INTEGERS FOR RADICAL EXTENSIONS OF ODD PRIME DEGREE AS PRODUCT OF SUBRINGS

JULIUS KRAEMER

ABSTRACT. For a radical extension $K$ of odd prime degree the ring $\mathcal{O}_K$ of integers is constructed as a product of subrings with the following property: for all prime divisors $q$ of the discriminant of $\mathcal{O}_K$ there is a $q$-maximal factor. The discriminant of $\mathcal{O}_K$ is the greatest common divisor of the discriminants of all factors. The results are applied to give a criterion for the monogeneity of $K$ where the opposite is not true.

Keywords Ring of algebraic integers · Radical extension · Pure extension · Wieferich prime · non-squarefree integer · Monogeneity

Mathematics Subject Classification 11R04 · 11R20

The author is grateful to Keith Conrad and Hanson Smith for hints and references. The author is grateful to Guido Kraemer for proofreading a previous version.

1. INTRODUCTION

For $n \geq 2$ and $a \in \mathbb{Z}, a \neq \pm 1$, consider the polynomial $A(X) = X^n - a$ and assume that it is irreducible over $\mathbb{Z}$. Define $\alpha = \sqrt[n]{a}, \beta = \alpha - a, K = \mathbb{Q}(\alpha)$ and denote by $\mathcal{O}_K$ the ring of integers of $K$. Such radical extensions are also known as pure extensions in the literature.

The present paper is based on the findings of [3] where it has been characterized when $\mathcal{O}_K = \mathbb{Z}[a]$. This is true under certain conditions (see Theorem 5.3 of [3]). Turning this theorem into the negative it follows that $\mathbb{Z}[a] \subsetneq \mathcal{O}_K$ is equivalent to

(i) $a$ is not squarefree

or

(ii) There is a prime factor of $n$ which is a Wieferich prime to base $a$.

Definition 1.1. Let $q$ be a natural prime and $r \neq \pm 1$ a nonzero rational integer.

(i) $q$ is a Wieferich prime to base $r$ if $q^2$ divides $r^{q-1} - 1$. 

In this paper we identify integers for radical extensions of odd prime degree as a product of subrings.

(ii) If the context is clear we will speak of the (non-)Wieferich case if \( q \) is (not) a Wieferich prime to base \( r \).

(iii) Let \( \mathcal{O} \subseteq \mathcal{O}_K \) be a subring. Then \( \mathcal{O} \) is said to be \( q \)-maximal if the index \( [\mathcal{O}_K: \mathcal{O}] \) is not divided by \( q \).

For more information concerning Wieferich primes see Section 4 of [3] and the references cited there. Note that \( q \) always divides \( r^{q-1} - 1 \) if \( q \) and \( r \) are coprime (Little Fermat Theorem). The definition of \( q \)-maximality can be found in 6.1.1 of [2].

In the present paper we assume that \( n = p \) is an odd prime. The oddness of \( p \) is not a real restriction because for \( p = 2 \) the ring of integers for radical extensions is already well-known.

In the main theorem we characterize \( \mathcal{O}_K \) as a product of subrings of the form \( \mathbb{Z}[\gamma_i] \), where \( \mathbb{Z}[\gamma_i] \) is \( q_i \)-maximal and \( q_i \) runs through all prime divisors of \( \alpha \); furthermore the minimal polynomial of all \( \gamma_i \) is of the form \( X^p - c_i \). In the Wieferich case an additional factor of the form \( \mathbb{Z}[\beta_i] \) is necessary to ensure \( p \)-maximality. The discriminant of \( \mathcal{O}_K \) is calculated as the greatest common divisor of the factors without using \( \mathbb{Z} \) bases of \( \mathcal{O}_K \).

The proof of the main theorem and its corollaries in Section 5 needs some preparation which is done in Sections 2 to 4:

In Section 2 preliminaries are handled which we need for the following sections.

In Section 3 the Wieferich case is handled: We prove that a specific subring of \( \mathcal{O}_K \) is \( p \)-maximal.

In Section 4 the non-squarefree case is handled: For every prime factor \( q \) of \( \alpha \) we construct a subring which is \( q \)-maximal.

In Section 6 we give examples and a criterion for the monogeneity of \( K \) where the opposite is not true.

We denote the greatest common divisor of elements \( x_1, \ldots, x_n \) of a unique factorization domain by \( (x_1, \ldots, x_n) \) or \( (x_i; 1 \leq i \leq n) \).

2. PRELIMINARIES

In this section we prove lemmas and propositions which are needed in the subsequent sections.

**Lemma 2.1.** Let \( q \) be a prime and \( r, s \) rational integers. Then:

(i) The polynomial \( X^q - r \) is irreducible over \( \mathbb{Z} \) if and only if \( X^q - rs^q \) is irreducible over \( \mathbb{Z} \).

(ii) If \( X^q - r \) is irreducible over \( \mathbb{Z} \) then \( \mathbb{Q}(\sqrt[q]{r}) = \mathbb{Q}(\sqrt[q]{rs^q}) \).

**Proof.** (i) A well-known theorem due to N. H. Abel (see Satz 277 together with Satz 180 of [7]) says that \( X^q - r \) is irreducible over \( \mathbb{Z} \) if and only if \( r \) is not a \( q \)-th power in \( \mathbb{Z} \). Then (i) follows immediately.
(ii) This is immediate. \[ \square \]

**Remark 2.2.** As an immediate consequence of Lemma 2.1 we can assume in the following without restriction that in the prime decomposition \( a = \prod_{i=1}^{m} q_i^{e_i} \) it holds that 1 \( \leq e_i \leq p - 1 \) for all 1 \( \leq i \leq m \).

\[ \square \]

The following lemma introduces some further notation and properties of bases of Wieferich primes.

**Lemma 2.3.** Let \( r \neq \pm 1 \) and \( s \) be nonzero integers coprime to \( p \). Then:

(i) If \( p \) is not a Wieferich prime to base \( r \) then, for 1 \( \geq 1 \), it holds that \( p \) is a Wieferich prime to base \( r^e \) if and only if \( p \) divides \( e \).

(ii) If \( p \) is a Wieferich prime to base \( r \) then \( p \) is a Wieferich prime to base \( r^e \) for all 1 \( \geq 1 \).

(iii) \( p \) is a Wieferich prime to base \( rs^p \) if and only if \( p \) is a Wieferich prime to base \( r \).

If \( s^p \) divides \( r \) then \( p \) is a Wieferich prime to base \( \frac{r}{s^p} \) if and only if \( p \) is a Wieferich prime to base \( r \).

