Approximating rings of integers in number fields

J. A. Buchmann and H. W. Lenstra, Jr.

Fachbereich Informatik
Universität des Saarlandes
D–6600 Saarbrücken
Germany
buchmann@cs.uni-sb.de

Department of Mathematics
University of California
Berkeley, CA 94720
U. S. A.
hwl@math.berkeley.edu

Abstract. In this paper we study the algorithmic problem of finding the ring of integers of a given algebraic number field. In practice, this problem is often considered to be well-solved, but theoretical results indicate that it is intractable for number fields that are defined by equations with very large coefficients. Such fields occur in the number field sieve algorithm for factoring integers. Applying a variant of a standard algorithm for finding rings of integers, one finds a subring of the number field that one may view as the "best guess" one has for the ring of integers. This best guess is probably often correct. Our main concern is what can be *proved* about this subring. We show that it has a particularly transparent local structure, which is reminiscent of the structure of tamely ramified extensions of local fields. A major portion of the paper is devoted to the study of rings that are "tame" in our more general sense. As a byproduct, we prove complexity results that elaborate upon a result of Chistov. The paper also includes a section that discusses polynomial time algorithms related to finitely generated abelian groups.

Key words: maximal order, tame extensions, algorithm.

1991 Mathematics subject classification: 11Y16, 11S15.

Acknowledgements. The first author was supported by the Deutsche Forschungsgemeinschaft. The second author was supported by the National Science Foundation under grants No. DMS 90-02939 and 92-24205. The second author is grateful to the Institute for Advanced Study (Princeton), where part of the work on which this paper is based was done.

1. Introduction

In this paper we are concerned with the following problem from algorithmic algebraic number theory: given an algebraic number field K, determine its ring of integers $\mathcal{O}$. Paradoxically, this problem is in practice considered well-solved (cf. [7, Chapter 6] and 7.2 below), whereas a result of Chistov [6] (Theorem 1.3 below) suggests that from a theoretical perspective the problem is intractable. The apparent contradiction is easy to resolve. Namely, all computational experience so far is limited to "small" number fields K, such as number fields that are given as $K = \mathbf{Q}[X]/f\mathbf{Q}[X]$, where $\mathbf{Q}$ is the field of rational numbers and f is an irreducible polynomial of small degree with small integer coefficients. The algorithms that are used for small fields will not always work when they are applied to "large" number fields. Large number fields are already making their appearance in applications of algebraic number theory (see [14]), and the determination of their rings of integers is generally avoided (see [5; 17, 9.4; 9]). The results of the present paper are mainly theoretically inspired, but they may become practically relevant if one wishes to do computations in large number fields.

In accordance with Chistov's result, we shall see that there is currently not much hope to find a good algorithm for the problem of constructing rings of integers. This is true if "good" is taken to mean "running in polynomial time", and it is equally true if, less formally, it is taken to mean "practically usable, also in hard cases". The same applies to the problem of *recognizing* rings of integers, i. e., the problem of deciding whether a given subring of a given algebraic number field K is equal to $\mathcal{O}$.

To appreciate the central difficulty it suffices to look at quadratic fields. If m is an integer that is not a square, then determining the ring of integers of $\mathbf{Q}(\sqrt{m})$ is equivalent to finding the largest square divisor of m. The latter problem is currently considered infeasible. Likewise, the problem of recognizing the ring of integers of a quadratic field is equivalent to the problem of recognizing squarefree integers, which is considered infeasible as well.

In the present paper we obtain some positive results. We shall prove that, even though $\mathcal{O}$ may be hard to determine, one can at least construct a subring B of K that comes "close" to $\mathcal{O}$, that is perhaps even likely to be *equal* to $\mathcal{O}$, that in any case has some of the good properties of $\mathcal{O}$, and that in computational applications of algebraic number theory can probably play the role of $\mathcal{O}$. Before we state our main result we give an informal outline of our approach.

Chistov [6] showed that the problem of determining the ring of integers of a given number field is polynomially equivalent to the problem of determining the largest squarefree divisor of a given positive integer (see Theorem 1.3 below). For the latter problem no good algorithm is known (see Section 7). However, there is a naïve approach that *often* works. It is based on the observation that positive integers with a large repeated prime factor are scarce: for most numbers it is true that all repeated prime factors are small and therefore easy to find. Thus, dividing a given positive integer d by all of its repeated prime factors that are less than a certain upper bound b one finds a number that may have a good chance of being the largest squarefree divisor of d, and that is often the best guess one has. The success probability of this method depends of b and on the way in which d was obtained in the first place. It is, of course, easy to construct numbers d that defeat the algorithm.

One can attempt to determine the ring of integers $\mathcal{O}$ of a given number field K in a similarly naïve manner. One starts from an *order* in K, i. e., a subring A of $\mathcal{O}$ for which the index $\langle \mathcal{O} : A \rangle$ of additive groups is finite; for example, one may take $A = \mathbf{Z}[\alpha]$, where $\alpha \in K$ is an algebraic integer with $K = \mathbf{Q}(\alpha)$. As we shall see, one can determine $\mathcal{O}$ if the largest squarefree divisor m of the discriminant Δ_A of A is known. This result suggests that one can determine a "best guess" for $\mathcal{O}$ by working with the best guess q that one has for m instead of m itself. If, in the course of the computations, the hypothesis that q is squarefree is contradicted because an integer $a > 1$ is found for which a^2 divides q, then one simply replaces q by q/a and one continues as if nothing has happened.

This vague idea can be made perfectly precise. It gives rise to a polynomial time algorithm that, given an order $A \subset K$, produces an order $B \subset K$ containing A as well as a positive integer q. One knows that $B = \mathcal{O}$ if q is squarefree. It will often be considered very likely that q is indeed squarefree, so that one is inclined to *believe* that $B = \mathcal{O}$. Our main concern is what one can *prove* about B without relying on any unproved assumptions regarding q. In particular, we shall prove that B equals $\mathcal{O}$ if *and only if* q is squarefree, and that finding an order in K that properly contains B is equivalent to finding a square

$a^2 > 1$ dividing q.

Our results are derived from a local property of B that we refer to as *tameness* at q. Loosely speaking, B is tame at q if B is trying to resemble a full ring of integers as closely as is possible in view of the fact that q is not known to be squarefree. Tameness is a strong property, which provides us with substantial control over the ring. Before we give the definition we remind the reader of the local structure of full rings of integers.

Let $\mathcal{O}$ be the ring of integers of an algebraic number field, let $\mathbf{p}$ be a maximal ideal of $\mathcal{O}$, and let $\mathcal{O}_{\mathbf{p}}$ be the $\mathbf{p}$-adic completion of $\mathcal{O}$ (see [1, Chapter 10]). Denote by p the unique prime number that belongs to $\mathbf{p}$. If the ramification index $e(\mathbf{p}/p)$ of $\mathbf{p}$ over p equals 1, then $\mathbf{p}$ is said to be *unramified* over p, and in that case $\mathcal{O}_{\mathbf{p}}$ is a local unramified algebra over the ring $\mathbf{Z}_p$ of p-adic integers (see Section 3). Local unramified $\mathbf{Z}_p$-algebras are easy to understand and to classify, and they have a very transparent structure [26, Section 3-2]; for example, they are, just like $\mathbf{Z}_p$ itself, principal ideal domains that have, up to units, only one prime element, namely p. If, more generally, p does not divide $e(\mathbf{p}/p)$, then $\mathbf{p}$ is said to be *tame* over p. In this case there is a local unramified $\mathbf{Z}_p$-algebra T and a unit v of T such that $\mathcal{O}_{\mathbf{p}} \cong T[X]/(X^{e(\mathbf{p}/p)} - vp)T[X] = T[(vp)^{1/e(\mathbf{p}/p)}]$ (see [26, Section 3-4]). Conversely, let p be a prime number, let T be a local unramified $\mathbf{Z}_p$-algebra, let v be a unit of T, and let e be a positive integer that is not divisible by p. Then there is an algebraic number field whose ring of integers $\mathcal{O}$ has a maximal ideal $\mathbf{p}$ containing p for which the ring $T[(vp)^{1/e}]$ is isomorphic to $\mathcal{O}_{\mathbf{p}}$, and then $e(\mathbf{p}/p) = e$. In summary, the rings $T[(vp)^{1/e}]$, which are relatively simple to understand, provide a full description of the completions of the rings of integers of all algebraic number fields at all tame maximal ideals.

In the *wild* case, in which p does divide $e(\mathbf{p}/p)$, the structure of $\mathcal{O}_{\mathbf{p}}$ is somewhat more complicated, but there is fortunately no need for us to consider it: it occurs only if p is small, and small primes can be taken care of directly.

Imitating the above description of $\mathcal{O}_{\mathbf{p}}$ we make the following definition. Let B be an order in a number field, and let q be a positive integer. We call B *tame at* q if for every prime number p dividing q and every maximal ideal $\mathbf{p}$ of B containing p there exist a local unramified $\mathbf{Z}_p$-algebra T, an integer e that is not divisible by p, and a unit u of T such that the $\mathbf{p}$-adic completion $B_{\mathbf{p}}$ of B is, as a $\mathbf{Z}_p$-algebra, isomorphic to $T[X]/(X^e - uq)T[X]$ (see

Section 4). If q is squarefree then p divides q only once; in that case $uq = vp$ for some unit v of T, and we are back at the ring $T[(vp)^{1/e}]$ considered above. However, if p^2 divides q then $T[X]/(X^e - uq)T[X]$ occurs as a ring $\mathcal{O}_{\mathbf{p}}$ as above only in the trivial case that $e = 1$ (cf. 3.5).

One of our main results now reads as follows.

Theorem 1.1. *There is a deterministic polynomial time algorithm that, given a number field K and an order A in K, determines an order B in K containing A and a positive integer q, such that B is tame at q and such that the prime numbers dividing $\langle \mathcal{O} : B \rangle$ are the same as the repeated prime divisors of q; here $\mathcal{O}$ denotes the ring of integers of K.*

This theorem is proved in Section 6, along with the other theorems stated in this introduction. The algorithms referred to in our theorems will be explicitly exhibited.

Clearly, the ring B in Theorem 1.1 equals $\mathcal{O}$ if and only if q is squarefree. Generally we shall see that exhibiting a square $a^2 > 1$ dividing q is, under polynomial transformations, equivalent to finding an order in K that strictly contains B (see Theorem 6.9).

Finding rings of integers is customarily viewed as a local problem, in the sense that it suffices to do it prime-by-prime. Algorithmically, however, the bottleneck is of a global nature: how to *find* the prime numbers that one needs to look at? Once these are known, the problem admits a solution. This is expressed in our next result. If m is an integer, then an order A in K is said to be *maximal at* m if $\gcd(m, \langle \mathcal{O} : A \rangle) = 1$.

Theorem 1.2. *There is a polynomial time algorithm that, given an algebraic number field K, an order A in K, and a squarefree positive integer m, determines an order B in K containing A that is maximal at m.*

From 1.2 we see in particular that if m is prime one can find, in polynomial time, an order in K that is maximal at m. If m is taken to be the product of the primes p for which p^2 divides the discriminant of A, then the order B in Theorem 1.2 equals $\mathcal{O}$.

We next formulate a few complexity results of purely theoretical interest.

Theorem 1.3. *Under polynomial transformations, the following two problems are equivalent:*

(a) *given an algebraic number field K, find the ring of algebraic integers of K;*

(b) *given a positive integer d, find the largest squarefree divisor of d.*

Theorem 1.3 represents a slight improvement over a theorem of Chistov [6], as explained in 6.11. We shall prove that the corresponding recognition problems are also equivalent (Theorem 6.12).

Suppose that an order A in an algebraic number field is given. In the proof of Theorem 1.3 we shall see that, given the largest squarefree divisor of the discriminant Δ_A of A, one can find the ring of integers $\mathcal{O}$ of K in polynomial time. In 6.13 we argue that it is hard to go in the opposite direction: if given $\mathcal{O}$ one can easily find the largest squarefree divisor of Δ_A, then problem 1.3(b) is easy as well. It is possible, however, to compute the largest *square* divisor of Δ_A quickly from $\mathcal{O}$; again it is hard to go in the opposite direction (see 6.14).

If the ring of integers of a number field K is known, then the discriminant of K is easy to compute. One may wonder whether, conversely, it is easy to compute the ring of integers of K from the discriminant of K. In 6.10 we shall see that this is currently not the case. However, we do have the following result.

Theorem 1.4. *There are polynomial time algorithms that given an algebraic number field K and one of* (a), (b), *determine the other:*

(a) *the ring of algebraic integers of K;*

(b) *the largest squarefree divisor of the discriminant of K.*

In the body of the paper we work with orders in products of number fields rather than orders in number fields. This presents no additional difficulty. One may remark, though, that the case of products of number fields can in polynomial time be reduced to the case of a single number field, by the main result of [15]. Also, several of our results are local in the sense that they are directed not at constructing $\mathcal{O}$, but at constructing an order that is maximal at a given integer m, as in Theorem 1.2.

We have refrained from considering more general base rings than the ring $\mathbf{Z}$ of rational integers. Over some base rings, the problem of finding maximal orders is, in substance, equivalent to the problem of resolving singularities of curves (see [24; 25]); but in that context there is a quick algorithm for problem 1.3(b), so that the issues considered in this paper do not arise. It may be interesting to consider base rings that are rings of integers of number fields or, more generally, orders in number fields as produced by our algorithms.

The contents of this paper are as follows. Sections 2, 3 and 4 contain the commutative algebra that we need. No algorithms occur in these sections. In Section 2 we assemble some well-known results concerning orders. Sections 3 and 4 are devoted to the notion of tameness, locally in Section 3 and globally in Section 4. Sections 5 and 6 deal with algorithms. In Section 5 we recall a few basic algorithms for which a convenient reference is lacking; they mostly concern linear algebra over the rings $\mathbf{Z}$ and $\mathbf{Z}/q\mathbf{Z}$, where q is a positive integer. In Section 6 we present the algorithm that underlies the proof of Theorem 1.1. It is a variant of an algorithm for determining maximal orders that is due to Zassenhaus [27; 28]. Section 6 also contains the proofs of the theorems stated above. In Section 7 we discuss the practical repercussions of our results.

For our conventions and notations on commutative algebra we refer to Section 2. For conventions concerning algorithms we refer to Section 5 and to [18].

2. Orders

In this section we establish the notation and terminology concerning rings and orders that we shall use, and we recall a few well-known facts. For background on commutative algebra, see [1].

2.1. *Rings and algebras.* All rings in this paper are supposed to be commutative with a unit element. Ring homomorphisms are supposed to preserve the unit element, and subrings contain the same unit element. By $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{F}_p$ we denote the ring of integers, the field of rational numbers, and the field of p elements, respectively, where p is a prime number. The group of units of a ring R is denoted by R^*. Let R be a ring. An R-module M is called *free* if it is isomorphic to the direct sum of a collection of copies of R; if $R \neq 0$ then the number of copies needed is uniquely determined by M, and it is called the *rank* of M; if $R = 0$, then the rank of M is defined to be 0. If an R-module M is free of finite rank n, then there is a *basis* of M over R, i. e., a collection of n elements $\omega_1, \omega_2, \ldots, \omega_n \in M$ such that for each $x \in M$ there is a unique sequence of n elements $r_1, r_2, \ldots, r_n \in R$ such that

$x = \sum_{i=1}^{n} r_i\omega_i$. By an *$R$-algebra* we mean a ring A together with a ring homomorphism $R \to A$. An R-algebra A is said to admit a *finite basis* if A is free of finite rank when considered as an R-module. If this is the case, then the rank of A as an R-module is called the *degree* of A over R, notation: $[A : R]$.

