mathematics

MDPI

Article

The Monogenity of Pure Quintic Fields: The Power of Sieving

István Gaál

Institute of Mathematics, University of Debrecen, Pf. 400, H-4002 Debrecen, Hungary; gaal.istvan@unideb.hu

Abstract

We provide a simple algorithm for calculating all generators of power integral bases in pure quintic fields. This procedure involves the usual standard elements like Baker's method and LLL reduction. The main purpose of this paper is to introduce a new idea to considerably diminish the number of small exponents to be considered after the reduction step. This new idea allows us to test all remaining small exponents within a few minutes, using an appropriate sieve method, which turns out to be surprisingly fast. This idea will be applicable in many similar cases.

Keywords: monogenity; power integral basis; pure quintic fields; Baker's method; LLL reduction; sieving

MSC: 11Y50; 11R04; 11D25

1. Introduction

Monogenity and power integral bases are classical topics in algebraic number theory, which is intensively studied even today; see [1,2].

A number field K of degree n with a ring of integers $\mathbb{Z}_K$ is called *monogenic* (cf. [2]) if there exists $\xi \in \mathbb{Z}_K$ such that $(1, \xi, \dots, \xi^{n-1})$ is an integral basis, called a *power integral basis*. We call ξ the *generator* of this power integral basis.

An irreducible polynomial $f(x) \in \mathbb{Z}[x]$ is called *monogenic* if a root ξ of $f(x)$ generates a power integral basis in $K = \mathbb{Q}(\xi)$. If $f(x)$ is monogenic, then K is also monogenic, but the converse is not true.

For $\alpha \in \mathbb{Z}_K$ (generating K over $\mathbb{Q}$), the module index

$$I(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$$

is called the *index* of α. The element α generates a power integral basis in K if and only if $I(\alpha) = 1$. The elements $\alpha, \beta \in \mathbb{Z}_K$ are called *equivalent* if $\alpha \pm \beta \in \mathbb{Z}$. Equivalent algebraic integers have equal indices. Searching for elements of $\mathbb{Z}_K$, generating power integral bases, leads to a Diophantine equation, called an *index form equation* (cf. [2]).

There are efficient algorithms for determining the generators of power integral bases in cubic and quartic number fields (cf. [2]), because in these cases, the corresponding index form equation can be reduced to Thue equations. Algorithms for solving absolute (over $\mathbb{Z}$) and relative (over $\mathbb{Z}_K$) Thue equations were also applied to solve index form equations in special higher-degree fields, like sextic and octic fields with a quadratic subfield (cf. [2]).

There was an attempt to solve index form equations in general quintic number fields (cf. [2]), but it turned out to be unusable, because of a very long CPU time (8 h, which is very long, even if there has been an improvement in hardware since then).

Academic Editor: Alvaro Anton-Sancho

Received: 30 April 2026
Revised: 21 May 2026
Accepted: 22 May 2026
Published: 23 May 2026

This showed that the method used to derive effective results for index form equations cannot be used in practice, not even if it is joined with an efficient enumeration algorithm (the so-called ellipsoid method; see [2,3]).

On the other hand, by using the Newton polygon method and Dedekind's criterion, many papers were written about the monogenity of several types of pure fields and binomials $x^n - m$.

Parallelly, we started to implement known methods to solve index form equations in certain pure fields. This was successful in pure sextic (cf., e.g., [4]) and pure octic fields. The reason is that in these cases, the pure field has a quadratic subfield, and the index form has a factor which implies a relative Thue equation.

It also turned out (cf. [4]) that the sieve method (see [2]) can be surprisingly efficient in such calculations.

In the present paper, we develop an algorithm for calculating all inequivalent generators of power integral bases in pure quintic fields. Our method involves the usual standard components like Baker's method and LLL reduction. The most difficult and time-consuming part of the method for general quintic fields is the enumeration of small exponent tuples remaining after the reduction procedure. Here we replace the complicated ellipsoid method with a simple sieve method. However, in the case of pure quintic fields, the sieve method is only sufficient if we use a specific idea, applied for the first time in this paper. This is the main novelty of this paper. This new idea allows us to present all generators of power integral bases in pure quintic fields within about 5 min of CPU time. It is guaranteed that this idea will have many further applications.