(iv) For 1 \( \leq j \leq m \) there are 1 \( \leq u_j \leq p - 1 \) and \( v_j \geq 0 \) such that \( e_j u_j - pv_j = 1 \).

(v) For 1 \( \leq j \leq m \) denote \( c_j = \frac{a^{u_j}}{q_j^{v_j}} \). Then \( c_j \) is an integer where \( q_j \) is a squarefree factor.

\( p \) is a Wieferich prime to base \( c_j \) if and only if \( p \) is a Wieferich prime to base \( a \).

(vi) \( (c_j; 1 \leq j \leq m) = \prod_{j=1}^{m} q_j \).

**Proof.** (i) and (ii) Decompose \( r^{e(p-1)} - 1 = (r^{p-1} - 1) \cdot \sum_{i=0}^{e-1} r^{i(p-1)} \). Then (i) is clear because \( p \) divides \( r^{p-1} - 1 \) (Little Fermat), and \( p \) divides \( \sum_{i=0}^{e-1} r^{i(p-1)} \) if and only if \( p \) divides \( e \) (again by Little Fermat). Also (ii) is clear because \( p^2 \) divides already \( r^{p-1} - 1 \).

(iii) Calculate \( (rs^p)^{p-1} - 1 = r^{p-1}s^{p(p-1)} - 1 = s^{p(p-1)}(r^{p-1} - 1) + (s^{p(p-1)} - 1) \).

From (i) and (ii) it follows that \( p^2 \) divides \( s^{p(p-1)} - 1 \), hence again applying (i) and (ii), it follows that \( p^2 \) divides \( (rs^p)^{p-1} - 1 \) if and only if \( p^2 \) divides \( r^{p-1} - 1 \) which is the first statement of (iii). The second statement of (iii) is proved analogously by using \( \left( \frac{r}{s^p} \right)^{p-1} - 1 = \frac{1}{s^{p(p-1)} - 1} \cdot \left( (r^{p-1} - 1) - (s^{p(p-1)} - 1) \right) \) which is divided by \( p^2 \) if and only if the numerator is divided by \( p^2 \).

(iv) This follows immediately because \( e_j \) and \( p \) are coprime: Choose \( u_j \) as a positive lift of \( e_j^{-1} \) mod \( p \) to \( \mathbb{Z} \) which lies between 1 and \( p - 1 \).

(v) From (iv) it follows that \( c_j = \frac{a^{u_j}}{q_j^{v_j}} = \prod_{i=1}^{m} q_i^{e_i u_j} \cdot \prod_{i \neq j} q_i^{e_i u_j} = q_j^{v_j} \cdot \prod_{i \neq j} q_i^{e_i u_j} \).
which is an integer where \( q_j \) is a squarefree factor. The second statement follows
from (i), (ii) and (iii) because \( u_j \) is coprime to \( p \) hence \( p \) is a Wieferich prime to
base \( c_j \) if and only if \( p \) is a Wieferich prime to base \( a^{u_j} \) if and only if \( p \) is a Wieferich
prime to base \( a \).

(vi) This follows immediately from (v).

\[ \square \]

Remark 2.4. For \( 1 \leq j \leq m \) it holds that \( e_j = 1 \) if and only if \( u_j = 1 \) and \( v_j = 0 \).
For \( e_i \geq 2 \) it follows that \( u_j \geq 2 \) and \( v_j \geq 1 \).

\[ \text{Proof. This is immediate from Lemma 2.3 (iv).} \quad \square \]

Lemma 2.5.

(i) It holds that \( \mathbb{Z}[\alpha] = \mathbb{Z}[\beta] \).

(ii) The minimal polynomial of \( \beta \) is
\[ B(X) = (X + a)^p - a = X^p + ap \left( \sum_{i=1}^{p-1} \frac{p}{i} a^{p-1-i} X^i + \frac{a^{p-1} - 1}{p} \right). \]

(iii) Also \( \{ \beta^i; 0 \leq i \leq p - 1 \} \) is a power base of \( \mathbb{Z}[\beta] \).

(iv) For a subring \( \mathcal{O} \subseteq \mathcal{O}_K \) the discriminants of all \( \mathbb{Z} \) bases of \( \mathcal{O} \) are equal.

(v) The discriminant \( \text{disc}(\mathbb{Z}[\beta]) \) equals \( (-1)^{\frac{p-1}{2}} \cdot a^{p-1} \cdot p^p \).

(vi) Exactly \( p \) and the prime factors of \( a \) can ramify in \( \mathcal{O}_K \), in particular
only \( p \) and the prime factors of \( a \) can divide \( \text{disc}(\mathcal{O}_K) \).

\[ \text{Proof. (i) This follows because } \beta \in \mathbb{Z}[\alpha] \text{ and } a \in \mathbb{Z}[\beta]. \]

(ii) This holds because \( A(X) = X^p - a \) is the minimal polynomial of \( a \).

(iii) This is clear.

(iv) This holds because the square of the determinant of every base change matrix \( B \) between the power bases is 1. Then the statement follows from the well-known theorem that the discriminants of two \( \mathbb{Z} \) bases differ by the factor \( \det(B)^2 = 1 \) (see Proposition 1 in §2.7 of [8]).

(v) For \( 0 \leq i, j \leq p - 1 \) evaluate the trace of \( a^{i+j} \):
It is 0 for \( i + j \neq p \) or \( i \neq 0 \); it is \( p \) if \( i = j = 0 \); it is \( ap \) if \( i + j = p \).

Then the discriminant can be calculated directly because it is the determinant of the
trace matrix. Note that a diagonal matrix can be reached with \( \frac{p-1}{2} \) interchanges of
rows.

(vi) This is a well-known theorem, see Theorem 1 in §5.3 of [8]). \( \square \)

We now state a criterion from which Dedekind’s Index Criterion is a special case. It is
stated in 6.1.4. of [2] and will be used intensively in the present paper. Denote by \( \mathbb{F}_q \)
the field with \( q \) elements.

Theorem 2.6 (Dedekind). Let \( K = \mathbb{Q}(\sqrt{D}) \) be a number field, \( T \in \mathbb{Z}[X] \) the
minimal polynomial of \( \sqrt{D} \) and let \( q \) be a prime number.

