Refereed. Pages 27–34 in *Algorithmic number theory: ANTS-II*, edited by Henri Cohen, Lecture Notes in Computer Science 1122, Springer, 1996.

Fast ideal arithmetic via lazy localization

Daniel J. Bernstein

Department of Mathematics, Statistics, and Computer Science,
The University of Illinois at Chicago, Chicago, IL 60607–7045
djb@math.uic.edu

Abstract. This paper proposes a new representation for ideals of any order in an algebraic number field. This representation is compact and highly readable; for example, $(95, x+65)(221^6)$ and $(7, x^2+4)(95, x+46)$ are two ideals of $\mathbf{Z}[x]/(x^4 - x^3 + 7x^2 - 11x + 5)$, with sum $(19, x + 8)$. Arithmetic on ideals in this form is generally much faster than arithmetic in the $\mathbf{Z}$-basis or two-element representations.

1 Introduction

I propose a new, highly readable representation for ideals of any order in a number field. Arithmetic in this representation is generally much faster than arithmetic in the $\mathbf{Z}$-basis or two-element representations.

The idea is as follows. Any nonzero ideal contains some positive integer N. Represent the ideal locally at all the primes of $\mathbf{Z}$ dividing N. This representation is compatible with arithmetic: all the usual ideal operations are local.

It is not possible in practice to find the set of primes dividing N. So, following a philosophy of Hendrik W. Lenstra, Jr., I work instead with a **coprime base** P for N: a pairwise coprime set of positive integers generating a semigroup that contains N. (Initially P may be taken as $\{N\}$.) A typical $p \in P$ might not be prime, but I nevertheless think of p as prime—until encountering a nonzero nonunit modulo p, at which point I factor p and continue the computation.

To add or multiply or intersect two ideals one must first find a common coprime base for them. This can be done in essentially linear time; see [1]. Once the ideals are represented on a common coprime base, all operations are "local"; see section 4.

Throughout this paper $\varphi \in \mathbf{Z}[x]$ is an irreducible monic integer polynomial. The ring $\mathbf{Z}[x]/\varphi$ is an order inside the number field $\mathbf{Q}[x]/\varphi$. Most of this paper focuses on the representation of ideals of $\mathbf{Z}[x]/\varphi$. For fractional ideals see section 8. For orders bigger than $\mathbf{Z}[x]/\varphi$ see section 9.

In this paper, all rings are commutative.

Thanks to Hendrik W. Lenstra, Jr., for his helpful comments.

2 Flat modules

The reader willing to accept Lemma 3.1 and Lemma 3.3 without proof may skip this section.

Let R be a ring, M an R-module. For any subgroup G of R^n, write MG for the subgroup of M^n generated by $\{mg : m \in M, g \in G\}$.

Definition: M is **flat over** R if the M-kernel of any R-matrix is M-generated by the R-kernel. In other words, if M is flat over R, and A is an n-column matrix with coefficients in R, and $z \in M^n$ satisfies $Az = 0$, then z is in $M\{x \in R^n : Ax = 0\}$. See [3, Theorem 7.6].

Lemma 2.1. *Let R be a ring, M a flat R-module. Let I and J be R-submodules of R^n. Then $MI \cap MJ = M(I \cap J)$.*

Proof. It suffices to show that $MI \cap MJ \subseteq M(I \cap J)$. Take $t \in MI \cap MJ$. By definition of MI, there are elements $b_1, b_2, \ldots, b_r \in M$ and $g_1, g_2, \ldots, g_r \in I$ with $t = b_1g_1 + b_2g_2 + \cdots + b_rg_r$. Similarly there are elements $c_1, c_2, \ldots, c_s \in M$ and $h_1, h_2, \ldots, h_s \in J$ with $t = c_1h_1 + c_2h_2 + \cdots + c_sh_s$.

Let A be the matrix for the map $R^n \times R^r \times R^s \to R^n \times R^n$ that takes (y, d, e) to $(y - d_1g_1 - \cdots - d_rg_r, y - e_1h_1 - \cdots - e_sh_s)$. Note that if $A(y, d, e) = 0$ then $y \in I \cap J$.