2. Pure Quintic Fields

Let $m \in \mathbb{Z}$, such that $f(x) = x^5 - m$ is irreducible. For simplicity, we also assume that it is also monogenic. For a straightforward extension of the method to non-monogenic polynomials, see Section 9.

The purpose of the present paper is to find all possible generators of power integral bases in $K = \mathbb{Q}(\xi)$, where ξ is a root of $f(x)$. We wonder whether there are any further inequivalent generators of power integral bases in K, in addition to ξ.

If $f(x)$ is monogenic, we can represent any $\alpha \in \mathbb{Z}_K$ in the form

$$\alpha = x_0 + x_1\xi + x_2\xi^2 + x_3\xi^3 + x_4\xi^4, \tag{1}$$

with $x_0, x_1, x_2, x_3, x_4 \in \mathbb{Z}$. Denote by D_K the discriminant of K, and let $\gamma^{(j)}$ be the conjugates of any $\gamma \in K$ ($j = 1, \dots, 5$). We have

$$\prod_{1 \le i < j \le 5} |\alpha^{(i)} - \alpha^{(j)}| = I(\alpha) \cdot \sqrt{|D_K|},$$

and

$$\prod_{1 \le i < j \le 5} |\xi^{(i)} - \xi^{(j)}| = I(\xi) \cdot \sqrt{|D_K|},$$

whence

$$\prod_{1 \le i < j \le 5} \frac{|\alpha^{(i)} - \alpha^{(j)}|}{|\xi^{(i)} - \xi^{(j)}|} = \frac{I(\alpha)}{I(\xi)}. \tag{2}$$

Using representation (1) of α, this can be written as

$$\prod_{1 \le i < j \le 5} |\ell_{ij}(x)| = \frac{I(\alpha)}{I(\xi)}, \tag{3}$$

where

$$\ell_{i,j}(x) = x_1 + x_2(\xi^{(i)} + \xi^{(j)}) + x_3((\xi^{(i)} + \xi^{(j)})^2 - \xi^{(i)}\xi^{(j)}) + x_4((\xi^{(i)} + \xi^{(j)})^3 - 2\xi^{(i)}\xi^{(j)}(\xi^{(i)} + \xi^{(j)})).$$

The Galois group of $f(x)$ is $D_5 = ST3$, which is doubly transitive (cf. [2]). Denote by $L_{i,j} = Q(\xi^{(i)} + \xi^{(j)}, \xi^{(i)}\xi^{(j)})$ the subfield of $Q(\xi^{(i)}, \xi^{(j)})$ which remains fixed under the action $(i,j) \to (j,i)$ of the Galois group. This is a proper subfield of $Q(\xi^{(i)}, \xi^{(j)})$ of degree 10. We denote by $\gamma^{(i,j)}$ the conjugates of any $\gamma^{(1,2)} \in L_{1,2}$ corresponding to $\xi^{(i)} + \xi^{(j)}, \xi^{(i)}\xi^{(j)}$. Obviously, $\gamma^{(i,j)} = \gamma^{(j,i)}$ $(1 \le i < j \le 5)$.

Equation (3) implies that $\ell_{i,j}(x)$ is contained in $L_{i,j}$. In our case $I(\xi) = 1$, and we are looking for $\alpha \in \mathbb{Z}_K$ with $I(\alpha) = 1$; therefore $\ell_{i,j}$ is a unit in $L_{i,j}$. The field $L_{i,j}$ has $s = 2$ real and $2t = 8$ complex conjugates; therefore its unit rank is $r = s + t - 1 = 5$. Let $\varepsilon_1^{(i,j)}, \ldots, \varepsilon_5^{(i,j)}$ be a set of fundamental units in $L_{i,j}$. We have

$$\ell_{i,j}(x) = \pm \prod_{h=1}^{5} (\varepsilon_h^{(i,j)})^{a_h}, \tag{4}$$

with $a_h \in \mathbb{Z}$ $(1 \le h \le 5)$.