Denote by \( \bar{T} \) the reduction mod \( q \) (in \( \mathbb{Z}, \mathbb{Z}[X], \) or \( \mathbb{Z}[\alpha] \)). Let
\[ \bar{T}(X) = \prod_{i=1}^{k} \bar{T}_i(X)^{e_i} \]
be the factorization of \( T \) mod \( q \) in \( \mathbb{F}_q[X] \), and set...
Let \( T_i \in \mathbb{Z}[X] \) be arbitrary monic lifts of \( T_i \). Then:

(i) Let \( H \in \mathbb{Z}[X] \) be a monic lift of \( \overline{T}(X) \) and set

\[
F = \frac{1}{q}(G \cdot H - T) \in \mathbb{Z}[X].
\]

Then \( \mathbb{Z}[\theta] \) is \( q \)-maximal if and only if \( (\overline{F}, \overline{G}, \overline{H}) = 1 \) in \( \mathbb{F}_q[X] \).

(ii) Let \( U \) be a monic lift of \( \overline{T} / (\overline{F}, \overline{G}, \overline{H}) \) to \( \mathbb{Z}[X] \). Then \( \mathcal{O}' = \mathbb{Z}[\theta] + \frac{1}{q}U(\theta)\mathbb{Z}[\theta] \)

is a subring of \( \mathcal{O}_K \), and if \( m = \deg(\overline{F}, \overline{G}, \overline{H}) \) then \( [\mathcal{O}' : \mathbb{Z}[\theta]] = q^m \) and

\[
\operatorname{disc}(\mathcal{O}') = \frac{\operatorname{disc}(\mathbb{Z}[\theta])}{q^{2m}}.
\]

Proof. 6.1.4. of [2]. \( \square \)

We apply Theorem 2.6 (i).

Lemma 2.7.

(i) Let \( q \) be a prime factor of \( a \). Then \( \mathbb{Z}[\beta] \) is \( q \)-maximal if and only if \( q \) does not occur squared in \( a \).

(ii) The ring \( \mathbb{Z}[\beta] \) is \( p \)-maximal if and only if \( p \) is not a Wieferich prime to base \( a \).

Proof. (i) Apply Theorem 2.6 (i) to \( T = A \). Then \( \overline{T} = X^p \) mod \( q \) hence \( X \) and \( X^{p-1} \) are monic lifts of \( \overline{G} \) and \( \overline{H} \), respectively. Then

\[
F = \frac{1}{q}(G \cdot H - T) = \frac{a}{q} \not\equiv 0 \mod q
\]

if and only if \( q \) is a squarefree factor of \( a \). Because \( (\overline{G}, \overline{H}) = (X, X^{p-1}) = X \) it follows that \( (\overline{F}, \overline{G}, \overline{H}) = X \) if \( q \) is not a squarefree factor of \( a \), and \( (\overline{F}, \overline{G}, \overline{H}) = 1 \) if \( q \) is a squarefree factor of \( a \). This proves (i).

(ii) Apply Theorem 2.6 (i) to \( T = B \). Then \( \overline{T}(X) = X^p \) mod \( p \) hence \( X \) and \( X^{p-1} \) are again monic lifts of \( \overline{G} \) and \( \overline{H} \), respectively. Then

\[
F = \frac{1}{p}(G \cdot H - T) = -a \left( \sum_{i=1}^{p-1} \frac{1}{p^i} \right) a^{p-1-i} X^i - \frac{a^{p-1} - 1}{p}.
\]

The constant factor of \( F \) equals \( 0 \) mod \( p \) if and only if \( p \) is a Wieferich prime to base \( a \). Then it follows immediately that \( (\overline{F}, \overline{G}, \overline{H}) = X \) if \( p \) is a Wieferich prime to base \( a \), and \( (\overline{F}, \overline{G}, \overline{H}) = 1 \) if \( p \) is not a Wieferich prime to base \( a \). This proves (ii). \( \square \)

Next we apply Theorem 2.6 (ii).

Lemma 2.8. Assume that \( p \) is a Wieferich prime to base \( a \) and let \( U \) be a monic lift of \( \overline{T} / (\overline{F}, \overline{G}, \overline{H}) \) to \( \mathbb{Z}[X] \). Then:
(i) It is possible to set $U(X) = X^{p-1}$ with $U(\beta) = \beta^{p-1}$. Then $O' = \mathbb{Z}[\beta] + \frac{\beta^{p-1}}{p} \mathbb{Z}[\beta]$ is a ring and $\{\beta^i; 0 \leq i \leq p-2\} \cup \{\frac{\beta^{p-1}}{p}\}$ is a \(\mathbb{Z}\)-base of $O'$.

(ii) The degree of $(\overline{F}, \overline{G}, \overline{H})$ is 1, the index $[O': \mathbb{Z}[\beta]]$ is $p^2$, and $\text{disc}(O') = (-1)^{\frac{p-1}{2}} \cdot p^{p-2} \cdot a^{p-1}$.

(iii) Denote $\beta' = \frac{\beta^{p-1}}{p}$. Then $\mathbb{Z}[\beta']$ is a subring of $O_K$.

Proof. This follows immediately from Theorem 2.6 (ii). Note that $(\overline{F}, \overline{G}, \overline{H}) = X$ and apply Lemma 2.5 (v). Statement (iii) is also clear from (i). \(\square\)

The following lemma has a more general context.

**Lemma 2.9.** Let $L$ be a number field of degree $n$ and denote by $O_L$ the ring of integers. Then:

(i) Let $O_1, \ldots, O_\ell$ be subrings of $O_L$. Then $O' = \prod_{i=1}^\ell O_i$ is a subring of $O_L$ with $O_i \subseteq O'$ for all $1 \leq i \leq \ell$.

(ii) Let $\eta, \sigma \in O_L$ and assume that $\eta^2 \in \mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$. Then $\mathbb{Z}[\eta] \cdot \mathbb{Z}[\sigma] = \mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$.

(iii) For a prime $q$ apply Theorem 2.6 to $\mathbb{Z}[\sigma]$ and assume, with the notations of Theorem 2.6, that $(\overline{F}, \overline{G}, \overline{H}) \neq 1 \mod q$.

Denote $\eta = \frac{\nu(\sigma)}{q}$. Then $\mathbb{Z}[\eta] \cdot \mathbb{Z}[\sigma] = \mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$.

(iv) In (i) let $\ell = 2$ and assume that the ranks of $O_1$ and $O_2$ are $n$. Then $\text{disc}(O_2) = \text{disc}(O_1) \cdot [O_1: O_2]^2$.

If $O_2 \subseteq O_1$ then $[O_1: O_2]$ is an integer.

(v) In (iv) let $B$ be a base change matrix from $O_1$ to $O_2$, then $\text{det}(B)^2 = [O_1: O_2]^2$.

(vi) In (i) it holds that $\text{disc}(O')$ divides $\text{disc}(O_i)$; $1 \leq i \leq \ell$.