2.2. *Trace and discriminant.* Let R be a ring and let A be an R-algebra admitting a finite basis $\omega_1, \ldots, \omega_n$. For each $a \in A$, the *trace* $\operatorname{Tr} a$ of a is defined to be the trace of the R-linear map $A \to A$ sending x to ax; so if $a\omega_i = \sum_{j=1}^{n} r_{ij}\omega_j$ with $r_{ij} \in R$, then $\operatorname{Tr} a = \sum_{j=1}^{n} r_{jj}$. The trace Tr is an R-linear map $A \to R$. In case of possible ambiguity, we may write Tr_A or $\operatorname{Tr}_{A/R}$ instead of Tr. The *discriminant* Δ_A or $\Delta_{A/R}$ of A over R is the determinant of the matrix $\left(\operatorname{Tr}(\omega_i\omega_j)\right)_{1\le i,j\le n}$. The discriminant is well-defined only up to squares of units of R. The R-ideal generated by Δ_A is well-defined, and we shall also denote it by Δ_A. If R' is an R-algebra, then $A' = A \otimes_R R'$ is an R'-algebra that also admits a finite basis. The trace function $A' \to R'$ is obtained from the trace function $A \to R$ by base extension, and the notation Tr, Tr_A, $\operatorname{Tr}_{A/R}$ used for the latter will also be used for the former. We have $\Delta_{A'/R'} = \Delta_{A/R}R'$ as ideals.

2.3. *Orders.* Let R be a principal ideal domain, and denote by F the field of fractions of R. An *order over R* is an R-algebra A that admits a finite basis and that satisfies $\Delta_A \neq 0$. An order over $\mathbf{Z}$ is simply called an *order*; equivalently, an order can be defined as a ring without non-zero nilpotent elements of which the additive group is free of finite rank as an abelian group. Let A be an order over R, and write $A_F = A \otimes_R F$. Then A_F is, as an F-algebra, the product of finitely many finite separable field extensions of F. By a *fractional A-ideal* we mean a finitely generated A-submodule of A_F that spans A_F as a vector space over F. If $\mathbf{a}$ and $\mathbf{b}$ are fractional A-ideals, then the *index* $\langle \mathbf{a} : \mathbf{b} \rangle$ of $\mathbf{b}$ in $\mathbf{a}$ is defined to be the determinant of any F-linear map $A_F \to A_F$ that maps $\mathbf{a}$ onto $\mathbf{b}$; the index is an element of F^* that is well-defined only up to units of R. If $\mathbf{b} \subset \mathbf{a}$ then the index belongs to $R - \{0\}$, and if in addition $R = \mathbf{Z}$ then it is, up to sign, equal to the usual index. If $\mathbf{a}$, $\mathbf{b}$ are fractional A-ideals, then we write $\mathbf{a} : \mathbf{b} = \{x \in A_F : x\mathbf{b} \subset \mathbf{a}\}$; this is also a fractional A-ideal. A fractional A-ideal $\mathbf{a}$ is called *invertible* if $\mathbf{ab} = A$ for some fractional A-ideal $\mathbf{b}$; if this is true, then $\mathbf{b} = A : \mathbf{a}$, and $\mathbf{a} = A : \mathbf{b} = A : (A : \mathbf{a})$. An example of a fractional ideal is the *complementary module* $A^\dagger = \{x \in A_F : \mathrm{Tr}(xA) \subset R\}$. If $(\omega_i)_{i=1}^n$ is a basis for A over R, then a basis for $A^\dagger$ over R is given by the *dual basis* $(\omega_i^\dagger)_{i=1}^n$, which is characterized by $\mathrm{Tr}(\omega_i\omega_j^\dagger) = 0$ or 1 according as $i \neq j$ or $i = j$. One has $A \subset A^\dagger$ and $\langle A^\dagger : A\rangle = \Delta_A$. By an *overorder* of A we mean a fractional A-ideal that is a subring of A_F. If $\mathbf{a}$ is a fractional A-ideal, then $\mathbf{a} : \mathbf{a}$ is an overorder of A. Each overorder B of A is an order, and it satisfies $A \subset B \subset B^\dagger \subset A^\dagger$ and $\Delta_A = \Delta_B\langle B : A\rangle^2$. Among all overorders of A there is a unique one that is maximal under inclusion; we shall denote it by $\mathcal{O}$. The ring $\mathcal{O}$ is equal to the integral closure of R in A_F, and it is the product of finitely many Dedekind domains. The discriminant of $\mathcal{O}$ is also called the discriminant of A_F. We call A *maximal* if $A = \mathcal{O}$; this is the case if and only if all fractional A-ideals are invertible. If $m \in R$, then the order A is said to be *maximal at* m if $\gcd(m, \langle\mathcal{O} : A\rangle) = 1$; this happens, for example, if $\gcd(m, \Delta_A) = 1$, because $\langle\mathcal{O} : A\rangle^2$ divides Δ_A. For the same reason, A itself is maximal if and only if it is maximal at Δ_A.

Proposition 2.4. *Suppose that R is a principal ideal domain, that $m \in R$ is a non-zero element, and that A is an order over R. Then there are only finitely many prime ideals $\mathbf{p}$ of A containing m, and they are all maximal. Moreover, if $\mathbf{b}$ denotes the intersection of these prime ideals, then we have:*

(a) *$\mathbf{b}/mA$ is the nilradical of the ring A/mA, and there exists a positive integer t such that $\mathbf{b} \supset mA \supset \mathbf{b}^t$;*

(b) *for each prime ideal $\mathbf{p}$ of A containing m one has $A : \mathbf{p} \not\subset A$;*

(c) *A is maximal at m if and only if $\mathbf{b} : \mathbf{b} = A$.*

Proof. Since A admits a finite basis over the principal ideal domain R, the R-module A/mA is of finite length. Therefore the ring A/mA is an Artin ring. From [1, Chapter 8] it follows that each prime ideal of A/mA is maximal, that there are only finitely many of them, and that their intersection is nilpotent. This proves the first two assertions of 2.4, as well as (a). To prove (b), we note that the annihilator of the prime ideal $\mathbf{p}/mA$ in the Artin ring A/mA is non-zero, so $mA : \mathbf{p}$ properly contains mA. Therefore $A : \mathbf{p}$ properly contains A. To prove (c), first assume that A is maximal at m. From $\langle\mathcal{O} : A\rangle\mathcal{O} \subset A$ and $\gcd(m, \langle\mathcal{O} : A\rangle) = 1$ it follows that for each maximal ideal pR of R dividing m

the localizations A_{pR} and $\mathcal{O}_{pR}$ are equal. Hence the order A_{pR} over R_{pR} is a product of finitely many Dedekind domains, and $\mathbf{b}_{pR}$ is a product of non-zero ideals in those Dedekind domains. Therefore $\mathbf{b}_{pR} : \mathbf{b}_{pR} = A_{pR}$. The same equality also holds for maximal ideals pR of R that do not contain m, since in that case $\mathbf{b}_{pR} = A_{pR}$. It follows that $\mathbf{b} : \mathbf{b} = A$, as required. For the converse, assume that $\mathbf{b} : \mathbf{b} = A$. The maximal ideals $\mathbf{p}$ of A containing m are pairwise coprime, so their intersection $\mathbf{b}$ is equal to their product. Hence if $\mathbf{b} : \mathbf{b} = A$ then all those $\mathbf{p}$ satisfy $\mathbf{p} : \mathbf{p} = A$. We claim that $(A : \mathbf{p})\mathbf{p} = A$ for each $\mathbf{p}$, so that each $\mathbf{p}$ is invertible. If not, then from $\mathbf{p} \subset (A : \mathbf{p})\mathbf{p} \subset A$ and the maximality of $\mathbf{p}$ one derives that $\mathbf{p} = (A : \mathbf{p})\mathbf{p}$, so $A : \mathbf{p} \subset \mathbf{p} : \mathbf{p} = A$, contradicting (b). From the invertibility of all maximal ideals containing m one deduces by induction that all A-ideals that contain a power m^k of m, with $k \geq 0$, are invertible, and the same is then true for all fractional ideals H with $A \subset H \subset m^{-k}A$ for some $k \geq 0$. Apply this to $H = \{x \in \mathcal{O} : m^i x \in A$ for some $i \geq 0\}$. This is a ring, so $HH = H$, and the invertibility of H implies $H = A$. Therefore $\langle \mathcal{O} : A \rangle$ is coprime to m. This proves 2.4.

Remark. Every maximal ideal $\mathbf{p}$ of an order A over a principal ideal domain R that is not a field contains a non-zero element of R, by [1, Corollary 5.8]. So 2.4(b) shows that $A : \mathbf{p} \not\subset A$ for each such $\mathbf{p}$.

Proposition 2.5. *Let A be an order over a principal ideal domain, and let $\mathbf{a}$ be a fractional A-ideal. Then $\mathbf{a}$ is invertible if and only if the overorder $(A : \mathbf{a}) : (A : \mathbf{a})$ of A equals A, and if and only if both $A : (A : \mathbf{a}) = \mathbf{a}$ and $\mathbf{a} : \mathbf{a} = A$.*

Proof. If $\mathbf{a}$ is invertible, then as we saw in 2.3 we have $A : (A : \mathbf{a}) = \mathbf{a}$, and $\mathbf{a} : \mathbf{a} = (\mathbf{a} : \mathbf{a})A = (\mathbf{a} : \mathbf{a})\mathbf{a}(A : \mathbf{a}) = \mathbf{a}(A : \mathbf{a}) = A$; also, $\mathbf{b} = A : \mathbf{a}$ is then invertible as well, so for the same reason we have $(A : \mathbf{a}) : (A : \mathbf{a}) = A$. Next suppose that $\mathbf{a}$ is not invertible. Then the A-ideal $(A : \mathbf{a})\mathbf{a}$ is different from A, so there is a maximal ideal $\mathbf{p}$ of A containing $(A : \mathbf{a})\mathbf{a}$. We have $A : \mathbf{p} \subset A : ((A : \mathbf{a})\mathbf{a}) = (A : \mathbf{a}) : (A : \mathbf{a})$, so from 2.4(b) we see that $(A : \mathbf{a}) : (A : \mathbf{a}) \neq A$. This proves that $\mathbf{a}$ is invertible if $(A : \mathbf{a}) : (A : \mathbf{a}) = A$. Applying this to $\mathbf{b} = A : \mathbf{a}$, we find that $\mathbf{b}$ is invertible if $A : \mathbf{b} = \mathbf{a}$ and $\mathbf{a} : \mathbf{a} = A$, and then its inverse $\mathbf{a}$ is invertible as well. This proves 2.5.

2.6. *Gorenstein rings.* Let A be an order over a principal ideal domain. We call A a *Goren-*

stein ring if $A:(A:\mathbf{a})=\mathbf{a}$ for every ideal $\mathbf{a}$ of A that contains a non-zero-divisor of A or, equivalently, for every fractional A-ideal $\mathbf{a}$. It is an easy consequence of [3, Theorem (6.3)] that this is, for orders over principal ideal domains, equivalent to the traditional notion. Note that A is a Gorenstein ring if it is a maximal order. The converse is not true (cf. 2.8).

Proposition 2.7. *Let A be an order over a principal ideal domain R, with complementary module $A^\dagger$. Then the following properties are equivalent:*

(a) *A is a Gorenstein ring;*

(b) *for any fractional A-ideal $\mathbf{a}$, we have $\mathbf{a}:\mathbf{a}=A$ if and only if $\mathbf{a}$ is invertible;*

(c) *$A^\dagger$ is invertible.*

Proof. From 2.5 and the definition of a Gorenstein ring it is clear that (a) implies (b). To prove that (b) implies (c), it suffices to prove that $A^\dagger : A^\dagger = A$. Generally, put $\mathbf{a}^\dagger = \{x \in A_F : \mathrm{Tr}(x\mathbf{a}) \subset R\}$ for any fractional A-ideal $\mathbf{a}$, where A_F is as in 2.3. Using dual bases one easily proves that $\mathbf{a}^{\dagger\dagger}=\mathbf{a}$, and from the definitions one sees that $\mathbf{a}^\dagger = A^\dagger : \mathbf{a}$. Applying this to $\mathbf{a}=A^\dagger$ one obtains $A^\dagger : A^\dagger = A$, as required. Finally, we prove that (c) implies (a). Suppose that $A^\dagger$ is invertible, and let $\mathbf{a}$ be a fractional ideal. Applying the equality $\mathbf{a}^\dagger = A^\dagger : \mathbf{a}$ twice we find that $\mathbf{a}=\mathbf{a}^{\dagger\dagger}=A^\dagger:(A^\dagger:\mathbf{a})$. We need to prove that this equals $A:(A:\mathbf{a})$. If $\mathbf{b}=A:A^\dagger$ denotes the inverse of $A^\dagger$, then we have $A^\dagger:\mathbf{a}=(A:\mathbf{b}):\mathbf{a}=A:(\mathbf{ab})=(A:\mathbf{a}):\mathbf{b}=(A:\mathbf{a})A^\dagger$ and $A^\dagger:(A^\dagger:\mathbf{a})=A^\dagger:((A:\mathbf{a})A^\dagger)=(A^\dagger:A^\dagger):(A:\mathbf{a})=A:(A:\mathbf{a})$. This proves 2.7.

2.8. *Example.* Let R be a principal ideal domain and let $f\in R[X]$ be a monic polynomial with non-vanishing discriminant. Then $A=R[X]/fR[X]$ is an order over R, and if we write $\alpha=(X \bmod f)\in A$ then $A^\dagger=f'(\alpha)^{-1}A$ (cf. [26, Proposition 3-7-12]). This shows that $A^\dagger$ is invertible, so 2.7 implies that A is a Gorenstein ring. It is well-known that A is not necessarily maximal.

Proposition 2.9. *Let R be an Artin ring, let L be a free R-module of finite rank, and let $N\subset L$ be a submodule. Then N is free over R if and only if L/N is free over R.*

Proof. Since each Artin ring is a product of finitely many local Artin rings, the proof immediately reduces to the case that R is local. It is convenient to use a few properties of *projective modules*, which can be found in [12, Chapter 1, Section 1]. First suppose that L/N is free. Then the exact sequence $0 \to N \to L \to L/N \to 0$ splits, so N is projective, and therefore free. For the converse, assume that N is free. Let $\mathbf{m}$ be the maximal ideal of R, and let $a \in R$ a non-zero element annihilated by $\mathbf{m}$. Then $\mathbf{m}N = \{x \in N : ax = 0\} = N \cap \{x \in L : ax = 0\} = N \cap (\mathbf{m}L)$, so $N/\mathbf{m}N$ is a subspace of the $R/\mathbf{m}$-vector space $L/\mathbf{m}L$. Supplementing an $R/\mathbf{m}$-basis of $N/\mathbf{m}N$ to one for $L/\mathbf{m}L$ and applying Nakayama's lemma one finds a surjection $N \oplus R^n \to L$, where $n = \operatorname{rank} L - \operatorname{rank} N$. Comparing the lengths of the two modules we see that it is an isomorphism. Hence $L/N \cong R^n$. This proves 2.9.

3. Tame algebras over the p-adic integers

This section and the next one are devoted to a study of *tameness*, which is one of the central notions of this paper.

We let in this section p be a prime number, and we denote by $\mathbf{Z}_p$ the ring of p-adic integers. We call a $\mathbf{Z}_p$-algebra T *local* if T is local as a ring with a residue class field of characteristic p. A local $\mathbf{Z}_p$-algebra T is said to be *unramified* if $T \cong \mathbf{Z}_p[Y]/g\mathbf{Z}_p[Y]$ for some monic polynomial $g \in \mathbf{Z}_p[Y]$ for which $(g \bmod p) \in \mathbf{F}_p[Y]$ is irreducible. Equivalently, a local unramified $\mathbf{Z}_p$-algebra is the integral closure of $\mathbf{Z}_p$ in a finite unramified extension of the field $\mathbf{Q}_p$ of p-adic numbers (see [26, Section 3-2]).