3. The Structure of the Degree 10 Field $L_{i,j}$

Using symmetric polynomials, it is easily seen that the field $L_{i,j} = Q(\xi^{(i)} + \xi^{(j)}, \xi^{(i)}\xi^{(j)})$ is generated by a root of

$$g(x) = x^{10} + 11mx^5 - m^2.$$

Denote by β a root of $g(x)$. Then

$$(\beta^5)^2 + 11m\beta^5 - m^2 = 0,$$

whence

$$\beta^5 = \frac{-11m \pm \sqrt{121m^2 + 4m^2}}{2} = m\frac{-11 \pm 5\sqrt{5}}{2},$$

which implies that $\sqrt{5} \in L_{i,j}$. Moreover,

$$\beta^5 = (\sqrt[5]{m})^5 \cdot (-1)^5 \cdot \left(\frac{1 \mp \sqrt{5}}{2}\right)^5,$$

whence a value of $\sqrt[5]{m}$ is also contained in $L_{i,j}$. These are the quadratic and quintic subfields of $L_{i,j}$. Let η be the fifth root of unity with the smallest positive argument; that is $\eta \approx \sqrt[5]{1} = -0.8090 - 0.5877I$, and let $\sqrt[5]{m}$ be the real value of the fifth root of m. Then $\xi^{(i)} = \eta^i \cdot \sqrt[5]{m}$ $(1 \le i \le 5)$. We observe that

$$\frac{(\xi^{(i)} + \xi^{(f)})^2}{\xi^{(i)}\xi^{(j)}} = \frac{\eta^{2i} + \eta^{2j} + 2\eta^{i+j}}{\eta^{i+j}} = \eta^{i-j}\eta^{j-i} + 2.$$

This value is equal to

$$f_1 = \frac{3 + \sqrt{5}}{2} \quad \text{for} \quad (i,j) = (1,3), (1,4), (2,4), (2,5), (3,5),$$

and

$$f_2 = \frac{3 - \sqrt{5}}{2} \quad \text{for} \quad (i,j) = (1,2), (1,5), (2,3), (3,4), (4,5). \tag{5}$$

This way we can detect in which $L_{i,j}$ the elements of the quadratic subfield $\mathbb{Q}(\sqrt{5})$ remain fixed. This will be important in the final step of our algorithm.

4. Baker's Method

The first components of our algorithm are the standard ones, Baker's method and reduction. We follow [2] but make the description more exact in our case.

Let $1 \le i, j, k \le 5$ be distinct indices. We have

$$(\alpha^{(i)} - \alpha^{(j)}) + (\alpha^{(j)} - \alpha^{(k)}) + (\alpha^{(k)} - \alpha^{(i)}) = 0, \tag{6}$$

whence

$$(\xi^{(i)} - \xi^{(j)})\ell_{i,j}(x) + (\xi^{(j)} - \xi^{(k)})\ell_{j,k}(x) + (\xi^{(k)} - \xi^{(i)})\ell_{k,i}(x) = 0. \tag{7}$$

That is

$$\frac{(\xi^{(i)} - \xi^{(j)})\ell_{i,j}(x)}{(\xi^{(i)} - \xi^{(k)})\ell_{i,k}(x)} + \frac{(\xi^{(k)} - \xi^{(j)})\ell_{j.k}(x)}{(\xi^{(k)} - \xi^{(i)})\ell_{i,k}(x)} = 1. \tag{8}$$

This can be written as

$$\delta_{ijk}\mu_{ijk} + \delta_{kji}\mu_{kji} = 1, \tag{9}$$

where

$$\delta_{ijk} = \frac{\xi^{(i)} - \xi^{(j)}}{\xi^{(i)} - \xi^{(k)}}, \quad \mu_{ijk} = \pm \prod_{h=1}^{5} \left(\frac{\varepsilon_h^{(i,j)}}{\varepsilon_h^{(i,k)}} \right)^{a_h}.$$

We have

$$a_1 \log \left| \frac{\varepsilon_1^{(i,j)}}{\varepsilon_1^{(j,k)}} \right| + \cdots + a_5 \log \left| \frac{\varepsilon_5^{(i,j)}}{\varepsilon_5^{(j,k)}} \right| = \log \left| \mu_{ijk} \right|.$$