Proof. The abelian group $O'$ consists of all finite sums of products $\sum_{k=1}^\ell \sigma_{k_1} \sigma_{k_2} \cdots \sigma_{k_\ell}$ with $\sigma_{k_i} \in O_i$.

(i) It is clear that $O'$ is a ring with $O_i \subseteq O'$ for all $1 \leq i \leq \ell$ because $\sigma_i = \sigma_i \cdot 1$ with $\sigma_i \in O_i$ and $1 \in \prod_{i=1}^\ell O_i$.

(ii) \(\eta^i \sigma^j\) This is clear from (i) because both summands of the righthand side are contained in the lefthand side.

\(\subseteq\): For $0 \leq i, j \leq n - 1$ it holds that $\eta^i \sigma^j \in \mathbb{Z}[\eta] \cdot \mathbb{Z}[\sigma]$. By induction on $i$ we show that $\eta^i \sigma^j \in \mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$ from which (ii) follows. For $i = 1$ the statement is clear. Assume that $\eta^i \sigma^j \in \mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$. Then there are $\varrho, \sigma \in \mathbb{Z}[\sigma]$ such that $\eta^{i+1} \sigma^j = \varrho + \eta \sigma$ hence $\eta^{i+1} \sigma^j = \eta - \eta^i \sigma^j = \eta (\varrho + \eta \sigma) = \eta \varrho + \eta \sigma \in \mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$ by assumption.

(iii) From Theorem 2.6 it follows that $\mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$ is a ring which contains $\eta$. Then $\mathbb{Z}[\eta]$ is a subring of $\mathbb{Z}[\sigma] + \eta \mathbb{Z}[\sigma]$ hence (iii) follows from (ii).

(iv) This follows from (2.4) in III.2 of [4] because the prerequisites of page 94 of [4] are fulfilled: $\mathbb{Z}$ is a Dedekind domain, $O_L$ has rank $n$ and this holds by assumption also for the subrings $O_1$ and $O_2$. 

- 6 -
If \( O_2 \subseteq O_1 \) then \( O_1 \cdot O_2 = O_1 \), and the statement follows from the Elementary Divisor Theorem (see Theorem 1 in §1.5 of [8]).

(v) Apply (iv) and the well-known statement \( \text{disc}(O_2) = \text{disc}(O_1) \cdot \det (B)^2 \) (see Proposition 1 in §2.7 of [8]).

(vi) This follows inductively from (iv) because \( O_\gamma \subseteq O' \) hence \([O' : O_\gamma]\) is an integer. \( \square \)

3. THE WIEFERICH CASE

In this section we assume that \( p \) is a Wieferich prime to base \( a \). Then \( p \) does not divide \( a \) and \( \beta' \) is an integer in \( K \) (Lemma 2.8 (iii)). We will prove

**Proposition 3.1.**

(i) If \( p \geq 5 \) then \( \mathbb{Z}[\beta'] \) is \( p \)-maximal.

(ii) If \( p = 3 \) then \( \mathbb{Z}[\beta'] \cdot \mathbb{Z}[\alpha] \) is \( p \)-maximal.

The proof is done at the end of this section because several preparative statements are necessary.

**Remark 3.2** (matrix notation).

We will use matrix notation because we need the characteristic polynomial and the analysis modulo powers of \( p \) seems to be easier.

Related to the base \( \{\beta^i; 0 \leq i \leq p - 1\} \) multiplication with \( \beta \) is represented by the \( p \times p \) matrix

\[
M_\beta = \begin{pmatrix}
0 & 0 & \cdots & 0 & a - a^p \\
1 & 0 & \cdots & 0 & -(\frac{p}{1})a^{p-1} \\
0 & 1 & \cdots & 0 & -(\frac{p}{2})a^{p-2} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & -(\frac{p}{p-1})a
\end{pmatrix}.
\]

For details see Proposition 1 in §2.6 of [8]. The matrix \( M_\beta \) has the following entries:

- Row 1: \( m_{1i} = a - a^p; \quad m_{1j} = 0 \) elsewhere
- Row \( i \) (\( 2 \leq i \leq p \)): \( m_{i,i-1} = 1; \quad m_{ip} = -(\frac{p}{i-1})a^{p-(i-1)}; \quad m_{ip} = 0 \) elsewhere.

Multiplication with \( \beta^k \) (\( 1 \leq k \leq p - 1 \)) is represented by \( M_\beta^k = M_\beta^k \) hence multiplication with \( \beta' \) is represented by \( M_{\beta'} = \frac{1}{p} M_\beta^{p-1} \).

In \( M_\beta \) every entry in the \( p \)-th column is divided by \( p \) hence
INTEGERS FOR RADICAL EXTENSIONS OF ODD PRIME DEGREE AS PRODUCT OF SUBRINGS

$$M_\beta \equiv \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \mod p.$$  

Then, for $1 \leq k \leq p - 1$,

$$M_{\beta}^k \equiv \begin{pmatrix} 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \ldots & \ldots & \ldots & 0 \\ 1 & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & 1 & 0 & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \end{pmatrix} \mod p$$  

with 1 in the entries $(k + 1, 1), \ldots, (p, p - k)$ (which is the $k$-th secondary diagonal below the main diagonal) and 0 mod $p$ elsewhere. This means also that every entry in the columns $p - k + 1, \ldots, p$ is divided by $p$.

For $1 \leq k \leq p - 1$ and $1 \leq i, j \leq p$ denote $M_{\beta}^k = (m_{ij}^{(k)})$ and $m_{ij} = m_{ij}^{(1)}$.

This finishes Remark 3.2. □

Lemma 3.3. Let $N = (n_{ij})$ be a $p \times p$ matrix with entries in the complex numbers and assume that $M_\beta \cdot N = N \cdot M_\beta$. Then $N' = (n_{ij}') = M_\beta \cdot N$ has the following entries:

(i) The columns $2 \leq j \leq p$ of $N$ are shifted one column to the left: $n_{ij}' = n_{i,j+1}$ for $1 \leq i \leq p$, $1 \leq j \leq p - 1$.

(ii) In the $p - th$ column of $N'$ the entry in the $i-th$ row is $n_{ip}' = (a - a^p) \cdot n_{pp}$ where $n_{ip}' = n_{i-1,p} + \left(\frac{p}{a^p}\right) \cdot a^{p-(i-1)} \cdot n_{pp}$ for $2 \leq i \leq p$.

(iii) If $p$ is a Wieferich prime to base $a$ then $p^2$ divides every entry in the first row of $M_{\beta}^k$ ($1 \leq k \leq p - 1$).

