MATHEMATICS OF COMPUTATION
Volume 68, Number 225, January 1999, Pages 345–350
S 0025-5718(99)01023-6

ON FACTOR REFINEMENT IN NUMBER FIELDS

JOHANNES BUCHMANN AND FRIEDRICH EISENBRAND

ABSTRACT. Let $\mathcal{O}$ be an order of an algebraic number field. It was shown by Ge that given a factorization of an $\mathcal{O}$-ideal $\mathfrak{a}$ into a product of $\mathcal{O}$-ideals it is possible to compute in polynomial time an overorder $\mathcal{O}'$ of $\mathcal{O}$ and a *gcd-free* refinement of the input factorization; i.e., a factorization of $\mathfrak{a}\mathcal{O}'$ into a power product of $\mathcal{O}'$-ideals such that the bases of that power product are all invertible and pairwise coprime and the extensions of the factors of the input factorization are products of the bases of the output factorization. In this paper we prove that the order $\mathcal{O}'$ is the smallest overorder of $\mathcal{O}$ in which such a gcd-free refinement of the input factorization exists. We also introduce a partial ordering on the gcd-free factorizations and prove that the factorization which is computed by Ge's algorithm is the smallest gcd-free refinement of the input factorization with respect to this partial ordering.

1. INTRODUCTION

Let $\mathcal{O}$ be an order in an algebraic number field K and let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. Important tasks of algorithmic algebraic number theory are to find the maximal order $\mathcal{O}_{\max}$ of K and the factorization of the extension ideal $\mathfrak{a}\mathcal{O}_{\max}$ into a product of prime ideals of $\mathcal{O}_{\max}$. For both tasks no polynomial time algorithms are known. Suppose that a factorization

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{b}_i^{e_i} \tag{1}$$

of $\mathfrak{a}$ is known. The $\mathfrak{b}_i$ are $\mathcal{O}$-ideals and the exponents e_i are positive integers, $1 \le i \le k$. The factor refinement algorithm of Ge [Ge93], [Ge94] computes in polynomial time a gcd-free refinement $\mathfrak{a}\mathcal{O}' = \prod_{j=1}^{l} \mathfrak{c}_j^{f_j}$ of (1), with $\mathcal{O}' \supset \mathcal{O}$ and with invertible pairwise coprime $\mathcal{O}'$-ideals $\mathfrak{c}_j$, such that the $\mathcal{O}'$-ideals $\mathfrak{b}_i\mathcal{O}'$ of the input factorization (1) are power products of the $\mathcal{O}'$-ideals $\mathfrak{c}_j$ for $1 \le j \le l$ and $1 \le i \le k$. In this paper we characterize the output of the refinement algorithm as the unique minimal element in a certain partial order derived from the input. Our result extends a theorem of Bach, Driscoll, and Shallit [BDS93] from $\mathbb{Z}$ to arbitrary algebraic numbers.

We formulate the problem and our result more precisely and in a more general setting. Let R be a Dedekind domain with field of fractions Q and let K be a finite extension of Q. $\mathcal{O}_{\max}$ shall denote the integral closure in R in K. An order $\mathcal{O}$ of K is a subring of $\mathcal{O}_{\max}$ containing R with field of fractions K.

Received by the editor November 21, 1996.
1991 *Mathematics Subject Classification.* Primary 11Y40, 11R27, 11R04, 11Y16.

Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal and assume that $\mathfrak{a}$ can be factored as in (1) into a power product of $\mathcal{O}$-ideals $\mathfrak{b}_i$, $1 \leq i \leq k$. The factorization (1) will be written as $F = (\mathcal{O}, (\mathfrak{b}_1, e_1), \ldots, (\mathfrak{b}_k, e_k))$. We call $\mathcal{O}$ the *order of* F. The *bases of* F are the $\mathfrak{b}_i$, and the e_i are the *exponents of* F for $1 \leq i \leq k$. We assume that in such a factorization all the bases are different from $\mathcal{O}$ and $\{0\}$. We say that two factorizations are *equal* if their orders are equal and the sequences of pairs (*basis, exponent*) are equal after appropriate reordering. We call a factorization $F' = (\mathcal{O}', (\mathfrak{b}'_1, e'_1), \ldots, (\mathfrak{b}'_l, e'_l))$ a *refinement* of F if the following conditions are satisfied.