Throughout this section, q denotes a non-zero element of $p\mathbf{Z}_p$. Let S be a $\mathbf{Z}_p$-algebra. If S is local, then we call S *tame at* q if there exist a local unramified $\mathbf{Z}_p$-algebra T, a positive integer e that is not divisible by p, and a unit $u \in T^*$, such that $S \cong T[X]/(X^e - uq)T[X]$ as $\mathbf{Z}_p$-algebras. In general, we call S *tame at* q if S is the product of finitely many local $\mathbf{Z}_p$-algebras that are tame at q.

If q is a *prime* element of $\mathbf{Z}_p$ then tameness at q is equivalent to the traditional notion, as expressed by the following result.

Proposition 3.1. *Suppose that $q \in p\mathbf{Z}_p$, $q \notin p^2\mathbf{Z}_p$, and let S be a $\mathbf{Z}_p$-algebra. Then S is local and tame at q if and only if S is isomorphic to the integral closure of $\mathbf{Z}_p$ in a finite tamely ramified field extension of $\mathbf{Q}_p$.*

Proof. This follows from the description of tamely ramified extensions given in [26, Sections 3-2, 3-3, 3-4].

We now prove various properties of $\mathbf{Z}_p$-algebras that are tame at q.

Proposition 3.2. *Let T be a local unramified $\mathbf{Z}_p$-algebra, let e be a positive integer that is not divisible by p, and let $u \in T^*$ be a unit. Let further $S = T[X]/(X^e - uq)T[X] = T[\pi]$, where $\pi = (X \bmod X^e - uq)$. Then S is local and tame at q, and its maximal ideal is generated by p and π. Further, the residue class field k of S is the same as that of T, and it satisfies $[k : \mathbf{F}_p] = [T : \mathbf{Z}_p] = [S : \mathbf{Z}_p]/e$.*

Proof. It is easy to see that the S-ideal $pS + \pi S$ is maximal and that its residue class field k is the same as the residue class field T/pT of T. Conversely, let $\mathbf{p} \subset S$ be a maximal ideal. Since S is integral over $\mathbf{Z}_p$, we have $\mathbf{p} \cap \mathbf{Z}_p = p\mathbf{Z}_p$ (see [1, Corollary 5.8]), so $p \in \mathbf{p}$. Also, from $\pi^e = uq \in \mathbf{p}$ it follows that $\pi \in \mathbf{p}$. This implies that $\mathbf{p} = pS + \pi S$, and that S is local. The fact that S is tame at q follows from the definition of tameness. The relations between the degrees follow from $[T/pT : \mathbf{Z}_p/p\mathbf{Z}_p] = [T : \mathbf{Z}_p]$ and $[S : T] = e$. This proves 3.2.

Proposition 3.3. *Let T, e, u, S and π be as in 3.2, and let* Tr *be the trace function of S over $\mathbf{Z}_p$. Then we have:*

(a) *the complementary module $S^\dagger$ of S over $\mathbf{Z}_p$ is given by $S^\dagger = \pi q^{-1} S$, and $S^\dagger/S$ is as a $\mathbf{Z}_p$-module isomorphic to the direct sum of $[k : \mathbf{F}_p](e-1)$ copies of $\mathbf{Z}_p/q\mathbf{Z}_p$.*

(b) $\Delta_{S/\mathbf{Z}_p} = q^{[k:\mathbf{F}_p](e-1)}\mathbf{Z}_p$;

(c) *the S-ideal $\mathbf{a} = \{x \in S : \mathrm{Tr}(xS) \subset q\mathbf{Z}_p\}$ satisfies $\mathbf{a} = \pi S$, $\mathbf{a}^e = qS$, and $S/\mathbf{a}$ is as a $\mathbf{Z}_p/q\mathbf{Z}_p$-module free of rank $[k : \mathbf{F}_p]$;*

(d) *for each positive integer i the $\mathbf{Z}_p/q\mathbf{Z}_p$-module $(\mathbf{a}^{i-1} + qS)(\mathbf{a}^{i+1} + qS)/(\mathbf{a}^i + qS)^2$ is free, and its rank equals 0 for $i \neq e$ and $[k : \mathbf{F}_p]$ for $i = e$.*

Proof. Since T is unramified over $\mathbf{Z}_p$, we have $T^\dagger = T$. Combining this with $\mathrm{Tr} = \mathrm{Tr}_T \circ \mathrm{Tr}_{S/T}$ one finds that $S^\dagger$ is also the complementary module of S over T. A T-basis of S is given by $1, \pi, \pi^2, \ldots, \pi^{e-1}$. A straightforward computation shows that the dual basis is given by e^{-1}, $(euq)^{-1}\pi^{e-1}$, $(euq)^{-1}\pi^{e-2}$, $(euq)^{-1}\pi$, and this is a basis for $\pi q^{-1}S$. Hence $S^\dagger = \pi q^{-1}S$, which is the first assertion of (a). Another T-basis for $S^\dagger$ is given by $1, q^{-1}\pi$, $q^{-1}\pi^2, \ldots, q^{-1}\pi^{e-1}$, from which it follows that $S^\dagger/S$ is, as a T-module, isomorphic to the direct sum of $e-1$ copies of T/qT. Since T/qT is free of rank $[k:\mathbf{F}_p]$ over $\mathbf{Z}_p/q\mathbf{Z}_p$ this implies the last assertion of (a).

To prove (b) it suffices, by 2.3, to compute the determinant of a $\mathbf{Z}_p$-linear map that maps $S^\dagger$ onto S (for example, multiplication by π^{e-1}). This is left to the reader. For (c) we note that $\mathbf{a} = (qS^\dagger) \cap S = \pi S \cap S = \pi S$, so $\mathbf{a}^e = \pi^e S = qS$ and $S/\mathbf{a} = S/\pi S \cong T/qT$; the last isomorphism follows from $S = T[X]/(X^e - uq)T[X]$. Finally, from (c) we obtain that $\mathbf{a}^i + qS = \pi^{\min\{e,i\}} S$ for any positive integer i, so $(\mathbf{a}^{i-1} + qS)(\mathbf{a}^{i+1} + qS)/(\mathbf{a}^i + qS)^2 = 0$ if $i \neq e$ and $(\mathbf{a}^{e-1} + qS)(\mathbf{a}^{e+1} + qS)/(\mathbf{a}^e + qS)^2 = \pi^{2e-1}S/\pi^{2e}S \cong S/\pi S = S/\mathbf{a}$, which implies (d). This proves 3.3.

3.4. *Remark.* Let S be a local $\mathbf{Z}_p$-algebra that is tame at q, and let k be its residue class field. We shall call $[k:\mathbf{F}_p]$ the *residue class field degree* of S over $\mathbf{Z}_p$. From 3.2 it follows that T and e are uniquely determined by S. Namely, T is, as a local unramified $\mathbf{Z}_p$-algebra, determined by its residue class field, which is k. Using Hensel's lemma one can show that T is even uniquely determined as a subring of S (cf. the construction of T in the proof of 3.7). Next, e is determined by $e = [S:\mathbf{Z}_p]/[k:\mathbf{F}_p]$. We shall call e the *ramification index* of S over $\mathbf{Z}_p$. If $e > 1$, then from 3.3(a) it follows that the ideal $q\mathbf{Z}_p$ is also uniquely determined by S. Hence a local $\mathbf{Z}_p$-algebra that is not unramified cannot be tame at two values of q that are not divisible by the same power of p. From 3.3(c) one can deduce that, for $e > 1$, not only the ideal $q\mathbf{Z}_p$ but also the set uqT^{*e} is uniquely determined by S. Conversely, S is clearly determined by T, e and uqT^{*e}.

Proposition 3.5. *Let the notation be as in 3.2, and let the positive integer g be such that $q\mathbf{Z}_p = p^g\mathbf{Z}_p$. Denote by $\tilde{S}$ be the integral closure of S in $S \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Then we have $\tilde{S} = \sum_{i=0}^{e-1} T\pi^i p^{-[gi/e]}$, and $qp^{-1}\tilde{S} \subset S$. Further, $\tilde{S}$ is equal to S if and only if $e = 1$ or $q \notin p^2\mathbf{Z}_p$. We have $\Delta_{\tilde{S}/\mathbf{Z}_p} = p^{[k:\mathbf{F}_p](e-\gcd(g,e))}\mathbf{Z}_p$, and this equals (1) if and only if g is divisible by e.*

Proof. We first prove the expression for $\tilde{S}$ under the added assumption that T contains a primitive eth root of unity ζ. In that case, there is a T-algebra automorphism σ of S with $\sigma\pi = \zeta\pi$, and σ generates a group Γ of order e. The action of Γ on S extends to an action of Γ on $S \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and on $\tilde{S}$. We consider the structure of $\tilde{S}$ as a module over the group ring $T[\Gamma]$. From $e \not\equiv 0 \bmod p$ it follows that there is an isomorphism of T-algebras $T[\Gamma] \to T^e = T \times T \times \ldots \times T$ that sends σ to $(\zeta^i)_{i=0}^{e-1}$. Therefore $\tilde{S}$ is, as a $T[\Gamma]$-module, the direct sum of modules $\tilde{S}_i$, $0 \le i < e$, where $\tilde{S}_i = \{x \in \tilde{S} : \sigma x = \zeta^i x\}$. We have $\pi^i \in \tilde{S}_i$, so σ acts as the identity on $\pi^{-i}\tilde{S}_i$, and therefore $\pi^{-i}\tilde{S}_i$ is contained in the field $T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Because T is unramified over $\mathbf{Z}_p$, any T-submodule of that field is determined by the integral powers of p that it contains; so it remains to see which powers of p belong to $\pi^{-i}\tilde{S}_i$. For $j \in \mathbf{Z}$, we have $p^j \in \pi^{-i}\tilde{S}_i$ if and only if $\pi^i p^j$ is integral over S, if and only if its eth power $(uq)^i p^{ej}$ is integral over S, if and only if $ej \ge -gi$, if and only if $j \ge -[gi/e]$. This shows that $\pi^{-i}\tilde{S}_i = p^{-[gi/e]}T$, as required.

Next we prove the expression for $\tilde{S}$ in the general case. From $e \not\equiv 0 \bmod p$ it follows that there exists a local unramified $\mathbf{Z}_p$-algebra T' containing T that contains a primitive eth root of unity. Apply the above to $S' = S \otimes_T T'$, and use that $\tilde{S}$ equals the intersection of $S \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ with the integral closure of S' in $S' \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. This leads to the desired result.

From $[gi/e] < g$ we see that $qp^{-1}\tilde{S} = p^{g-1}\tilde{S} \subset S$. We have $\tilde{S} = S$ if and only if $[gi/e] = 0$ for $0 \le i \le e-1$, if and only if $g(e-1) < e$, if and only if $g = 1$ or $e = 0$. This proves the second statement of 3.5.

The formula for the discriminant follows by an easy computation from 3.3(b) and the formula $\Delta_{\tilde{S}/\mathbf{Z}_p} = \Delta_{S/\mathbf{Z}_p}/\langle \tilde{S} : S\rangle^2$ from 2.3. The last assertion is obvious. This proves 3.5.

Let now S be a $\mathbf{Z}_p$-algebra that is tame at q but that is not necessarily local. Then S is the product of the localizations $S_{\mathbf{p}}$ of S at its maximal ideals $\mathbf{p}$, of which there are only finitely many, and each $S_{\mathbf{p}}$ is a local $\mathbf{Z}_p$-algebra that is tame at q. We shall denote the residue class field degree and the ramification index of $S_{\mathbf{p}}$ over $\mathbf{Z}_p$ by $f(\mathbf{p})$ and $e(\mathbf{p})$, respectively.

Proposition 3.6. *Let S be a $\mathbf{Z}_p$-algebra that is tame at q, and put $\mathbf{a} = \{x \in S : \mathrm{Tr}(xS) \subset q\mathbf{Z}_p\}$, where Tr is the trace of S over $\mathbf{Z}_p$. Denote by $\tilde{S}$ the integral closure of S in $S \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Then $S/\mathbf{a}$ is free as a $\mathbf{Z}_p/q\mathbf{Z}_p$-module, and we have*

(a) $\Delta_{S/\mathbf{Z}_p} = q^{\sum_{\mathbf{p}} f(\mathbf{p})(e(\mathbf{p})-1)}\mathbf{Z}_p = q^{[S:\mathbf{Z}_p]-[S/\mathbf{a}:\mathbf{Z}_p/q\mathbf{Z}_p]}\mathbf{Z}_p$;

(b) *for each positive integer i the $\mathbf{Z}_p/q\mathbf{Z}_p$-module $(\mathbf{a}^{i-1} + qS)(\mathbf{a}^{i+1} + qS)/(\mathbf{a}^i + qS)^2$ is free of rank $\sum_{\mathbf{p},\, e(\mathbf{p})=i} f(\mathbf{p})$;*

(c) *if $\mathbf{a} = qS$, then $\Delta_{S/\mathbf{Z}_p} = (1)$ and $\tilde{S} = S$;*

(d) *if* $\mathbf{a} \neq qS$, *then* q *divides* $\Delta_{S/\mathbf{Z}_p}$, *we have* $qp^{-1}\tilde{S} \subset S$, *and* $\tilde{S}$ *equals* S *if and only if* $q \notin p^2\mathbf{Z}_p$;

(e) *if* e *denotes the least common multiple of the numbers* $e(\mathbf{p})$, *with* $\mathbf{p}$ *ranging over the maximal ideals of* S, *then we have* $\Delta_{\tilde{S}/\mathbf{Z}_p} = (1)$ *if and only if* $q\mathbf{Z}_p$ *is the* e*th power of an ideal of* $\mathbf{Z}_p$.

Proof. The ideal $\mathbf{a}$ is the product of the similarly defined ideals $\mathbf{a_p}$ of the rings $S_\mathbf{p}$. By 3.3(c), each of the $\mathbf{Z}_p/q\mathbf{Z}_p$-modules $S_\mathbf{p}/\mathbf{a_p}$ is free, so the same is true for $S/\mathbf{a}$. To prove (a), we may likewise assume that S is local, in which case it suffices to apply 3.3(b), 3.2, and 3.3(c). In the same way (b) follows from 3.3(d). If $\mathbf{a} = qS$, then we have $[S : \mathbf{Z}_p] - [S/\mathbf{a} : \mathbf{Z}_p/q\mathbf{Z}_p] = 0$, which implies the first statement of (c); the second follows by 2.3. Next suppose that $\mathbf{a} \neq qS$. Then we have $[S : \mathbf{Z}_p] - [S/\mathbf{a} : \mathbf{Z}_p/q\mathbf{Z}_p] > 0$, which implies the first statement of (d). Also, for at least one $\mathbf{p}$ one has $[S_\mathbf{p} : \mathbf{Z}_p] - [S_\mathbf{p}/\mathbf{a_p} : \mathbf{Z}_p/q\mathbf{Z}_p] > 0$, which means that $e_\mathbf{p} > 1$. Since S is integrally closed in $S \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ if and only if each $S_\mathbf{p}$ is integrally closed in $S_\mathbf{p} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, it now follows from 3.5 that this is also equivalent to $q \notin p^2\mathbf{Z}_p$. This proves (d). Finally, (e) follows from the last statement of 3.5. This proves 3.6.

The main result of this section enables us to recognize whether a given $\mathbf{Z}_p$-algebra is tame at q, provided that it has sufficiently small degree over $\mathbf{Z}_p$.