Proof. (i) and (ii) Use the structure of $M_\beta$ and matrix multiplication: $N' = N \cdot M_\beta$ for (i), and $N' = M_\beta \cdot N$ for (ii).

(iii) This follows from (i) and (ii) by induction on $k$, setting $N = M_{\beta}^k$, hence every entry in the first row is created by multiplication with $a - a^p$ or 0 which both are divided by $p^2$. □

It is obvious that in the preceding lemma $M_\beta \cdot N = N \cdot M_\beta$ if $N$ is a power of $M_\beta$.

Proposition 3.4. The minimal polynomial of $\beta'$ equals the characteristic polynomial of $\beta'$.

Proof. Denote the $p \times p$ unit matrix by $E_p$. Then the characteristic polynomial $\chi$ of $\beta'$ is given by
\[
\chi(X) = \det(X \cdot E_p - M_{p'}) = \det \left( X \cdot E_p - \frac{1}{p} M_{p}^{p-1} \right).
\]

The matrix \( M_{p}^{p-1} \) has the following properties (see Remark 3.2):

(a) It has integral entries in the columns 2, ..., \( p \) which are all divided by \( p \).
(b) Every entry in the first row is divided by \( p^2 \) (Lemma 3.3 (iii)).
(c) The entry \((p, 1)\) equals \( \frac{1}{p} \), all other entries in the first column are 0.

Using the Laplace development for determinants along the first column it follows that \( \chi \) is monic of degree \( p \) and has integral coefficients. It remains to be shown that \( \chi \) is the minimal polynomial of \( \beta' \).

Because \( \beta' \notin \mathbb{Q} \) it follows that the minimal polynomial \( B' \) of \( \beta' \) has degree \( p \) as there are no further fields between \( \mathbb{Q} \) and \( K \). Our statement follows now from the well-known fact that \( B' \) divides \( \chi \) (which is the Cayley-Hamilton Theorem, see Satz 6 in Algebraische Ergänzung §2 of [1]). \( \square \)

Next we analyze \( M_{p}^{k} \mod p^2 \).

**Proposition 3.5.** For \( 1 \leq k \leq p - 1 \) the following holds for \( M_{p}^{k} \):

(i) For \( 1 \leq j \leq p - k \) the values are: \( m_{ij}^{(k)} = 1 \) for \( j = i - k \) and

\( m_{ij}^{(k)} = 0 \) for \( j \neq i - k \).

(ii) In the first row the values are:

\( m_{1j}^{(k)} = 0 \) for \( 1 \leq j \leq p - k \);

\( m_{1,p+1-k}^{(k)} = a - a^p \);

\( p(a - a^p) \) divides \( m_{ij}^{(k)} \) for \( p + 2 - k \leq j \leq p \),

in particular \( p^3 \) divides \( p(a - a^p) \).

(iii) For \( 2 \leq i \leq p \) it holds that \( m_{ij}^{(k)} \equiv 0 \mod p^2 \) for \( p + i - k \leq j \leq p \).

(iv) For \( 2 \leq i \leq p \) it holds that

\[
m_{ij}^{(k)} \equiv - \left( \frac{p}{i - (j - (p - k))} \right) \cdot a^{p - (i - (p - k))} \mod p^2
\]

for \( p - k + 1 \leq j \leq p - k + i - 1 \).

(v) For \( p \geq 5 \) and \( 3 \leq k \leq p - 1 \) it holds that \( m_{2p}^{(k)} \equiv 0 \mod p^3 \).

**Proof.** (i) Consider in Remark 3.2 the first \( p - k \) columns of \( M_{p}^{k} \). The first \( k \) rows are zeroes, the remaining \( p - k \) rows form the unit matrix \( E_{p-k} \). Then (i) follows immediately.

(ii) By Lemma 3.3 (i), applied inductively, the \( p \)-th column of \( M_{p} \) is the \((p + 1 - k)\)-th column of \( M_{p}^{k} \) hence the first two statements of (ii) follow. For the third statement set \( N = M_{p} \) in Lemma 3.3. Then \( n_{ip} = (a - a^p) \cdot n_{pp} = -(a - a^p) p a \), and the third statement follows inductively from Lemma 3.3 (i). It is immediate that \( p^3 \) divides \( p(a - a^p) \) because we are in the Wieferich case.

(iii) Use again Lemma 3.3 (i) with \( N = M_{p} \). From \( p + i - k \leq j \leq p \) and \( i \geq 2 \) it follows that \( k \geq i \geq 2 \). The proof is done by induction on \( k \). Put \( k = 2 \). Then \( i = 2 \)
hence only row 2 is relevant which means that \( j = p \). Applying Lemma 3.3 (ii) yields that \( n'_{2p} = n_{1p} + \binom{p}{1} a^{p-1} \cdot \binom{p}{p-1} a \) which is divided by \( p^2 \) because \( n_{1p} = a - ap \).

Now assume that \( m_{kj}^{(k)} \equiv 0 \mod p^2 \) for \( p + i - k \leq j \leq p \) and put \( N = M_{p}^k \). Then \( n_{i+1,p} = n_{1p} + \binom{p}{i} a^{p-i} \cdot n_{pp} \). Because \( n_{ip} \) is divided by \( p^2 \) (induction hypothesis) and \( n_{pp} \) is divided by \( p \), the statement follows for the \( p \)-th column. Then statement (iii) follows by applying again Lemma 3.3 (i).

(iv) The proof is done by induction on \( k \). For \( k = 1 \) it follows that \( p \leq j \leq p - 2 + i \) hence \( j = p \). Then

\[
-\left( i - (j - (p-k)) \right) \cdot a^{p-(i-(j-(p-k)))} \equiv -\left( i - 1 \right) \cdot a^{p-(i-1)} \equiv m_{ip} \mod p^2
\]

for \( 2 \leq i \leq p \) hence (iv) holds for \( k = 1 \). Now assume that (iv) holds for \( k \). Put again \( N = M_{p}^k \) and \( N' = M_{p}^{k+1} \) then

\[
m_{ip}^{(k+1)} = n_{i+1,p} = n_{i-1,p} + \binom{p}{i-1} \cdot a^{p-(i-1)} \cdot n_{pp} \equiv n_{i-1,p} \equiv m_{i-1,p}^{(k)}
\]

\[
\equiv -\left( i - 1 \right) \cdot a^{p-(i-1)} \cdot (p-(p-k)) \equiv -\left( i - (k+1) \right) \cdot a^{p-(i-(k+1))} \mod p^2 \text{ for } i \geq k + 1.
\]

(For the first congruence use Lemma 3.3 (iii) and \( n_{pp} \equiv 0 \mod p \); for the third congruence use the induction hypothesis and the results for \( k \).) Hence statement (iv) follows for the \( p \)-th column. Then statement (iv) follows inductively from Lemma 3.3 (i).

