mathbb{Z}/q\mathbb{Z}$, rather than $\mathbb{F}_p$, with q being a square-free number (see [B-L], [Ch] and [L3]). This reduces the need of factorizing some (potentially large) integer numbers, to finding their largest square(-free) divisors. Since no significantly better solution, other than explicit factorization, is known for the latter problem, this result is not very useful in practice, but theoretically, it is still very interesting.

Apart from a few facts from commutative algebra, the main difficulty we are going to conquer will be the need to do some linear algebra over the ring $\mathbb{Z}$. It turns out, that a straightforward approach to computing *the Hermite normal form* of a matrix, which is a standard tool for such problems, fails to produce a polynomial-time algorithm, as it is known to produce matrices with large coefficients (see [C]). Fortunately, there are some strategies to deal with this issue. One of these is an application of the LLL algorithm (see [LLL]).

We start by recalling some fundamental definitions concerning the number rings in general. Then, we introduce the notion of a lattice and a *reduced basis*, which enable us to formulate and prove the correctness of the LLL algorithm.

2. Orders in a number field

In this section we give a brief description of the theory of *orders*, which are a particular class of rings contained in a *number field*, i.e. a finite extension $K/\mathbb{Q}$ of the field of rational numbers. We define degree of K to be the degree of field extension $[K : \mathbb{Q}] = \dim_{\mathbb{Q}} K$. A number field of degree 2 is called a *quadratic field*.

2.1. Number rings and orders.

We now introduce the notion of the *number ring* and the *order*. We also provide some basic results concerning the structure of these rings.

Definition 2.1. We say that a ring A is a *number ring*, if it is contained in some number filed K. A number ring $A \subset K$ is said to be an order in K, if it is finitely generated as an abelian group and K is its field of fractions.

Example 2.2. Suppose, that K is a number field. Since any extension of $\mathbb{Q}$ is separable, there exists a primitive element $\theta \in K$, i.e. $K = \mathbb{Q}(\theta)$. Suppose further, that $f \in \mathbb{Z}[X]$ is an irreducible polynomial annihilating θ and let a_0 be the leading coefficient of f. Then $a_0^{n-1} f(X/a_0) \in \mathbb{Z}[X]$ is a monic polynomial with $a_0\theta$ as its root. This shows, that given

any number field, there exists a primitive element with minimal (monic!) polynomial whose coefficients are integer numbers.

Now let θ be a primitive element of K, with minimal polynomial $f \in \mathbb{Z}[X]$. Then $\mathbb{Z}[\theta]$ is an order in K. To see this, either consider the ring isomorphism:

$$\mathbb{Z}[\theta] \cong \mathbb{Z}[X]/(f),$$

or observe, that thanks to the relation $\theta^n = -a_1\theta^{n-1} - \ldots - a_n$ ([1]) one is capable of computing the higher powers of θ in terms of $1, \theta, \ldots, \theta^{n-1}$. This implies, that the $\mathbb{Z}$-module $\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \ldots \oplus \mathbb{Z}\theta^{n-1} \subset \mathbb{Z}[\theta]$ is in fact a ring. Actually, one has even "=", since $\mathbb{Z}[\theta]$ is defined to be the smallest ring containing θ. Moreover:

$$\mathbb{Z}[\theta] \otimes \mathbb{Q} = \mathbb{Q}[\theta] = K,$$

so K is the filed of fractions of $\mathbb{Z}[\theta]$.

Observation 2.3. *Any non-zero ideal I of an order $A \subset K$ is a free $\mathbb{Z}$-module of finite rank equal to $n = [K : \mathbb{Q}]$.*

Proof. For $I = A$, the assertion follows directly form Definition 2.1 and classification of finitely generated abelian groups. Namely, since A has no torsion elements, it is a free abelian group of finite rank. Moreover:

$$\operatorname{rank} A = \dim_{\mathbb{Q}} A \otimes \mathbb{Q} = \dim_{\mathbb{Q}} K = n.$$

For the general case take $0 \neq a \in I$. By virtue of the previous argument, I is a free $\mathbb{Z}$-module of finite rank. Furthermore $aA \subset I \subset A$ and $aA \cong A$ as $\mathbb{Z}$-modules, so one has the following inequalities:

$$n = \operatorname{rank} aA \leq \operatorname{rank} I \leq \operatorname{rank} A = n,$$

which prove our assertion. □

Corollary 2.4. *Any non-zero ideal I of an order $A \subset K$ has finite index in A, i.e. the rank $[A : I]$ of the abelian group A/I is finite. Any order is a Noetherian ring.*

Proof. Let us consider the exact sequence:

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0.$$

After multiplying by "$\otimes\mathbb{Q}$" and taking into account the equality:

$$\operatorname{rank} I = \operatorname{rank} A = [K : \mathbb{Q}],$$

one argues that $(A/I) \otimes \mathbb{Q} = 0$, i.e. A/I has only torsion elements. Since it is finitely generated abelian group, it has to be finite.

The Noetherian part is easy. Since every non-zero ideal I is finitely generated as $\mathbb{Z}$-module, then a fortiori it is finitely generated as A-module. □

Remark 2.5. Alternatively, one may use the first part of the thesis to prove, that every ideal $I \lhd A$ is finitely generated. ([2]) Namely, if $I \neq 0$, then it contains a non-zero element $x \in I$. Now, the ideal $\overline{I} = I/xA \lhd A/xA$ is a finite set $\overline{I} = \{\overline{x}_1, \ldots, \overline{x}_k\}$. It follows, that I is generated (over A) by $x, x_1, \ldots, x_k$.

Remark 2.6. Observe, that the argument used in the proof of Corollary 2.4 can be applied in the same form to an arbitrary pair $M' \subset M$ of free $\mathbb{Z}$-modules having the same finite rank. In particular, the index $[M : M']$ is finite (see also Proposition 2.13).

[1] Here, $a_1, \ldots, a_n$ denote the corresponding coefficients of f.

[2] We will use this argument in the proof of Proposition 2.7.

It may be surprising, that the same assertion as in the Corollary 2.4, actually holds true for an arbitrary number ring. Although, we could have settled for a single proof, we decided to present them separately, as they reveal a slightly different techniques.

Proposition 2.7. *Any non-zero ideal I of a number ring A has a finite index in A. As a consequence, any number ring is a Noetherian ring.*

Proof. First, take $x \in I \setminus 0$ and let $f(x) \in \mathbb{Z}[X]$ be its irreducible polynomial. Then observe, that $f(0) \in \mathbb{Z} \cap I$, so I contains a non-zero integer $k := f(0)$. To finish the proof, it is sufficient to verify, that A/kA is a finite group.

Let A'/kA be a finitely generated subgroup of A/kA. In such an instance, A' is a free abelian group of rank $r \leq n := [K : \mathbb{Q}]$. It follows, that:

$$\#A'/kA \leq \#A'/kA' = k^r \leq k^n. \ ([3])$$

Since A/kA equals the sum of its finitely generated subgroups, one concludes that $\#A/kA \leq k^n$. The Noetherian part now follows from Remark 2.5. □

Corollary 2.8. *Any number ring has Krull dimension ≤ 1. ([4])*

Proof. We need to verify, that any non-zero prime ideal of a number ring is already maximal. This follows from Proposition 2.7 and the fact, that a finite integral domain is necessarily a field. □

Remark 2.9. The reader may notice, that Proposition 2.7 is in fact a special case of the famous Krull-Akizuki Theorem, which we could not resist mentioning (see Theorem 2.10). It generalizes Proposition 2.7 by replacing $\mathbb{Z}$ with any *Dedekind ring* (see Definition 2.23). It seems interesting, that the idea standing behind the proofs of booth theorems is almost the same. The main difficulty, that occurs it the general case, is that one needs to deal with Artinian rings instead of finite ones. This is a typical scenario.

Theorem 2.10 (Krull-Akizuki)**.** *Let A be a one-dimensional, Noetherian domain, denote by k its field of fractions, and let K/k be a finite field extension. Then for any ring $A \subset B \subset K$ and a non-zero ideal $J \lhd B$ the ring B/J is an A-module of a finite length. In particular, B is a Noetherian ring of Krull dimension ≤ 1.*

Proof. See for example [E]. □

2.2. **The determinant.** A fundamental invariant associated with orders and their ideals is the ubiquitous *determinant*. We provide a definition in a slightly more general context.

Definition 2.11. Let $M \subset K$ be a free $\mathbb{Z}$-module of rank n equal to $[K : \mathbb{Q}]$. We define *determinant* of M to be the usual "quadratic form determinant" of the *trace form*:

$$M \times M \ni (x, y) \longmapsto \mathrm{Tr}(xy) \in \mathbb{Q}$$

It means, that given a $\mathbb{Z}$-basis $x_1, \ldots, x_n$ of M, the determinant $d(M)$ equals:

$$d(M) = \det \begin{bmatrix} \mathrm{Tr}(x_1x_1) & \cdots & \mathrm{Tr}(x_1x_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(x_nx_1) & \cdots & \mathrm{Tr}(x_nx_n) \end{bmatrix}. \tag{1}$$

[3]For the first inequality, observe that $kA' \subset kA$.

[4]Let us recall, that the Krull dimension of a ring A equals:

$$\dim A = \sup\{n \in \mathbb{Z}_{\geq 0} : \text{there exists a chain of prime ideals of length } n\}.$$

In general, this definition depends on the choice of basis. Namely, $d(M)$ is only determined up to multiplication by an element which is a square of a unit in the base ring. However, since $U(\mathbb{Z}) = \{\pm 1\}$, the number $d(M)$ is unique in case of $\mathbb{Z}$-modules.

Corollary 2.12. *If A is an order of K, then the determinant $d(A)$ is an integer number.*

Proof. To see this, write down the matrix M of the linear map $y \mapsto xy$ in terms of any basis of A. Then all the entries of M are integers. It follows, that the characteristic polynomial of x has integral coefficients. In particular $\mathrm{Tr}(x) \in \mathbb{Z}$. This proves, that all entries of the matrix in equation (1) are integer numbers, and so is its determinant. □

The following result express the relation between the determinants of two free $\mathbb{Z}$-modules $M' \subset M$ of the same rank, and the index $[M : M']$ (see also Remark 2.6).

Proposition 2.13. *For any free $\mathbb{Z}$-modules $M' \subset M$ with* $\operatorname{rank} M' = \operatorname{rank} M < \infty$*:*

$$d(M') = [M : M']^2 d(M),$$

where the determinants are evaluated with respect to any bilinear map $b : M \times M \longrightarrow B$ into a commutative ring B.

Sketch of the proof. One can verify, that there exists a basis $x_1, \ldots, x_n$ of M and numbers $k_1, \ldots, k_n \in \mathbb{Z}$, such that at the same time $k_1 x_1, \ldots, k_n x_n$ is a basis of M'. Now, the result follows from the formula (1), bilinearity of b and $\#M/M' = |k_1| \cdots |k_n|$. □

Corollary 2.14. *If $A \subset K$ is an order with square-free determinant, then A is maximal.*

Proof. Suppose. that $A \subset B \subset K$ and B is also an order. From Proposition 2.13 it follows, that $d(A) = [B : A]^2 d(B)$. Since booth $d(A)$ and $d(B)$ are integer numbers (by Corollary 2.12), and $d(A)$ is square-free, it follows that $[B : A] = 1$. □

Remark 2.15. Sometimes a different formula for determinant may be useful from the computational point of view. Let $\sigma_1, \ldots, \sigma_n$ denote all different ([5]) embeddings of K into $\overline{\mathbb{Q}}$, where $n = [K : \mathbb{Q}]$ as usual. Then for any $x \in K$:

$$\mathrm{Tr}(x) = \sigma_1(x) + \ldots + \sigma_n(x).$$

In particular:

$$\begin{bmatrix} \sigma_1(x_1) & \cdots & \sigma_n(x_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(x_n) & \cdots & \sigma_n(x_n) \end{bmatrix} \cdot \begin{bmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \cdots & \sigma_n(x_n) \end{bmatrix} = \begin{bmatrix} \mathrm{Tr}(x_1 x_1) & \cdots & \mathrm{Tr}(x_1 x_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(x_n x_1) & \cdots & \mathrm{Tr}(x_n x_n) \end{bmatrix},$$

and so, one has the following equality:

$$d(M) = \det \left(\begin{bmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \cdots & \sigma_n(x_n) \end{bmatrix} \right)^2. \tag{2}$$

Example 2.16. Let $\mathbb{Z}[\theta] \subset K$ be an order generated by an element θ, with minimal polynomial $f \in \mathbb{Z}[X]$ (see Example 2.2). In such an instance $d(\mathbb{Z}[\theta])$ equals the *discriminant* $d(f)$ of f, which is defined as:

$$d(f) = \prod_{i<j} (\theta_i - \theta_j)^2,$$

[5] Since $\operatorname{char} \mathbb{Q} = 0$, then a finite filed extension $K/\mathbb{Q}$ is always separable.

where $\theta_1, \ldots, \theta_n$ denotes all (different!) roots of f. On the other hand, from (2), one gets the following Vandermonde determinant:

$$d(\mathbb{Z}[\theta]) = \det\left(\begin{bmatrix} \sigma_1(1) & \sigma_1(\theta) & \cdots & \sigma_1(\theta)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(1) & \sigma_n(\theta) & \cdots & \sigma_n(\theta)^{n-1} \end{bmatrix}\right)^2 = \left(\prod_{i<j}(\sigma_i(\theta) - \sigma_j(\theta))\right)^2 = d(f).$$

In particular, the determinant of $\mathbb{Z}[\theta]$ is always non-zero.