Theorem 3.7. *Let* p *be a prime number, and let* $q \in p\mathbf{Z}_p$, $q \neq 0$, *where* $\mathbf{Z}_p$ *denotes the ring of* p*-adic integers. Let further* S *be a* $\mathbf{Z}_p$*-algebra that admits a finite basis, with* $[S : \mathbf{Z}_p] < p$. *Put* $\mathbf{a} = \{x \in S : \mathrm{Tr}(xS) \subset q\mathbf{Z}_p\}$, *where* Tr *is the trace of* S *over* $\mathbf{Z}_p$. *Then* S *is tame at* q *if and only if* $\mathbf{a} : \mathbf{a} = S$ *and both* $\mathbf{a}/qS$ *and* $(S : \mathbf{a})/S$ *are free as* $\mathbf{Z}_p/q\mathbf{Z}_p$*-modules.*

Proof. We first remark that by 2.9, applied to $R = \mathbf{Z}_p/q\mathbf{Z}_p$, $L = S/qS$, and $N = \mathbf{a}/qS$, the $\mathbf{Z}_p/q\mathbf{Z}_p$-module $\mathbf{a}/qS$ is free if and only if $S/\mathbf{a}$ is. Hence we may replace $\mathbf{a}/qS$ by $S/\mathbf{a}$ in the statement of Theorem 3.7.

For the proof of the "only if" part we may assume that S is not only tame at q but also local, as in the proof of 3.6. Then by 3.3(c) we have $\mathbf{a} = \pi S$, so $\mathbf{a} : \mathbf{a} = S$. Also, $S/\mathbf{a}$ is free over $\mathbf{Z}_p/q\mathbf{Z}_p$, by 3.3(c), and the same applies to $(S:\mathbf{a})/S = \pi^{-1}S/S \cong S/\pi S = S/\mathbf{a}$. This proves the "only if" part.

Next we prove the "if" part. Assume that $\mathbf{a}:\mathbf{a} = S$ and that both $S/\mathbf{a}$ and $(S:\mathbf{a})/S$ are free as $\mathbf{Z}_p/q\mathbf{Z}_p$-modules. We first reduce to the case that S is local. Since S is free of finite rank as a $\mathbf{Z}_p$-module, we may identify S with the projective limits of the rings S/p^nS, $n \geq 0$. From 2.4(a) we know that there is a positive integer t such that $\prod_{\mathbf{p}} \mathbf{p} \supset pS \supset \prod_{\mathbf{p}} \mathbf{p}^t$, where $\mathbf{p}$ ranges over the prime ideals of S containing p. It follows that the system of ideals $(p^nS)_{n=1}^{\infty}$ is cofinal with the system of ideals $(\prod_{\mathbf{p}} \mathbf{p}^n)_{n=1}^{\infty}$, so that S is also the projective limit of the rings $S/\big(\prod_{\mathbf{p}} \mathbf{p}^n\big)$. For each n, the ideals $\mathbf{p}^n$ are pairwise coprime, so $S/\big(\prod_{\mathbf{p}} \mathbf{p}^n\big) \cong \prod_{\mathbf{p}} S/\mathbf{p}^n$. Hence if we let $S_{\mathbf{p}}$ denote the projective limit of the rings $S/\mathbf{p}^n$, $n \geq 0$, then we have an isomorphism $S \cong \prod_{\mathbf{p}} S_{\mathbf{p}}$ of $\mathbf{Z}_p$-algebras, the product extending over the prime ideals $\mathbf{p}$ of S containing p. In addition, each $S_{\mathbf{p}}$ is local, and it is actually the localization of S at $\mathbf{p}$. As a $\mathbf{Z}_p$-module, each $S_{\mathbf{p}}$ is a direct summand of S, so it is free, with $[S_{\mathbf{p}}:\mathbf{Z}_p] \leq [S:\mathbf{Z}_p] < p$. Also, the assumptions on $\mathbf{a}$ carry over to each $S_{\mathbf{p}}$. Since S is tame if each of the $S_{\mathbf{p}}$ is, we conclude that we may assume that S is local, which we do for the remainder of the proof.

Denote by $\mathbf{p}$ the maximal ideal of S. As above, we have $\mathbf{p} \supset pS \supset \mathbf{p}^t$ for some positive integer t, and S is $\mathbf{p}$-adically complete.

We first prove that $\mathbf{p} = pS + \mathbf{a}$. From $[S:\mathbf{Z}_p] < p$ it follows that $\operatorname{Tr} 1 = [S:\mathbf{Z}_p]\cdot 1 \notin q\mathbf{Z}_p$, so $1 \notin \mathbf{a}$. This implies that $\mathbf{a} \subset \mathbf{p}$, so $pS + \mathbf{a} \subset \mathbf{p}$. To prove the other inclusion, we first note that the definition of $\mathbf{a}$ gives rise to an exact sequence

$$0 \to \mathbf{a}/qS \to S/qS \to \operatorname{Hom}(S/\mathbf{a}, \mathbf{Z}_p/q\mathbf{Z}_p) \to 0$$

of $\mathbf{Z}_p/q\mathbf{Z}_p$-modules, the third arrow mapping $x \bmod qS$ to the map sending $y \bmod \mathbf{a}$ to $\operatorname{Tr}(xy) \bmod q\mathbf{Z}_p$; this arrow is surjective because $S/\mathbf{a}$ and $\operatorname{Hom}(S/\mathbf{a}, \mathbf{Z}_p/q\mathbf{Z}_p)$ are free of the same rank over $\mathbf{Z}_p/q\mathbf{Z}_p$ and hence have the same cardinality. Since $S/\mathbf{a}$ is $\mathbf{Z}_p/q\mathbf{Z}_p$-free, we have a natural isomorphism

$$\operatorname{Hom}(S/\mathbf{a}, \mathbf{Z}_p/q\mathbf{Z}_p) \otimes_{\mathbf{Z}_p/q\mathbf{Z}_p} \mathbf{F}_p \cong \operatorname{Hom}((S/\mathbf{a}) \otimes_{\mathbf{Z}_p/q\mathbf{Z}_p} \mathbf{F}_p, \mathbf{F}_p) = \operatorname{Hom}(S/(pS+\mathbf{a}), \mathbf{F}_p).$$

Hence if we tensor the above exact sequence with $\mathbf{F}_p$ we obtain an exact sequence

$$\mathbf{a}/(qS + p\mathbf{a}) \to S/pS \to \operatorname{Hom}(S/(pS+\mathbf{a}), \mathbf{F}_p) \to 0$$

of $\mathbf{F}_p$-vector spaces. From this sequence we deduce that $\mathbf{p} \subset pS + \mathbf{a}$, as follows. Let $x \in \mathbf{p}$. We have $\mathbf{p}^t \subset pS$, so for any $y \in S$ the multiplication-by-xy map $S/pS \to S/pS$ is nilpotent and has therefore trace 0 when considered as an $\mathbf{F}_p$-linear map. This implies that $x \bmod pS$ belongs to the kernel of the map $S/pS \to \mathrm{Hom}(S/(pS+\mathbf{a}), \mathbf{F}_p)$. This kernel equals the image of $\mathbf{a}/(qS + p\mathbf{a})$, so that $x \in pS + \mathbf{a}$. This completes the proof of the equality $\mathbf{p} = pS + \mathbf{a}$.

The next step in the proof is the construction of an unramified subring T of S that has the same residue class field as S. Let $k = S/\mathbf{p}$ be the residue class field of S, and let T be the unique unramified local $\mathbf{Z}_p$-algebra with residue class field $T/pT \cong k$. If $T \cong \mathbf{Z}_p[Y]/g\mathbf{Z}_p[Y]$, then by Hensel's lemma g has a zero in S (see [1, Exercise 10.9]); at this point we use that S is $\mathbf{p}$-adically complete. This gives a $\mathbf{Z}_p$-algebra homomorphism $T \to S$, which makes S into a T-algebra. Let e be the dimension of S/pS as a vector space over $T/pT = k$. By Nakayama's lemma there is a surjective T-linear map $T^e \to S$. We have $e \cdot [T : \mathbf{Z}_p] = e \cdot [k : \mathbf{F}_p] = [S/pS : \mathbf{F}_p] = [S : \mathbf{Z}_p]$, so comparing $\mathbf{Z}_p$-ranks we see that the map $T^e \to S$ must be injective. This implies in particular that the map $T \to S$ is injective. Hence we may view T as a subring of S, and S is free of rank e as a T-module.

In the definition of $\mathbf{a}$ we may now replace $\mathbf{Z}_p$ by T, i.e., we have $\mathbf{a} = \{x \in S : \mathrm{Tr}_{S/T}(xS) \subset qT\}$, where $\mathrm{Tr}_{S/T}$ is the trace map for the extension $T \subset S$. This is an immediate consequence of the formula $\mathrm{Tr} = \mathrm{Tr}_{T/\mathbf{Z}_p} \circ \mathrm{Tr}_{S/T}$ and the fact that $qT = \{x \in T : \mathrm{Tr}_{T/\mathbf{Z}_p}(xT) \subset q\mathbf{Z}_p\}$; the last equality holds because T is unramified over $\mathbf{Z}_p$.

Any T/qT-module N that is finitely generated and free as a $\mathbf{Z}_p/q\mathbf{Z}_p$-module is also free as a T/qT-module, the rank being $[T : \mathbf{Z}_p]$ times as small; one proves this by lifting a k-basis of N/pN to a T/qT-basis of N, in the same way as we proved above that S is free as a T-module. Hence the hypotheses on $\mathbf{a}$ now imply that $S/\mathbf{a}$ and $(S : \mathbf{a})/S$ are free as T/qT-modules. The rank of $S/\mathbf{a}$ over T/qT can be computed over the residue class field; using that $pS + \mathbf{a} = \mathbf{p}$ we find that $[S/\mathbf{a} : T/qT] = [S/(pS + \mathbf{a}) : T/pT] = [k : k] = 1$, so the natural map $T/qT \to S/\mathbf{a}$ is an isomorphism.

Next we prove that $\mathbf{a}$ is invertible. From $\mathbf{a} \subset \mathbf{p}$ and 2.4(b) we see that $S : \mathbf{a} \neq S$, so the module $(S : \mathbf{a})/S$ is non-zero. Also, it is free over $T/qT = S/\mathbf{a}$, so the annihilator of $(S : \mathbf{a})/S$ in $S/\mathbf{a}$ is zero. This means that $S : (S : \mathbf{a}) = \mathbf{a}$. From our hypothesis $\mathbf{a} : \mathbf{a} = S$

and 2.5 it now follows that $\mathbf{a}$ is invertible, so $\mathbf{a}(S:\mathbf{a}) = S$.

We deduce that $\mathbf{a}$ is principal. Namely, choose $\rho \in \mathbf{a}$ with $\rho(S : \mathbf{a}) \not\subset \mathbf{p}$. Then $1 \in \rho(S:\mathbf{a})$, and multiplying by $\mathbf{a}$ we find $\mathbf{a} \subset \rho S$. Since we also have $\rho S \subset \mathbf{a}$ this proves that $\mathbf{a} = \rho S$.

We claim that $S = T[\rho]$. To see this, we first note that $T[\rho]$ is local with maximal ideal $\mathbf{p}' = \mathbf{p} \cap T[\rho]$. This follows from the fact that S is integral over $T[\rho]$ and local. Next, from $T/qT \cong S/\mathbf{a} = S/\rho S$ we see that $S = T + \rho S$ and therefore $S = T[\rho] + \mathbf{p}'S$. Applying Nakayama's lemma to the $T[\rho]$-module S we now see that $S = T[\rho]$.

Let $f \in T[X]$ be the characteristic polynomial of ρ over T. Then f is a monic polynomial of degree e, and $f(\rho) = 0$. Hence there is a surjective T-algebra homomorphism $T[X]/fT[X] \to T[\rho] = S$ sending X mod f to ρ, and comparing ranks over T we see that this is an isomorphism.

We show that f is an "Eisenstein polynomial at q", i. e., if we write $f = \sum_{i=0}^{e} a_i X^{e-i}$ then $a_j \in qT$ for $0 < j < e$ and $a_e \in qT^*$. We have

$$T/qT \cong S/\mathbf{a} = T[\rho]/\rho T[\rho] \cong T[X]/(fT[X] + XT[X]) \cong T/f(0)T = T/a_e T,$$

and therefore $a_e \in qT^*$. For each positive integer i, the element $p_i = \mathrm{Tr}_{S/T}(\rho^i)$ of T belongs to $\mathrm{Tr}_{S/T}\, \mathbf{a}$ and therefore to qT. Hence Newton's formulas, which assert that $ja_j + \sum_{i=1}^{j} p_i a_{j-i} = 0$ for $1 \le j \le e$, imply that $ja_j \in qT$ for $1 \le j \le e$. From $p > [S : \mathbf{Z}_p] \ge e$ it now follows that $a_j \in qT$.

The next step is to modify ρ so that its eth power becomes a unit times q. From $f(\rho) = 0$ and the fact that f is Eisenstein at q we see that $\rho^e = -\sum_{i=1}^{e} a_i \rho^{e-i} \in -a_e(1 + \rho S)$. Hensel's lemma and the fact the $\gcd(e, p) = 1$ imply that each element of $1 + \rho S$ is an eth power in S^*. Hence there exists $v \in S^*$ such that $\pi = \rho v$ satisfies $\pi^e = -a_e$, which equals uq for some $u \in T^*$.

Since π is, just as ρ, a generator of the ideal $\mathbf{a}$, anything that we proved for ρ applies to π as well. In particular, there is a monic polynomial $h \in T[X]$ of degree e such that there is an isomorphism $T[X]/hT[X] \cong S$ of T-algebras that maps X mod h to π. Then $X^e - uq$ is divisible by h, and comparing degrees and leading coefficients we see that $X^e - uq = h$. Therefore $S \cong T[X]/(X^e - uq)T[X]$, and S is tame at q. This proves Theorem 3.7.

Remark. With only minor changes, the results of this section and their proofs can be carried over to the case that $\mathbf{Z}_p$ and q are replaced by a one-dimensional noetherian complete local ring R and an element q of the maximal ideal of R that is not a zero-divisor; in 3.1, 3.5, and 3.6(c, d, e) it should in addition be required that R is regular, so that it is a complete discrete valuation ring.

4. Tame orders

Let A be an order and let q be a positive integer. For a prime number p, we write $A_p = A \otimes_{\mathbf{Z}} \mathbf{Z}_p$. We call A *tame at* q if for each prime number p dividing q the $\mathbf{Z}_p$-algebra A_p is tame at q in the sense of the previous section. Note that, as in the third paragraph of the proof of Theorem 3.7, one has $A_p \cong \prod_{\mathbf{p}} A_{\mathbf{p}}$, where $\mathbf{p}$ ranges over the prime ideals of A containing p and $A_{\mathbf{p}}$ denotes the completion of A at $\mathbf{p}$; this implies that the present definition of "tame" coincides with that given in the introduction.

We denote by $\mathcal{O}$ the maximal overorder of A, as in 2.3, and by Tr the trace of A over $\mathbf{Z}$.

Proposition 4.1. *Let A be an order and let q be a positive integer with the property that each prime dividing q exceeds $[A : \mathbf{Z}]$. Put $\mathbf{a} = \{x \in A : \mathrm{Tr}(xA) \subset q\mathbf{Z}\}$. Suppose that both $\mathbf{a}/qA$ and $(A : \mathbf{a})/A$ are free when considered as $\mathbf{Z}/q\mathbf{Z}$-modules, and that $\mathbf{a} : \mathbf{a} = A$. Then A is tame at q. In addition, we have:*

(a) *if $\mathbf{a} = qA$, then $\gcd(q, \Delta_A) = 1$ and A is maximal at q;*

(b) *if $\mathbf{a} \neq qA$, then q divides Δ_A, and the primes dividing $\gcd(q, \langle \mathcal{O} : A \rangle)$ are those that appear at least twice in q.*

Proof. Let p be a prime dividing q. One easily verifies that $\mathbf{a}_p = \mathbf{a} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ may be identified with the ideal $\{x \in A_p : \mathrm{Tr}(xA_p) \subset q\mathbf{Z}_p\}$ of A_p, and that $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ may be identified with the integral closure of A_p in $A_p \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Proposition 4.1 now follows immediately from Theorem 3.7 and Proposition 3.6, applied to $S = A_p$.