1. F' is a factorization of $\mathfrak{a}\mathcal{O}'$, where $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{b}_i^{e_i}$, i.e.,
$$\mathfrak{a}\mathcal{O}' = \prod_{i=1}^{l} (\mathfrak{b}'_i)^{e'_i}.$$
2. The order $\mathcal{O}$ of F is contained in the order $\mathcal{O}'$ of F', i.e., $\mathcal{O} \subset \mathcal{O}'$.
3. The extension of each basis of F in $\mathcal{O}'$ is a product of the bases of F'. This means that for $1 \leq i \leq k$ there is a sequence $(f_{ij})_{1 \leq j \leq l}$ of non-negative integers such that
$$\mathfrak{b}_i\mathcal{O}' = \prod_{j=1}^{l} (\mathfrak{b}'_j)^{f_{ij}}.$$

If F is a refinement of F, we write $F \leq F'$. The factorization F of $\mathfrak{a}$ is called *invertible gcd-free* if the bases $\mathfrak{b}_i$ are invertible $\mathcal{O}$-ideals for $1 \leq i \leq k$ and if they are pairwise *coprime*, i.e., $\mathfrak{b}_i + \mathfrak{b}_j = \mathcal{O}$ for $1 \leq i < j \leq k$. Ge [Ge93], [Ge94] proved that an invertible gcd-free refinement of F can be computed in polynomial time in the case $R = \mathbb{Z}$.

In this paper we prove that $\leq$ is a partial ordering on the set of all invertible gcd-free factorizations. We show that there is exactly one maximal invertible gcd-free factorization of $\mathfrak{a}$, namely the prime ideal factorizatiton of $\mathfrak{a}\mathcal{O}_{\max}$ in $\mathcal{O}_{\max}$. We also show that a given factorization F of $\mathfrak{a}$ has exactly one minimal invertible gcd-free refinement and that this minimal invertible gcd-free refinement is computed by Ge's algorithm.

2. Preliminaries

Throughout, let R denote a Dedekind domain with field of fractions Q, K a finite algebraic extension of Q, and $\mathcal{O}$ an order in K. Let $\mathfrak{a}$ and $\mathfrak{b}$ denote fractional $\mathcal{O}$-ideals. Their sum
$$\mathfrak{a} + \mathfrak{b} = \{\alpha + \beta \colon \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\},$$
their product
$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{(\alpha,\beta) \in S} \alpha\beta \colon S \subset \mathfrak{a} \times \mathfrak{b} \text{ finite} \right\},$$
and their quotient
$$\mathfrak{a} : \mathfrak{b} = \{\alpha \in K \colon \alpha\mathfrak{a} \subset \mathfrak{b}\}$$
are again fractional $\mathcal{O}$-ideals. If $R = \mathbb{Z}$, those can be computed in polynomial time. The fractional ideal $\mathfrak{a} : \mathfrak{a}$ is an order $\mathcal{O}'$ of K. It it called the *ring of multipliers* of $\mathfrak{a}$. That ring is the largest order $\widetilde{\mathcal{O}}$ in K such that $\mathfrak{a}$ is a fractional $\widetilde{\mathcal{O}}$-ideal. It is

also the smallest order $\widetilde{\mathcal{O}}$ in K such that the extension $\mathfrak{a}\widetilde{\mathcal{O}}$ is a fractional invertible $\widetilde{\mathcal{O}}$-ideal.

If $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal, then by the lying over theorem $\mathfrak{a}\mathcal{O}_{\max}$ is a proper $\mathcal{O}_{\max}$-ideal. The *length* of an $\mathcal{O}_{\max}$-ideal $\mathfrak{a}$ shall be the sum of the exponents in the unique prime power representation of $\mathfrak{a}$.