In addition, one may verify that the discriminant $d(f)$ may be expressed in terms of *resultant* (see Observation 2.17) in the following manner:

$$d(f) = (-1)^{n(n-1)/2}\operatorname{res}(f', f). \tag{3}$$

This is a consequence of the following observation:

Observation 2.17. *Let $g, h \in \mathbb{Q}[X]$, and denote:*

$$g(X) = b\prod_{i=1}^{r}(X - \beta_i), \quad h(X) = c\prod_{j=1}^{s}(X - \gamma_j) \quad \textit{with} \quad \beta_i, \gamma_i \in \overline{\mathbb{Q}}.$$

If one defines $\underline{\operatorname{res}}(g, h) := b^s c^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\beta_i - \gamma_j)$, then the following identities hold true:

(R1) $\underline{\operatorname{res}}(g, h) = (-1)^{rs}\,\underline{\operatorname{res}}(h, g)$,
(R2) $\underline{\operatorname{res}}(g, h) = b^s h(\beta_1)\cdots h(\beta_r)$,
(R3) $\underline{\operatorname{res}}(g, h) = b^{s-s_1}\,\underline{\operatorname{res}}(g, h_1)$, *where* $s_1 = \deg h_1$ *and* $h \equiv h_1 \mod g$.

Remark 2.18. The properties (R1) and (R3) from Observation 2.17 can be easily turned into an Euclidean-like algorithm that computes booth the greatest common divisor, and the resultant "$\underline{\text{res}}$" of two given polynomials at the same time. Clearly, this computation can be performed within the field of definition of the given polynomials.

In particular, the identities (R1) and (R3) determine the resultant uniquely. It can be easily verified, that the resultant "res", satisfies booth (R1) and (R3), so in fact res = $\underline{\text{res}}$.

Corollary 2.19. *For any polynomial $f \in \mathbb{Q}[X]$ one has:*

$$a^n d(f) = (-1)^{n(n-1)/2}\operatorname{res}(f', f),$$

where a denotes the leading coefficient of f. In particular identity (3) holds true.

Proof. Let us denote $f = a(X - \alpha_1)\cdots(X - \alpha_n)$ where $\alpha_i \in \overline{\mathbb{Q}}$. Then clearly:

$$f'(X) = a\sum_{i=1}^{n}\prod_{j\neq i}(X - \alpha_j),$$

and by Observation 2.17(R2):

$$\operatorname{res}(f', f) = a^n\prod_{i=1}^{n} f'(\alpha_i) = a^n\prod_{i=1}^{n}\left(\prod_{j=1}^{i-1}(\alpha_i - \alpha_j)\cdot\prod_{j=i+1}^{n}(\alpha_i - \alpha_j)\right) =$$

$$(-1)^{n(n-1)/2}a^n\prod_{i=1}^{n}\left(\prod_{j=1}^{i-1}(\alpha_j - \alpha_i)\cdot\prod_{j=i+1}^{n}(\alpha_i - \alpha_j)\right) = (-1)^{n(n-1)/2}a^n\prod_{i<j}(\alpha_i - \alpha_j)^2.$$

□

2.3. **Integral closure.** From the point of view of this article, the most important object connected with a number field K is the *ring of integers*, i.e. the *integral closure* of $\mathbb{Z}$ in K. It is defined to be a subset of K consisting of all elements which are *integral* over $\mathbb{Z}$ (see Definition 2.20). At this point, it is not even clear, that this set forms a ring. We will prove, that in fact it is a maximal order of K. It will be denoted by $\mathcal{O}_K$.

Definition 2.20. Consider a ring extension $A \subset B$. An element $b \in B$ is said to be *integral* over A, if there exists a monic polynomial $f \in A[X]$ such that $f(b) = 0$. The ring A is *integrally closed* in B if it coincides with its integral closure in B. The extension $A \subset B$ is called *integral* if all elements of B are integral over A.

Proposition 2.21. *Suppose, that $A \subset B$ is an extension of rings and let $\theta \in B$. Then the following conditions are equivalent:*

(i) *θ is integral over A,*
(ii) *the ring $A[\theta] \subset B$ is a finitely generated A-module,*
(iii) *there exists a ring $A \subset C \subset B$, which is finitely generated A-module and $\theta \in C$,*
(iv) *there exists a finitely generated A-module M with $\theta M \subset M$ and $\mathrm{Ann}(M) = 0$.*

Proof. We only need to show, that (iv)$\Longrightarrow$(i). Let $x_1, \ldots, x_k$ be a set of the generators of M. According to the assumption, there exist $a_{ij} \in A$ for $i, j = 1, \ldots, k$ such that:

$$bx_i = \sum_{j=1}^{k} a_{ij}x_j \iff 0 = \sum_{j=1}^{k} (\delta_{ij}b - a_{ij})x_j,$$

where δ_{ij} denotes Kronecker delta. From Crammer theorem it follows, that:

$$d(b)M = 0 \quad \text{where} \quad d(b) := \det(\delta_{ij}b - a_{ij})_{ij}. \tag{4}$$

Since $d(b) \in \mathrm{Ann}(M) = 0$, one has in fact $d(b) = 0$. The determinant (4) is a monic polynomial in variable b with coefficients in A, so it gives rise to an integral relation. □

Corollary 2.22. *The integral closure of A in any ring B is still a ring. In particular $\mathcal{O}_K \subset K$ is a number ring. Since any order $A \subset K$ is a finitely generated $\mathbb{Z}$-module, then according to (iv) $A \subset \overline{\mathbb{Z}} = \mathcal{O}_K$. Moreover, using (ii) and (iii), one can easily show, that the notion of being an integral extension is transitive. It follows, that $\mathcal{O}_K$ is already closed in K.*

Definition 2.23. An integral domain A is said to be a *normal ring* if it is integrally closed in its field of fractions. An integral domain A, which is a Noetherian, normal ring of Krull dimension equal to 1, is called a *Dedekind ring*.

Example 2.24. Any factorial ring is a *normal ring*. If K is a number field, than $\mathcal{O}_K$ is a Dedekind ring. ([6]) More generally, if A is a Dedekind ring with field of fractions k, and K/k is a finite field extension, than the integral closure of A in K is again a Dedekind ring. It follows directly from Theorem 2.10. Observe, that the Noetherian part is the main difficulty.

The following result is of a great importance. It basically, says that the ring $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. In particular, it can be described by means of some finite data structure. This is the least we can expect from an object, that we want to be able to compute.

[6]The fact that the Krull dimension of $\mathcal{O}_K$ is equal to 1, follows from general properties of integral extensions. Namely, if $A \subset B$ is an integral extension, then $\dim A = \dim B$. Alternatively, one may observe, that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, and so $\mathcal{O}_K$ is definitely not a field.

It should be stressed, that the corresponding fact fails to hold true in the case of integral closure of arbitrary Dedekind ring ([7])

Theorem 2.25. *Let K be a number field. Then $\mathcal{O}_K$ is a maximal order in K.*

Proof. Let $K = \mathbb{Q}(\theta)$, where θ is integral over $\mathbb{Z}$. ([8]) Then, for any $x \in \mathcal{O}_K$ there exist $a_1, \ldots, a_n \in \mathbb{Q}$ with:

$$x = a_1\theta^{n-1} + \ldots + a_{n-1}\theta + a_0, \tag{5}$$

Let $\sigma_1, \ldots, \sigma_n$ denote all different embeddings of K into $\overline{\mathbb{Q}}$. Applying this to (5), we get the following system of linear equations for a_i:

$$\sigma_j(x) = a_1\sigma_j(\theta)^{n-1} + \ldots + a_{n-1}\sigma_j(\theta) + a_0\sigma_j(1). \tag{6}$$

Let us denote the determinant of this system by d. Then d^2 is the determinant of the order $\mathbb{Z}[\theta]$ (see Example 2.16). In particular $d \neq 0$ and $d^2 \in \mathbb{Z}$ (see also Corollary 2.12). By Cramer's rule $d^2 a_i \in \mathbb{Q}$ can be computed as a polynomial in elements $\sigma_j(x), \sigma_j(\theta)$ for $j = 1, \ldots, n$, which are all integral over $\mathbb{Z}$. As a consequence, $d^2 a_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. This shows, that the following inclusions hold true:

$$d^2\mathcal{O}_K \subset \mathbb{Z}[\theta] \subset \mathcal{O}_K. \tag{7}$$

Since $d^2\mathcal{O}_K \cong \mathcal{O}_K$ as $\mathbb{Z}$-modules, it follows, that $\mathcal{O}_K$ is a free of rank n, as asserted. □

Definition 2.26. The maximal order $\mathcal{O}_K \subset K$ is also called the *ring of integers* of K. The *determinant of a number field* K, denoted by d_K, is the determinant of its ring of integers, namely $d(\mathcal{O}_K) \in \mathbb{Z}$.

Corollary 2.27. *If $A \subset K$ is an order, then $d(A) \neq 0$.*

Proof. Since $d(A) = [\mathcal{O}_K : A]^2 d(\mathcal{O}_K)$ and any order is contained in $\mathcal{O}_K$, the result follows from the fact, that there exist orders with non-zero determinant (see Example 2.16). □

Example 2.28. Consider the quadratic field $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer. In such an instance:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[(1+\sqrt{d})/2], & \text{if } d \equiv 1 \mod 4, \\ \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \mod 4. \end{cases} \tag{8}$$

The inclusion "$\supset$" is clear, as the generating elements are roots of the polynomials:

$$X^2 - X - (d-1)/4, \quad X^2 - d,$$

respectively. To check the other inclusion, one needs to verify, that the corresponding orders are integrally closed, i.e. they equal $\mathcal{O}_K$. In the first case, this is easy. Since the determinant of $\mathbb{Z}[(1+\sqrt{d})/2]$ equals d (it is square-free), then by Corollary 2.14 this order is already maximal. Similarly, the determinant of $\mathbb{Z}[\sqrt{d}]$ equals $4d$. The same argument tells us, that the index $[\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]]$ is at most 2. In particular $2\mathcal{O}_K \subset \mathbb{Z}[\sqrt{d}]$, so one only needs to verify, whether elements of the form $(a + b\sqrt{d})/2$ are integral over $\mathbb{Z}$. If they were, then their norms would be integers, namely $(a^2 - b^2 d)/4 \in \mathbb{Z}$. This is clearly true for even a and b. However, as long as at least one of them is odd, then in the view of $d \equiv 2, 3 \mod 4$ the equation $a^2 - b^2 d = 4c$ admits no integer solution, which can be easily verified "by hand".

[7] Compare with Theorem 2.10, which gives a little less information in this particular case.

[8] Observe, that according to Abel's theorem a finite extension $K/\mathbb{Q}$ is necessarily primitive. The primitive element becomes integral after multiplying by some integer number.

Corollary 2.29. *Suppose, that $K = \mathbb{Q}(\sqrt{d})$ with d being a non-square integer (not necessarily square-free). One has the unique factorization $d = f^2 d_0$ with d_0 being square-free. Then the following holds true:*

$$d_K = \begin{cases} d_0, & \text{if } d_0 \equiv 1 \mod 4, \\ 4d_0, & \text{if } d_0 \equiv 2, 3 \mod 4. \end{cases} \tag{9}$$

In particular, one recognizes, that the problem of finding the determinant of a quadratic number field is at least as hard as finding the largest square divisor of a given integer number. Later, we will see, that these problems are actually equivalent.

2.4. **The Pohst-Zassenhaus Theorem.** Let $A \subset K$ be an order. Suppose, that we want to verify whether this order is already maximal. To do so, one can use the following exact sequence:

$$0 \longrightarrow A \longrightarrow \mathcal{O}_K \longrightarrow \mathcal{O}_K/A \longrightarrow 0$$

Namely, the following equivalence holds true:

$$A \otimes \mathbb{Z}_{(p)} = \mathcal{O}_K \otimes \mathbb{Z}_{(p)} \iff (\mathcal{O}_K/A) \otimes \mathbb{Z}_{(p)} = 0 \iff p \nmid [\mathcal{O}_K : A]. \tag{10}$$

This leads to the following definition:

Definition 2.30. Let p be a prime number. An order $A \subset K$ is said to be *p-maximal*, if any of the equivalent conditions (10) holds true.

Remark 2.31. The criterion given by (10) may seem very impractical at the first glance, since it is not clear how any of the objects involved in the equation can be computed without any previous knowledge about $\mathcal{O}_K$. However, we already know from Proposition 2.13, that $[\mathcal{O}_K : A]^2$ divides $d(A)$, and the latter can be easily evaluated as long as any base of A is given. Hence, at least one can see that, the "verification", whatever it could be, may be restricted to a finite number of primes, namely those, whose square divides $d(A)$. We know give a brief description of what this "verification" could mean.

Definition 2.32. For any ideal I of A, let us define its *multiplier ring* as follows:

$$R_I = I : I := \{x \in K : xI \subset I\}. \ ([9])$$

Remark 2.33. Since I is an A-module, one has clearly $A \subset R_I$. Moreover, from Proposition 2.21 it follows, that $R_I \subset \mathcal{O}_K$. So it seems, that for suitably chosen I, the multiplier ring R_I can be used to measure if the order A equals $\mathcal{O}_K$. If this fails to hold true, then at least R_I is a natural choice if one is looking for some extension of A. This is summarized in the following result.

Theorem 2.34 (Phost-Zassenhaus)**.** *Let A be an order in a number field K, and let $p \in \mathbb{Z}$ be a prime number. Let us define:*

$$\mathfrak{r} = \operatorname{rad}(pA) = \bigcap \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{p} \cap \mathbb{Z} = (p)\}.$$

Then either $A = A' := R_{\mathfrak{r}}(= \mathfrak{r} : \mathfrak{r})$, in which case A is p-maximal, or $A \subsetneq A'$ and one has $p \mid [A : A'] \mid p^k$ with $k \geq 1$.