Select five distinct triples (i, j, k) for which the coefficient matrix T of this system of linear equations is regular. Denote by c_1 the row norm (the maximum sum of the absolute values of entries in a row) of T^{-1}. Then we obtain

$$A = \max_{1 \le h \le 5} |a_h| \le c_1 \left| \log \left| \mu_{i_0 j_0 k_0} \right| \right|,$$

where

$$\left| \log \left| \mu_{i_0 j_0 k_0} \right| \right| = \max_{i,j,k} \left| \log \left| \mu_{ijk} \right| \right|.$$

If $\log \left| \mu_{i_0 j_0 k_0} \right| < 1$, then this implies

$$\left| \mu_{i_0 j_0 k_0} \right| \le \exp\left(-\frac{A}{c_1} \right),$$

otherwise the same holds for $\mu_{i_0 k_0 j_0} = 1/\mu_{i_0 j_0 k_0}$.

We omit the subindices of i_0, j_0, k_0 and assume that

$$\left| \mu_{ijk} \right| \le \exp\left(-\frac{A}{c_1} \right).$$

Remark 1. *As we cannot predict for which triple i, j, k this inequality is satisfied, we have to apply the following estimates and the reduction procedure for all possible triples i, j, k. After obtaining the reduced bound for A in all possible cases, the enumeration procedure must be performed only once. In enumeration, we have to use the maximum of the reduced bounds obtained for the possible triples i, j, k.*

We have

$$\Lambda = \left|\log\left|\frac{\xi^{(k)}-\xi^{(j)}}{\xi^{(k)}-\xi^{(i)}}\right| + a_1\log\left|\frac{\varepsilon_1^{(j,k)}}{\varepsilon_1^{(i,k)}}\right| + \cdots + a_5\log\left|\frac{\varepsilon_5^{(j,k)}}{\varepsilon_5^{(i,k)}}\right|\right|$$

$$= \left|\log\left|\delta_{kji}\mu_{kji}\right|\right| \le 2\left|1-\left|\delta_{kji}\mu_{kji}\right|\right| \le 2\left|1-\delta_{kji}\mu_{kji}\right| = 2\left|\delta_{ijk}\mu_{ijk}\right| \le c_2\exp\left(-\frac{A}{c_1}\right),$$

where

$$c_2 = 2\max_{i,j,k}|\delta_{ijk}|.$$

Note that here we used the inequality $|\log z| < 2|1-z|$, valid for $z \in \mathbb{C}$ if the right-hand side is <0.795. This is satisfied, because even the reduced bound for A will be about 45. Also, in all our examples, $\log\left|\frac{\xi^{(k)}-\xi^{(j)}}{\xi^{(k)}-\xi^{(i)}}\right|$ was linearly dependent on $\log\left|\frac{\varepsilon_1^{(j,k)}}{\varepsilon_1^{(i,k)}}\right|, \ldots, \log\left|\frac{\varepsilon_5^{(j,k)}}{\varepsilon_5^{(i,k)}}\right|$; therefore we have to deal with an inequality of the form

$$\Lambda = \left|a_1\log\left|\frac{\varepsilon_1^{(j,k)}}{\varepsilon_1^{(i,k)}}\right| + \cdots + a_5\log\left|\frac{\varepsilon_5^{(j,k)}}{\varepsilon_5^{(i,k)}}\right|\right| \le c_2\exp\left(-\frac{A}{c_1}\right), \tag{10}$$

(with an obvious transformation of $a_1, \ldots, a_5$, depending on the example).

Applying a Baker-type lower estimate for Λ (for example, the estimates of [5]), we obtain

$$\lambda < \exp(-C\log A),$$

with a large constant C. Comparing it with the upper estimate (10), we conclude with an upper bound A_B for A. In our example, this was about 10^{34}.