Proposition 4.2. *Let A be an order, let $q > 1$ be an integer dividing Δ_A, and suppose that A is tame at q. Put $\mathbf{a} = \{x \in A : \mathrm{Tr}(xA) \subset q\mathbf{Z}\}$. Then there exists an integer h with $2 \leq h \leq [A : \mathbf{Z}]$ for which the $\mathbf{Z}/q\mathbf{Z}$-module $(\mathbf{a}^{h-1} + qA)(\mathbf{a}^{h+1} + qA)/(\mathbf{a}^h + qA)^2$ is* *non-zero; if for some such h that module is actually free over $\mathbf{Z}/q\mathbf{Z}$, and $\gcd(q, \Delta_{\mathcal{O}}) = 1$, then q is an hth power.*

Proof. Let p be a prime number dividing q, and let $\mathbf{a}_p = \mathbf{a} \otimes_{\mathbf{Z}} \mathbf{Z}_p \subset A_p$. Since p divides Δ_A, it divides $\Delta_{A_p/\mathbf{Z}_p}$. Applying 3.6(a) we see that there exists a maximal ideal $\mathbf{p}$ of A_p with $e(\mathbf{p}) > 1$. By 3.6(b), we have $(\mathbf{a}_p^{h-1} + qA_p)(\mathbf{a}_p^{h+1} + qA_p)/(\mathbf{a}_p^h + qA_p)^2 \neq 0$ for $h = e(\mathbf{p})$, so also $(\mathbf{a}^{h-1} + qA)(\mathbf{a}^{h+1} + qA)/(\mathbf{a}^h + qA)^2 \neq 0$. This implies the first assertion, since $2 \leq h \leq [A : \mathbf{Z}]$.

Next let h be a positive integer for which $M = (\mathbf{a}^{h-1} + qA)(\mathbf{a}^{h+1} + qA)/(\mathbf{a}^h + qA)^2$ is a free non-zero $\mathbf{Z}/q\mathbf{Z}$-module, and suppose that $\gcd(q, \Delta_{\mathcal{O}}) = 1$. Let p again be a prime number dividing q. Tensoring M with $\mathbf{Z}_p$ we see that the $\mathbf{Z}_p/q\mathbf{Z}_p$-module $(\mathbf{a}_p^{h-1} + qA_p)(\mathbf{a}_p^{h+1} + qA_p)/(\mathbf{a}_p^h + qA_p)^2$ is free of positive rank. Thus $e(\mathbf{p}) = h$ for some maximal ideal $\mathbf{p}$ of A_p, by 3.6(b). Since p does not divide $\Delta_{\mathcal{O}/\mathbf{Z}}$, we have $\Delta_{\mathcal{O}_p/\mathbf{Z}_p} = (1)$, so by 3.6(e) the ideal $q\mathbf{Z}_p$ is the hth power of an ideal of $\mathbf{Z}_p$. This means that the number of factors p in q is divisible by h. Because p is arbitrary, this implies that q is an hth power. This proves 4.2.

The following result describes a natural class of examples of tame orders.

Proposition 4.3. *Let $f \in \mathbf{Z}[X]$ be a monic polynomial of which the discriminant Δ is non-zero, and let q be the largest divisor of Δ that is not divisible by any prime number $p \leq \deg f$. Put $A = \mathbf{Z}[X]/f\mathbf{Z}[X] = \mathbf{Z}[\alpha]$, where $\alpha = (X \bmod f)$. Then A is tame at q if and only if $A/f'(\alpha)A$ has an element of additive order q.*

Remark. Note that the order of $A/f'(\alpha)A$ equals $|\Delta|$, which is divisible by q. The proposition asserts that A is tame at q if and only if the exponent of $A/f'(\alpha)A$ is divisible by q as well. This condition is satisfied, for example, if $A/f'(\alpha)A \cong \mathbf{Z}/\Delta\mathbf{Z}$.

Proof. Let p be a prime number dividing q, and put $A_p = A \otimes_{\mathbf{Z}} \mathbf{Z}_p$. As we saw in 2.8, the complementary module $A_p^\dagger$ of A_p over $\mathbf{Z}_p$ is given by $A_p^\dagger = f'(\alpha)^{-1}A_p$, and the order of $A_p^\dagger/A_p$ equals that of $\mathbf{Z}_p/q\mathbf{Z}_p$. Assume now first that A is tame at q. Then by 3.3(a) the $\mathbf{Z}_p/q\mathbf{Z}_p$-module $A_p^\dagger/A_p$ is free, and the rank must be 1. It follows that we have $A_p/f'(\alpha)A_p \cong \mathbf{Z}_p/q\mathbf{Z}_p$. Since this is true for each prime number p dividing q one concludes that $A/f'(\alpha)A$ contains an element of order q. This proves the "only if" part.

For the "if" part, assume that $A/f'(\alpha)A$ contains an element of order q. Then we have $A_p^\dagger/A_p \cong A_p/f'(\alpha)A_p \cong \mathbf{Z}_p/q\mathbf{Z}_p$. Hence the ideal $\mathbf{a}_p = \{x \in A_p : \mathrm{Tr}(xA_p) \subset q\mathbf{Z}_p\}$ is given by $\mathbf{a}_p = (qA_p^\dagger) \cap A_p = qA_p^\dagger = qf'(\alpha)^{-1}A_p$. Then we have $\mathbf{a}_p/qA_p = qA_p^\dagger/qA_p \cong A_p^\dagger/A_p \cong \mathbf{Z}_p/q\mathbf{Z}_p$, which is free over $\mathbf{Z}_p/q\mathbf{Z}_p$. Also, because $\mathbf{a}_p$ is principal one has $\mathbf{a}_p : \mathbf{a}_p = A_p$ and $(A_p : \mathbf{a}_p)/A_p \cong A_p/\mathbf{a}_p$, which is free over $\mathbf{Z}_p/q\mathbf{Z}_p$ because of 2.9. From Theorem 3.7 it now follows that the $\mathbf{Z}_p$-algebra A_p is tame at q. Therefore A is tame at q. This proves 4.3.

Proposition 4.4. *Let A be an order, and let q and q' be positive integers dividing Δ_A such that A is tame both at q and at q'. Let p be a prime number dividing* $\gcd(q, q')$. *Then the number of factors p in q equals the number of factors p in q'. Also, the number of factors p dividing the exponent of the finite abelian group $\mathcal{O}/A$ is smaller than the number of factors p in q.*

Proof. The order A_p over $\mathbf{Z}_p$ is tame at q, and because q divides Δ_A not all ramification indices of A_p are equal to 1. Thus by 3.4 the ideal $q\mathbf{Z}_p$ is uniquely determined by A_p. Therefore we have $q\mathbf{Z}_p = q'\mathbf{Z}_p$. The last assertion follows from 3.6(d). This proves 4.4.

Suppose that the order A is tame at q. If q is not squarefree, then A is not necessarily maximal at q, by 4.1(b), but it does have many agreeable properties that distinguish it from arbitrary orders. These can be deduced from the results of Section 3. For example, each maximal ideal $\mathbf{p}$ of A containing q satisfies $\dim_{A/\mathbf{p}} \mathbf{p}/\mathbf{p}^2 \leq 2$, which means that locally (and even globally) it can be generated by two elements (see 3.2). In geometric terms, this means that all singularities of A are *plane singularities*. The following two propositions mention a few additional properties of orders that are tame at q. Roughly speaking, they express that even though not *all* fractional A-ideals need be invertible, at least *many* of them are (cf. 2.7). Since these results do not play a logical role in the rest of the paper we only sketch their proofs.

Proposition 4.5. *Let A be an order and let q be a positive integer, and suppose that A is tame at q. Put $\mathbf{a} = \{x \in A : \mathrm{Tr}(xA) \subset q\mathbf{Z}\}$, where* Tr *denotes the trace of A over $\mathbf{Z}$. Then all fractional A-ideals that one can obtain from A, $\mathbf{a}$ and qA by applying the operations $+, \cap, \cdot, :, (- \cap \mathbf{Q}) \cdot A$ a finite number of times are invertible, and these ideals form, under multiplication, a finitely generated free abelian group.*

Proof. In the situation of Proposition 3.3—with $\mathbf{Z}$ and A replaced by $\mathbf{Z}_p$ and a local $\mathbf{Z}_p$-algebra S that is tame at q—the corresponding set of ideals is equal to the set $\{\pi^n S : n \in \mathbf{Z}\}$, and the assertions are clear. The reduction of 4.5 to the situation of 3.3 is straightforward. This proves 4.5.

Proposition 4.6. *Let A be an order and let q be a positive integer, and suppose that A is tame at q. Then for each prime number p dividing q the order A_p over $\mathbf{Z}_p$ is a Gorenstein ring. If in addition A is maximal at all prime numbers not dividing q, then A is a Gorenstein ring.*

Proof. In the local situation of 3.3 this follows from 2.7 and the fact that $S^\dagger$ is invertible (3.3(a)). The first assertion follows immediately. If A is maximal at all primes p not dividing q, then A_p is a Gorenstein ring for *all* p. From this it follows in a straightforward way that A itself is a Gorenstein ring. This proves 4.6.

5. Basic algorithms

All algorithms in this section and the next one are deterministic. For a general discussion of basic notions related to algorithms in algebraic number theory we refer to [18, Section 2]. In particular, one finds in [18, 2.9] the definition of the phrase "given an algebraic number field K" that occurs in the theorems formulated in the introduction. In the present section we elaborate upon several points that were only briefly mentioned in [18], and we provide some of the proofs that were left out in [18].

5.1. *Linear algebra* (cf. [18, 2.4]). Let $q \in \mathbf{Z}$, $q > 1$. If q is a prime number, then $\mathbf{Z}/q\mathbf{Z}$ is a field, and the traditional algorithms from linear algebra can be used to do computations with vector spaces over $\mathbf{Z}/q\mathbf{Z}$. We shall see that if q is not necessarily prime, then the same algorithms lead *either* to a non-trivial divisor q' of q *or* to a result that can be interpreted in terms of free modules over $\mathbf{Z}/q\mathbf{Z}$. Here we call a divisor q' of q *non-trivial* if $1 < q' < q$.

As in [18, 2.4], giving a free $\mathbf{Z}/q\mathbf{Z}$-module of finite rank means giving its rank n (in unary). The elements of such a module are encoded as sequences of n elements of $\mathbf{Z}/q\mathbf{Z}$. Homomorphisms between two such modules are encoded as matrices in the usual way. A free submodule of a free module is encoded as a sequence of elements of the free module that is a basis for the submodule. When we write, in this paper, that an algorithm *determines* a submodule of a free module, we will always mean that it determines a *basis* for that submodule. In particular, if an algorithm determines a submodule, then that submodule is free.

Proposition 5.2. *There is a polynomial time algorithm that, given an integer $q > 1$ and a homomorphism f from one free $\mathbf{Z}/q\mathbf{Z}$-module of finite rank to another one, either determines a non-trivial divisor q' of q or determines the kernel of f and the image of f. There is a polynomial time algorithm that, given an integer $q > 1$ and two free submodules of a free $\mathbf{Z}/q\mathbf{Z}$-module of finite rank, either determines a non-trivial divisor q' of q or determines the sum and the intersection of these submodules.*

Proof. An $m \times n$ matrix $H = (h_{ij})$ with entries $h_{ij} \in \mathbf{Z}/q\mathbf{Z}$ is said to be *row reduced* if the following conditions are satisfied: (i) there exists $k \leq m$ such that the ith row of H is zero if and only if $i > k$; (ii) for each $i \leq k$, there exists $j_i \in \{1, 2, \ldots, n\}$ such that $h_{ij_i} = 1$, $h_{ij} = 0$ for $j < j_i$, and $h_{i'j_i} = 0$ for all $i' \neq i$; (iii) $j_i < j_{i'}$ whenever $1 \leq i < i' \leq k$.

Let $H = (h_{ij})$ be a row-reduced $m \times n$ matrix over $\mathbf{Z}/q\mathbf{Z}$, and let $j_1, j_2, \ldots, j_k \in \{1, 2, \ldots, n\}$ be as above. Then one verifies easily that several modules associated to H are free. First of all, the row space of H, which is the submodule of $(\mathbf{Z}/q\mathbf{Z})^n$ generated by the rows of H, is free of rank k, a basis being formed by the non-zero rows of H. Secondly, the column space of H, which is the submodule of $(\mathbf{Z}/q\mathbf{Z})^m$ generated by the columns of H, is likewise free of rank k, a basis being formed by the columns with indices $j_1, j_2, \ldots, j_k$. Thirdly, the nullspace of H, which equals $\{x \in (\mathbf{Z}/q\mathbf{Z})^n : Hx = 0\}$, is free of rank $n - k$, and one obtains a basis by taking, for each $j \in \{1, 2, \ldots, n\} - \{j_1, j_2, \ldots, j_k\}$, the vector whose j_ith coordinate equals $-h_{ij}$, for $1 \leq i \leq k$, whose jth coordinate equals 1, and that is 0 at the remaining $n - k - 1$ positions.

It is well-known from elementary textbooks in linear algebra that, if q is prime, so that $\mathbf{Z}/q\mathbf{Z}$ is a field, there exists for every $m \times n$ matrix H over $\mathbf{Z}/q\mathbf{Z}$ an invertible $m \times m$ matrix U over $\mathbf{Z}/q\mathbf{Z}$ such that UH is row reduced. In addition, given H one can find the row reduced matrix UH by performing the following operations $O(m^2)$ times: (i) interchange two rows; (ii) divide a non-zero row by its first non-zero entry; (iii) add a multiple of one row to another one.

If q is not necessarily prime, the same operations can still be performed, except that (ii) is impossible if the first non-zero entry $a \bmod q$ that one wishes to divide by does not have an inverse. In that case the divisor $q' = \gcd(a, q)$ of q is non-trivial. It follows that there is a polynomial time algorithm that, given q and an $m \times n$ matrix H over $\mathbf{Z}/q\mathbf{Z}$, either determines a non-trivial divisor q' of q or a row reduced matrix that is obtained from H by finitely many applications of the above three operations. Clearly, the matrix that is obtained in the latter case is of the form UH, where U is an invertible $m \times m$ matrix over $\mathbf{Z}/q\mathbf{Z}$.

We can now prove 5.2. Let $f\colon (\mathbf{Z}/q\mathbf{Z})^n \to (\mathbf{Z}/q\mathbf{Z})^m$ be a homomorphism, and let it be given by the $m \times n$ matrix H. Then the image of f is the column space of H, and the kernel of f is the nullspace of H. We can in polynomial time either determine a non-trivial divisor q' of q or a row-reduced matrix of the form UH, with U invertible. Assume that we are in the latter case. As we saw above, we can write down a basis for the nullspace of UH, and this is the same as the nullspace of H. Further, if the columns with indices j_1, $j_2, \ldots, j_k$ form a basis for the column space of UH, then the columns of H with the same indices form a basis for the column space of H.