Proof. First observe, that since $p \in \mathfrak{r}$, then by definition of $\mathfrak{r} : \mathfrak{r}$ one has $xp \in \mathfrak{r} \subset A$ for any $x \in A'$. Equivalently $pA' \subset A$ and it follows that A'/A is non-zero vector space over $\mathbb{F}_p$. In particular $[A' : A] = p^k$, where $k = \dim_{\mathbb{F}_p} A'/A$. ([10])

[9] It can be thought, as the largest number ring contained in K, for which I is an ideal.

[10] It is not very useful, but clearly $\dim_{\mathbb{F}_p} A'/A \leq \operatorname{rank} A' = [K : \mathbb{Q}]$.

Now suppose that $A = A'$, and define

$$A_p := \{x \in \mathcal{O}_K : \text{ there exists } i \geq 1, p^i x \in A\}. \tag{11}$$

It can be easily verified, that $A \subset A_p$ and A_p is a p-maximal order. We will now prove, that in fact $A = A_p$.

Since A_p is finitely generated, it follows by (11), that $p^r A_p \subset A$ for some $r \geq 1$. Furthermore, there exists some m with $\mathfrak{r}^m \subset pA$. In particular, $\mathfrak{r}^{mr} A_p \subset A$. To achieve a contradiction, suppose that $A_p \not\subset A$. Let $0 \leq n < mr$ be the largest integer with $\mathfrak{r}^n A_p \not\subset A$. Then, clearly $\mathfrak{r}^{n+1} A_p \subset A$. Take any $x \in \mathfrak{r}^n A_p \setminus A$. One has $x\mathfrak{r} \subset A$, and moreover $\mathfrak{r}^{n+m+1} A_p \subset \mathfrak{r}^m \subset pA$. It follows, that for any $y \in \mathfrak{r}$, $(xy)^{n+m+1} \in pA$, hence $xy \in \mathfrak{r}(= \operatorname{rad}(pA))$. As a consequence $xI_p \subset I_p$, so $x \in A'$. This contradicts, with the assumption $A = A'$. □

2.5. **Evaluating the multiplier ring.** As we could see from Theorem 2.34, being able to determine the multiplier ring of a certain ideal of A suffices to find an order $A \subset A'$ which is already p-maximal, for a given prime p. Applying the same procedure to all "suspected primes" (see Remark 2.31) one would eventually get the maximal order $\mathcal{O}_K$.

We will see in a moment, that computing $\mathfrak{r} = \operatorname{rad}(pA)$ and $A' := \mathfrak{r} : \mathfrak{r}$ is actually a matter of linear algebra over $\mathbb{F}_p$. In fact, the following proposition will show, how to find a set of generators for pA'.

Proposition 2.35. *Let A be an order in K. Take $0 \neq \mathfrak{a} \lhd A$ and a non-zero element $a \in \mathfrak{a} \cap \mathbb{Z}$. Then the following sequence is exact:*

$$0 \longrightarrow aR_\mathfrak{a}/aA \longrightarrow A/aA \longrightarrow \operatorname{End}(\mathfrak{a}/a\mathfrak{a}), \tag{12}$$

where the last arrow sends x to "multiplication by x" map.

Proof. To see this, take $ax \in aR_\mathfrak{a}$, and observe that for any $y \in \mathfrak{a}$ one have $xy \in \mathfrak{a}$, by definition of $R_\mathfrak{a}(= \mathfrak{a} : \mathfrak{a})$. This implies $a(xy) \in a\mathfrak{a}$.

Now let x be an element of A, for which $x\mathfrak{a} \subset a\mathfrak{a}$. Clearly $a^{-1}x \in R_\mathfrak{a}$, and in consequence $x = a(a^{-1}x) \in aR_\mathfrak{a}$. □

Remark 2.36. The Proposition 2.35 applied to the element-ideal pair $p \in \mathfrak{r} := \operatorname{rad}(pA)$ shows that $pR_\mathfrak{r}/pA$ can be computed as the kernel of an $\mathbb{F}_p$ linear map:

$$\mathbb{F}_p^n \cong A/pA \ni x \mapsto (y \mapsto xy) \in \operatorname{End}(\mathfrak{r}/p\mathfrak{r}) \cong \operatorname{Mat}(n \times n; \mathbb{F}_p^n) \cong \mathbb{F}_p^{n^2}.$$

This can be clearly determined by means of the Gauss elimination performed over the field $\mathbb{F}_p^{n^2}$. However, what we actually get is a set of elements $\overline{y}_1, \ldots, \overline{y}_k$ in the quotient ring A/pA. It follows that the ideal $pR_\mathfrak{r}$, that we are looking for is generated by $y_1, \ldots, y_k$ and $px_1, \ldots, px_n$ where $x_1, \ldots, x_n$ is any basis of A.

As we already know from Observation 2.3, the ideal $pR_\mathfrak{r}$ is a free $\mathbb{Z}$-module of rank n, so what one want to do next is finding a basis of this ideal in terms of the generating set. It does not seem difficult at the first glance, since this is again a matter of linear algebra, but this time over the ring $\mathbb{Z}$. Namely, one starts by identifying $A \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules. Then considering a $\mathbb{Z}$-linear mapping:

$$\mathbb{Z}^{k+n} \ni (a_i) \mapsto a_1 y_1 + \ldots + a_k y_k + a_{k+1} p x_1 + \ldots + a_{k+n} p x_n \in \mathbb{Z}^n$$

and its associated matrix M, one may want to compute the *Hermite normal form* of M. ([11]) However, it turns out, that a straightforward implementation of this algorithm is known to produce large coefficients even the initial matrix is not of a great size (see [C]).

[11] This amounts to adopting the Gaussian elimination strategy to the case of a principal ideal domain.

A possible solution is to use an algorithm, that not only performs some operations on a given matrix, but also controls the magnitude of its entries. This amounts to acquiring some additional structure on $\mathbb{Z}^n$, that enables one to measure the length of a vector. More or less, it leads us to the notion of a *lattice* (see ...).

It remains to find a way of computing the ideal $\mathfrak{r} \subset A$. The key observation here is, that $\mathfrak{r}/pA$ coincides with the set of nilpotents of the ring A/pA. Moreover, the ring A/pA is a subalgebra of the ring of matrices $\mathrm{Mat}(n \times n; \mathbb{F}_p)$ with $n = \operatorname{rank} A$. It follows, that any nilpotent $x \in A/pA$ satisfies $x^k = 0$ for $k \geq n$. ([12]) This leads to the following observation:

Observation 2.37. *Let A be an order in K, and let p be a prime number. Define $\mathfrak{r}$ to be the intersection of all primes of A lying over pA. If $t \geq 1$ is such that $p^t \geq n = [K : \mathbb{Q}]$, then the following sequence is exact:*

$$0 \longrightarrow \mathfrak{r}/pA \longrightarrow A/pA \longrightarrow A/pA$$

with the last arrow given as $x \mapsto x^{p^t}$.

This already shows, that $\mathfrak{r}$ is pretty easy to compute, at least if one knows the prime p, for which the computation need to be performed. Practically, this prime may not be given explicitly, in which case, a less restrictive formula for $\mathfrak{r}$ may be useful. In fact, we will need the following result in the proof of Chistov's theorem.

Proposition 2.38. *Let A be an order in K, $n = [K : \mathbb{Q}]$ and let q be a square-free integer, which is not dividable by any prime number $p \leq n$. Define $\mathfrak{r}$ to be the intersection of all primes of A dividing qA. ([13]) Then, the following sequence is exact:*

$$0 \longrightarrow \mathfrak{r}/qA \longrightarrow A/qA \longrightarrow \mathrm{Hom}(A/qA, \mathbb{Z}/q\mathbb{Z})$$

where the last arrow is defined as follows:

$$x \longmapsto (A/qA \ni y \mapsto \mathrm{Tr}(xy) \in \mathbb{Z}/q\mathbb{Z}).$$

Remark 2.39. Note, that the assumption $q > n$ is necessary. To see this, consider the ring R of matrices of the form $\begin{bmatrix} a & 0 \\ b & a \end{bmatrix}$ with $a, b \in \mathbb{F}_2$. This is isomorphic to $\mathbb{F}_2[X]/(X^2)$, that one would get after reducing the order $\mathbb{Z}[\sqrt{2}]$ modulo 2. Clearly $\mathrm{Tr}(x) = 0$ for any $x \in R$, but $\mathrm{nil}(R) \subsetneq R$.

Proof of Proposition 2.38. From the assumption about q it follows that the ring $\mathbb{Z}/q\mathbb{Z}$ is reduced. As a consequence, one only needs to verify the following equivalence:

$$x \in \mathrm{nil}(A/qA) \iff \mathrm{Tr}(xy) \in \mathrm{nil}(\mathbb{Z}/q\mathbb{Z}) \text{ for any } y \in A/qA. \tag{13}$$

Let us start by proving "$\Longrightarrow$". If $x \in \mathrm{nil}(A/qA)$, then for any $y \in A/qA$, $xy \in \mathrm{nil}(A/qA)$ and a fortiori $xy \in \mathrm{nil}(A/pA)$. Such an element gives rise to a nilpotent mapping:

$$\mathbb{F}_p^n \cong A/pA \ni z \longmapsto xyz \in A/pA \cong \mathbb{F}_p^n. \tag{14}$$

Clearly its trace equals zero. ([14]) It follows, that $Tr(xy) \in p$ for all primes p dividing q, and so $Tr(xy) \in \mathrm{nil}(\mathbb{Z}/q\mathbb{Z})$.

To see why "$\Longleftarrow$" holds true, we will need the following lemma:

[12] This is a property of all nilpotent matrices.

[13] Let us recall, that $\mathfrak{r}/qA = \mathrm{nil}(A/qA)$.

[14] One need to verify, that all eigenvalues a nilpotent matrix equal zero.

Lemma 2.40 (Newton's identities)**.** *For any $n > 0$, $k \geq 1$ define a polynomial:*

$$p_k(X_1, \ldots, X_n) = X_1^k + \ldots + X_n^k.$$

Let $e_0(= 1), e_1, \ldots, e_n$ denote the elementary symmetric polynomials, and set $e_i = 0$ for $i > n$. Then for any $k \geq 1$:

$$ke_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i. \tag{15}$$

Proof of the lemma. For $k \geq n$, the identities follow immediately from:

$$\sum_{i=1}^{n} x^{n-k}(x_i - x_1) \cdots (x_i - x_n) = 0.$$

For $k < n$, one can apply the formula (15) to any k-element subset of $\{X_1, \ldots, X_n\}$. Summing up the equations obtained in this manner, over all possible choices of the subset, one clearly gets the desired identity multiplied by the factor of $\binom{n}{k}$.

Back to the proof of Proposition 2.38. Now take $x \in A/qA$, such that $\mathrm{Tr}(xy) \in \mathrm{nil}(\mathbb{Z}/q\mathbb{Z})$ for any $y \in A/qA$. In particular $\mathrm{Tr}(x^k) = 0$ in $\mathbb{F}_p$ for any $k \geq 1$ and for any p dividing q. This implies $\lambda_1^k + \ldots + \lambda_n^k = 0$ with $k \geq 1$, where $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{F}}_p$ denotes the eigenvalues of the matrix associated with x in terms of (14). By Lemma 2.40, and $n < p$ it follows, that $(X - \lambda_1) \cdots (X - \lambda_n) = X^n$. Hence $\lambda_i = 0$ for any i, and as a consequence x is nilpotent in A/pA. Since $\dim A/pA = n$, one has at least $x^n = 0$ in A/pA, but this holds true for all p dividing q. The ring A/qA is a free $\mathbb{Z}/q\mathbb{Z}$-algebra, so the previous statement already implies $x^n = 0$ in A/qA, ([15]) i.e. $x \in \mathrm{nil}(A/qA)$ as asserted. □

3. Lattices

Before we give any details on the Zassenhaus "Round 2" algorithm, we would like to address the problem of performing linear algebraic calculations over $\mathbb{Z}$, that was indicated in Remark 2.36. The typical problem that we need to deal with, is to compute a basis of a free $\mathbb{Z}$-module, which is given in terms of its generators. This will be done by means of MLLL algorithm (for "Modified LLL", see [C]), which is a variant, due to M. Pohst (see [P]), of the famous algorithm invented by Lenstra brothers, and Laszlo Lovàsz, for efficient factorization of polynomials over $\mathbb{Q}$.

3.1. **Lattices and determinants.** First, we need to introduce some notion from the theory of *lattices*. As we will see, the fundamental tool is the ubiquitous determinant – a very important lattice invariant, with simple geometrical interpretation.

Definition 3.1. A *lattice* is a finitely generated subgroup of a finite dimensional Euclidean vector space, equipped with the induced scalar product. It follows, that any lattice $L \subset \mathbb{R}^k$ is necessarily a free $\mathbb{Z}$-module of some finite rank n.

Remark 3.2. It can be easily verified, that the mapping

$$q : \mathbb{R}^k \supset L \ni x \longmapsto \langle x, x \rangle \in \mathbb{R}$$

with $\langle \cdot, \cdot \rangle$ denoting the standard scalar product on $\mathbb{R}^k$, satisfies the following conditions:

(L1) $q(x + y) + q(x - y) = 2q(x) + 2q(y)$ for all $x, y \in L$,
(L2) $q(x) \neq 0$ for all $x \in L$ with $x \neq 0$,
(L3) $\#\{x \in L : q(x) \leq r\} < \infty$ for each real number r.