5. Reduction

Let H be a constant. Consider the lattice spanned by the columns of the 6-by-5 matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ H\log\left|\frac{\varepsilon_1^{(j,k)}}{\varepsilon_1^{(i,k)}}\right| & H\log\left|\frac{\varepsilon_2^{(j,k)}}{\varepsilon_2^{(i,k)}}\right| & H\log\left|\frac{\varepsilon_3^{(j,k)}}{\varepsilon_3^{(i,k)}}\right| & H\log\left|\frac{\varepsilon_4^{(j,k)}}{\varepsilon_4^{(i,k)}}\right| & H\log\left|\frac{\varepsilon_5^{(j,k)}}{\varepsilon_5^{(i,k)}}\right| \end{pmatrix}.$$

We apply a special case of Lemma 2.4 of [2]:

Lemma 1. *If $a_1, \ldots, a_5$ satisfy (10), $A = \max_{1\le h\le 5}|a_h| \le A_0$ and H is large enough so that the first vector b_1 of the LLL-reduced basis of the above lattice satisfies*

$$|b_1| \ge \sqrt{96}\cdot A_0,$$

then

$$A \le c_1(\log H + \log c_2 - \log A_0).$$

The original bound obtained in the previous section is reduced in several subsequent steps. A typical sequence is shown in the following Table 1, starting with $A_0 = 10^{34}$:

Table 1. The reduction procedure

A_0	H	Reduced Bound
10^{34}	10^{174}	344
344	10^{17}	59
59	10^{13}	45
45	$2 \cdot 10^{12}$	43

Using such large values, we must be very cautious in terms of the accuracy of our calculations. We used 250 digits. In the first steps, the reduction is very efficient; after a few steps, the reduced bound is not smaller than the original bound, so then we stop the procedure.

6. Sieving

In our case, we only have five exponents instead of nine in the general case (see [2]). However, if the reduced bound is A_R, then the total number of possible exponent vectors $(a_1, \dots, a_5)$ for us to check is $(2A_R + 1)^5$, which, in the case where $A_R = 45$, is more than $6 \cdot 10^9$. In this section, we introduce a new idea, which helps us to overcome this difficulty and can be applied in several similar cases.

The first idea is to use sieving, which was very efficient in a previous work [4].

The main idea is to utilize the fact that in all our examples, one of the fundamental units comes from the quadratic subfield.

Consider an equation of the form (8). As mentioned above, in all of our examples, one of the fundamental units was from the quadratic subfield $\mathbb{Q}(\sqrt{5})$. Assume this is ε_1. In terms of type

$$\frac{(\xi^{(i)} - \xi^{(j)})\ell_{i,j}(x)}{(\xi^{(i)} - \xi^{(k)})\ell_{i,k}(x)} = \frac{\xi^{(i)} - \xi^{(j)}}{\xi^{(i)} - \xi^{(k)}} \prod_{1 \le h \le 5} \left(\frac{\varepsilon_h^{(i,j)}}{\varepsilon_h^{(i,k)}} \right)^{a_h}$$

it may happen that $\varepsilon_1^{(i,j)} = \varepsilon_1^{(i,k)}$. In Section 3, we explicitly selected conjugates (i, j) that leave the elements of the quadratic subfield unchanged. The problem is that there exists no triple (i, j, k) such that all of $(i, j), (j, k), (k, i)$ leaves the quadratic subfield fixed. Therefore identities of type (8) can not be used to get rid of ε_1.

But it turns out from (5) that all of

$$(1,2), (2,3), (3,4), (4,5), (5,1)$$

has this property. We have

$$(\xi^{(1)} - \xi^{(2)})\ell_{1,2}(x) + (\xi^{(2)} - \xi^{(3)})\ell_{2,3}(x) + (\xi^{(3)} - \xi^{(4)})\ell_{3,4}(x)$$
$$+(\xi^{(4)} - \xi^{(5)})\ell_{4,5}(x) + (\xi^{(5)} - \xi^{(1)})\ell_{5,1}(x) = 0,$$

whence

$$\frac{(\xi^{(1)} - \xi^{(2)})\ell_{1,2}(x)}{(\xi^{(1)} - \xi^{(5)})\ell_{1,5}(x)} + \frac{(\xi^{(2)} - \xi^{(3)})\ell_{2,3}(x)}{(\xi^{(1)} - \xi^{(5)})\ell_{1,5}(x)} + \frac{(\xi^{(3)} - \xi^{(4)})\ell_{3,4}(x)}{(\xi^{(1)} - \xi^{(5)})\ell_{1,5}(x)} + \frac{(\xi^{(4)} - \xi^{(5)})\ell_{4.5}(x)}{(\xi^{(1)} - \xi^{(5)})\ell_{1,5}(x)} = 1. \tag{11}$$