Now the vector $z = (t, b_1, b_2, \ldots, b_r, c_1, c_2, \ldots, c_s)$ satisfies $Az = 0$. By flatness, z is a combination with coefficients in M of vectors $x \in R^n \times R^r \times R^s$ satisfying $Ax = 0$. Hence t is the same combination of vectors $y \in I \cap J$. □

Lemma 2.2. *Let R be a ring, B a flat extension of R. Let I be an R-submodule of R^n. If $x \in BI \cap R^n$ then $1 = b_1m_1 + b_2m_2 + \cdots + b_sm_s$ for some $b_1, b_2, \ldots, b_s \in B$ and $m_1, m_2, \ldots, m_s \in R$ with $m_1x, m_2x, \ldots, m_sx \in I$.*

Proof. By definition of BI, there are coefficients $c_1, c_2, \ldots, c_r \in B$ and elements $g_1, g_2, \ldots, g_r \in I$ with $x = c_1g_1 + \cdots + c_rg_r$. Let A be the matrix for the map $R \times R^r \to R^n$ that takes (m, d) to $mx - d_1g_1 - \cdots - d_rg_r$. Note that if $A(m, d) = 0$ then $mx \in I$.

Now the vector $z = (1, c_1, \ldots, c_r)$ satisfies $Az = 0$. By flatness, there are coefficients $b_1, \ldots, b_s \in B$ and vectors $(m_1, d_1), \ldots, (m_s, d_s) \in R \times R^r$ satisfying $A(m_i, d_i) = 0$ and $z = b_1(m_1, d_1) + \cdots + b_s(m_s, d_s)$. In particular $m_ix \in I$ and $1 = b_1m_1 + \cdots + b_sm_s$. □

3 The ring $\mathbf{Z}_p$

Let p be an integer. The **completion of Z at** p, written $\mathbf{Z}_p$, is the projective limit of $\mathbf{Z}/p^n$. An element of $\mathbf{Z}_p$ is a sequence $(x_1, x_2, \ldots)$, with $x_n \in \mathbf{Z}/p^n$, such that $x_{n+1} \bmod p^n = x_n$. For $p > 1$, $\mathbf{Z}_p$ is an extension of $\mathbf{Z}$.

$\mathbf{Z}_p$ is flat over $\mathbf{Z}$. This follows from the fact that $\mathbf{Z}_p$ is torsion-free. Indeed, $\mathbf{Z}$ is a **Prüfer domain**—any torsion-free $\mathbf{Z}$-module is flat. (Any Dedekind domain is a Prüfer domain; see [3, Exercise 11.8].)

More generally, any completion of a Noetherian ring is flat. See [3, Theorem 8.8].

Lemma 3.1. *Let p be an integer. Let I and J be subgroups of $\mathbf{Z}^n$. Then $\mathbf{Z}_pI \cap \mathbf{Z}_pJ = \mathbf{Z}_p(I \cap J)$.*

Proof. Lemma 2.1. □

Lemma 3.2. *Let $p > 1$ be an integer. If $Q \in \mathbf{Z}_p$ and $p^eQ \in \mathbf{Z}$ then $Q \in \mathbf{Z}$.*

Proof. The image of p^eQ in $\mathbf{Z}/p^e$ is 0, so p^eQ is divisible by p^e in $\mathbf{Z}$; let $q \in \mathbf{Z}$ be the quotient. Now $p^e(q - Q) = 0$, but $\mathbf{Z}_p$ is torsion-free, so $q = Q$. □

Lemma 3.3. *Let p and u be integers with $p > 1$. Let I be a subgroup of $\mathbf{Z}^n$ containing $p^eu\mathbf{Z}^n$. Then $u(\mathbf{Z}_pI \cap \mathbf{Z}^n) \subseteq I$.*

Proof. Pick $x \in \mathbf{Z}_pI \cap \mathbf{Z}^n$. By Lemma 2.2 there are $b_1, b_2, \ldots, b_s \in \mathbf{Z}_p$ and $m_1, m_2, \ldots, m_s \in \mathbf{Z}$ such that $m_ix \in I$ and $1 = b_1m_1 + b_2m_2 + \cdots + b_sm_s$. Write $b_i = p^eq_i + r_i$ with $q_i \in \mathbf{Z}_p$ and $r_i \in \mathbf{Z}$, and define $Q = q_1m_1 + \cdots + q_sm_s$; then $1 = p^eQ + r_1m_1 + \cdots + r_sm_s$, so Q is an integer by Lemma 3.2. Finally $ux = p^euQx + ur_1m_1x + \cdots + ur_sm_sx \in I$. □

4 Ideals of $\mathbf{Z}[x]/\varphi$ versus ideals of $\mathbf{Z}_p[x]/\varphi$

For any ideal I of $\mathbf{Z}[x]/\varphi$ consider $\mathbf{Z}_pI$, the smallest subgroup of $\mathbf{Z}_p[x]/\varphi$ containing $\{ci : c \in \mathbf{Z}_p, i \in I\}$. $\mathbf{Z}_pI$ is an ideal of $\mathbf{Z}_p[x]/\varphi$.