[15] Thanks to the fact, that $\mathbb{Z}/q\mathbb{Z}$ is reduced.

Conversely, giving a lattice is equivalent to giving a finitely generated abelian group L, together with a mapping $q : L \longrightarrow \mathbb{R}$, satisfying (L1), (L2) and (L3). Clearly, (L1) assures that the mapping

$$(x, y) \longmapsto b(x, y) := \frac{1}{2}(q(x + y) - q(x) - q(y)) \tag{16}$$

is bilinear (over $\mathbb{Z}$). Once verified, that L is a free group, and $q(x) > 0$ holds for any $x \neq 0$, the hardest part is to show, that L can be embedded into $\mathbb{R}^k$, for some k, so that the bilinear mapping b coincides with the standard scalar product induced form $\mathbb{R}^n$. This amounts to the fact, that any positively definite symmetric matrix $A \in \mathrm{Mat}(n \times n; \mathbb{R})$ can be written in the form $A = B^T B$, for some matrix $B \in \mathrm{Mat}(k \times n; \mathbb{R})$ with $k \geq n$. Actually, one can always take $k = n$. ([16]) It follows, that a lattice of rank n, may be always viewed as a discrete subgroup of $\mathbb{R}^n$ with induced (standard) scalar product.

It depends on the situation, which model of a lattice suits better for our needs. In fact we will switch from one to another, always notifying the reader if this will not be clear from the context.

Remark 3.3. In an algorithmic context a lattice L of rank n may be encoded in terms of positively definite symmetric matrix $A \in \mathrm{Mat}(n \times n; \mathbb{R})$ representing the bilinear form (16) in some basis of L. This is usually called *Gram matrix*. In practice, we will only consider A with rational entries.

Example 3.4. A nontrivial example of a lattice comes from algebraic number theory. Namely, given a number field K of degree n, let $\sigma_1, \ldots, \sigma_n$ denote all embeddings of K into $\overline{\mathbb{Q}} \subset \mathbb{C}$. It turns out, that the mapping

$$K \ni x \longmapsto \sum_{i=1}^{n} |\sigma_i(x)|^2 \in \mathbb{R}$$

endows any finitely generated submodule $M \subset K$ with a lattice structure. The corresponding scalar product coincide with the complex scalar product induced on K in terms of the embedding $K \subset K \otimes \mathbb{C} \cong \mathbb{C}^n$. Explicitly, this is given as

$$\langle x, y \rangle = \sum_{i=1}^{n} \sigma_i(x)\overline{\sigma_i(y)}.$$

The lattices of this type, play a crucial role in the proofs of finiteness theorems for the groups of units and ideal class group (see [S]) of a number ring.

Since L is free of finite rank, we can apply to L any definition/result that we already discussed in the context of free $\mathbb{Z}$-modules. In particular, one can define the determinant of L, as well as prove its basic properties.

Definition 3.5. Given a lattice $L \subset \mathbb{R}^k$ with $k \geq n = \operatorname{rank} L$, one defines its *determinant*

$$d(L) := \left(\det \begin{bmatrix} \langle x_1, x_1 \rangle & \cdots & \langle x_1, x_n \rangle \\ \vdots & \ddots & \vdots \\ \langle x_n, x_1 \rangle & \cdots & \langle x_n, x_n \rangle \end{bmatrix} \right)^{1/2} \tag{17}$$

where $x_1, \ldots, x_n$ denote some basis of L. Clearly the number $d(L)$, does not depend on the choice of basis (compare it with Definition 2.11).

[16] However, supposing that A has rational entries, and we want to find B with rational entries, then in general $k > n$ need to be consider (see [L2]).

Remark 3.6. One easily recognizes in (17) a formula for the n-dimensional volume of a parallelepiped spanned by vectors $x_1, \ldots, x_n \in \mathbb{R}^k$, which gives a nice geometric interpretation of $d(L)$. The reader may verify, that the determinant can be also computed from the formula

$$d(L) = \lim_{r\to\infty} \frac{\operatorname{vol} B(\sqrt{r})}{\#\{y \in L : q(y) \leq r\}}$$

with $\operatorname{vol} B(\sqrt{r})$ denoting the volume of an n-dimensional ball of radius $\sqrt{r}$, and q defining the lattice structure. This gives rise to a particularly elegant, basis-independent definition of the determinant, which relies only on the basic lattice structure.

Definition 3.7. Suppose, that L is a lattice, and $L' \subset L$. By saying "L' is a *sublattice* of L", we mean, that L' is a submodule of L with a lattice structure induced from L.

The following result relate the determinant of a lattice to the determinant of its sublattice of finite index (i.e. the same rank). Clearly, it is a straightforward consequence of Proposition 2.13.

Observation 3.8. *Let L' be a sublattice of L with* $\operatorname{rank} L' = \operatorname{rank} L$. *Then*

$$d(L') = [L : L']d(L).$$

3.2. **Hermite constant.** Usually, it is convenient to know some bounds, booth lower and upper, for the lattice determinant $d(L)$, in terms some properties of the quadratic form q. A well known result of this type is Hadamard's inequality

$$d(L) \leq \|x_1\| \cdots \|x_n\|, \tag{18}$$

which holds true for any basis $x_1, \ldots, x_n$ of L, with $\|\cdot\|$ denoting the Euclidean norm, as long as L is viewed as a subgroup of $\mathbb{R}^k$, or simply $\|\cdot\| = \sqrt{q(\cdot)}$ in the abstract case.

A lower bound for $d(L)$ is harder to find, but it can be achieve for bases with some special properties (see Proposition 3.21). Another result of this type, which is independent of the basis choice, relies on the following theorem:

Theorem 3.9 (Minkowski)**.** *Supposing that $X \subset L \subset R^n$ is a bounded, convex and symmetric set (i.e. $X = -X$), such that*

$$\operatorname{vol} X > 2^n d(L),$$

with $n = \operatorname{rank} L$. Then X contains a non-zero lattice point. If furthermore X is assumed to be closed, than the same is true under a weaker assumption $\operatorname{vol} X \geq 2^n d(L)$.

Proof. For any basis $x_1, \ldots, x_n$ of L define

$$F = \{\lambda_1 x_1 + \ldots + \lambda_n x_n : 0 \leq \lambda_i < 1\}.$$

Then clearly $\operatorname{vol}(F) = d(L)$ (see Remark 3.6), and $\mathbb{R}^n = \bigcup_{y\in L}(y + F)$ is a disjoint union. In particular

$$\operatorname{vol}(F) = d(L) < \frac{1}{2^n}\operatorname{vol}(X) = \operatorname{vol}(2^{-1}X) = \sum_{y\in L} \operatorname{vol}(2^{-1}X \cap (y + F)) = \sum_{y\in L} \operatorname{vol}((2^{-1}X - y) \cap F).$$

It follows, that the sets $(2^{-1}X - y) \cap F$ are not pairwise disjoint, so there exist $y_1 \neq y_2 \in L$, such that the set $(2^{-1}X - y_1) \cap (2^{-1}X - y_2)$ is non empty. Hence, for some $x_1, x_2 \in X$ one has $x_1/2 - y_1 = x_2/2 - y_2$, and so

$$\frac{x_1 - x_2}{2} = y_1 - y_2 \in L \cap X.$$

In the case of weaker inequality $\operatorname{vol} X \geq 2^n d(L)$, one can apply the result proved so far for the set $X_\varepsilon(1+\varepsilon)X$ for some $\varepsilon > 0$. Since, $X = \bigcap_{\varepsilon>0} X_\varepsilon$ and $X_\varepsilon \cap L$ is always finite and nonempty, the assertion follows. □

Corollary 3.10. *A lattice L always contains an element x with*

$$q(x) \leq \frac{4}{\pi}\left(\frac{n}{2}!\right)^{2/n} d(L)^{2/n} \leq n \cdot d(L)^{2/n}. \tag{19}$$

Proof. Use Minkowski's theorem for $X = tB(1)$ with $B(1)$ denoting the n-dimensional unit ball, and $t = 2(d(L)/\operatorname{vol} B(1))^{1/n}$. The result follows, form

$$\operatorname{vol} B(1) = \frac{\pi^{n/2}}{\Gamma(1+n/2)} = \frac{\pi^{n/2}}{(n/2)!}. \text{ ([17])}$$

with Γ denoting the Euler Γ-function. The second inequality in (19) can be derived from Stirling's theorem. □

Corollary 3.11. *For any lattice define $\lambda(L) = \min\{q(x) : x \in L\}$. Then*

$$\gamma_n := \sup\{\lambda(L)/d(L)^{2/n} : L \text{ is a lattice of rank } n\} < \frac{4}{\pi}\left(\frac{n}{2}!\right)^{2/n} \leq n.$$

In particular, $\lambda(L) \leq \gamma_n d(L)^{2/n}$ for any lattice L.

Definition 3.12. The number γ_n defined in Corollary 3.11 is called *Hermite constant*.

Example 3.13. The exact value of γ_n is known only for $n \leq 8$ (see [C]):

$$\gamma_1 = 1,\ \gamma_2^2 = \frac{4}{3},\ \gamma_3^3 = 2,\ \gamma_4^4 = 4,\ \gamma_5^5 = 8,\ \gamma_6^6 = \frac{64}{3},\ \gamma_7^7 = 64,\ \gamma_8^8 = 256.$$

It is an interesting exercise, to verify that $\gamma_2^2 = 4/3$. ([18])

3.3. **Gram-Schmidt process.** We now recall a well known routine of finding an orthonormal basis of a linear space endowed with a scalar product. This is usually called *Gram-Schmidt orthonormalization*. The reason, we use a different name is that we do not necessarily want the resulting vectors to be of length 1.

Definition 3.14. Given any sequence of linearly independent vectors $x_1, \ldots, x_n$ in $\mathbb{R}^k$, define $x_1^*, \ldots, x_n^*$ by the inductive formula

$$x_1^* := x_1, \quad x_i^* = x_i - \sum_{j<i} \mu_{ij} x_j^* \quad \text{for} \quad i > 1 \quad \text{with} \quad \mu_{ij} = \langle x_i, x_j^*\rangle / \langle x_j^*, x_j^*\rangle. \tag{20a}$$

This is called *Gram-Schmidt process*. By induction, $x_j^* \in \mathbb{R}x_1 + \ldots + \mathbb{R}x_j$ for any j. In particular, the formula for μ_{ij} remains valid for $i > j$, since $\langle x_j^*, x_j^*\rangle = 0$ would imply $x_j \in \mathbb{R}x_1^* + \ldots + \mathbb{R}x_{j-1}^* \subset \mathbb{R}x_1 + \ldots + \mathbb{R}x_{j-1}$, which contradicts with the linear independence of $x_1, \ldots, x_n$.

Furthermore, one can easily verify, that the resulting vectors $x_1^*, \ldots, x_n^*$ are pairwise orthogonal. Conversely, given a sequence $y_1^*, \ldots, y_n^*$ of pairwise orthogonal vectors (note, that we do not need to assume, they are non-zero) as well as coefficients λ_{ij} satisfying

$$y_i^* = x_i - \sum_{j<i} \lambda_{ij} y_j^* \quad \text{for} \quad i \geq 1, \tag{20b}$$

then one has necessarily $y_i^* = x_i^*$ and $\lambda_{ij} = \mu_{ij}$ for any i, j. In particular the outputs of Gram-Schmidt process, both vectors and coefficients, are uniquely determined by orthogonality, and the equations (20b).

[17] We use the notation $x! := \Gamma(1+x)$.

[18] **Hint:** use the notion of reduced binary quadratic forms.

Remark 3.15. As we can see, the linear independence of $x_1, \dots, x_n$ plays an important role in Definition 3.14. However, one can also consider a *modified Gram-Schmidt process*, which works even if a linear dependency occurs. Namely, we use the formula (20a), until $\langle x_j^*, x_j^* \rangle = 0$ for some j. In such an instance we simply set $\mu_{ij} = 0$ for any $i > j$.

Note, that the uniqueness indicated in Definition 3.14, also holds for modified Gram-Schmidt, under an additional assumption, that if $y_j^* = 0$ for some j, then necessarily $\mu_{ij} = 0$ for any $i > j$.

Suppose, that $x_1^*, \dots, x_n^*$ together with μ_{ij} encode the output of modified Gram-Schmidt process, applied to $x_1, \dots, x_n$. Then, the restriction of this data, to those i with $x_i^* \neq 0$, coincide with the output of the (standard) Gram-Schmidt process, applied to the subsequence of $x_1, \dots, x_n$ consisting of x_i, such that $x_i^* \neq 0$.