In all fractions of type

$$\frac{(\xi^{(i)}-\xi^{(j)})\ell_{i,j}(x)}{(\xi^{(1)}-\xi^{(5)})\ell_{1,5}(x)}=\frac{\xi^{(i)}-\xi^{(j)}}{\xi^{(1)}-\xi^{(5)}}\left(\frac{\varepsilon_1^{(i,j)}}{\varepsilon_1^{(1,5)}}\right)^{a_1}\left(\frac{\varepsilon_2^{(i,j)}}{\varepsilon_2^{(1,5)}}\right)^{a_2}\left(\frac{\varepsilon_3^{(i,j)}}{\varepsilon_3^{(1,5)}}\right)^{a_3}\left(\frac{\varepsilon_4^{(i,j)}}{\varepsilon_4^{(1,5)}}\right)^{a_4}\left(\frac{\varepsilon_5^{(i,j)}}{\varepsilon_5^{(1,5)}}\right)^{a_5}$$

$\frac{\varepsilon_1^{(i,j)}}{\varepsilon_1^{(1,5)}}=1$, whence for $(i,j)=(1,2),(2,3),(3,4),(4,5)$, we have

$$\frac{(\xi^{(i)}-\xi^{(j)})\ell_{i,j}(x)}{(\xi^{(1)}-\xi^{(5)})\ell_{1,5}(x)}=\frac{\xi^{(i)}-\xi^{(j)}}{\xi^{(1)}-\xi^{(5)}}\left(\frac{\varepsilon_2^{(i,j)}}{\varepsilon_2^{(1,5)}}\right)^{a_2}\left(\frac{\varepsilon_3^{(i,j)}}{\varepsilon_3^{(1,5)}}\right)^{a_3}\left(\frac{\varepsilon_4^{(i,j)}}{\varepsilon_4^{(1,5)}}\right)^{a_4}\left(\frac{\varepsilon_5^{(i,j)}}{\varepsilon_5^{(1,5)}}\right)^{a_5}.$$

This yields that when testing equations of the form (11), instead of the usual identity (8), we have to calculate four fractions for $(2A_R+1)^4$ exponent tuples, instead of two fractions for $(2A_R+1)^5$ exponent tuples. In the case where $A_R=45$, it yields the calculation of only 274,299,844 fractions, instead of 12,480,642,902 ($2.7\cdot10^8$ instead of $1.2\cdot10^{10}$). Finally, it is important to note that the integer arithmetic of Maple is very fast, so calculating $2.7\cdot10^8$ fractions can be performed within a few minutes, which makes our method feasible, in contrast with the method for general quintic fields (see [2]). Also, it is much simpler to implement this procedure.

We choose primes p such that the polynomial $f(x)=x^5-m$ splits into linear factors modulo p; that is

$$f(x)\equiv\prod_{1\le i\le5}(x-m_i)\pmod p,$$

with some $m_i\in\mathbb{Z}$. This yields $\xi^{(i)}\equiv m_i$ modulo a prime ideal $\mathfrak{p}$ of the normal closure of $K=\mathbb{Q}(\xi)$, lying above p. Then $\xi^{(1)}/\xi^{(2)}\equiv m_1/m_1\pmod{\mathfrak{p}}$ gives a primitive fifth root of unity, which allows us to determine $\xi^{(j)}\pmod{\mathfrak{p}}$ $(2\le j\le5)$ from $\xi^{(1)}$, similarly, as in Section 3. Then we obtain $\xi^{(i)}+\xi^{(j)},\xi^{(i)}-\xi^{(j)}$ and the corresponding conjugates of the units modulo $\mathfrak{p}$. Assume that

$$\frac{\xi^{(i)}-\xi^{(j)}}{\xi^{(1)}-\xi^{(5)}}\equiv s_{ij15}\pmod{\mathfrak{p}},\quad\frac{\varepsilon_h^{(i,j)}}{\varepsilon_h^{(1,5)}}\equiv e_{hij15}\pmod{\mathfrak{p}},$$