If I is generated by β then $\mathbf{Z}_pI$ is generated by the image of β in $\mathbf{Z}_p[x]/\varphi$.

If J is another ideal of $\mathbf{Z}[x]/\varphi$ then $\mathbf{Z}_p(I + J) = \mathbf{Z}_pI + \mathbf{Z}_pJ$; $\mathbf{Z}_p(IJ) = (\mathbf{Z}_pI)(\mathbf{Z}_pJ)$; and, by Lemma 3.1, $\mathbf{Z}_p(I \cap J) = \mathbf{Z}_pI \cap \mathbf{Z}_pJ$.

Lemma 4.1. *Let $p > 1$ be an integer. Let I be a nonzero ideal of $R = \mathbf{Z}[x]/\varphi$. Then the natural map $R \to \mathbf{Z}_p[x]/\varphi$ induces an isomorphism $R/(\mathbf{Z}_pI \cap R) \to (\mathbf{Z}_p[x]/\varphi)/\mathbf{Z}_pI$.*

Proof. Let f be the natural map from R to $(\mathbf{Z}_p[x]/\varphi)/\mathbf{Z}_pI$. It is enough to show that f is surjective.

Since I is nonzero it contains some positive integer N. Given any $g \in \mathbf{Z}_p[x]/\varphi$, write $g = qN + r$ with $q \in \mathbf{Z}_p[x]/\varphi$ and $r \in R$. Then $qN \in \mathbf{Z}_p I$ so $g \bmod \mathbf{Z}_p I = f(r)$. □

Lemma 4.2. *Let I be an ideal of $R = \mathbf{Z}[x]/\varphi$ containing a positive integer N. Let P be a coprime base for N. Then R/I is isomorphic to $\prod_{p \in P - \{1\}} (R/(\mathbf{Z}_p I \cap R))$.*

Proof. $\mathbf{Z}_p I \cap R$ contains the maximum power of p dividing N, for $p \in P$. Hence $\mathbf{Z}_p I \cap R$ and $\mathbf{Z}_q I \cap R$ are coprime whenever p and q are coprime.

It thus suffices to show that $I = \bigcap_p (\mathbf{Z}_p I \cap R)$. Certainly $I \subseteq \mathbf{Z}_p I \cap R$. For the converse it is convenient to write u_p for the non-p-part of N; i.e., N is u_p times a power of p, and u_p is coprime to p. Now say $\beta \in R$ is in $\mathbf{Z}_p I$. By Lemma 3.3, $u_p \beta \in I$. If this is true for all p then $\beta \in I$ since $\gcd\{u_p : p \in P, p \neq 1\} = 1$. □

5 A standard representation for ideals of $\mathbf{Z}_p[x]/\varphi$

Let $p > 1$ be an integer. In this section I describe a standard representation for finite-norm ideals of $\mathbf{Z}_p[x]/\varphi$. Not every ideal can be written in this representation, unless p is prime; however, there is an algorithm that, given generators for an ideal, either (1) finds a standard representation for the ideal or (2) finds a nontrivial factor of p. The algorithm appears in section 6.

I begin with the representation in [2, Theorem 4.7.5], which is an improvement (specific to ideals) of the Hermite normal form ([2, section 2.4.2]). Recall that a representation for I is a $\mathbf{Z}_p$-basis for I of the form $\{c_n f_n : 0 \le n < \deg \varphi\}$. Here $f_n \in \mathbf{Z}_p[x]$ is a monic polynomial of degree n, and $c_n \in \mathbf{Z}_p$ is some nonzero coefficient. (One can take $c_n \in \mathbf{Z}$ and $f_n \in \mathbf{Z}[x]$.)