(v) From (iv) it follows, with \( j = p \), that \( m_{ip}^{(k)} \equiv -\binom{p}{i-k} \cdot a^{p-(i-k)} \mod p^2 \) for \( 1 \leq k \leq i - 1 \), in particular \( m_{ip}^{(k)} \equiv 0 \mod p \) and \( \not\equiv 0 \mod p^2 \). From (iii) it follows that \( m_{2p}^{(k)} \equiv 0 \mod p^2 \) (put \( i = 2 \) and \( j = p \), then \( p + 2 - k \leq p \) hence \( k \geq 2 \)).

For \( k = 2 \) it follows, with \( N = M_{p}^{2} \), from Lemma 3.2 (iii) that

\[
m_{ip}^{(2)} = -(a - ap) \binom{p}{p-1} a
\]

\[
m_{2p}^{(2)} = (a - ap) + p^2 a^p \equiv 0 \mod p^2
\]

\[
m_{ip}^{(2)} = m_{i-1,p} - \binom{p}{i-1} \cdot a^{p-(i-1)} \cdot \binom{p}{p-1} \cdot a
\]

\[
= -\binom{p}{i-2} \cdot a^{p-(i-2)} - p \binom{p}{i-1} \cdot a^{p+2-i}
\]

which is \( \equiv 0 \mod p \) and \( \not\equiv 0 \mod p^2 \) for \( 3 \leq i \leq p \).

For \( k = 3 \) (this is possible because \( p \geq 5 \)) it follows, with \( N = M_{p}^{3} \), again from Lemma 3.3 (ii), applied twice, that

\[
m_{3p}^{(3)} = m_{ip}^{(2)} + p a^{p-1} m_{pp}^{(2)} = -(a - ap) \cdot a - p^3 \cdot a^{p+1} - p \binom{p}{p-2} \cdot a^{p+1}
\]

which is \( \equiv 0 \mod p^2 \) and \( \not\equiv 0 \mod p^3 \); \n
\[
m_{ip}^{(3)} \equiv -\binom{p}{i-3} \cdot a^{p-(i-3)} \mod p^2 \text{ for } i \geq 4
\]

which is \( \equiv 0 \mod p \) and \( \not\equiv 0 \mod p^2 \) for \( 3 \leq i \leq p \).

The proof is now done by induction on \( 3 \leq k \leq p - 2 \). Put \( N = M_{p}^{k} \) and assume that \( m_{2p}^{(k)} \equiv 0 \mod p^3 \). Then \( m_{2p}^{(k+1)} = m_{ip}^{(k)} + p a^{p-1} m_{pp}^{(k)} \).
From $m_{pp}^{(k)} \equiv 0 \mod p$ and $\not\equiv 0 \mod p^2$ (by (iv), because $k \leq p - 1 < p$) it follows that $p \cdot a^{p-1} \cdot m_{pp}^{(k)} \equiv 0 \mod p^2$ and $\not\equiv 0 \mod p^3$. Then statement (v) follows because $m_{1p}^{(k)}$ is (by (ii)) divided by $p(a - a^p)$ hence $m_{1p}^{(k)} \equiv 0 \mod p^3$. \hfill $\square$

The reason why $p = 3$ has to be treated separately is illustrated in Remark and Example 3.10.

**Corollary 3.6.**

(i) For $j = p + (i - 1) - k$ and $i \leq k + 1$ it holds that $m_{ij}^{(k)} \equiv -p \mod p^2$.

(ii) For $k = p - 1$ Proposition 3.5 reads as follows:

(i) First column: $m_{p1}^{(p-1)} = 1$; $m_{11}^{(p-1)} = 0$ for $1 \leq i \leq p - 1$.

(ii) First row: $m_{11}^{(p-1)} = 0$; $m_{12}^{(p-1)} = a - a^p$.

$p(a - a^p)$ divides $m_{1j}^{(p-1)}$ for $3 \leq j \leq p$.

In particular $p(a - a^p) \equiv 0 \mod p^3$.

(iii) For $2 \leq i \leq p$ it holds that $m_{ij}^{(p-1)} \equiv 0 \mod p^2$ for $i + 1 \leq j \leq p$.

In particular there are integers $m_{ij}'$ such that $m_{ij}^{(p-1)} = p^2 \cdot m_{ij}'$.

(iv) For $2 \leq i \leq p$ it holds that $m_{ij}^{(p-1)} \equiv -\frac{p}{i - (j-1)} \cdot a^{p-(i-(j-1))} \mod p^2$ for $2 \leq j \leq i$.

In particular $m_{ij}^{(p-1)} = p \cdot m_{ij}'$ where $m_{ij}'$ is a unit mod $p^2$.

(iii) For $k = p - 1$ it holds that $m_{1i}^{(p-1)} \equiv -p \mod p^2$ for $2 \leq i \leq p$.

(iv) The matrix $M_{p}^{p-1}$ reads mod $p^2$ as follows:

$$M_{p}^{p-1} = \begin{pmatrix} 0 & 0 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & -p & 0 & \ldots & \ldots & 0 & 0 \\ 0 & -\left(\frac{p}{2}\right) a^{p-2} & -p & 0 & \ldots & 0 & 0 \\ 0 & -\left(\frac{p}{3}\right) a^{p-3} & -\left(\frac{p}{2}\right) a^{p-2} & -p & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & -\left(\frac{p}{p-2}\right) a^2 & -\left(\frac{p}{p-3}\right) a^3 & \ldots & \ddots & -p & 0 \\ 1 & -\left(\frac{p}{p-1}\right) a & -\left(\frac{p}{p-2}\right) a^2 & \ldots & -\left(\frac{p}{2}\right) a^{p-2} & -p \\ \end{pmatrix}$$

**Proof.** (i) From the assumption it follows that

$$i - (j - (p - k)) = i - (p + (i - 1) - k - (p - k)) = 1$$

hence $m_{ij}^{(k)} \equiv -p \cdot a^{p-1} \mod p^2$ from Proposition 3.5 (iv). Then (i) follows because we are in the Wieferich case.

(ii) to (iv) They follow immediately by applying Proposition 3.5 for $k = p - 1$. \hfill $\square$
Now it is possible to calculate the minimal polynomial \( \chi(X) \) of \( \beta' \) mod \( p \) (see Proposition 3.4).

**Proposition 3.7.**

(i) \( \chi(X) \equiv X(X + 1)^{p-1} \mod p \)

(ii) \( \mathbb{Z}[\beta'] \) is \( p \)-maximal if and only if \( p^2 \) does not divide \( \chi(-1) \).