Determining the sum and intersection of two free submodules V_1, V_2 of $(\mathbf{Z}/q\mathbf{Z})^n$ can be reduced to determining images and kernels, as follows. Let $f\colon V_1 \oplus V_2 \to (\mathbf{Z}/q\mathbf{Z})^n$ be the map that sends (x_1, x_2) to $x_1 + x_2$. Then $V_1 + V_2$ is equal to the image of f, and $V_1 \cap V_2$ is the isomorphic image of the kernel of f under the natural projection $V_1 \oplus V_2 \to V_1$. This proves 5.2.

5.3. *Hermite normal form.* We shall say that an $m \times n$ matrix $H = (h_{ij})$ with entries $h_{ij} \in \mathbf{Z}$ is in *Hermite normal form* if the following conditions are satisfied: (i) there exists $k \leq m$ such that the ith row of H is zero if and only if $i > k$; (ii) for each $i \leq k$, there exists $j_i \in \{1, 2, \ldots, n\}$ such that $h_{ij_i} > 0$, $h_{ij} = 0$ for $j < j_i$, and $0 \leq h_{i'j_i} < h_{ij_i}$ for all $i' < i$; (iii) $j_i < j_{i'}$ whenever $1 \leq i < i' \leq k$. This definition is a little more general than the one commonly found in the literature (see [10]), so as to accommodate matrices of rank less than n. For each $m \times n$ matrix H over $\mathbf{Z}$ there is a unique matrix of the form UH that is in Hermite normal form, and for which U is an invertible $m \times m$-matrix over $\mathbf{Z}$ (however,

U is not necessarily unique); the matrix UH is called the *Hermite normal form* of H.

Proposition 5.4. *There is a polynomial time algorithm that given an $m \times n$ matrix $H = (h_{ij})$ over $\mathbf{Z}$ finds an invertible $m \times m$ matrix U over $\mathbf{Z}$ for which UH is in Hermite normal form.*

Proof. First suppose that H has rank n. In this case the Hermite normal form UH can be found in polynomial time by [10, Theorem 2.1] (applied to the transpose of H), and U can be found in polynomial time as well (see [10, Section 5, end]). To reduce the general case to the case of rank n, we let J be the set of those j, $1 \leq j \leq n$, for which the jth column of H is not a $\mathbf{Q}$-linear combination of the earlier columns. If $J = \{j_1, j_2, \ldots, j_k\}$ with $j_1 < j_2 < \ldots < j_k$, then $k = \operatorname{rank} H$, and j_l is, for each $l \in \{1, 2, \ldots, k\}$, equal to the smallest value of j for which the matrix formed by columns $j_1, \ldots, j_{l-1}, j$ of H has rank l. Since ranks of matrices over $\mathbf{Z}$ can be computed in polynomial time (see [10, Proposition 2.3]), this shows that J can be determined in polynomial time. The $m \times k$ matrix H_J that is formed by columns $j_1, \ldots, j_k$ of H now has rank k, so by the above we can find, in polynomial time, the Hermite normal form UH_J of H_J, as well as the matrix U. It is easy to verify that UH is then also in Hermite normal form. This proves 5.4.

5.5. *Free abelian groups of finite rank* (cf. [18, 2.5]). Giving a free abelian group of finite rank means giving its rank n (in unary). The elements of such a group are encoded as sequences of n integers, and homomorphisms between two such groups are encoded as matrices, in the usual way. A subgroup of a free abelian group of finite rank is itself free, and it is encoded by means of a sequence of elements that is a basis for the subgroup.

Proposition 5.6. *There is a polynomial time algorithm for each of the following problems: given a homomorphism f from one free abelian group of finite rank to another one, find the kernel of f and the image of f; given two subgroups of a free abelian group of finite rank, find the sum and the intersection of these subgroups; given a homomorphism f from one free abelian group of finite rank to another one, and a subgroup L of the latter, find $f^{-1}L$.*

Proof. Let $f: \mathbf{Z}^m \to \mathbf{Z}^n$ be a homomorphism, and let it be given by the transpose of the $m \times n$ matrix H. By 5.4, we can find an invertible $m \times m$ matrix U such that UH is in

Hermite normal form. Then the non-zero rows of UH form a basis for the image of f, and if k is equal to the number of non-zero rows of UH, so that $k = \operatorname{rank} H$, then the last $m-k$ rows of U^{-1} form a basis for the kernel of f. This implies the assertion on finding the kernel and image of f. Finding sums and intersections of subgroups can be reduced to finding kernels and images, as in the proof of 5.2. Finally, let $f\colon F_1 \to F_2$ be a homomorphism, and let $L \subset F_2$ be a subgroup. Denote by $g\colon F_1 \oplus L \to F_2$ the map sending (x, y) to $f(x) - y$. Then $f^{-1}L$ is the isomorphic image of the kernel of g under the projection $F_1 \oplus L \to F_1$. This implies the assertion concerning $f^{-1}L$. This proves 5.6.

5.7. *Orders and fractional ideals.* As in [18, 2.7 and 2.10], an order A will be given by its degree n over $\mathbf{Z}$ and the multiplication map $A \otimes A \to A$. This comes down to specifying a system of n^3 integers a_{ijk} such that $\omega_i\omega_j = \sum_{k=1}^{n} a_{ijk}\omega_k$ for some basis $\omega_1, \omega_2, \ldots, \omega_n$ of A over $\mathbf{Z}$. Note that one can verify in polynomial time whether or not a given system of n^3 integers a_{ijk} encodes an order, by checking the ring axioms and the non-vanishing of the discriminant Δ_A in a straightforward way; here Δ_A is computed directly from its definition (see 2.2). An ideal of an order A will be specified by means of a basis of the ideal over $\mathbf{Z}$, expressed in terms of the given basis of A over $\mathbf{Z}$, as was done for subgroups in 5.5; this may for practical purposes not always be the most efficient representation, but for theoretical purposes it will suffice. To make the representation of an ideal $\mathbf{a}$ unique, we may require that the given basis consists of the rows of a matrix in Hermite normal form. In that case all entries of the matrix are bounded by the index of $\mathbf{a}$ in A. This is often useful if an algorithm deals with many ideals and one wishes to control the growth of the numbers occurring in the algorithm. A fractional ideal $\mathbf{a}$ is given by means of a pair d, $\mathbf{b}$, where d is a positive integer and $\mathbf{b}$ is an ideal of A of finite index; then $\mathbf{a} = d^{-1}\mathbf{b}$. This is unique if we require that d is coprime to the largest integer e for which $\mathbf{b} \subset eA$.

Proposition 5.8. *There are polynomial time algorithms that given an order A and fractional A-ideals $\mathbf{a}_1$, $\mathbf{a}_2$, determine $\mathbf{a}_1 + \mathbf{a}_2$, $\mathbf{a}_1 \cdot \mathbf{a}_2$, $\mathbf{a}_1 \cap \mathbf{a}_2$, and $\mathbf{a}_1 : \mathbf{a}_2$.*

Proof. For sum and intersection this follows directly from Proposition 5.6. The computation of $\mathbf{a}_1 \cdot \mathbf{a}_2$ is easily reduced to the case that $\mathbf{a}_1$, $\mathbf{a}_2$ are contained in A. In that case, $\mathbf{a}_1 \cdot \mathbf{a}_2$ is the image of the multiplication map $\mathbf{a}_1 \otimes \mathbf{a}_2 \to A$, which can be calculated by

Proposition 5.6. The computation of $\mathbf{a}_1 : \mathbf{a}_2$ can be reduced to the case that $\mathbf{a}_2 \supset A \supset \mathbf{a}_1$. In that case, we have $\mathbf{a}_1 : \mathbf{a}_2 \subset A : A = A$, which implies that $\mathbf{a}_1 : \mathbf{a}_2$ is equal to the inverse image of $\mathrm{Hom}(\mathbf{a}_2, \mathbf{a}_1)$ under the map $A \to \mathrm{Hom}(\mathbf{a}_2, \mathbf{a}_2)$ that sends $x \in A$ to the multiplication-by-x map. This inverse image can, again, be calculated by Proposition 5.6. This proves 5.8.

5.9. *Overorders.* Let A be an order, given by integers a_{ijk} as above. Overorders of A and their fractional ideals will be represented as fractional ideals of A itself. Several algorithms in Section 6 compute many overorders of A, and for the complexity analysis of these algorithms it is important to note that the length of the data encoding any overorder B of A is uniformly bounded by a polynomial function of $\sum_{i,j,k} \log(|a_{ijk}|+2)$, i. e., of the length of the data encoding A itself. This follows from what was said above about fractional ideals and the fact that the index of A in B divides Δ_A.

6. Approximating maximal orders

In this section we prove the results stated in the introduction. We begin with an auxiliary algorithm that corresponds to the case that the number m in Theorem 1.2 is a prime number.

Algorithm 6.1. We describe an algorithm that, given an order A and a prime number p, determines an overorder B of A that is maximal at p. The algorithm begins by putting $B = A$. Let t be the least positive integer for which $p^t \geq [A : \mathbf{Z}]$.

Calculate the kernel $\mathbf{b}$ of the $\mathbf{F}_p$-linear map $B/pB \to B/pB$ that sends every $x \in B/pB$ to x^{p^t}, as well as the inverse image $\mathbf{a}$ of $\mathbf{b}$ under the natural map $B \to B/pB$; this can be done by the algorithms of Section 5. Calculate the overorder $B' = \mathbf{a} : \mathbf{a}$ of B (see 5.8). If $B' = B$, then the algorithm stops. If $B' \neq B$, then replace B by B' and iterate. This completes the description of the algorithm.

Proposition 6.2. *Given an order A and a prime number p, Algorithm* 6.1 *determines in polynomial time the unique overorder B of A that is maximal at p and for which $\langle B : A \rangle$ is a power of p.*

Proof. Let B be any overorder of A that is encountered in the algorithm. Then B/pB is a finite ring containing $\mathbf{F}_p$, and we have $[B/pB : \mathbf{F}_p] = [B : \mathbf{Z}] = [A : \mathbf{Z}]$. Let $y \in B/pB$. Then two of the subspaces

$$B/pB \supset y(B/pB) \supset y^2(B/pB) \supset \ldots \supset y^{[A:\mathbf{Z}]}(B/pB) \supset y^{[A:\mathbf{Z}]+1}(B/pB)$$

of B/pB must have the same dimension over $\mathbf{F}_p$ and are therefore equal. Hence there exists i, $0 \le i \le [A : \mathbf{Z}]$, such that $y^i(B/pB) = y^{i+1}(B/pB)$, and this space is then equal to $y^j(B/pB)$ for all $j \ge i$. In particular, y is nilpotent if and only if $y^{[A:\mathbf{Z}]} = 0$, and if and only if $y^{p^t} = 0$. This proves that an element x of B belongs to $\mathbf{a}$ if and only if $(x \bmod pB)$ belongs to the nilradical of B/pB. Therefore $\mathbf{a}$ is an ideal of B containing pB. This implies that $B \subset B' \subset p^{-1}B$, so that $\langle B' : B\rangle$ is a power of p. It follows that either $B' = B$ or $\Delta_{B'} = \Delta_B/p^{2s}$ for some positive integer s. Hence the algorithm goes through at most $(\log|\Delta_A|)/\log(p^2)$ iterations before it stops. From Section 5 one sees that each iteration can be done in polynomial time. Hence the entire algorithm runs in polynomial time. We also find that $\langle B : A\rangle$ is a power of p for each B that occurs in the algorithm.

Let now B be the final overorder that is obtained. Then we have $B = B' = \mathbf{a} : \mathbf{a}$, so by 2.4(c) the order B is maximal at p. From $\gcd(p, \langle \mathcal{O} : B\rangle) = 1$ and the fact that $\langle B : A\rangle$ is a power of p it follows that B/A is the p-primary subgroup of the quotient $\mathcal{O}/A$ of additive groups. This determines B uniquely. This completes the proof of 6.2.

The second auxiliary algorithm corresponds to the case that the number m in Theorem 1.2 is built up from prime numbers that exceed the degree of A over $\mathbf{Z}$, but without the squarefree-ness assumption.

Algorithm 6.3. In this algorithm, an order A and an integer $q > 1$ are given with the property that each prime divisor p of q satisfies $p > [A : \mathbf{Z}]$. The algorithm determines an overorder B of A and a divisor q' of q, such that either q' is non-trivial or B is well-behaved, as expressed in 6.4. The algorithm begins by putting $B = A$.

Let $\mathbf{a}$ be the B-ideal $\{x \in B : \mathrm{Tr}(xB) \subset q\mathbf{Z}\}$, and $\mathbf{b} = \mathbf{a}/qB$. Note that $\mathbf{b}$ is the kernel of the map $B/qB \to \mathrm{Hom}(B/qB, \mathbf{Z}/q\mathbf{Z})$ that sends each $(x \bmod q) \in B/qB$ to the map sending $(y \bmod q)$ to $\mathrm{Tr}(xy) \bmod q$. Use the algorithm of Proposition 5.2 to find a basis of $\mathbf{b}$ over $\mathbf{Z}/q\mathbf{Z}$; this fails only if a non-trivial divisor q' of q is found, in which case the algorithm stops. If it is found that $\mathbf{b} = 0$, then $\mathbf{a} = qB$, and the algorithm stops, with $q' = 1$. Now suppose that $\mathbf{b} \neq 0$, so that $\mathbf{a} \neq qB$. Determine the overorder $B' = \mathbf{a} : \mathbf{a}$ of B (Proposition 5.8). If $B' \neq B$, replace B by B' and iterate. Next suppose that $B' = B$. Determine $B : \mathbf{a}$, and attempt to find a basis of $(B : \mathbf{a})/B$ as a $\mathbf{Z}/q\mathbf{Z}$-module, using the algorithm of Proposition 5.2. If this attempt is not successful, then one has found a non-trivial divisor q' of q, and the algorithm stops. If the attempt is successful, one searches for the smallest integer $h > 1$ for which $(\mathbf{a}^{h-1} + qB)(\mathbf{a}^{h+1} + qB)/(\mathbf{a}^h + qB)^2$ is non-zero (we shall see below that h exists and is at most $[A : \mathbf{Z}]$). Using the algorithm of Proposition 5.2, one attempts to find a basis for $(\mathbf{a}^{h-1} + qB)(\mathbf{a}^{h+1} + qB)/(\mathbf{a}^h + qB)^2$ as a $\mathbf{Z}/q\mathbf{Z}$-module. If this attempt is not successful, then one has found a non-trivial divisor q' of q, and the algorithm stops. If the attempt is successful, one tests whether q is the hth power of an integer; this can be done with Newton's method, or simply by means of a bisection. If this is not the case, then one stops at this point, with $q' = q$. If q is an hth power, then one puts $q' = q^{1/h}$, and the algorithm also stops.

Proposition 6.4. *Given A and q as in Algorithm 6.3, the above method determines in polynomial time a pair B, q' such that $\langle B : A \rangle$ divides a power of q and such that exactly one of (a), (b), (c) is true:*

(a) *q' divides q, and $1 < q' < q$;*

(b) *$q' = 1$, the order B is maximal at q, and $\gcd(q, \Delta_B) = 1$;*

(c) *$q' = q$; the order B is tame at q and has discriminant divisible by q; if $\mathcal{O}$ denotes the maximal overorder of A then $\gcd(q, \Delta_{\mathcal{O}}) > 1$, and the prime numbers dividing $\gcd(q, \langle \mathcal{O} : B \rangle)$ are exactly those that appear at least twice in q; and the order B is maximal at q if and only if q is squarefree.*

Proof. In each iteration of the algorithm, the order B is replaced by a strictly larger one. This implies, as in the proof of 6.2, that the algorithm runs in polynomial time. At each step, $\mathbf{a}$ is a B-ideal containing q, so $B \subset B' \subset q^{-1}B$. Hence each index $\langle B' : B \rangle$ divides a power of q, and the same is then true for the final index $\langle B : A \rangle$.