I improve this representation in two ways. First, if several polynomials f_n have the same leading coefficient c_n, I record only the polynomial of lowest degree. The ideals of $\mathbf{Z}_p[x]$ that show up in practice seem to contain few distinct coefficients. This makes arithmetic much faster, at the expense of a more complicated implementation, for the simple reason that there are fewer numbers to manipulate. It also makes the output more readable, for the same reason.

Second, I insist that each leading coefficient be a power of p. This again improves speed and readability: I can store, manipulate, and print the exponent rather than the power. If p is not prime, there is no guarantee that one can successfully write an ideal this way, but failure reveals a nontrivial factor of p.

My representation is thus a sequence $(d_0, e_0, f_0), (d_1, e_1, f_1), \ldots$, with $0 = d_0 < d_1 < \cdots < \deg \varphi$, $e_0 > e_1 > \cdots \ge 0$, and f_i a monic integer polynomial of degree d_i, such that

$$\begin{aligned} I = {} & p^{e_0} f_0 \mathbf{Z}_p + p^{e_0} f_0 x \mathbf{Z}_p + p^{e_0} f_0 x^2 \mathbf{Z}_p + \cdots + p^{e_0} f_0 x^{d_1 - 1} \mathbf{Z}_p \\ & + p^{e_1} f_1 \mathbf{Z}_p + p^{e_1} f_1 x \mathbf{Z}_p + p^{e_1} f_1 x^2 \mathbf{Z}_p + \cdots + p^{e_1} f_1 x^{d_2 - d_1 - 1} \mathbf{Z}_p \\ & + p^{e_2} f_2 \mathbf{Z}_p + p^{e_2} f_2 x \mathbf{Z}_p + p^{e_2} f_2 x^2 \mathbf{Z}_p + \cdots + p^{e_2} f_2 x^{d_3 - d_2 - 1} \mathbf{Z}_p \\ & + \cdots . \end{aligned}$$

I is generated as an ideal by $p^{e_0}f_0, p^{e_1}f_1, \ldots$. The norm of I is $\#((\mathbf{Z}_p[x]/\varphi)/I) = p^{e_0 d_1 + e_1(d_2-d_1) + e_2(d_3-d_2)+\cdots}$. One can impose bounds upon the coefficients of each f_i to make this representation unique; see [2, section 2.4.2].

In practice I display $(p^{e_0}f_0, p^{e_1}f_1, \ldots)$. Five examples of ideals, with $\varphi = x^4 - x - 3$: $(11, x+5)$; $(11, x^2+3x+1)$; $(11^2, 11(x+5), x^2+91x+12)$; (10^{25}); $(65, x^3+58x^2+49x+46)$.

6 Computing a representation for an ideal of $\mathbf{Z}_p[x]/\varphi$

Let $p > 1$ be an integer. Let I be the ideal of $\mathbf{Z}_p[x]/\varphi$ generated by a finite set B. Assume that I contains a positive integer N. Given p, N, B, Algorithm 6.1 attempts to compute a standard representation for I. It may instead take a "side exit," producing a nontrivial factor of p.

Algorithm 6.1 works with a set C of nonnegative integer polynomials contained in I. At the beginning of steps 3, 4, and 5, C has exactly one polynomial of each degree from 0 through $\deg\varphi - 1$. The leading coefficient of each polynomial is a power of p.

Write M for the $\mathbf{Z}_p$-module generated by C. Algorithm 6.1 uses a subroutine, Algorithm 6.2, which expands M to contain any given polynomial h, printing 1 if C was changed or 0 if h was already in M. Algorithm 6.1 repeatedly invokes Algorithm 6.2 to ensure that $B \subseteq M$ and that M is closed under multiplication by x. Algorithm 6.1 and Algorithm 6.2 terminate because the norm of M, $\#((\mathbf{Z}_p[x]/\varphi)/M)$, decreases whenever Algorithm 6.2 prints 1.

Algorithm 6.1.

1. Compute the maximum n such that p^n divides N. If N/p^n is not coprime to p, side exit: $\gcd\{N/p^n, p\}$ is a nontrivial factor of p.
2. (Now $p^n \in I$.) Set $N \leftarrow p^n$. Set $C \leftarrow \{N, Nx, Nx^2, \ldots, Nx^{\deg\varphi - 1}\}$.
3. (Now $C \cup B$ generates I as an ideal.) For each $\beta \in B$: Apply Algorithm 6.2 to β.
4. (Now C generates I as an ideal.) For each $g \in C$: Apply Algorithm 6.2 to gx; if Algorithm 6.2 prints 1, go back to the beginning of step 4.
5. (Now C generates I as an ideal; and $gx \in M$ for each $g \in C$. Thus $M = I$. Each polynomial in C is divisible by its leading coefficient, and by the leading coefficients of all higher-degree polynomials in C; see the proof of [2, Theorem 4.7.5].) Remove from C any polynomial whose leading coefficient appears on a polynomial of smaller degree. Now the set of $(\deg f, e, f)$, where e is an integer and f is a monic integer polynomial with $p^e f \in C$, is a standard representation for I.