Proposition 3.16. *Let $x_1, \dots, x_n$ be a basis of L, and let $x_1^*, \dots, x_n^*$ be the result of Gram-Schmidt process. Then*

$$d(L) = \|x_1^*\| \cdots \|x_n^*\|.$$

Proof. By definition of $x_1^*, \dots, x_n^*$, properties of matrix determinant, and the fact that $\langle x_i, x_j^* \rangle = 0$ for $i < j$, one has

$$\begin{vmatrix} \langle x_1, x_1 \rangle & \cdots & \langle x_1, x_n \rangle \\ \vdots & \ddots & \vdots \\ \langle x_n, x_1 \rangle & \cdots & \langle x_n, x_n \rangle \end{vmatrix} = \begin{vmatrix} \langle x_1, x_1^* \rangle & \cdots & \langle x_1, x_n^* \rangle \\ \vdots & \ddots & \vdots \\ \langle x_n, x_1^* \rangle & \cdots & \langle x_n, x_n^* \rangle \end{vmatrix} = \begin{vmatrix} \langle x_1, x_1^* \rangle & \cdots & 0 \\ \vdots & \ddots & \vdots \\ \langle x_n, x_1^* \rangle & \cdots & \langle x_n, x_n^* \rangle \end{vmatrix} = \prod_{i=1}^{n} \langle x_i, x_i^* \rangle.$$

The result now follows from $\langle x_i, x_i^* \rangle = \langle x_i^*, x_i^* \rangle$. □

Remark 3.17. With the above notation, define L_i to be the lattice spanned by vectors $x_1, \dots, x_i$. From Proposition 3.16, it follows that

$$\|x_1^*\| \cdots \|x_i^*\| = d(L_i) = \left(\det \begin{bmatrix} \langle x_1, x_1 \rangle & \cdots & \langle x_1, x_i \rangle \\ \vdots & \ddots & \vdots \\ \langle x_i, x_1 \rangle & \cdots & \langle x_i, x_i \rangle \end{bmatrix} \right)^{1/2}. \tag{21}$$

We will call the product $d(L_1) \cdots d(L_n)$ the *size* of the basis $x_1, \dots, x_n$ (see [L2]), and we will denote it by $s(x_1, \dots, x_n)$. From Corollary 3.11, it follows that

$$\frac{\lambda(L)^{n(n+1)/2}}{1^1 \cdot 2^2 \cdot \ldots \cdot n^n} \leq s(x_1, \dots, x_n)^2. \tag{22}$$

In particular, the value of $s(x_1, \dots, x_n)$ is bounded from below by a positive constant, which is independent of the choice of basis.

The following result will play an auxiliary role in the analysis of the LLL algorithm.

Proposition 3.18. *Suppose, that $x_1, \dots, x_n \in \mathbb{Z}^n$, and let us define*

$$\det \begin{bmatrix} \langle x_1, x_1 \rangle & \cdots & \langle x_1, x_i \rangle \\ \vdots & \ddots & \vdots \\ \langle x_i, x_1 \rangle & \cdots & \langle x_i, x_i \rangle \end{bmatrix} =: d_i.$$

Then, writing $x_1^*, \dots, x_n^*$ for the output of Gram-Schmidt process on $x_1, \dots, x_n$, one has

$$d_{i-1} x_i^* \in \mathbb{Z}^n \text{ for any } i = 1, \dots, n.$$

Proof. It follows from the definition of x_i^*, that there exist $\lambda_{i1}, \ldots, \lambda_{i,i-1} \in \mathbb{R}$ with

$$x_i - x_i^* = \lambda_{i1} x_1 + \ldots + \lambda_{i,i-1} x_{i-1}.$$

These coefficients can be found by solving a system of linear equations

$$\mathbb{Z} \ni \langle x_i, x_j \rangle = \langle x_i - x_i^*, x_j^* \rangle = \lambda_{i1} \langle x_1, x_j \rangle + \ldots + \lambda_{i,i-1} \langle x_{i-1}, x_j \rangle.$$

with $j = 1, \ldots, i-1$. Since the determinant of this system equals d_{i-1}, then by Cramer's rule, $d_{i-1}\lambda_{ij} \in \mathbb{Z}$ for any $j = 1, \ldots, i-1$. In particular $d_{i-1} x_i^* \in \mathbb{Z}^n$ as asserted. □

Corollary 3.19. *With the above notation, $d_j \mu_{ij} \in \mathbb{Z}$ for any $i > j$.*

Proof. By Propositions 3.16 and 3.18, one has

$$d_j \mu_{ij} = d_j \cdot \frac{\langle x_i, x_j^* \rangle}{\|x_j^*\|^2} = d_{j-1} \langle x_i, x_j^* \rangle = \langle x_i, d_{j-1} x_j^* \rangle \in \mathbb{Z}.$$

□

3.4. **Reduced basis.** From the practical point of view, there are some bases, which are better to work with. In the algorithmic context, if the lattice is represented by symmetric, positively definite matrix (see Remark 3.3), then one clearly wants to have a basis $x_1, \cdots, x_n$, for which the entries $\langle x_i, x_j \rangle$ are as small as possible. For simplicity, let us assume that the numbers $\langle x_i, x_j \rangle$ are integers. Then, the amount of resources required to encode the Gram matrix is proportional to

$$\sum_{i,j=1}^{n} \log |\langle x_i, x_j \rangle| \leq \sum_{i,j=1}^{n} \log \|x_i\| \|x_j\| = 2n \sum_{i=1}^{n} \log \|x_i\| = 2n \log \|x_1\| \cdots \|x_n\|$$

where $\| \cdot \|$ denotes the Euclidean norm. We will show, that given any $c > 4/3$, one is actually capable of finding a basis $x_1', \ldots, x_n'$ of L, for which

$$\|x_1'\| \cdots \|x_n'\| \leq c^{n(n-1)/4} d(L).$$

We now introduce the notion of *c-reduced basis*, which can be thought to be a basis that is not very far from being orthogonal, in sense of the above inequality (note, that one have "=", if and only, if $x_1', \ldots, x_n'$ are orthogonal). Basically speaking, the LLL algorithm enables one to find a c-reduced basis of a given *lattice*.

Definition 3.20. Let $c \geq 1$, and let $x_1^*, \ldots, x_n^*$ denote the output of Gram-Schmidt process applied to a basis $x_1, \ldots, x_n$. We say, that it is *c-reduced*, if and only, if

$$\|x_i^*\|^2 \leq c \|x_{i+1}^*\|^2 \quad \text{for each} \quad 1 \leq i < n, \tag{23}$$

$$-\frac{1}{2} \leq \mu_{ij} \leq \frac{1}{2} \quad \text{for any} \quad 1 \leq j < i \leq n. \tag{24}$$

Proposition 3.21. *If $x_1, \ldots, x_n$ is a c-reduced basis of L with $c \geq 4/3$, then*

$$\|x_1\| \cdots \|x_n\| \leq c^{n(n-1)/4} d(L).$$

Proof. Define $x_1^*, \ldots, x_n^*$ as in Definition 3.20. Then, by (20a), (23) and (24):

$$\|x_i\|^2 = \|x_i^*\|^2 + \sum_{j<i} \mu_{ij}^2 \|x_j^*\|^2 \leq$$

$$\|x_i^*\|^2 + \frac{1}{4} \sum_{j<i} c^{i-j} \|x_i^*\|^2 = \|x_i^*\|^2 \left(1 + \frac{1}{4}(c^i - c)/(c-1)\right).$$

By the assumption $c \geq 4/3$, one clearly has $c/(c-1) \leq 4$, which implies:

$$\left(1 + \frac{1}{4}(c^i - c)/(c-1)\right) \leq c^{i-1}.$$

As a consequence, the inequality $\|x_i\|^2 \leq c^{i-1}\|x_i^*\|^2$ holds for any $i = 1, \ldots, n$. Taking product over all i, one gets

$$\|x_1\|^2 \cdots \|x_n\|^2 \leq c^{n(n-1)/2}\|x_1^*\|^2 \cdots \|x_n^*\|^2 = c^{n(n-1)/2} d(L)^2.$$

The last equality follows from Proposition 3.16. □

Theorem 3.22. *For any lattice L, and $c > 4/3$, there exists a c-reduced basis of L.*

Proof. Let $x_1, \ldots, x_n$ be any basis, and let $x_1^*, \ldots, x_n^*$, together with μ_{ij} for $1 \leq j < i \leq n$ encode the output of Gram-Schmidt process, as described in (20a). This is equivalent to saying, that

$$x_i^* = x_i - \sum_{j<i} \mu_{ij} x_j^* \quad \text{for any} \quad i \geq 1,$$

and $x_1^*, \ldots, x_n^*$ are pairwise perpendicular. Supposing, that the condition

$$-\frac{1}{2} \leq \mu_{ij} \leq \frac{1}{2} \tag{25}$$

does not hold for some $i > j$, one can use the `Size-Reduce` routine, as described in Algorithm 1, to modify $x_1, \ldots, x_n$, in a way, that the condition (25) holds for any $i > j$.

Algorithm 1 Given $i > j$, assures that $|\mu_{ik}| \leq 1/2$, as long as $k < j$.

1: **procedure** SIZE-REDUCE(i, j) ▷ should be used with $i > j$
2: **if** $|\mu_{ij}| \leq 1/2$ **then** terminate
3: otherwise, set $m \leftarrow$ the integer nearest to μ_{ij}
4: $x_i \leftarrow x_i - m x_j$; $\mu_{ij} \leftarrow \mu_{ij} - m$ ▷ clearly, $|\mu_{ij}| \leq 1/2$ at this point
5: for any $k < j$ set $\mu_{ik} \leftarrow \mu_{ik} - m\mu_{jk}$ ▷ still having $x_i^* = x_i - \sum_{k<i} \mu_{ik} x_k^*$
6: **end procedure**

First, observe that the modified vectors $x_1, \ldots, x_n$ forms a basis of the same $\mathbb{Z}$-module, since the only change to x_i, which occurs in line 4, is invertable. Furthermore, the invariant indicated at line 5 is correct, due to:

$$x_i^* = (x_i - m x_j) + m x_j - \sum_{k<i} \mu_{ik} x_k^* =$$

$$(x_i - m x_j) + m x_j^* + m \sum_{k<j} \mu_{jk} x_k^* - \sum_{k<i} \mu_{ik} x_k^* =$$

$$(x_i - m x_j) - \sum_{k<j} (\mu_{ik} - m\mu_{jk}) x_k^* - (\mu_{ij} - m) x_j^* - \sum_{j<k<i} \mu_{ik} x_k^*.$$

It follows that, together with the resulting coefficients μ_{ij}, the vectors $x_1^*, \ldots, x_n^*$, which were unchanged during the course of algorithm, still encode the result of Gram-Schmidt process applied to modified $x_1, \ldots, x_n$. Clearly, $|\mu_{ij}| < 1/2$ holds in line 4, and it remains unchanged afterward. Also notice, that the algorithm does not make any changes to μ_{ik} with $j < k < i$. It is know clear, that in order to provide a size-reduced basis $x_1, \ldots, x_n$, one needs to call `Size-Reduce`(i, j) for each $i = 1, \ldots, n$ and then for $j = (i-1), \ldots, 1$ (necessarily in this order).

The next step is to show, that one is actually capable of finding a basis $x_1, \ldots, x_n$, such that $\|x_i^*\|^2 \leq c\|x_{i+1}^*\|^2$ for any $1 \leq i < n$. To prove this, we will use the notion of *size*, as introduced in Remark 3.17. Namely, assuming that we already have a basis $x_1, \ldots, x_n$, which is not c-reduced, we show, that there exists another basis $y_1, \ldots, y_n$ with

$$s(y_1, \ldots, y_n) < \sqrt{(1/c + 1/4)}s(x_1, \ldots, x_n). \tag{26}$$

Since, $(1/c + 1/4) < 1$ and the number $s(y_1, \ldots, y_n)$ is bounded from below by a positive constant which is independent of the choice of the basis (see Remark 3.17), this already proves, that one will eventually end up with a c-reduced basis.

Now Suppose, that for some i one has

$$\|x_i^*\|^2 > c\|x_{i+1}^*\|^2. \tag{27}$$

By virtue of the previous considerations, we can already assume, that $|\mu_{ij}| \leq 1/2$. ([19]) Let $y_1, \ldots, y_n$ denote a basis obtained from $x_1, \ldots, x_n$ by exchanging the vectors x_i and x_{i+1}. We clearly have

$$x_{i+1}^* + \mu_{i+1,i}x_i^* = x_{i+1} - \sum_{j<i} \mu_{i+1,j}x_j^*. \tag{28}$$

Since furthermore, the vector $x_{i+1}^* + \mu_{i+1,i}x_i^*$ is perpendicular to x_j^* for any $j < i$, it follows, that $y_1^* = x_1^*, \ldots, y_{i-1}^* = x_{i-1}^*$, $y_i^* = x_{i+1}^* + \mu x_i^*, \ldots$ with $y_1^*, \ldots, y_n^*$ denoting the output of Gram-Schmidt process applied to basis $y_1^*, \ldots, y_n^*$. In particular, by (27):

$$\|y_i^*\|^2 = \|x_{i+1}^*\|^2 + \mu_{i+1,i}^2\|x_i^*\|^2 < \left(\frac{1}{c} + \frac{1}{4}\right)\|x_i^*\|^2$$

with $(1/c + 1/4) < 1$. By computing sizes of these two bases, as shown in Remark 3.17, one proves that (26) holds. □

Remark 3.23. One can use (22), to estimate the number of steps, needed to find a c-reduced basis, in terms of $\lambda(L) = \min\{q(x) : x \in L\}$ and the initial size s_{init} of a given basis. Namely:

$$\text{number of steps} \leq \frac{\log(s_{\text{init}}/s_{\min})}{-\log\sqrt{(1/c + 1/4)}} \quad \text{with} \quad s_{\min} = \frac{\lambda(L)^{n(n+1)/2}}{1^1 \cdot 2^2 \cdot \ldots \cdot n^n}.$$

Further analysis gives the following bounds:

$$\text{number of steps} \leq \frac{\log(s_{\text{init}}) + \frac{1}{2}n(n+1)(\log n - \log\lambda(L))}{\log\sqrt{4c/(4+c)}}. \tag{29}$$

Observe, that in practice the number $\lambda(L)$ can be usually bounded from below in an obvious way; for example if $q : L \longrightarrow \mathbb{Z}$, then clearly $\lambda(L) \geq 1$.