It is clear that the number q' obtained from the algorithm divides q and satisfies $1 \leq q' \leq q$. Hence if (a) is not satisfied then we have $q' = 1$ or $q' = q$.

First suppose that $q' = 1$. This means that, when the algorithm terminates, we have $\mathbf{a} = qB$. Then $B : \mathbf{a} = q^{-1}B$, so $\mathbf{a}/qB$ and $(B : \mathbf{a})/B$ are both free as modules over $\mathbf{Z}/q\mathbf{Z}$. Also, we have $\mathbf{a} : \mathbf{a} = qB : qB = B$. Hence by 4.1(a) the order B is maximal at q and satisfies $\gcd(q, \Delta_B) = 1$, so we are in case (b).

Next suppose that $q' = q$. Then we have $\mathbf{a} \neq qB$ and $\mathbf{a} : \mathbf{a} = B$, and the $\mathbf{Z}/q\mathbf{Z}$-modules $\mathbf{a}/qB = \mathbf{b}$ and $(B : \mathbf{a})/B$ are free. Hence by 4.1 the order B is tame at q, and by 4.1(b) all assertions of (c) except the one about $\gcd(q, \Delta_{\mathcal{O}})$ are true. By 4.2 the integer h that the algorithm is looking for exists, and it satisfies $h \leq [A : \mathbf{Z}]$. Also, from $q' = q$ it follows that $(\mathbf{a}^{h-1} + qB)(\mathbf{a}^{h+1} + qB)/(\mathbf{a}^h + qB)^2$ is free as a $\mathbf{Z}/q\mathbf{Z}$-module, and that q is not an hth power. By 4.2 this implies that $\gcd(q, \Delta_{\mathcal{O}}) > 1$. This proves Proposition 6.4.

An application of Algorithm 6.3 is considered *successful* if one is in case (b) or (c). If the algorithm is unsuccessful (case (a)), one is inclined to repeat the algorithm first with q' and next with q/q' in the role of q. However, in order to keep the logical structure of the resulting algorithm as clear as possible, it is desirable that once an order B has been made maximal or tame at q, one does not change it "at q" any more. This leads to the problem of refining the factorization $q = q' \cdot q/q'$ to a factorization into pairwise coprime factors. For an extensive discussion of this problem we refer to [2]. In our case the following simple result suffices. We say that an integer a can be *built up* from integers $c_1, \ldots, c_t$ if there exist non-negative integers $n_1, \ldots, n_t$ such that $a = \prod_{i=1}^{t} c_i^{n_i}$.

Proposition 6.5. *There is a polynomial time algorithm that, given two integers a and b with $a > 1$, $b > 1$, computes a collection of pairwise coprime divisors $c_1, \ldots, c_t$ of ab, such that $c_i > 1$ for each i and such that each of a and b can be built up from $c_1, \ldots, c_t$.*

Proof. We first describe the algorithm. It works with finite sequences $c_1, \ldots, c_r$ of positive integers from which a and b can be built up, with the property that $\gcd(c_i, c_j) = 1$ whenever $|i - j| > 1$, and such that there does not exist an index $i < r$ with $c_i = c_{i+1} = 1$. At the beginning of the algorithm the sequence has only the two members a and b. The algorithm proceeds with a given sequence as follows. First it searches for two successive members d, e of the sequence that are both greater than 1. If these cannot be found, then the members of the sequence are pairwise coprime, and the algorithm terminates after deletion of the

1's in the sequence. Next suppose that d, e can be found. Then one uses the Euclidean algorithm to calculate $f = \gcd(d, e)$, and one replaces the terms d, e of the sequence by d/f, f, e/f (in that order). If this creates two successive 1's in the sequence, delete one of them, and do this until no two successive 1's remain. Next one iterates the algorithm on the new sequence; it is easy to see that it satisfies the same conditions as the original one. This completes the description of the algorithm.

The correctness proof of this algorithm is straightforward. To estimate the running time we remark that $\gcd(d, e)$ can be computed in $O((\log d)(\log e))$ steps, for integers $d > 1$, $e > 1$ (cf. [11, Exercise 4.5.2.30]). From this it follows by induction that the running time of the algorithm, when starting with a sequence $c_1, \ldots, c_r$, is $O\big(\sum_{i=1}^{r-1}(\log(c_i c_{i+1}))^2\big)$. For the sequence a, b this is $O((\log(ab))^2)$. This proves 6.5.

We now combine the algorithms above into a single algorithm, which will prove Theorem 1.1.

Algorithm 6.6. In this algorithm, an order A and a positive integer m are given. The algorithm determines an overorder B of A and a collection Q of pairwise coprime divisors > 1 of m such that B and Q have the properties listed in Theorem 6.7. At each stage of the algorithm, one has an overorder B of A. The algorithm begins by putting $B = A$. Also, we put $m_0 = m$.

Step 1. For each prime number $p \leq [A : \mathbf{Z}]$ do the following. Test whether p divides m_0; if it does, apply Algorithm 6.1 to B and p, replace B by the order that one obtains from 6.1, and divide m_0 by the largest power of p that divides it. When all primes $p \leq [A : \mathbf{Z}]$ have been processed, m_0 is equal to the largest divisor of m that is not divisible by any prime number p with $p \leq [A : \mathbf{Z}]$. If now $m_0 = 1$ then the algorithm stops at this point, with $Q = \emptyset$.

In each stage of the remaining part of the algorithm one keeps track of two collections M, Q of pairwise coprime divisors > 1 of m_0; the elements of M are the numbers that need to be processed, and Q consists of the numbers that have been processed. One begins with $M = \{m_0\}$, $Q = \emptyset$.

Step 2. If the set M is empty, the algorithm stops. Next suppose that M is non-empty. Choose an element $q \in M$, and apply Algorithm 6.3 to B and q. Replace B by the order that one obtains from 6.3. Next there are three cases, depending on the value of the number q' that is obtained from 6.3. First suppose that $q' = 1$. In this case, remove q from the set M and iterate Step 2. Next, suppose that $q' = q$. Then transfer q from M to Q, and iterate Step 2. Finally, let it be supposed that $1 < q' < q$. In this case, apply the algorithm of Proposition 6.5 to q' and q/q'. This gives rise to a collection of pairwise coprime divisors $c_1, \ldots, c_t$ of q. Now remove q from M, add each of $c_1, \ldots, c_t$ to M, and iterate Step 2.

This completes the description of the algorithm.

Theorem 6.7. *Given an order A and a positive integer m, Algorithm 6.6 determines in polynomial time an overorder B of A and a set Q of pairwise coprime divisors $q > 1$ of m that have the following properties: all primes dividing $\langle B : A\rangle$ divide m; each $q \in Q$ divides Δ_B; the order B is tame at each $q \in Q$ and maximal at all prime numbers that divide m but not $\prod_{q\in Q} q$; if $\mathcal{O}$ denotes the maximal overorder of A then the prime numbers dividing $\gcd(m, \langle \mathcal{O} : B\rangle)$ are exactly those that appear at least twice in some $q \in Q$, and one has $\gcd(q, \Delta_{\mathcal{O}}) > 1$ for each $q \in Q$; and B is maximal at m if and only if $\prod_{q\in Q} q$ is squarefree.*

Proof. We first show that Algorithm 6.6 runs in polynomial time. By 5.9, all orders B that occur in the algorithm are specified by data of length polynomial in the length of the data specifying A itself, and all numbers p, q, q' are bounded by m. From this and 6.2, 6.4, 6.5 it follows that each time that Algorithm 6.1 or 6.3 or the algorithm of 6.5 is invoked, it runs in time polynomial in the length of the original data. This implies, first of all, that Step 1 runs in polynomial time, since there are at most $[A : \mathbf{Z}]$ values of p to consider. To show that Step 2 runs in polynomial time it suffices to show that the number of iterations is polynomially bounded. Each iteration calls Algorithm 6.3 once, and this call is either successful ($q' \in \{1, q\}$) or not ($1 < q' < q$). If the call is successful, then M is replaced by $M - \{q\}$, which implies that q is coprime to any later value of q for which Algorithm 6.3 is called. This implies that the number of successful calls of Algorithm 6.3 is bounded by the number of distinct prime divisors of m_0. To bound the number of unsuccessful calls of Algorithm 6.3, we consider the quantity $n(M) = \prod_{q\in M} \frac{q}{P(q)}$, where $P(q)$ denotes the largest prime divisor of q. Each time that M is changed in the algorithm, $n(M)$ is replaced by a divisor, and this is a *proper* divisor when the change is made after an unsuccessful call of Algorithm 6.3. Therefore the number of unsuccessful calls of 6.3 is bounded by the total number of prime divisors of m_0, counting multiplicities. Since this is $O(\log m)$, this concludes the proof that the algorithm runs in polynomial time.

Next we prove that the final B and Q have the properties listed in the theorem. The assertion about $\langle B : A\rangle$ is clear from 6.2 and 6.4. Note that Q consists of those numbers q for which Algorithm 6.3 has been called successfully in Step 2 with $q' = q$. As we have just seen, these numbers q are pairwise coprime, and they divide m. Fix $q \in Q$, and let $B_{(q)}$ be the order that was obtained from the corresponding successful call of Algorithm 6.3. Since later calls of 6.3 concern only numbers that are coprime to q, the first assertion of 6.4 implies that $\langle B : B_{(q)}\rangle$ is coprime to q. Also, $B_{(q)}$ has the properties listed in Proposition 6.4(c), and from $\gcd(\langle B : B_{(q)}\rangle, q) = 1$ it then follows easily that B itself has these properties as well. This implies the assertions made in the theorem, except those relating to prime numbers dividing m that do not divide $\prod_{q\in Q} q$. Let p be such a prime number. If $p \leq [A : \mathbf{Z}]$, then in the course of Step 1 an order is obtained that is maximal at p, by 6.2, and the overorder B of this order is then also maximal at p. Next let $p > [A : \mathbf{Z}]$. Then p divides m_0, so at the beginning of Step 2 the number p divides a member of M, but at the end it doesn't, since then $M = \emptyset$. Since the set of primes dividing the elements of M does not change after an unsuccessful call of 6.3, it must have happened that p divides a number q for which 6.3 was called successfully; and since p does not divide $\prod_{q\in Q} q$, this successful call must have led to $q' = 1$. Thus Proposition 6.4(b) implies that it also led to an order that is maximal at p, and the final B, which is an overorder of this order, is then likewise maximal at p. This completes the proof of Theorem 6.7.

Corollary 6.8. *There is a polynomial time algorithm that, given an order A and a positive integer m, decides whether or not $\gcd(m, \Delta_{\mathcal{O}}) = 1$, where $\mathcal{O}$ denotes the maximal overorder of A; in addition, if $\gcd(m, \Delta_{\mathcal{O}}) = 1$, then the algorithm determines an overorder of A that is maximal at m.*

Proof. Run Algorithm 6.6 on A and m to obtain B and Q. If $Q \neq \emptyset$, then $\gcd(m, \Delta_{\mathcal{O}}) > 1$, by 6.7. If $Q = \emptyset$, then B is maximal at m, by 6.7, so $\gcd(m, \Delta_{\mathcal{O}}) = 1$ if and only if $\gcd(m, \Delta_B) = 1$. This proves 6.8.

Theorem 6.9. *There are polynomial time algorithms that, given an order A, a positive integer m dividing Δ_A such that A is tame at m, and one of the following, construct the other:*

(a) *an integer $a > 1$ for which a^2 divides m;*

(b) *an overorder $B \neq A$ of A for which $\langle B : A \rangle$ divides a power of m.*

Proof. First suppose that we know an integer a as in (a). Applying Algorithm 6.6 to A and a we find an overorder B of A and a set Q of divisors of $\gcd(a, \Delta_B)$ with the properties listed in Theorem 6.7 (with a in the role of m). Then B is an overorder of A for which $\langle B : A \rangle$ divides a power of m. We need to prove that $B \neq A$. To this end, let p be a prime number dividing a. We distinguish two cases. First suppose that p does not divide any $q \in Q$. In that case, B is maximal at p, by 6.7, but A is not, by 4.1(b), so $B \neq A$. Next, suppose that p does divide some $q \in Q$. Then p divides q and m to different positive powers, so 4.4 shows that A is not tame at q; but B is tame at q, by 6.7, so $B \neq A$. This shows that (a) can be used to construct (b). For the converse, suppose that a ring B as in (b) is given. Denote by d the exponent of the finite abelian group B/A. From $d\mathbf{Z} = \mathbf{Z} \cap (A : B)$ and Section 5 it follows that d can be computed in polynomial time. From $B \neq A$ we see that $d > 1$. Proposition 4.4 implies that d divides m, and that every prime factor of m divides m/d. Therefore $a = \gcd(d, m/d)$ has the properties in (a). This proves 6.9.

Proof of Theorem 1.1. Consider the following algorithm: given an order A in a number field K, calculate the discriminant m of A, and apply Algorithm 6.6 to A and m to find an order B in K and a finite set Q of integers; let q be the product of the elements of Q.

It is obvious that this algorithm runs in polynomial time. From Theorem 6.7 it follows that B, q have the properties stated in 1.1. This proves Theorem 1.1.

Proof of Theorem 1.2. This is a consequence of Theorem 6.7, since if m is squarefree then so are all its divisors $q \in Q$.

Proof of Theorem 1.4. Let it first be supposed that the ring of integers $\mathcal{O}$ of K is given, and let d be the exponent of the abelian group $\mathcal{O}^\dagger/\mathcal{O}$; note that $d\mathbf{Z} = \mathbf{Z} \cap (\mathcal{O} : \mathcal{O}^\dagger)$, so d can be computed in polynomial time. Since the order of $\mathcal{O}^\dagger/\mathcal{O}$ equals the discriminant Δ

of K, the prime divisors of d are the same as those of Δ. Also, if p is a prime dividing Δ, and $p > [K : \mathbf{Q}]$, then 3.1 and 3.3(a) (applied to $q = p$) imply that p occurs only once in d. Hence if one removes the repeated prime factors $\leq [K : \mathbf{Q}]$ from d one obtains the largest squarefree divisor of Δ.

Next suppose that the largest squarefree divisor m of the discriminant Δ of K is given. As in [18, 2.10], one can construct an order A in K. Using Euclid's algorithm one readily calculates the largest divisor m_1 of Δ_A that is coprime to m. Then $\gcd(m_1, \Delta) = 1$, so by Corollary 6.8 one can calculate, in polynomial time, an overorder B of A that is maximal at m_1. By Theorem 1.2 one can determine, in polynomial time, an overorder of B that is maximal at m. The latter order is maximal at Δ_A, so it is equal to the ring of integers of K. This proves 1.4.

6.10. *Remark.* One may wonder whether there is a polynomial time algorithm that, given K and the discriminant Δ of K, determines the ring of integers $\mathcal{O}$ of K. We argue that such an algorithm is currently beyond reach by showing that it would enable us to factor integers n that are known to be of the form p^2q^3, where p, q are distinct prime numbers; no good algorithm, practically or otherwise, is known for the latter problem.

To prove this, let n be such an integer. To factor n, we may clearly assume that p and q are odd. Let $K = \mathbf{Q}(n^{1/4})$. This is a fourth degree number field, and it is a straightforward exercise to show that its discriminant Δ is of the form $\Delta = -4^h n$ (cf. 3.5), where h is a positive integer that by Theorem 1.2 (with $m = 2$) can be computed in polynomial time. Thus, we can compute Δ. By hypothesis, we can compute $\mathcal{O}$ from Δ in polynomial time, so by Theorem 1.3 we can now determine the largest squarefree divisor $2pq$ of Δ as well. This obviously enables us to factor n completely, which finishes the proof.