Algorithm 6.2.

1. Set $h \leftarrow (h \bmod \varphi) \bmod N$.
2. (Now $\deg h < \deg\varphi$.) If $h = 0$: Print 0 and stop.

3. (Now $0 \le \deg h < \deg \varphi$.) Let g be the polynomial in C with $\deg g = \deg h$. Set L to the leading coefficient of h. If the leading coefficient of g divides L, set $h \leftarrow (h \bmod g) \bmod N$ and go back to step 2.
4. (Now $0 \le \deg g = \deg h < \deg \varphi$; $g \in C$; and the leading coefficient of g does not divide L, the leading coefficient of h. Thus $h \notin M$.) Compute the maximum n such that p^n divides L. If L/p^n is not coprime to p, side exit: $\gcd\{L/p^n, p\}$ is a nontrivial factor of p.
5. Find integers u and v so that $uh - vg$ has leading coefficient p^n. Set $h \leftarrow (uh - vg) \bmod N$. (Note that u is coprime to p; thus this does not change the $\mathbf{Z}_p$-module generated by $C \cup \{h\}$.)
6. Set $C \leftarrow (C - \{g\}) \cup \{h\}$. (This decreases the norm of M.)
7. Apply Algorithm 6.2, recursively, to g.
8. Print 1.

In practice, step 4 of Algorithm 6.1 should tag each element $g \in C$ for which gx is already known to be in M; then it can avoid feeding gx to Algorithm 6.2 more than once.

7 A representation for nonzero ideals of $\mathbf{Z}[x]/\varphi$

Let I be a nonzero ideal of the ring $R = \mathbf{Z}[x]/\varphi$. I propose to represent I by $\{(p, \mathbf{Z}_p I) : p \in P\}$, where P is a coprime base (not containing 1) for some positive integer in I. This representation is compatible with computing principal ideals, ideal sums, and ideal norms; *a fortiori* it determines I.

In practice I display the concatenation of $\{\mathbf{Z}_p I : p \in P\}$. For example, the ideal generated by 27075 and $3(x^2+36x+2010)$ modulo $x^4 - x^3 + 7x^2 - 11x + 5$ is $(3)(5^2, 5(x+1), x^2+x)(19^2, 19(x+9), x^2+17x+34)$.

Basic operations. To find the ideal generated by $\beta \neq 0$: Let N be the absolute value of the norm of β. Set $P = \{N\}$. Then find a standard representation for the ideal generated by β in $\mathbf{Z}_N[x]/\varphi$. (Exception: If $N = 1$, set $P = \{\}$.)

To find the norm $\#(R/I)$ of an ideal I: Multiply the local norms. By Lemma 4.1 and Lemma 4.2, $\#(R/I) = \prod_p \#((\mathbf{Z}_p[x]/\varphi)/\mathbf{Z}_p I)$.

To add or multiply or intersect two ideals: Say they have coprime bases Q and Q'. Find a coprime base P for $Q \cup Q'$, as discussed in [1], and split each ideal into P-pieces. Then find a standard representation for the sum or product or intersection of local pieces. For more details on intersection see [2, Exercise 4.18]; an alternate method appears in section 8.

As noted in section 5, some ideals of $\mathbf{Z}_p[x]/\varphi$ do not have a standard representation. Whenever Algorithm 6.1 or Algorithm 6.2 discovers a nontrivial factor q of $p \in P$, I replace p by a coprime base for $\{p, q\}$. Then I restart the computation.