On the other hand, one can easily give some upper bounds for s_{init} by means of Hadamard's inequality. Namely, if $|\langle x_i, x_j\rangle| < M$ holds for any i, j with some constant $M > 0$, then $\|x_1^*\| \cdots \|x_i^*\| \leq (M\sqrt{i})^i$ for any i, and in the view of Remark 3.17, one has

$$\prod_{i=1}^{n} \|x_i^*\|^{n-i+1} = s(x_1, \ldots, x_n) \leq M^{n(n+1)/2}(1 \cdot 2^2 \cdot \ldots \cdot n^n)^{1/2}.$$

Suppose now, that one would like to turn the procedure described in the proof, into an algorithm. By the the above inequality, and the fact, that the size of the basis does not increase during the computations, we can see, that the one can give some safe upper bounds for the magnitude of $x_1^*, \ldots, x_n^*$, at least in terms of $\|\cdot\|$.

[19] Since the vectors $x_1^*, \ldots, x_n^*$ remain unchanged during the size-reduction, then so does $s(x_1, \ldots, x_n)$.

Remark 3.24. Let us recall, that the key observation in the proof was, that the size $s(x_1, \ldots, x_n)$ decreases, as long as $\|x_i^*\|^2 > c\|x_{i+1}^*\|^2$, and one replaces this basis with $y_1, \ldots, y_n$ obtained from $x_1, \ldots, x_n$ by exchanging the vectors x_i and x_{i+1}. It can be easily deduced by analyzing the output of Gram-Schmidt process for $y_1^*, \ldots, y_n^*$, namely the vector $y_i^* = x_{i+1}^* + \mu x_i^*$.

In algorithmic situation it may be convenient to compute all the vectors $y_1^*, \ldots, y_n^*$, as well as the Gram-Schmidt coefficients λ_{ij}, in terms of $x_1^*, \ldots, x_n^*$ and μ_{ij}. Let us denote $\mu = \mu_{i+1,i}$, $\lambda = \mu\|x_i^*\|^2/(\|x_{i+1}^*\|^2 + \mu^2\|x_i^*\|^2)$. Then, clearly

$$x_{i+1}^* + \mu x_i^* = x_{i+1} - \sum_{j<i} \mu_{i+1,j} x_j^*, \tag{30}$$

$$(1 - \lambda\mu)x_i^* - \lambda x_{i+1}^* = x_i - \sum_{j<i} \mu_{i,j} x_j^* - \lambda(x_{i+1}^* + \mu x_i^*). \tag{31}$$

Furthermore, a straightforward verification for $k > i + 1$ leads to:

$$\begin{aligned} x_k^* = x_k - \sum_{j\neq i,i+1} \mu_{kj} x_j^* - \mu_{k,i} x_i^* - \mu_{k,i+1} x_{i+1}^* = \\ \sum_{j\neq i,i+1} \mu_{kj} x_j^* - ((1 - \lambda\mu)\mu_{k,i+1} + \lambda\mu_{k,i})(x_{i+1}^* + \mu x_i^*) - \\ (\mu_{k,i} - \mu_{k,i+1}\mu)((1 - \lambda\mu)x_i^* - \lambda x_{i+1}^*). \end{aligned} \tag{32}$$

By (30), (31), (32), and the fact that $x_{i+1}^* + \mu x_i^*$ and $(1 - \lambda\mu)x_i^* - \lambda x_{i+1}^*$ are orthogonal, ([20]) it follows that

$$\begin{gathered} y_k^* = x_k^*, \text{ and } \lambda_{kj} = \mu_{kj} \text{ for } j < k < i, \\ y_i^* = x_{i+1}^* + \mu x_i^*,\ y_{i+1}^* = (1 - \lambda\mu)x_i^* - \lambda x_{i+1}^* \\ \lambda_{i+1,i} = \lambda \text{ and } \lambda_{i,j} = \mu_{i+1,j}, \lambda_{i,j} = \mu_{i+1,j},\ \lambda_{i+1,j} = \mu_{i,j} \text{ for } j < i, \\ y_k^* = x_k^* \text{ for } k > i + 1 \\ \lambda_{k,i} = (1 - \lambda\mu)\mu_{k,i+1} + \lambda\mu_{k,i},\ \lambda_{k,i+1} = \mu_{k,i} - \mu_{k,i+1}\mu \end{gathered}$$

These observations are summarized in the following algorithm:

Algorithm 2 Updates the Gram-Schmidt parameters of a basis, after exchanging x_i with x_{i-1}.

procedure SWAP(i)
  set $\mu \leftarrow \mu_{i,i-1}$; $\lambda \leftarrow \mu\|x_{i-1}^*\|^2/(\|x_i^*\|^2 + \mu^2\|x_{i-1}^*\|^2)$
  for any $j < i - 1$ exchange $\mu_{i,j}$ and $\mu_{i-1,j}$; eventually set $\mu_{i,i-1} \leftarrow \lambda$
  exchange x_i with x_{i-1}
  `temp1` $\leftarrow x_i^* + \mu x_{i-1}^*$; `temp2` $\leftarrow (1 - \lambda\mu)x_{i-1}^* - \lambda x_i^*$
  $x_{i-1}^* \leftarrow$ `temp1`; $x_i^* \leftarrow$ `temp2`
  for $k = i + 1, \ldots, n$ **do**
    `temp1` $\leftarrow (1 - \lambda\mu)\mu_{ki} + \lambda\mu_{k,i-1}$; `temp2` $\leftarrow \mu_{k,i-1} - \mu_{ki}\mu$
    $\mu_{k,i-1} \leftarrow$ `temp1`; $\mu_{ki} \leftarrow$ `temp2`
  end for
end procedure

[20] It is due to the choice of λ.

3.5. **The LLL algorithm.** Thanks to the results presented so far, we are now able to introduce, a simple version (see [LLL], or [C] for other implementations) of the LLL algorithm, which for any constant $c > 4/3$, finds a c-reduced basis of a given lattice. Practically, it does not matter, if the lattice is given in terms of a basis in $\mathbb{Q}^n$, or in terms of Gram matrix. However, in order to provide a more readable code, we have chosen the first type of representation. The reader can easily modify the algorithm to deal with the other case.

Algorithm 3 A version of LLL algorithm

1: compute Gram-Schmidt coefficients μ_{ij}, as well as $x_1^*, \ldots, x_n^*$
2: $i \leftarrow 2$
3: **while** $i \leq n$ **do**
4: **while** $i > 1$ **and** $\|x_{i-1}^*\|^2 > c\|x_i^*\|^2$ **do**
5: SIZE-REDUCE$(i, i-1)$
6: SWAP(i); $i \leftarrow i-1$
7: **end while**
8: for any $j < i$ call SIZE-REDUCE(i, j)
9: set $i \leftarrow i+1$
10: **end while**

Observation 3.25. *The Algorithm 3 stops in a finite number of steps, and the resulting $x_1, \ldots, x_n$ forms a c-reduced basis.*

Proof. The only difference between this algorithm, and the procedure described during the proof of Theorem 3.22, is the strategy of performing the size-reduction. Theoretically, the only condition, we need to assure, so that the algorithm works correctly, is $|\mu_{i,i-1}| \leq 1/2$ just before `Swap(`i`)` is performed (see line 5). This implies, that the size of the basis decreases after exchanging x_i with x_{i-1} (see proof of Theorem 3.22). □

From Remark 3.23, it already follows, that the algorithm stops in a number of steps, that depends polynomially on the size of input, so we will only concentrate on the magnitude of data, one needs to deal with during the course of the algorithm. Providing precise estimation of the upper bounds for numbers, that occur in calculations is rather technical. The reader can always see the original paper [LLL] for more details.

3.6. **The LLL algorithm for linearly dependent vectors.** Unfortunately, the presented version of LLL algorithm does not fits our needs yet. This is due to the fact, that it founds a reduced basis, assuming that any basis is already known. However, as we indicated in Remark 2.36, the main problem we need to deal with, is computing a basis of $\mathbb{Z}$-module, which is given in terms of some generating set.

There exists, a surprisingly simple solution. Generally speaking, the algorithm is almost the same as Algorithm 3, but instead of standard Gram-Schmidt process, the modified version need to be used as the initial step. Furthermore, a slightly different version of `Swap` sub-routine (see Algorithm 4) need to be used, so as to keep track on the conditions indicated in Remark 3.15. This idea is due to M. Pohst (see [P]), and it is called MLLL algorithm (for "modified LLL").

Observation 3.26. *During the course of MLLL algorithm, coefficients μ_{ij} and vectors $x_1^*, \ldots, x_n^*$ output of the modified Gram-Schmidt process applied to $x_1, \ldots, x_n$.*

Proof. It is a matter of straightforward verification (see Algorithm 4). □

Algorithm 4 A modified version of `Swap` routine, that can be used with LLL algorithm for not necessarily linearly independent vectors.

procedure MODIFIED-SWAP(i)
  set $\mu \leftarrow \mu_{i,i-1}$
  if $\|x_i^*\| \neq 0$ **then**
    SWAP($i, i_{\max}$)
  else
    exchange x_i with x_{i-1}
    for any $j < i-1$ exchange μ_{ij} with $\mu_{i-1,j}$
    if $\mu \neq 0$ **then**
      $\mu_{i,i-1} \leftarrow 1/\mu$
      set $x_{i-1}^* \leftarrow \mu x_{i-1}^*$
      for any $k = i+1, \ldots, n$ set $\mu_{k,i-1} \leftarrow \mu^{-1}\mu_{k,i-1}$
    else
      exchange x_i^* with x_{i-1}^*
      for any $k = i+1, \ldots, n$ exchange μ_{ki} with $\mu_{k,i-1}$
    end if
  end if
end procedure

Corollary 3.27. *Suppose, that the MLLL algorithm stops with output $x_1, \ldots, x_n$, and $r \geq 0$ is the number of nonzero vectors among $x_1, \ldots, x_n$. Then $x_1 = \ldots = x_{n-r} = 0$, and the vectors $x_{n-r+1}, \ldots, x_n$ are linearly independent. In particular, they form a c-reduced basis of the lattice given on input.*

Proof. Let $x_1^*, \ldots, x_n^*$ denote the modified Gram-Schmidt parameters of $x_1, \ldots, x_n$. Thanks to Observation 3.26, and the fact that algorithm stopped, it follows that $\|x_{i-1}^*\|^2 \leq c\|x_i^*\|^2$ for any $i = 2, \ldots, n$. Since there are exactly r zero vectors, we must have $x_1^* = \ldots = x_r^* = 0$. Furthermore, there are no other zero vectors among $x_{n-r+1}^*, \ldots, x_n^*$. By Remark 3.15 it now follows, that $x_{n-r+1}, \ldots, x_n$ are linearly independent. □

Proposition 3.28. *The MLLL algorithm stops in a finite number of steps. Moreover, there exists an upper bound, that depends polynomially on the size of input.*

Proof. We proceed as in the proof of Theorem 3.22. However, the notion of *size* must be replaced by the following:

$$d_i = \prod_{x_i^* \neq 0} \|x_i\|^2, \quad D = \left(\prod_{x_i^* \neq 0} d_i\right) \cdot \left(\prod_{x_i^* = 0} 2^i\right).$$

First observe, that each `Swap(`i`)` with $\|x_i\|^2 + \mu_{i,i-1}^2\|x_{i-1}\|^2 \neq 0$ reduces D by the factor of $(1/c+1/4)$ as it was in the case of Theorem 3.22. On the other hand calling, `Swap(`i`)` when $\|x_i\|^2 + \mu_{i,i-1}^2\|x_{i-1}\|^2 = 0$, i.e. $x_i = 0$ and $\mu_{i,i-1} = 0$, ([21]) results in exchanging vectors x_i^* and x_{i+1}^*. One can easily verify, that D decreases by factor of 2 in this case. □

4. Evaluating the maximal order

This section is devoted to the proof of Chistov's theorem (see Theorem 1.1), which states that finding a maximal order of a given number field is essentially equivalent to finding the largest square divisor of a given integer. One way, this is easy. Namely, given a

[21] Note, that $x_{i-1} \neq 0$, since `Swap(`i`)` is only called if $\|x_{i-1}\|^2 > c\|x_i\|^2$.

non-square integer d, one can retrieve the largest square divisor of d from the determinant of the quadratic number field $\mathbb{Q}(\sqrt{d})$ (see Corollary 2.14). Clearly, this determinant can be easily computed (e.g. from the formula (1)), as long as any basis of $\mathcal{O}_K$ is known. To prove Chistov's theorem, we need to present an algorithm, that is capable of finding a basis of $\mathcal{O}_K$ in polynomial time, modulo a sub-algorithm, which returns the largest square-free divisor of a given integer. ([22])

The main idea goes back to Zassenhaus' "Round 2" algorithm. ([23]) Namely, one starts by finding any order of a number field. If the field is given in terms of an irreducible polynomial, then an order can be easily found, as we described in Example 2.2, and so can be its determinant. Once evaluated, the determinant needs to be factored, so as to find the prime numbers p, for which the given order may not be p-maximal (see Definition 2.30). Eventually, for one of the "suspected" primes, the corresponding radical is evaluated due to Observation 2.37. The radical gives rise to a multiplier ring (computed according to Proposition 2.35), which can be used as a potential extension of the order evaluated so far. If the inclusion is not strict, then one may repeat this procedure for another "suspected" prime. If there are no other primes, then the result of Pohst and Zassenhaus (see Theorem 2.34) assures, that the obtained order is already maximal.

As we can see, the theoretical results on number rings presented so far, are already sufficient for writing an algorithm, and proving its correctness. However, it may be not clear, that the running time of this algorithm is actually polynomial, of course, modulo factoring the initial determinant. It may be surprising, that the main difficulty arises from the need to control the magnitude of the data we are working with.