3. The refinement algorithm

We present an algorithm for computing an invertible gcd-free refinement of a factorization of an ideal. It is very similar to the algorithm of Ge [Ge93], [Ge94]. The idea is that the algorithm computes better and better refinements F' of the input factorization F. In each round the algorithm checks whether the factorization F' is already invertible gcd-free. Suppose that the algorithm finds a pair $(\mathfrak{b}'_i, \mathfrak{b}'_j)$ of bases of F' such that $i \neq j$ and $\mathfrak{c} = \mathfrak{b}'_i + \mathfrak{b}'_j$ is different from the order $\mathcal{O}'$ of F'. If $\mathfrak{c}$ is an invertible $\mathcal{O}'$-ideal, then the algorithm divides the bases $\mathfrak{b}'_i$ and $\mathfrak{b}'_j$ by $\mathfrak{c}$ and inserts the new basis $\mathfrak{c}$. If $\mathfrak{c}$ is not invertible, then the algorithm replaces the order $\mathcal{O}'$ by the ring of multipliers of $\mathfrak{c}$. It also replaces the bases $\mathfrak{b}_i$ by their extensions in the new $\mathcal{O}'$. Then the division by $\mathfrak{c}'$ and the insertion of $\mathfrak{c}$ are carried out.

In the algorithm we denote by ring_of_mult($\mathfrak{a}$) the ring of multipliers of an $\mathcal{O}$-ideal $\mathfrak{a}$.

Algorithm 3.1.

Factor refinement for ideals in number fields

Input: A factorization $F = (\mathcal{O}, (\mathfrak{b}_1, e_1), \ldots, (\mathfrak{b}_k, e_k))$ of an $\mathcal{O}$-ideal $\mathfrak{a}$.
Output: An invertible gcd-free refinement $F' = (\mathcal{O}', (\mathfrak{b}'_1, e'_1), \ldots, (\mathfrak{b}'_l, e'_l))$ of F.

(1) $\mathcal{O}' = \sum_{i=1}^{k}$ ring_of_mult $(\mathfrak{b}_i)$
(2) **for** $(i = 1, i \leq k, i++)$ **do**
(3) $\quad \mathfrak{b}'_i = \mathfrak{b}_i\mathcal{O}'$
(4) **od**
(5) $l = k$
(6) **while** (There exists $i, j \in \{1, \ldots, l\}$ with $i \neq j$ and $\mathfrak{c} = \mathfrak{b}'_i + \mathfrak{b}'_j \neq \mathcal{O}'$) **do**
(7) $\quad$ **if** $(\mathfrak{c} : \mathfrak{c} \neq \mathcal{O}')$ **then**
(8) $\quad\quad \mathcal{O}' = \mathfrak{c} : \mathfrak{c}$
(9) $\quad\quad$ **for** $(i = 1, i \leq l, i++)$ **do**
(10) $\quad\quad\quad \mathfrak{b}'_i = \mathfrak{b}_i\mathcal{O}'$
(11) $\quad\quad$ **od**
(12) $\quad$ **fi**
(13) $\quad$ Delete $(\mathfrak{b}'_i, e'_i)$, $(\mathfrak{b}'_j, e'_j)$ in F'
(14) $\quad$ Insert $(\mathfrak{b}'_i \cdot (\mathcal{O}' : \mathfrak{c}), e'_i)$, $(\mathfrak{c}, e'_i + e'_j)$, $(\mathfrak{b}'_j \cdot (\mathcal{O}' : \mathfrak{c}), e'_j)$ in F'
(15) $\quad$ Delete all pairs $(\mathfrak{b}'_s, e'_s)$ with $\mathfrak{b}'_s = \mathcal{O}'$ in F'
(16) $\quad$ Update l
(17) **od**

Theorem 3.2. *Algorithm 3.1 terminates with the correct result after at most* $\text{length}(\mathfrak{a}\mathcal{O}_{\max})$ *refinements steps.*

Proof. It is easy to verify that any factorization F' which is computed in Algorithm 3.1 is a refinement of F. Also, upon termination of Algorithm 3.1, the factorization F' is invertible gcd-free. Hence, it suffices to prove that the algorithm terminates. This will be done now.

In Algorithm 3.1 set

$$S = \sum_{i=1}^{l} (e_i' - 1).$$

Then we have

$$\text{length}(\mathfrak{a}\mathcal{O}_{\max}) = \text{length}\left(\prod_{i=1}^{l} \mathfrak{b}_i' \mathcal{O}_{\max}^{e_i'}\right) \geq \sum_{i=1}^{l} e_i'.$$

Hence

$$S \leq \text{length}(\mathfrak{a}\mathcal{O}_{\max}).$$

Analysis like the one in [Ge93] shows that in each refinement step the positive integer S is increased by at least 1. Therefore, the number of refinement steps is bounded by $\text{length}(\mathfrak{a}\mathcal{O}_{\max})$. □

4. The output of refinement algorithm

In this section we characterize the output of refinement Algorithm 3.1. We first prove that the relation $\leq$ defined in the introduction is a partial ordering on the set of all invertible gcd-free factorizations of $\mathfrak{a}$.