**Proof.** (i) \( \chi(X) = \det(X \cdot E_p - M_{\beta'}) = \det\left(X \cdot E_p - \frac{1}{p} \cdot M_{\beta'}^{p-1}\right) \)

\[
= \det \begin{pmatrix}
X & -\frac{1}{p}m_{12}^{(p-1)} & \ldots & -\frac{1}{p}m_{1p}^{(p-1)} \\
0 & X & -\frac{1}{p}m_{22}^{(p-1)} & \ldots & -\frac{1}{p}m_{2p}^{(p-1)} \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
-\frac{1}{p} & \ldots & \ldots & X & -\frac{1}{p}m_{pp}^{(p-1)}
\end{pmatrix}
\]

\[
= X \cdot \det \begin{pmatrix}
-\frac{1}{p}m_{22}^{(p-1)} & \ldots & -\frac{1}{p}m_{2p}^{(p-1)} \\
\vdots & \ddots & \ddots & \vdots \\
-\frac{1}{p}m_{p2}^{(p-1)} & \ldots & X & -\frac{1}{p}m_{pp}^{(p-1)}
\end{pmatrix}
\]

\[
= \frac{1}{p} \cdot \det \begin{pmatrix}
-\frac{1}{p}m_{12}^{(p-1)} & \ldots & \ldots & -\frac{1}{p}m_{1p}^{(p-1)} \\
-\frac{1}{p}m_{22}^{(p-1)} & \ddots & \ldots & -\frac{1}{p}m_{2p}^{(p-1)} \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
-\frac{1}{p}m_{p-1,2}^{(p-1)} & \ldots & X & -\frac{1}{p}m_{p-1,p}^{(p-1)} & -\frac{1}{p}m_{p-1,p}^{(p-1)}
\end{pmatrix}
\]

Look at the first summand: All entries \(-\frac{1}{p}m_{ij}^{(p-1)}\) above the main diagonal are congruent 0 mod \( p \) (Corollary 3.6 (iv)). Because \( m_{ii}^{(p-1)} \equiv -p \) for \( 2 \leq i \leq p \) it follows that the first summand is mod \( p \) congruent to \( X(X + 1)^{p-1} \).

Look at the second summand: It equals
because $\frac{-1}{p}$ can be put in the first row. The right column is congruent 0 mod $p$ because $p^2$ divides every entry from the second row on (Corollary 3.6 (iv)) and $p(a - a^p)$ divides the entry $m_{1p}^{(p-1)}$ (Corollary 3.6 (ii) property (ii)) because we are in the Wieferich case. Then the second summand is congruent 0 mod $p$ which proves (i).

(ii) Apply Theorem 2.6 to $T = \chi$. Then $X \cdot (X + 1)$ and $(X + 1)^{p-2}$ are monic lifts of $G$ and $H$, respectively, and $F = \frac{1}{p}(X \cdot (X + 1)^{p-1} - \chi(X))$ with $F(-1) = \frac{-\chi(-1)}{p}$ and $(G, H) = X + 1$. It follows that $(F, G, H) = X + 1$ if and only if $X + 1$ divides $F$, and this is equivalent to $\frac{-\chi(-1)}{p} \equiv 0$ mod $p$. Then (ii) follows because $\frac{-\chi(-1)}{p} \neq 0$ mod $p$ if and only if $-\chi(-1) \equiv 0$ mod $p^2$.

Before showing that $p^2$ does not divide $\chi(-1)$ for $p \geq 5$ we need the following

**Lemma 3.8.** Let $r \geq 2$ be an integer and $N = (n_{ij})$ be a $r \times r$ matrix with integer entries and the following property: There is an integer $s$ such that $n_{ij} \equiv 0 \text{ mod } s$ for $i \leq j$. Then

$$\det(N) \equiv n_{1r} \prod_{i=2}^{r} n_{i,i-1} \text{ mod } s^2.$$  

**Proof.** By assumption there are integers $n_{ij}$ with $n_{ij} = s \cdot n'_{ij}$ for $i \leq j$. Then (standard calculation for determinants)

$$\det(N) = \sum_{i=1}^{r} (-1)^{i-1} \cdot s \cdot n'_{1i} \cdot \det(N_i)$$  

where the $(r - 1) \times (r - 1)$ matrix $N_i$ is defined by deleting the first row and the $i$-th column from $N$. For $1 \leq i \leq r - 1$ the entries in the right column of $N_i$ are $s \cdot n'_{ij}$ hence $s$ divides $\det(N_i)$, and then $s^2$ divides every summand of $\det(N)$ except the $r$-th one. Then $\det(N) \equiv s \cdot n'_{1r} \cdot \det(N_r) \text{ mod } s^2$. The entries on the main diagonal of $N_r$ are $n_{i,i-1}$ $(2 \leq i \leq r)$, above the main diagonal all entries are divided by $s$ hence $\det(N_r) \equiv \prod_{i=2}^{r} n_{i,i-1} \text{ mod } s$ because $N_r$ is mod $s$ a lower triangular matrix. This proves the statement. 

**Remark 3.9.** $\det(N) \equiv 0 \text{ mod } s^2$ if and only if $s^2$ divides $n_{1r}$ or $s$ divides one of the $n_{i,i-1}$ $(2 \leq i \leq r)$. 

Now we can prove Proposition 3.1.
Proof of Proposition 3.1.

(i) From the prerequisite we have \( p \geq 5 \).
From Corollary 3.6 (ii) (property (iii)), (iii) and (iv) it follows that all entries of \( M_{p}^{p-1} \) above the main diagonal are congruent \( 0 \mod p^2 \), and all entries below the main diagonal are not divided by \( p^2 \).
Now look at the first summand of \( \chi(X) \) in the proof of Proposition 3.7 (i).
Because \( m_{ii}^{(p-1)} \equiv -p \mod p^2 \) (Corollary 3.6 (iii)) the first summand reads \( \mod p^2 \) as follows:

\[
\begin{pmatrix}
X + 1 & \cdots & pm_{2p}' \\
\vdots & \ddots & \vdots \\
m_{p2}' & \cdots & X + 1
\end{pmatrix}
\]

where the \( m_{ij}' \) \( (2 \leq j < i \leq p) \) below the main diagonal are units \( \mod p \). Evaluation at \(-1\) gives

\[
-\det\begin{pmatrix}
0 & \cdots & pm_{2p}' \\
\vdots & \ddots & \vdots \\
m_{p2}' & \cdots & 0
\end{pmatrix}
\]