Here is a numerical example. Fix $\varphi = x^4 - x^3 + 7x^2 - 11x + 5$. Consider the ideals $I = (95, x+65)(221^6)$ and $J = (7, x^2+4)(95, x+46)$; what is $I + J$? I start with $P = \{7, 95, 221\}$ and add the 7-pieces, 95-pieces, and 221-pieces separately. Focus on 95: the 95-piece of the sum is generated by $95, x+65, 95, x+46$. I feed these generators to Algorithm 6.1, which discovers the factor 19 of 95, so I replace 95 with $5, 19$ and restart. To split $(95, x+65)$ into a 5-piece and a 19-piece, I feed the generators $95, x+65$ to Algorithm 6.1, first with $p = 5$, producing $(5, x)$, and then with $p = 19$, producing $(19, x+8)$. Similarly, I split $(95, x+46)$ into $(5, x+1)(19, x+8)$. Then I add the 5-pieces and 19-pieces separately. The final result is $I + J = (19, x+8)$.

Other operations. The above operations suffice to construct many further operations. For example, $J \subseteq I$ if and only if $\#(R/(I+J)) = \#(R/I)$; $\beta \in I$ if and only if $\beta R \subseteq I$; $J = I$ if and only if $\#(R/I) = \#(R/J) = \#(R/(I+J))$. In practice it is better to implement these other operations separately.

8 Fractional ideals

I represent a fractional ideal as a nonzero ideal divided by an integer. It is convenient to break the integer into local pieces.

Fractional ideals admit several new operations. All of them are special cases of **ratio**: if I and J are subgroups of $K = \mathbf{Q}[x]/\varphi$ then the ratio $J \div I = \{x \in K : xI \subseteq J\}$ is also a subgroup of K.

Define $T = \{x \in K : \operatorname{trace}_{K:\mathbf{Q}} x \in \mathbf{Z}\}$. For any fractional ideal I, the ratio $T \div I$ is also a fractional ideal; it is the **dual of I with respect to the trace**, written $\operatorname{Dual} I$. This is called a dual because $\operatorname{Dual}\operatorname{Dual} I = I$. It is easy to compute $\operatorname{Dual} I$; see [2, section 4.8.4].

If J and I are both fractional ideals then $J \div I$ is a fractional ideal. The operation $(J, I) \mapsto J \div I$ is called **ideal division**.

Lemma 8.1. *If I and J are fractional ideals then $J \div I = \operatorname{Dual}(I \operatorname{Dual} J)$.*

Thus $J \div I$ is easy to compute. It appears that this observation was first due to Peter Montgomery. My thanks to Hendrik W. Lenstra, Jr., for pointing out that this works in all orders, not just Dedekind domains. Lenstra also notes that $J \cap I = \operatorname{Dual}(\operatorname{Dual} J + \operatorname{Dual} I)$, so intersection can be implemented in terms of addition (or vice versa).

Proof. In general $A \div BC = (A \div B) \div C$. Thus $\operatorname{Dual}(I \operatorname{Dual} J) = T \div (I \operatorname{Dual} J) = (T \div \operatorname{Dual} J) \div I = (\operatorname{Dual}\operatorname{Dual} J) \div I = J \div I$. □

9 Ideals of non-equation orders

An order in a number field need not be of the form $\mathbf{Z}[x]/\varphi$. The technique of lazy localization applies in tremendous generality; one can straightforwardly tensor the known computational universe with $\mathbf{Z}_p$, or with completions of other convenient base rings. However, the ideal representation in section 5 is specific to $\mathbf{Z}_p[x]/\varphi$, and it is not clear how to preserve the benefits of that representation in more general settings.

There is a very simple solution. If A is an order of $\mathbf{Q}(\alpha)$ containing $\mathbf{Z}[\alpha]$, where α is a root of φ, then any fractional ideal over A is—and can be represented as—a fractional ideal over $\mathbf{Z}[\alpha]$. In particular, I represent A itself as a fractional ideal over $\mathbf{Z}[\alpha]$; then I can compute a principal ideal βA by multiplying $\beta\mathbf{Z}[\alpha]$ and A.

An alternate approach avoids fractional ideals. Say I is an ideal of A. One can multiply I by the discriminant of $\mathbf{Z}[\alpha]$, or the different $\varphi'(\alpha)$, to obtain an ideal of $\mathbf{Z}[\alpha]$.

References

1. Daniel J. Bernstein, *Computing coprime bases in essentially linear time*, preprint.
2. Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.
3. Hideyuki Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.
4. Michael E. Pohst, *Computational algebraic number theory*, Birkhaüser, Basel, 1993.

This article was processed by the author using the TEX macro package from Springer-Verlag.