The proof of the following lemma can be found in [ZS58, p. 177].

Lemma 4.1. *Let* $\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{c}$ *be ideals of a commutative ring with unit* R *with* $\mathfrak{b}_1 + \mathfrak{c} = \mathfrak{b}_2 + \mathfrak{c} = R$. *Then* $\mathfrak{b}_1\mathfrak{b}_2 + \mathfrak{c} = R$.

Corollary 4.2. *Let* $(\mathfrak{b}_1, \ldots, \mathfrak{b}_k)$ *be a finite sequence of pairwise coprime ideals of a commutative ring with unity* R *and let* $(e_i)_{1 \leq i \leq k}$ *and* $(f_i)_{1 \leq i \leq k}$ *be sequences of non-negative integers. Then*

$$\prod_{i=1}^{k} \mathfrak{b}_i^{e_i} + \prod_{i=1}^{k} \mathfrak{b}_i^{f_i} = \prod_{i=1}^{k} \mathfrak{b}_i^{\min\{e_i, f_i\}}.$$

Proof. It follows by induction from Lemma 4.1 that

$$\prod_{i=1}^{k} \mathfrak{b}_i^{e_i - \min\{e_i, f_i\}} + \prod_{i=1}^{k} \mathfrak{b}_i^{f_i - \min\{e_i, f_i\}} = R.$$

If this equation is multiplied by $\prod_{i=1}^{k} \mathfrak{b}_i^{\min\{e_i, f_i\}}$ we obtain the desired result. □

Corollary 4.3. *Let* R *be an integral domain. If* $\mathfrak{a}$ *is a power product of pairwise coprime invertible ideals* $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$ *of* R, *which are all strictly contained in* R, *then the exponents in that power product represention are uniquely determined.*

Proof. Suppose we have two different factorizations of $\mathfrak{a}$

$$\prod_{i=1}^{k} \mathfrak{b}_i^{e_i} = \prod_{i=1}^{k} \mathfrak{b}_i^{f_i}$$

into pairwise coprime invertible R-ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$ which are all different from R. Assume without loss of generality that $e_1 > f_1$. Then we have

$$\mathfrak{b}_1^{e_1 - f_1} \prod_{i=2}^{k} \mathfrak{b}_i^{e_i} = \prod_{i=2}^{k} \mathfrak{b}_i^{f_i}.$$

If one adds the ideal $\mathfrak{b}_1$ to the product on the left, then the result is $\mathfrak{b}_1$. Adding $\mathfrak{b}_1$ to the product on the right yields R, which is a contradiction. □

Theorem 4.4. *The relation $\leq$ is reflexive and transitive and a partial ordering on the set of invertible gcd-free factorizations.*

Proof. Reflexivity and transitivity are trivial.

For symmetry let F and F' be invertible gcd-free factorizations, not necessarily of the same ideal. Assume that $F \leq F'$ and $F' \leq F$. We have to prove that $F = F'$. Clearly the orders of F and F' are equal. Also, F and F' are factorizations of the same ideal $\mathfrak{a}$. We show that F and F' have the same bases. Since F is invertible gcd-free the bases of F are pairwise distinct. The same is true for F'. Let B be the set of bases F and let B' be the set of bases of F'. It suffices to prove that $B' \subset B$. Let $\mathfrak{b}' \in B'$. Then $\mathfrak{b}'$ contains an element $\mathfrak{b}_1$ of B since otherwise we can write $\mathfrak{a}$ as a power product of the ideals in $B' - \mathfrak{b}'$ which contradicts Corollary 4.3.

Also $\mathfrak{b}'$ has a representation

$$\mathfrak{b}' = \prod_{\mathfrak{b} \in B} \mathfrak{b}^{e(\mathfrak{b})},$$

with $e(\mathfrak{b}) \geq 0$ for $\mathfrak{b} \in B$. Let $\mathfrak{b} \in B$ with $e(\mathfrak{b}) > 0$. Then

$$\mathfrak{b}_1 \subset \mathfrak{b}' \subset \mathfrak{b}^{e(\mathfrak{b})}.$$

Since the elements of B are pairwise coprime this implies that $\mathfrak{b} = \mathfrak{b}_1$ and Corollary 4.3 shows that $e(\mathfrak{b}) = 1$. Hence $\mathfrak{b}' = \mathfrak{b}$. Finally, the equality of the exponents follows from another application of Corollary 4.3. □

The following statement is easy to verify.