Then (11) implies that

$$s_{1215}\prod_{h=2}^{4}e_{h1215}^{a_h}+s_{2315}\prod_{h=2}^{4}e_{h2315}^{a_h}+s_{3415}\prod_{h=2}^{4}e_{h3415}^{a_h}+s_{4515}\prod_{h=2}^{4}e_{h4515}^{a_h}\equiv1\pmod{\mathfrak{p}}.$$

But these are all integers in $\mathbb{Z}$; hence the congruence is valid also modulo the prime p:

$$s_{1215}\prod_{h=2}^{4}e_{h1215}^{a_h}+s_{2315}\prod_{h=2}^{4}e_{h2315}^{a_h}+s_{3415}\prod_{h=2}^{4}e_{h3415}^{a_h}+s_{4515}\prod_{h=2}^{4}e_{h4515}^{a_h}\equiv1\pmod{p}.$$

This is the modulo p congruence that we test for $-A_R\le a_2,a_3,a_4,a_5\le A_R$. If a tuple (a_2,a_3,a_4,a_5) survives the test, then we test it modulo another suitable prime. All together we used five primes, and only very few exponent tuples survived all of them.

If (a_2,a_3,a_4,a_5) passed these tests, then we substituted (a_2,a_3,a_4,a_5) into an identity of the form (8), also involving a_1. We checked the identity for $-A_R\le a_1\le A_R$ modulo some primes p, similarly as above.

If $(a_1, a_2, a_3, a_4, a_5)$ passed, we explicitly calculated $\nu_{ij} = \prod_{h=1}^{5} (\varepsilon_h^{(ij)})^{a_h}$ (cf. (4)) for four pairs i, j such that the system of linear equations

$$\ell_{ij}(x) = \nu_{ij}$$

is uniquely solvable in x_1, x_2, x_3, x_4. If the solutions are integers, we checked whether the index of α in (1) is indeed equal to 1.

7. Some Computational Results

Using our algorithm, we calculated all inequivalent generators of power integral bases in ten pure quintic fields generated by a root of an irreducible monogenic polynomial $f(x) = x^5 - m$ with the smallest positive m.

In the following Table 2, we display m, the bound A_B obtained by Baker's method, and the bound A_R obtained after reduction. We include the primes that we used for sieving, the total number of exponent tuples to be tested and the number of exponent tuples that survived the modulo p tests and were further tested by the next prime. Finally, all (x_1, x_2, x_3, x_4) are listed such that $\alpha = x_0 + x_1\zeta + x_2\zeta^2 + x_3\zeta^3 + x_4\zeta^4$ generates a power integral basis in K ($x_0 \in \mathbb{Z}$ arbitrary).

Table 2. Results of our calculations

$m = 2$, $A_B = 10^{34}$, $A_R = 54$, CPU time: 9 min
primes: 151, 241, 251, 431, 571 tested: 141,158,161 survived: 1,869,184, 15,734, 254, 139, 136 solutions: (1, 0, 0, 0), (1, 1, 1, 1)
$m = 3$, $A_B = 10^{34}$, $A_R = 47$, CPU time: 6 min
primes: 41, 431, 491, 661, 761 tested: 81,450,625 survived: 3,963,567, 18,458, 131, 44, 44 solutions: (1, 0, 0, 0)
$m = 5$, $A_B = 10^{34}$, $A_R = 47$, CPU time: 5 min
primes: 31, 191, 251, 271, 601 tested: 81,450,625 survived: 5,254,688, 55,052, 454, 9, 6 solutions: (1, 0, 0, 0)
$m = 6$, $A_B = 10^{34}$, $A_R = 41$, CPU time: 3 min
primes: 31, 101, 191, 281, 421 tested: 47,458,321 survived: 2,936,318, 58,581, 633, 13, 8 solutions: (1, 0, 0, 0), (1, −1, −1, 0)
$m = 10$, $A_B = 10^{34}$, $A_R = 43$, CPU time: 4 min
primes: 11, 101, 251, 281, 521 tested: 57,289,761 survived: 9,894,424, 195,800, 1538, 15, 3 solutions: (1, 0, 0, 0)