4.1. **Representing an order.** First, we need to decide what kind of output we are actually looking for, and how it would be represented. If the number field K of degree n is given in terms of a minimal polynomial of a primitive (integral) element $\theta \in K$, then it seems natural to represent the elements of K as n-vectors with rational coefficients corresponding to the coordinates in the power basis $1, \theta, \ldots, \theta^{n-1}$, i.e. $K \cong \mathbb{Q}^n$ (as $\mathbb{Q}$-vector spaces) where the isomorphism is given by identifying (in this order) $1, \theta, \ldots, \theta^{n-1}$ with the canonical basis of $\mathbb{Q}^n$. Clearly, under this identification, the ring $\mathbb{Z}[\theta] \subset K$ corresponds to the subset $\mathbb{Z}^n \subset \mathbb{Q}^n$. Furthermore, any finitely generated subgroup of K will be considered as a lattice, with the scalar product induced from $\mathbb{Q}^n$, where it is given naturally. This is only due to some technical reason (see Proposition 4.8); we do not claim, that this lattice structure is better than any other in any way.

After all these identifications, knowing $\mathcal{O}_K \subset K \cong \mathbb{Q}^n$ would probably mean knowing some vectors $x_1, \ldots, x_n \in \mathbb{Q}^n$, for which $\mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_n = \mathcal{O}_K$. This is usually called an *integral basis* of K. Unfortunately, representing an order in terms of its basis alone, is only convenient, as long as the only operation one needs to perform is adding elements. The obvious method of multiplying elements, which amounts to multiplying polynomials in $\mathbb{Q}[X]/(f)$, does not directly apply to an order $A = \mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_n \subset K$. Namely, given $y, z \in A$ one would like to view the result of a multiplication $y \cdot z$ in terms of basis $x_1, \ldots, x_n$. Clearly, this amounts to solving a system of linear equations, however, we would rather not to do it for every single multiplication. Instead, we will do it only once. Namely, for a given order we compute an $n \times n^2$ matrix, determining the linear mapping

$$\mathbb{Z}^n \otimes \mathbb{Z}^n \cong \mathcal{O}_K \otimes \mathcal{O}_K \longrightarrow \mathcal{O}_K \cong \mathbb{Z}^n,$$

[22]The reader may easily verify, that this is in fact equivalent to finding the largest square divisor.

[23]As one may expect, this is the second version of Zassenhaus' algorithm. The latest is "Round 4" (for more information see [C]).

associated to multiplication in $\mathcal{O}_K$ in bases $x_i \otimes x_j$ for $1 \leq i, j \leq n$ and $x_1, \ldots, x_n$. In other words, one find coefficients $a_{ij}^{(k)} \in \mathbb{Z}$, such that

$$x_i \cdot x_j = \sum_{k=1}^{n} a_{ij}^{(k)} x_k \quad \text{for any} \quad 1 \leq i, j \leq n. \tag{33}$$

It is clear, that once they are known, the multiplication in $\mathcal{O}_K$, amounts to standard multiplication of matrices. We now give a few examples, of how this notion can be used in some practical situations.

Observation 4.1. *Supposing that* (33) *holds, then matrix of the "multiplication by x_i" linear mapping, with respect to basis $x_1, \ldots, x_n$, equals*

$$\begin{bmatrix} a_{i1}^{(1)} & \cdots & a_{in}^{(1)} \\ \vdots & \ddots & \vdots \\ a_{i1}^{(n)} & \cdots & a_{in}^{(n)} \end{bmatrix}.$$

Remark 4.2. The reader may notice, that computing the coefficients $a_{ij}^{(k)}$, amounts to finding a representation of an order as a subalgebra of the ring of $n \times n$ matrices with integral coefficients.

One may also think of representing an order abstractly as a group $\mathbb{Z}^n$, with the multiplication structure given by means of the coefficients $a_{ij}^{(k)}$. After computing the maximal order int terms of its multiplication structure (which can be done "abstractly"), one can find an integral basis in K, by analyzing the minimal polynomials of elements of some basis $x_1, \ldots, x_n \in \mathbb{Z}^n$.

Corollary 4.3. *Suppose, that $y = b_1 x_1 + \ldots + b_n x_n \in \mathcal{O}_K$. Then* $\mathrm{Tr}(y) = \sum_{i,j=1}^{n} a_{ij}^{(j)} b_i$.

In particular $\mathrm{Tr}(x_i x_j) = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl}^{(l)} a_{ij}^{(k)}$.

Proof. By Observation 4.1 one has $\mathrm{Tr}(x_i) = \sum_{j=1}^{n} a_{ij}^{(j)}$. The thesis now follows from the linearity of trace. □

Remark 4.4. Corollary 4.3 is of particular importance in the context of computing the radical $\mathfrak{r} = \mathrm{rad}(qA)$ with A denoting and order and q being a square-free integer (see Proposition 2.38). Namely, the matrix of the mapping:

$$A/qA \ni x \longmapsto (A/qA \ni y \mapsto \mathrm{Tr}(xy) \in \mathbb{Z}/q\mathbb{Z}) \in \mathrm{Hom}(A/qA, \mathbb{Z}/q\mathbb{Z})$$

equals

$$\begin{bmatrix} \mathrm{Tr}(x_1 x_1) & \cdots & \mathrm{Tr}(x_n x_1) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(x_1 x_n) & \cdots & \mathrm{Tr}(x_n x_n) \end{bmatrix}.$$

In particular, it is desirable to have a simple formula for $\mathrm{Tr}(x_i x_j)$.

Example 4.5. Let us compute the coefficients $a_{ij}^{(k)}$ with respect to basis $1, \theta, \ldots, \theta^{n-1}$ of the order $\mathbb{Z}[\theta]$. First, write $f = X^n + f_1 X^{n-1} + \ldots + X_n$ for the minimal polynomial of θ. Thanks, to the relation:

$$\theta^n = -f_1 \theta^{n-1} - \ldots - f_n,$$

one easily finds a recursive formula:

$$\theta^i\theta^j = \theta\cdot\theta^{i-1}\theta^j = \theta\sum_{k=1}^{n} a_{i-1,j}^{(k)}\theta^{k-1} = \tag{34}$$
$$\sum_{k=1}^{n-1} a_{i-1,j}^{(k)}\theta^k + a_{i-1,j}^{(n)}(-f_1\theta^{n-1} - \ldots - f_n) =$$
$$- a_{i-1,j}^{(n)} f_n + \sum_{k=2}^{n}\left(a_{i-1,j}^{(k-1)} - a_{i-1,j}^{(n)} f_{n-k+1}\right)\theta^{k-1}.$$

Writing $a_{1j}^{(k)} = \delta_{jk}$ for any $j,k = 1,\ldots,n$, with δ_{jk} denoting the Kronecker delta, this already enables us to compute all $a_{ij}^{(k)}$.

Remark 4.6. To deal with the coefficients $a_{ij}^{(k)}$ in the case of power basis, one may also use Observation 4.1. Namely, the matrix of "multiplication by θ" map is clearly

$$\Theta = \begin{bmatrix} 0 & 0 & \cdots & 0 & -f_n \\ 1 & 0 & \cdots & 0 & -f_{n-1} \\ 0 & 1 & \cdots & 0 & -f_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -f_1 \end{bmatrix},$$

and clearly the matrices associated to θ^i, for $i \geq 1$ equal Θ^i respectively. This is particularly useful if one needs to analyze the magnitude of this matrices in terms of some norms. More precisely, if we let $\|\cdot\|$ denote any sub-multiplicative matrix norm, which can be for example Frobenius norm $\|\cdot\|_2$, ([24]) then

$$\|\Theta^i\| \leq \|\Theta\|^i, \quad \text{for any} \quad i > 0. \tag{35}$$

4.2. **Zassenhaus's "Round 2".** We already have every single tool that is needed to write down, and analyze an algorithm for computing the maximal order of a number field K. Although its correctness follows immediately from the results presented so far, we give some comments at the end, as well as we refer to the corresponding theorems. We will also give some general estimation on the running time and the magnitude of data that one needs to deal with.

As usual, suppose that K is given in terms of monic irreducible polynomial $f \in \mathbb{Z}[X]$, i.e. $K \cong \mathbb{Q}[X]/(f)$. Then, to compute the maximal order $\mathcal{O}_K$, proceed as follows:

1. `[Find any order]` Use the formula (34) to determine the coefficients $a_{ij}^{(k)}$. For each $i = 1,\ldots,n$ set $x_i \leftarrow e_i$ where $e_1,\ldots,e_n$ denotes the canonical basis of $\mathbb{Q}^n$.
2. `[Find the trace form]` For every $i,j = 1,\ldots,n$ set $T_{ij} \leftarrow \sum_{k,l=1}^{n} a_{ij}^{(k)} a_{kl}^{(l)}$.
3. `[Compute the determinant]` This should be done only once, so if you have already been here, proceed to the next step. Otherwise, set $d \leftarrow \det[T_{ij}]_{i,j=1}^{n}$ and find a factorization $d = d_0 e^2$ with d_0 being square-free. Compute the largest square-free divisor of e and denote it by e_0. Find prime divisors $p_1,\ldots,p_t$ of e_0 with $p_i \leq n$. Then, for each $i = 1,\ldots,t$ put p_i on the top of the `stack` . Also put $e_0/(p_1\cdots p_t)$ on the top of `stack` .
4. `[Loop]` If `stack` is empty then finish. Otherwise remove an element from the top of `stack` and denote it by q.

[24] Let us recall, that $\|A\|_2 = (\mathrm{Tr}(A^TA))^{1/2} = (\sum_{ij}|a_{ij}|^2)^{1/2}$.

5a. `[Find nilpotents]` If $q \leq n$, ([25]) then find $l \geq 1$, such that $q^l \geq n$. Furthermore evaluate the matrix $B \in \mathrm{Mat}(n \times n; \mathbb{Z}/q\mathbb{Z})$ associated to the l-th power of Frobenius map $x \mapsto x^{q^l}$. This amounts to solving some linear equations over $\mathbb{Z}/q\mathbb{Z}$, which is a field in this case. Otherwise, i.e. if $q > n$, set $B \leftarrow [T_{ij}]_{i,j=1}^n$.

5b. `[Find nilpotents]` Use Gaussian elimination to find a basis $\overline{y}_1, \ldots, \overline{y}_k \in (\mathbb{Z}/q\mathbb{Z})^n$ of the kernel of matrix B ([26]) modulo q. Since in general, $\mathbb{Z}/q\mathbb{Z}$ may not be a field, the elimination routine may fail, if one is forced to divide by a nonzero element which is not a unit in $\mathbb{Z}/q\mathbb{Z}$. Supposing, that such an element has been found, it is necessarily a zero divisor, and so it gives rise to a nontrivial factorization $q_1 q_2 = q$. In such an instance, put q_1 and q_2 on the top of `stack` , and go back to step 4. Otherwise, i.e. the kernel has been successfully determined, proceed to the next step.

6. `[Find radical]` Let $y_1, \ldots, y_s \in \mathbb{Z}^n$ be any lift of $\overline{y}_1, \ldots, \overline{y}_s$. ([27]) Apply the MLLL algorithm to compute a 2-reduced basis $z_1, \ldots, z_n$ of $\mathbb{Z}$-module generated by $y_1, \ldots, y_k$ and $qe_1, \ldots, qe_n$ with $e_1, \ldots, e_n$ denoting the canonical basis. It is important, to use the standard scalar product induced from $\mathbb{Q}^n$. Note, that it the current context, this scalar product is given in terms of Gram matrix $[\langle x_i, x_j \rangle]_{i,j=1}^n$.

7. `[Big matrix]` For any $i, j = 1, \ldots, n$ find the solution $E_{ij}^{(1)}, \ldots, E_{ij}^{(n)}$ to the system of equations $x_i z_j = \sum_{k=1}^n E_{ij}^{(k)} z_k \in \mathbb{Z}^n$. ([28]) Use $E_{ij}^{(k)}$ to form an $n^2 \times n$ matrix E, with k varying horizontally. Eventually, find a basis $\overline{w}_1, \ldots, \overline{w}_t$ of the kernel of E modulo q, by means of Gaussian elimination. If this routine fails, then find a nontrivial factorization $q = q_1 q_2$, put q_1 and q_2 at the top of the `stack` and go back to step 4. Otherwise, proceed to the next step.

8. `[Multiplier ring]` Let $w_1, \ldots, w_t$ be any lift of $w_1, \ldots, w_t$. Apply the MLLL algorithm to find a 2-reduced basis $r_1, \ldots, r_n$ (use the scalar product given by the Gram matrix $[\langle x_i, x_j \rangle]_{i,j=1}^n$) of the $\mathbb{Z}$-module generated by $w_1, \ldots, w_t, qe_1, \ldots, qe_n$ with $e_1, \ldots, e_n$ denoting to canonical basis.

9. `[Extend the order]` If $r_1, \ldots, r_n \in q\mathbb{Z}^n$, then go back to step 4. ([29]) Otherwise, for any $i, j, k = 1, \ldots, n$ find the (unique!) solution $b_{ij}^{(1)}, \ldots, b_{ij}^{(n)}$ to the system of equations $r_i r_j = \sum_{k=1}^n b_{ij}^{(k)} r_k \in \mathbb{Z}^n$. Then, for any $i, j, k = 1, \ldots, n$ set $a_{ij}^{(k)} \leftarrow b_{ij}^{(k)}/q$, and multiply the matrix $[x_i]_{i=1}^n \in \mathrm{Mat}(n \times n; \mathbb{Q})$ by another matrix $[q^{-1} r_i]_{i=1}^n \in \mathrm{Mat}(n \times n; q^{-1}\mathbb{Z})$ so as to get a basis for the extended order. Finally, put q on the top of the `stack` and go back to step 2.