Theorem 4.5. *Among the invertible gcd-free factorizations of $\mathfrak{a}$ there is a uniquely determined maximal one with respect to $\leq$. It is the prime ideal factorization of $\mathfrak{a}\mathcal{O}_{\max}$.*

We will now show that among the invertible gcd-free refinements of F there is exactly one minimal element with respect to the partial ordering $\leq$ and that Algorithm 3.1 computes this factorization.

Lemma 4.6. *If F_1 is an invertible gcd-free refinement of the input factorization F of Algorithm 3.1, then F_1 is a refinement of any of the factorizations F' which are computed in the course of Algorithm 3.1.*

Proof. Let F' be the initial factorization computed in Algorithm 3.1 from F. Its order $\mathcal{O}'$ is the smallest order (with respect to inclusion) such that the extensions of all bases in $\mathcal{O}'$ are invertible. Since the extensions of the bases of F in the order

$\mathcal{O}_1$ of F_1 are products of the invertible bases of F_1 they are invertible $\mathcal{O}_1$-ideals. This shows that $\mathcal{O}' \subset \mathcal{O}_1$. Also, since the bases of F' are simply extensions of the bases of F in the order $\mathcal{O}'$ and because $\mathcal{O}' \subset \mathcal{O}_1$, it follows that their extensions in $\mathcal{O}_1$ are still products of the bases of F_1.

Now assume that F_1 is an invertible gcd-free refinement of a factorization F', which is computed before a refinement step starts. If a refinement step is necessary, then there are $i, j \in \{1, \ldots, l\}$ such that $i \neq j$ and $\mathfrak{c} = \mathfrak{b}'_i + \mathfrak{b}'_j \neq \mathcal{O}'$. Suppose that $\mathfrak{c}$ is not invertible. Then $\mathcal{O}'$ is replaced by the smallest overorder in which the extension of $\mathfrak{c}$ is invertible. But since the extensions $\mathfrak{b}_i\mathcal{O}_1$ and $\mathfrak{b}_j\mathcal{O}_1$ are both products of the pairwise coprime basis elements of F_1, it follows from Corollary 4.2 that this is also true for the sum $\mathfrak{b}_i + \mathfrak{b}_j$. Hence, this sum is invertible and this shows that the new $\mathcal{O}'$ is still contained in $\mathcal{O}_1$. Also the extensions of the bases in that new order are still products of the bases of F_1 and so are their gcd's. This shows that $F' \leq F$ still holds for the new F'. □

Now we are able to prove the main result of this paper.

Theorem 4.7. *Among the invertible gcd-free refinements of F there is exactly one minimal element with respect to $\leq$ and this factorization is the output of Algorithm 3.1.*

Proof. The output F' of Algorithm 3.1 is invertible gcd-free and it follows from Lemma 4.6 that all other invertible gcd-free refinements of F are refinements of F'. This proves the result. □

Acknowledgments

We would like to thank the anonymous referee for pointing out to us that our earlier result on number fields can also be proved for arbitrary Dedekind domains. Thanks also to Robert Berger and Sachar Paulus for several helpful comments and suggestions.

References

[BDS93] E. Bach, J. Driscoll, and J. Shallit, *Factor refinement*, J. Algorithms **15** (1993), 199–222. MR **94m:**11148

[Ge93] Guoqiang Ge, *Algorithms related to multiplicative representations of algebraic numbers*, PhD thesis, U.C. Berkeley, 1993.

[Ge94] Guoqiang Ge, *Recognizing units in number fields*, Math. Comp. **63** (1994), 377–387. MR **94i:**11107

[ZS58] O. Zariski and P. Samuel, *Commutative algebra*, Van Nostrand, Princeton, 1958. MR **19:**833e

Technische Hochschule Darmstadt, Alexanderstr. 10, D-64283 Darmstadt, Germany
E-mail address: buchmann@cdc.informatik.th-darmstadt.de

Max-Planck-Institut für Informatik, Im Stadtwald, D-66123 Saarbrücken, Germany
E-mail address: eisen@mpi-sb.mpg.de