Table 2. *Cont.*

$m = 11$, $A_B = 10^{34}$, $A_R = 46$, CPU time: 5 min
primes: 61,191,241,311,541 tested: 74,805,201 survived: 2,463,570, 25,691, 265, 48, 46 solutions: (1, 0, 0, 0), (1, −1, 0, 0)
$m = 13$, $A_B = 10^{34}$, $A_R = 45$, CPU time: 5 min
primes: 61, 271, 311, 331, 461 tested: 68,574,961 survived: 2,263,594, 16,640, 127, 11, 10 solutions: (1, 0, 0, 0)
$m = 14$, $A_B = 10^{34}$, $A_R = 46$, CPU time: 5 min
primes: 41,61,101,191,211 tested: 74,805,201 survived: 3,665,415, 119,766, 2389, 28, 1 solutions: (1, 0, 0, 0)
$m = 15$, $A_B = 10^{34}$, $A_R = 43$, CPU time: 4 min
primes: 211, 241, 311, 541, 761 tested: 57,289,761 survived: 543,159, 4619, 17, 1, 1 solutions: (1, 0, 0, 0)
$m = 17$, $A_B = 10^{34}$, $A_R = 46$, CPU time: 5 min
primes: 101, 181, 491, 601, 701 tested: 74,805,201 survived: 1,477,946, 16,109, 80, 1, 1 solutions: (1, 0, 0, 0)

8. Remarks on the Calculations

The units of the degree 10 fields were calculated by Magma [6], and all other calculations were performed by Maple [7]. The codes were run on a standard PC with a 2.5 GHz processor. For the reduction procedure, we used 250-digit accuracy. In addition to the modulo p test of the possible exponent tuples, all remaining calculations took a negligible amount of CPU time, only a few seconds.

9. Conclusions

Introducing a new idea for testing small exponent tuples, we succeeded in presenting an algorithm to determine all generators of power integral bases in pure quintic fields.

This idea will certainly have further applications.

For simplicity, we present our method for monogenic polynomials $x^5 - m$. However, our procedure can obviously be extended to the case of non-monogenic polynomials $f(x) = x^5 - m$. In this case, instead of (1), we represent $\alpha \in \mathbb{Z}_K$ in the form

$$\alpha = \frac{x_0 + x_1\xi + x_2\xi^2 + x_3\xi^3 + x_4\xi^4}{d},$$

with a common denominator $d \in \mathbb{Z}$. This implies that

$$\prod_{1 \le i < j \le 5} |\ell_{i,j}(x)| = \frac{d^{10}}{I(\xi)} = N,$$

that is, instead of being a unit in $L_{i,j}$, $\ell_{i,j}(x)$ are algebraic integers of norm N in $L_{i,j}$. Then we have to determine all non-associated integers $\gamma^{(i,j)}$ of $L_{i,j}$ of norm N,

$$\ell_{i,j}(x) = \pm\gamma^{(i,j)} \prod_{h=1}^{5} (\varepsilon_h^{(i,j)})^{a_h},$$

and the above procedure must be performed for all possible values of γ.

Funding: This research received no external funding

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The author thanks the editor and the referees for their careful reading and for their comments that improved the quality of this paper.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed.; Springer: Berlin/Heidelberg, Germany, 2004.
2. Gaál, I. Diophantine equations and power integral bases. In *Theory and Algorithms*, 2nd ed.; Birkhäuser: Boston, MA, USA, 2019.
3. Wildanger, K. Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern. *J. Number Theory* **2000**, *82*, 188–224. [CrossRef]
4. Gaál, I. Calculating generators of power integral bases in sextic fields with a real quadratic subfield. *JP J. Algebra Number Theory Appl.* **2025**, *64*, 289–306. [CrossRef]
5. Baker, A.; Wüstholz, G. Logarithmic forms and group varieties. *J. Reine Angew. Math.* **1993**, *442*, 19–62.
6. Bosma, W.; Cannon, J.; Playoust, C. The Magma Algebra System. I. The User Language. *J. Symb. Comput.* **1997**, *24*, 235–265. [CrossRef]
7. Char, B.W.; Geddes, K.O.; Gonnet, G.H.; Monagan, M.B.; Watt, S.M. (Eds.) *MAPLE, Reference Manual*; Watcom Publications: Waterloo, ON, Canada, 1988.