Observation 4.7. *The algorithm stops after finite number of steps, with an upper bound proportional to $\Delta := \Delta(\mathbb{Z}[\theta])$ (see Example 2.16). Furthermore, the resulting $x_1, \ldots, x_n$ is an integral basis of K, and $a_{ij}^{(k)}$ represents the multiplication structure on $\mathcal{O}_K$.*

Proof. The first assertion follows from the fact, that during the course of algorithm the number $[\mathcal{O}_K : \mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_n] \leq \sqrt{\Delta}$ does not decrease, and the product of all elements

[25] Observe, that q is a prime number in this case. This is due to step 3.

[26] Which is either $[T_{ij}]_{i,j=1}^n$ or, it represents the l-th power of the Frobenius map.

[27] Lets say, that we want the absolute values of coordinates of y_i to be less that $q/2$.

[28] Note, that the system of equations might not have a unique solution modulo q. It seems, that there is no other option, but perform the computations over $\mathbb{Z}$.

[29] Since, the order is already p-maximal for any $p \mid q$.

the `stack` , which is at most $e_0 \leq \sqrt{\Delta}$ (as defined in step 3), does not increase. Moreover, if the algorithm enters a loop in step 9, then at least one of these number changes by a factor > 1. The algorithm may still enter a loop in step 5b or 7 (after a linear algebra failure). If it does, then it is necessarily because a denser factorization of e_0 was found. In particular, the number of times it can happen, does not exceed the number of prime factors of e_0.

The correctness of the output follows form Observation 2.37, Proposition 2.35, Proposition 2.38, which basically state, that the computations we made were correct, ([30]) as well as Theorem 2.34, which says, that once we are no longer able to extend the order with our methods, then it is already maximal. The fact, that $a_{ij}^{(k)}$ represents the multiplication structure on $\mathcal{O}_K$ follows from the definition of $b_{ij}^{(k)}$ and the obvious identity:

$$\frac{r_i}{q} \cdot \frac{r_j}{q} = \sum_{i,j=1}^{n} \frac{b_{ij}^{(k)}}{q} \cdot \frac{r_k}{q}.$$

□

Proposition 4.8. *With the above notation, suppose furthermore, that $N > 0$ satisfies $N > \|\Theta\|_2$, i.e. the Frobenius norm of matrix Θ associated to multiplication by θ (see Remark 4.6), and define $M = n + N^2 + \ldots + N^{2(n-1)}$. Then, during the course of the algorithm, the following conditions remain satisfied:*

$$x_i \Delta \in \mathbb{Z}^n \text{ for any } i = 1, \ldots, n, \tag{36a}$$

$$\sum_{i=1}^{n} \log \|x_i\| \leq \frac{n(n-1)}{4}, \tag{36b}$$

$$\sum_{1 \leq i,j,k \leq n} \log |a_{ij}^{(k)}| \leq \frac{n^3(n-1)^2}{4} + n^3 \log M, \tag{36c}$$

$$\sum_{1 \leq i,j,k \leq n} \log |E_{ij}^{(k)}| \leq \frac{n^3(n-1)^2}{4} + n^3 \log M. \tag{36d}$$

Proof. Let us start by proving the first property. Write A for the order generated by $x_1, \ldots, x_n$. By Proposition 2.13 one has $[A : \mathbb{Z}[\theta]] \mid \Delta$. It follows, that $\Delta \cdot A \subset \mathbb{Z}[\theta]$, and so any element $\Delta \cdot x_i \in \Delta \cdot A$ has integer coefficients, as asserted.

The second inequality follows from the fact, that $x_1, \ldots, x_n$ forms a 2-reduced basis, with respect to the standard scalar product in $\mathbb{Q}^n$. Hence, by Proposition 3.21

$$\|x_1\| \cdots \|x_n\| \leq 2^{n(n-1)/4} d(A) \tag{37}$$

with A denoting $\mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_n \subset \mathbb{Q}^n$. Since

$$1 = d(\mathbb{Z}^n) = [A : \mathbb{Z}^n] d(A), \tag{38}$$

then clearly $d(A) = 1/[A : \mathbb{Z}^n] \leq 1$. After applying logarithms to booth sides of (37) one gets (36b).

Before we prove (36c), let us verify, that for any $x, y \in K$, one has

$$\|xy\| \leq M \|x\| \|y\| = (n + N^2 + \ldots + N^{2(n-1)})^{1/2} \|x\| \|y\| \tag{39}$$

with $\|\cdot\|$ denoting the Euclidean norm in $\mathbb{Q}^n$. To see this, write $x^{(i)}, y^{(i)}$ for the coordinates of x, y in basis $1, \theta, \ldots, \theta^{n-1}$, and let $a_{ij}^{(k)}$ describe the multiplication structure in $\mathbb{Z}[\theta]$ (see

[30] Notice, that the different treating of primes $\leq n$ is due to the hypothesis of Proposition 2.38.

Example 4.5). Then

$$xy = \sum_{i,j=1}^{n} x^{(i)} y^{(j)} \theta^{i-1} \theta^{j-1} = \sum_{k=1}^{n} \left(\sum_{i,j=1}^{n} x^{(i)} y^{(j)} a_{ij}^{(k)} \right) \theta^{k-1}.$$

Inequality (39) now follows from

$$\sum_{i=1}^{n} \sum_{j=1}^{n} x^{(i)} y^{(j)} a_{ij}^{(k)} \leq \sum_{i=1}^{n} x^{(i)} \|y\| \left(\sum_{j=1}^{n} |a_{ij}^{(k)}|^2 \right)^{1/2} \leq \|x\| \|y\| \left(\sum_{i,j=1}^{n} |a_{ij}^{(k)}|^2 \right)^{1/2},$$

and the fact, that $\sum_{i,j,k=1}^{n} |a_{ij}^{(k)}|^2 = n + \sum_{i=1}^{n-1} \|\Theta\|^i$ (see Observation 4.1 and Remark 4.6).

We will now prove (36c). First, let us recall, that the coefficients $a_{ij}^{(k)}$ are evaluated in step 9 as $a_{ij}^{k} \leftarrow b_{ij}^{k}/q$ where, for any $i, j = 1, \ldots, n$, the sequence $b_{ij}^{(1)}, \ldots, b_{ij}^{(n)}$ is the unique solution to the following system of linear equations:

$$r_i r_j = \sum_{k=1}^{n} b_{ij}^{(k)} r_k$$

Denote $d = \det[r_i]_{i=1}^{n}$, and recall, that $r_1, \ldots, r_n$ forms a 2-reduced basis. Then, by Cramer's rule, Hadamard's inequality, (39) and Proposition 3.21 one has

$$|b_{ij}^{k}| \leq \frac{\|r_1\| \cdots \|r_n\|}{|d| \cdot \|r_k\|} \cdot M \|r_i\| \|r_j\| \leq 2^{n(n-1)/4} \cdot \frac{M \|r_i\| \|r_j\|}{\|r_k\|}. \tag{40}$$

Taking product over all $i, j, k = 1, \ldots, n$, we get

$$q^{n^3} \prod_{i,j,k=1}^{n} |a_{ij}^{(k)}| = \prod_{i,j,k=1}^{n} |b_{ij}^{(k)}| \leq 2^{n^4(n-1)/4} \cdot M^{n^3} \cdot (\|r_1\| \cdots \|r_n\|)^{n^2} \leq$$

$$2^{n^4(n-1)/4} \cdot M^{n^3} \cdot (2^{n(n-1)/4} \cdot |d|)^{n^2}$$

We still need to bound $|d|$ in terms of Δ. Again, by Proposition 2.13 we have

$$d = [A : qR] d(A) \leq [A : qR]$$

with $R = \mathbb{Z}q^{-1}r_1 \oplus \ldots \oplus \mathbb{Z}q^{-1}r_n$. Since $qA \subset qR \subset A$, then clearly $[A : qR] \mid [A : qA] = q^n$, and in consequence $|d| \leq q^n$.

We now move to the case of (36d). Since for every $i, y = 1, \ldots, n$, the sequence $E_{ij}^{(1)}, \ldots, E_{ij}^{(n)}$ forms a solution to the system of linear equations (see step 7)

$$x_j z_j = \sum_{k=1}^{n} E_{ij}^{(k)} z_k,$$

then by similar arguments as before

$$|E_{ij}^{(k)}| \leq \frac{\|z_1\| \cdots \|z_n\|}{|d| \cdot \|z_k\|} \cdot M \|x_i\| \|z_j\| \leq 2^{n(n-1)/4} \cdot \frac{M \|x_i\| \|z_j\|}{\|z_k\|} \tag{41}$$

with $d = \det[z_i]_{i=1}^{n}$ this time. The last inequality follows from the fact, that $z_1, \ldots, z_n$ forms a 2-reduced basis. Taking product over all $i, j.k = 1, \ldots .n$ we get

$$\prod_{i,j,k=1}^{n} |E_{ij}^{(k)}| \leq 2^{n^4(n-1)/4} \cdot M^{n^3} \cdot (\|x_1\| \cdots \|x_n\|)^{n^2} \leq 2^{n^4(n-1)/4} \cdot M^{n^3} \cdot (2^{n(n-1)/4} d(A))^{n^2},$$

which is exactly what we needed, since $d(A) \leq 1$. □

Remark 4.9. One can give some upper bounds for the constant N as well as Δ in terms of the magnitude of the polynomial f, which is our only input data. Namely, if one assumes that $\max\{|f_1|,\dots,|f_n|,n-1\} \leq F$, then by $|\Delta(\mathbb{Z}[\theta])| = |\operatorname{res}(f',f)|$ (see Example 2.16), by Hadamard's inequality, and the matrix formula for resultant

$$|\Delta| \leq (1+f_1^2+\ldots+f_n^2)^{(n-1)/2}(n^2+(n-1)^2f_1^2+\ldots+f_n^2)^{n/2} \leq$$
$$F^{2n-1}(n+1)^{(n-1)/2}\left(\frac{n(n+1)(2n+1)}{6}\right).$$

Similarly, due to Remark 4.6, one gets

$$\|\Theta\|^2 = (n-1+f_1^2+\ldots+f_n^2) \leq (n+1)F^2.$$

Remark 4.10. The upper bounds given in (40), and (41) can be used to deal with the problem of solving linear equations over $\mathbb{Z}$ in steps 7 and 9. Namely, one need to finds prime numbers $p_1,\dots,p_t$ with $p_1\cdots p_t > 2|E_{ij}^{(k)}|$ for any $k=1,\dots,n$, which do not divide the determinant of the system. After finding a solution for each p_i separately, one can reconstruct the numbers $E_{ij}^{(k)}$ modulo $p_1\cdot p_t$, by using the Chinese remainder theorem. Since $p_1\cdots p_t > 2|E_{ij}^{(k)}|$, then the integer $E_{ij}^{(k)}$ is already uniquely determined.

Note, that this procedure gives a correct answer, only because we know a priori, that the solution exists. Generally, a solution with rational $E_{ij}^{(k)}$ can not be found in this way, without any further knowledge about denominators.

Also, uniqueness plays an crucial role. Note, that we could not use this technique, to find a basis of a $\mathbb{Z}$-module in terms of its generators. The main obstruction here is that, without additional structure, there are no obvious way to distinguish any particular basis.

Corollary 4.11. *The running time of presented algorithm, would be polynomial modulo step 3, where we need to find the largest square factor, and the largest square-free factor (this problems are actually equivalent) of a potentially large integer. In particular, this implies Chistov's theorem.*

References

[B-L] J. A. Buchmann, H. W. Lenstra, *Approximating rings of integers in number fields*, Journal de Thorie des Nombres de Bordeaux 6 (1995), 221–260

[Ch] A. L. Chistov, *The complexity of constructing the ring of integers of a global field*. Dokl. Akad. Nauk SSSR 306 (1989), 1063–1067; English translation: Soviet Math. Dokl. 39 (1989), 597–600

[C] H. Cohen, *A course in computational algebraic number theory*, Springer 1996, GTM 138

[E] D. Eisenbud, *Commutative algebra; witha a view toward algebraic geometry*, Springer, GTM 150

[LLL] A. K. Lenstra, H. W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515–534

[L1] H. W. Lenstra, *On the calculation of regulators and class numbers of quadratic fields*, Report 80-08, Mathematisch Instituut, Universiteit van Amsterdam

[L2] H. W. Lenstra, *Lattices*, pp. 127–181 in: J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, Mathematical Sciences Research Institute Publications, Cambridge University Press.

[L3] H. W. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. 26 (1995), 211–244

[P] M. Pohst, *A modification of the LLL-algorithm*, J. Symb. Comp. 4 (1987), 123–128

[Sh1] D. Shanks, *Class number, a theory of factorization, and genera*, pp. 415–440 in Proc. Symp. Pure Math. 20 (1969 Institute on number theory), Amer. Math. Soc., Providence 1971

[Sh2] D. Shanks, *The infrastructur of real quadratic field and its applications*, Proc. 1972 number theory conference, Boulder, 1972

[S] P. Stevenhagen *The arithmetic of number rings*, pp. 209–266 in: J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, Mathematical Sciences Research Institute Publications, Cambridge University Press.

[Sch] R. Schoof, *Computing Arakelov class groups*, pp. 447–495 in: J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, Mathematical Sciences Research Institute Publications, Cambridge University Press.