Proof of Theorem 1.3. We first reduce (a) to (b). Given an algebraic number field K, one can in polynomial time construct an order A in K (see [18, 2.10]). If the algorithm of Theorem 1.2 is applied with m equal to the largest squarefree divisor of Δ_A, then the overorder B of A determined by the algorithm is maximal at Δ_A and therefore equal to $\mathcal{O}$. Hence $\mathcal{O}$ can be determined in polynomial time if m is known. This shows that (a) can be reduced to (b).

For the opposite reduction, let d be the positive integer of which the largest squarefree divisor is to be found. Determine the least positive integer n for which $(n+1)^n > d$, and the least prime number l not dividing d. Note that both n and l are $O(1 + \log d)$, and that they can be found by a direct search. Let d_0 be the largest divisor of d that is free of prime factors $\leq n$. Since we can deal with the small prime factors directly, it will suffice to determine the largest squarefree divisor of d_0. By Eisenstein's criterion, $X^n - d_0 l$ is irreducible, so $K = \mathbf{Q}((d_0 l)^{1/n})$ is an algebraic number field of degree n. We claim that from the ring of algebraic integers $\mathcal{O}$ of K one can compute, in polynomial time, the largest squarefree divisor of d_0. Namely, there is no prime number p dividing d_0 with the property that the number of factors p in d_0 is divisible by n; this follows from $(n+1)^n > d_0$ and the fact that all primes dividing d_0 are at least $n+1$. By 3.5, this implies that each prime factor p of d_0 divides $\Delta_{\mathcal{O}}$. Hence if we use 1.3 to compute the largest squarefree divisor d_1 of $\Delta_{\mathcal{O}}$, then the largest squarefree divisor of d_0 is given by $\gcd(d_1, d_0)$. This proves 1.3.

6.11. *Remark.* Chistov's reduction of 1.3(b) to 1.3(a) makes use of a sequence of number fields of the form $K = \mathbf{Q}(\sqrt{b})$, where b divides d (see [6]). His reduction is, in the language of [8], a "Turing reduction". Our proof shows that, for a given d, a *single* algebraic number field K suffices. For this reason we used the term "polynomial transformation" in 1.3 (cf. [8]).

Theorem 6.12. *Under polynomial transformations, the following two problems are equivalent:*

(a) *given an algebraic number field K and a subring A of the ring of integers $\mathcal{O}$ of K, decide whether A is equal to $\mathcal{O}$;*

(b) *given a positive integer d, decide whether d is squarefree.*

Proof. We first reduce (a) to (b). Applying the algorithm of Theorem 1.1 to the order A, we find in polynomial time an overorder B of A and a positive integer q. If $B \neq A$, then clearly A is not maximal. If $B = A$, then A is maximal if and only if q is squarefree, by Theorem 1.1. This shows that (a) can be reduced to (b). For the opposite reduction, let d be a positive integer. If $d \equiv 0 \bmod 4$, then d is not squarefree. If $d \equiv 1$ or $2 \bmod 4$, then d is squarefree if and only if the order $A = \mathbf{Z}[\sqrt{-d}]$ equals the ring of algebraic integers of the algebraic number field $K = \mathbf{Q}(\sqrt{-d})$. If $d \equiv 3 \bmod 4$, then d is squarefree if and only if the order $A = \mathbf{Z}[(1 + \sqrt{-d})/2]$ equals the ring of algebraic integers of $K = \mathbf{Q}(\sqrt{-d})$. This shows that (b) can be reduced to (a) and concludes the proof of Theorem 6.12.

6.13. *Remark.* Suppose that an order A in an algebraic number field K is given. As we saw in the proof of 1.3, we can compute the ring of integers $\mathcal{O}$ of K in polynomial time if the largest squarefree divisor m of Δ_A is known. However, computing m from $\mathcal{O}$ is currently intractable. Namely, suppose we had a good algorithm to do this; applying it to $A = \mathbf{Z}[d\sqrt{-1}]$, which has $\Delta_A = -4d^2$ and $\mathcal{O} = \mathbf{Z}[\sqrt{-1}]$, we would then easily find the largest squarefree divisor of an arbitrary positive integer d, for which no good algorithm is known.

6.14. *Remark.* Suppose, again, that an order A in an algebraic number field K is given. Then from $\mathcal{O}$ one can compute, in polynomial time, the largest square dividing Δ_A. This is a fairly straightforward consequence of 1.4 and the fact that $\Delta_A/\Delta_{\mathcal{O}}$ is a square. However, computing $\mathcal{O}$ from the largest square dividing Δ_A is currently intractable. Namely, suppose we had a good algorithm to do this. Let d be an integer that is not divisible by 3 and that is not a cube. The order $A = \mathbf{Z}[d^{1/3}]$ has $\Delta_A = -27d^2$, and the largest square dividing Δ_A is $(3d)^2$. Thus the algorithm could be used to find $\mathcal{O}$. Since A is tame at d we have $\gcd(d, \langle \mathcal{O} : A \rangle) = 1$ if and only if d is squarefree. This would provide an easy squarefreeness test for d, which is not known to exist.

7. Practical considerations

7.1. *Finding largest squarefree divisors.* Theorem 1.3 expresses that finding the ring of integers of a given algebraic number field is essentially equally hard as finding the largest squarefree divisor of a given positive integer. In [13] one finds a discussion of complexity results concerning the latter question. We make here a few remarks that are mostly of a practical nature.

The problem of determining the largest squarefree divisor a of a given positive integer m is a very hard one, and the best methods that are known for its solution are derived from methods for factoring m. When applying factoring methods to this problem, one has to keep in mind that in order to determine a it suffices to know all prime divisors of m up to the *cube* root of m, rather than up to its *square* root. Namely, let $m = n \cdot \prod_p p^{t(p)}$, where p ranges over the primes $\leq m^{1/3}$ dividing m, and n has no prime factor $\leq m^{1/3}$; then $a = n' \cdot \prod_p p$, where $n' = \sqrt{n}$ if n is a square and $n' = n$ otherwise. This leads to the following complexity bounds for the problem of finding the largest squarefree divisor of a given positive integer m, for $m \to \infty$. The best completely proved deterministic algorithm is derived from the "fast factorials" factoring method of Pollard and Strassen (see [22, Section 4]), and it runs in time at most $m^{1/6+o(1)}$. The fastest completely proved probabilistic algorithm is the class group relations method (see [21]), which runs in expected time $L_m[1/2, 1 + o(1)]$, where $L_x[a, b] = \exp\bigl(b(\log x)^a(\log\log x)^{1-a}\bigr)$. The elliptic curve method (see [19]) is conjectured to solve the problem in expected time at most $L_m[1/2, \sqrt{2/3} + o(1)]$, and the number field sieve (see [5]) in time $L_m[1/3, O(1)]$.

In practice, one would apply a variety of factoring methods to m, with a preference for methods that are apt at finding small prime factors, such as the elliptic curve method. For the unfactored part of m one then *hopes* that it is squarefree, this hope being based on the fact that a random integer that has no small prime factors is very likely to be squarefree. It depends, of course, on the way in which the integer m has been obtained in the first place whether the latter fact is relevant at all; for example, in our context one may wonder to which extent discriminants of random polynomials can be viewed as random integers for this purpose. See also the remarks make in [16, Section 2].

Any algorithm for finding the largest squarefree divisor of a given positive integer can clearly also be used for recognizing squarefree integers. There is not much else that we know about the latter problem. One can prove that an integer $m > 4$ is squarefree if there exists a positive integer n with $\gcd(n, m) = 1$ such that $a^n \equiv 1 \bmod m$ for all positive integers a with $a < (\log m)^2$ (cf. [20, Theorem 2]). However, such a value for n does not exist for each squarefree m; if it does exist it may be hard to find; and once it has been found it is very likely—though unproved—that it can be used to factor m completely. For numbers that are not squarefree the situation is even worse: any numerical evidence that we can think of that would imply that a specific number m is not squarefree can be used to readily find a non-trivial square factor of m. As an example, we mention the following. If A is a $\mathbf{Z}/m\mathbf{Z}$-algebra that admits a finite basis and for which Δ_A is a unit (for example,

A may be equal to $\mathbf{Z}/m\mathbf{Z}$ itself), and A contains a nilpotent element x with $x \neq 0$, then one can prove that m is not squarefree; and indeed there exists a deterministic polynomial time algorithm that, given such A and x, finds a non-trivial square factor of m.

7.2. *Finding the ring of integers.* Suppose that one is given an algebraic number field K, and that one wishes to approximate its ring of integers $\mathcal{O}$. Elaborating upon a procedure sketched in the introduction, we describe how one might, in principle, proceed in practice. Let A be the largest order in K that one knows; this is often an order of the form $\mathbf{Z}[\alpha]$, with $\alpha \in K$, but depending on additional information that is available about K one may know a larger order that is possibly not of this form. Next, one determines a sequence q_1, q_2, ..., q_t of positive integers with the property that $\prod_{i=1}^{t} q_i$ is divisible by each prime number p for which p^2 divides Δ_A; in addition, one tries to make $\sum_{i=1}^{t} q_i$ as small as possible. If one knows the complete prime factorization of $|\Delta_A|$ one can simply let the q_i be the prime numbers that appear at least twice in Δ_A, but in general one isn't so lucky. Of course, it is always possible to take $t = 1$, $q_1 = |\Delta_A|$, but in many cases one can do better. For example, one can determine the complementary module $A^\dagger$ (see 2.3), write the finite abelian group $A^\dagger/A$ of order $|\Delta_A|$ as $\bigoplus_{i=1}^{t} \mathbf{Z}/d_i\mathbf{Z}$ where d_{i+1} divides d_i for $1 \leq i < t$, and put $q_i = d_i/d_{i+1}$, where $d_{t+1} = 1$. Also, one may profit from non-trivial factors of Δ_A that one happens to know, either from known properties of K or from attempts to factor $|\Delta_A|$. In order to try and improve a sequence q_1, q_2, ..., q_t, one can apply a factoring algorithm to the q_i. Using the algorithm of 6.5 one can achieve that the q_i are pairwise coprime. It is easy to see that one may also assume that none of the q_i is a square or a higher power of an integer. Let it now be supposed that q_1, q_2, ..., q_t are as above, and that any attempt to improve the sequence—i.e., to decrease $\sum_{i=1}^{t} q_i$—has failed. Then one applies Algorithm 6.6 successively to all q_i, and one ultimately obtains an overorder B of A as well as a set Q of pairwise coprime integers $q > 1$, with each $q \in Q$ dividing $\gcd(q_i, \Delta_B)$ for some i, such that B is tame at $\prod_{q \in Q} q$ and maximal at all prime numbers not dividing that product. This is as close to $\mathcal{O}$ as one gets: one can only *hope* that $B = \mathcal{O}$ or, equivalently, that all $q \in Q$ are squarefree; this hope is fulfilled if all q_i are squarefree. In any case, B is a Gorenstein ring, and many ideals of B are invertible, by 4.5 and 4.6. If it is later discovered that some $q \in Q$ has a non-trivial square factor, then by Theorem 6.9 one can enlarge B.

There are cases in which the original order A is never enlarged during the entire procedure. Suppose, for example, that $A = \mathbf{Z}[\alpha] \neq \mathbf{Z}$ and that $A^\dagger/A$ is cyclic of order $|\Delta_A|$. Then one can show that Δ_A is odd and that it is not a square. If in fact Δ_A has no small prime factors and is not a higher power of an integer either, then none of the methods mentioned above is likely to improve the sequence given by $t = 1$, $q_1 = |\Delta_A|$. The order A is tame at q_1 (cf. 4.3), and it can be argued that in these circumstances Algorithm 6.6 is unlikely to enlarge A.

The procedure described above may lead to an order that is not guaranteed to be the maximal order. Whether it can nevertheless be used for the purpose one has in mind clearly depends on what that purpose is. Two things may happen. The first is, that during any subsequent calculations that one performs with the order, the hypothesis that it is the maximal order is never contradicted. In this case, one may be able to show that the same conclusions can be drawn from these calculations that one could draw if the order were known to be maximal. For this to be feasible, it is obviously desirable that much of our theoretical and algorithmic knowledge of maximal orders be extended to more general orders. This has been done for orders in quadratic fields (cf. [4; 21]). Orders in general number fields have been less thoroughly studied (cf. [23; 5, Section 7]).

The second thing that may happen is that during later computations one does obtain evidence that the order is not maximal. In all situations known to us in which this can occur such evidence readily yields a strictly larger order. In this case one can start all over again with the procedure described above, the role of A now being played by the larger order that has been found. To give an example, one is certain that the order A is not maximal if one finds a fractional ideal $\mathbf{a}$ that is not invertible. The one can compute the order $B = (A : \mathbf{a}) : (A : \mathbf{a})$, which by Proposition 2.5 is strictly larger than A.

References

1. M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.
2. E. Bach, J. Driscoll, J. O. Shallit, *Factor refinement*, J. Algorithms **15** (1993), 199–222.
3. H. Bass, *On the ubiquity of Gorenstein rings*, Math. Z. **82** (1963), 8–28.
4. Z.I. Borevič, I.R. Šafarevič, *Teorija čisel*, Izdat. "Nauka", Moscow, 1964; English translation: *Number theory*, Academic Press, New York, 1966.
5. J.P. Buhler, H.W. Lenstra, Jr., C. Pomerance, *Factoring integers with the number field sieve*, [14], 50–94.
6. 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.
7. H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.
8. M.R. Garey, D.S. Johnson, *Computers and intractability, a guide to the theory of NP-completeness*, Freeman, New York, 1979.
9. G. Ge, *Algorithms related to multiplicative representations of algebraic numbers*, Ph. D. thesis, Department of Mathematics, University of California, Berkeley, May 1993.
10. J.L. Hafner, K.S. McCurley, *Asymptotically fast triangularization of matrices over rings*, SIAM J. Comput. **20** (1991), 1068–1083.
11. D.E. Knuth, *The art of computer programming*, volume 2, second edition, Addison-Wesley, Reading, Mass., 1981.
12. T.Y. Lam, *Serre's conjecture*, Lecture Notes in Math. **635**, Springer-Verlag, Berlin, 1978.
13. S. Landau, *Some remarks on computing the square parts of integers*, Inform. and Comput. **78** (1988), 246–253.
14. A.K. Lenstra, H.W. Lenstra, Jr. (eds), *The development of the number field sieve*, Lecture Notes in Math. **1554**, Springer-Verlag, Berlin, 1993.

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

16. A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, J.M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349.

17. A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, J.M. Pollard, *The number field sieve*, [14], 11–42.

18. H.W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), 211–244.

19. H.W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673.

20. H.W. Lenstra, Jr., *Miller's primality test*, Inform. Process. Lett. **8** (1979), 86–88.

21. H.W. Lenstra, Jr., C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), 483–516.

22. C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, in: H. W. Lenstra, Jr., R. Tijdeman (eds), *Computational methods in number theory*, Mathematical Centre Tracts **154/155**, Mathematisch Centrum, Amsterdam, 1982, 89–139.

23. J.W. Sands, *Generalization of a theorem of Siegel*, Acta Arith. **58** (1991), 47–57.

24. J. Teitelbaum, *The computational complexity of the resolution of plane curve singularities*, Math. Comp. **54** (1990), 797–837.

25. A. T. Vasquez, *Rational desingularization of a curve defined over a finite field*, Number Theory Seminar, 229–250.

26. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963; reprinted, Chelsea, New York, 1976.

27. H. Zassenhaus, *Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung*, in: L. Collatz, G. Meinardus, H. Unger (eds), *Funktionalanalysis, Approximationstheorie, numerische Mathematik, Oberwolfach 1965*, Birkhäuser, Basel, 1967, 90–103.

28. H.G. Zimmer, *Computational problems, methods and results in algebraic number theory*, Lecture Notes in Math. **262**, Springer-Verlag, Berlin, 1972.