which is by Lemma 3.8 (with \( r = s = p \)) congruent to \(-pm_{2p}' \cdot \prod_{i=3}^{p} m_{i(i-1)}' \mod p^2 \).
This is not congruent \( 0 \mod p^2 \) because all factors except \( p \) are units \( \mod p \), and then also \( \mod p^2 \): \( m_{2p}' \) by Proposition 3.5 (v), and \( m_{i(i-1)}' \) by Corollary 3.6 (ii) property (iv). Note that \( m_{2p}' \) is a unit \( \mod p^2 \) because \( m_{2p}^{(p-1)} = p^2 m_{2p}' \) is not divided by \( p^3 \).
Now look at the second summand of \( \chi(X) \) in the proof of Proposition 3.7 (ii) and evaluate at \(-1\). Because we are in the Wieferich case it follows from Corollary 3.6 (ii) property (ii) that \( p^3 \) divides \( m_{1j}^{(p-1)} \) for \( 3 \leq j \leq p \). Then the second summand reads \( \mod p^2 \) as follows:
\[
\begin{pmatrix}
\frac{a - a^p}{p^2} & pm'_{13} & \cdots & \cdots & \cdots & pm'_{1p} \\
0 & pm'_{23} & \cdots & \cdots & \cdots & pm'_{2p} \\
\vdots & \ddots & \ddots & \ddots & \cdots & \vdots \\
m'_{12} & \cdots & 0 & \ddots & \cdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
m'_{p-2,2} & m'_{p-2,3} & \cdots & \cdots & 0 & pm'_{p-2,p} \\
m'_{p-1,2} & m'_{p-1,3} & \cdots & \cdots & 0 & pm'_{p-1,p}
\end{pmatrix}
\]

det

which is congruent 0 mod \(p^2\) because all entries in the last two columns are divided by \(p\).

Putting together the results for both summands statement (i) follows for \(p \geq 5\).

(ii) From the prerequisite we have \(p = 3\).

From Lemma 2.9 (iii) it follows that \(\mathbb{Z}[\beta'] \cdot \mathbb{Z}[\alpha] = \mathbb{Z}[\alpha] + \beta' \mathbb{Z}[\alpha]\). From \(\text{disc}(\mathbb{Z}[\alpha]) = -27a^2\) (Lemma 2.5 (v)) and Theorem 2.6 (ii) it follows that \(\text{disc}(\mathbb{Z}[\beta'] \cdot \mathbb{Z}[\alpha]) = -3a^2\) which is not divided by 9. Then (ii) follows from Proposition 1 in §2.7 of [8].

The proof of Proposition 3.1 is now completed. \(\square\)

**Remark and Example 3.10.** For \(p = 3\) we see from the proof of Proposition 3.5 (v) that \(m'_{2p}^{(2)} \equiv 0 \mod p^2\) but not necessarily \(\not\equiv 0 \mod p^3\). For \(p = 3\) the entry \(m'_{23}^{(2)} = (a - a^3) + 9a^3 = a(8a^2 + 1)\) in the matrix \(M_2^2\) can be congruent 0 mod 27. Put, for example, \(a = 19\). Then \(m_{23}^{(2)} = 27 \cdot 19 \cdot 107\).

The minimal polynomial of \(\beta'\) is

\[
X^3 - a^2X^2 + a^2 \frac{a^2 + 2}{3} X - a^2 \frac{(a^2 - 1)^2}{27}.
\]

Applying Theorem 2.6 to \(\mathbb{Z}[\beta']\) shows that \(\mathbb{Z}[\beta']\) is 3-maximal if and only if \(\frac{a^2 - 1}{9} \not\equiv 1 \mod 3\). Again \(a = 19\) is an example where \(\mathbb{Z}[\beta']\) is not 3-maximal. \(\square\)

4. **The Non-Squarefree Case**

Due to Remark 2.2 it holds for the exponents of the prime decomposition of \(a = \prod_{i=1}^m q_i^{e_i}\) without restriction that \(1 \leq e_i \leq p - 1\) for all \(1 \leq i \leq m\).

Let \(1 \leq i \leq m\). For \(\alpha_i = p_i^{-1/2} \sqrt{q_i}\) it follows that \(\alpha = \prod_{i=1}^m \alpha_i^{e_i}\). For \(c_i = \frac{a_{u_i}}{q_i^{e_{u_i}}} \) (introduced in Lemma 2.3 (v)) denote \(\gamma_i = \frac{a_{u_i}}{q_i^{e_{u_i}}} \). Then \(\gamma_i = p_i^{1/2} \sqrt{c_i} = a_i \cdot \prod_{k \neq i}^{m} \alpha_k^{e_ku_i} \) (proof of Lemma 2.3 (v)).
Proposition 4.1. Let $1 \leq i \leq m$. Then:

(i) $y_i \in \mathcal{O}_K$ and $\mathbb{Q}(y_i)$ is a radical extension.
(ii) $\mathbb{Z}[y_i]$ is $q_i$-maximal.
(iii) $\text{disc}(\mathbb{Z}[y_i]) = (-1)^{\frac{p-1}{2}} \cdot p^p \cdot c_i^{p-1}$.
(iv) $\mathbb{Z}[y_i]$ is $p$-maximal if and only if $\mathbb{Z}[\alpha]$ is $p$-maximal.
(v) The ring $\mathcal{O}^* = \prod_{j=1}^m \mathbb{Z}[y_j]$ is $q_i$-maximal for all $1 \leq i \leq m$.
(vi) $\mathbb{Z}[\alpha] \subseteq \mathcal{O}^*$.

Proof. (i) The number $y_i = \frac{a^{x_i}}{q_i^{e_i}}$ is a root of $X^p - c_i \in \mathbb{Z}[X]$ and lies in $\mathcal{O}$. Then (i) follows.
(ii) This follows from the representation $c_i = q_i \cdot \prod_{k=1}^{\text{max}} q_k^{e_k}$ (see Lemma 2.3, proof of (v)) where $q_i$ is a squarefree factor. Now (ii) follows from Lemma 2.7 (i).
(iii) The argumentation is identical to Lemma 2.5 (v) because $\{y_i^k; 0 \leq k \leq p-1\}$ is a power base of $\mathbb{Z}[y_i]$ and $X^p - c_i$ is the minimal polynomial of $y_i$.
(iv) Apply Lemma 2.3 (v) and Lemma 2.7 (ii).
(v) This follows from Lemma 2.9 (i).
(vi) This follows from (v) and the prime decomposition of $a$.

5. Main Theorem and Corollaries

We can start immediately with the main theorem of this paper.

Theorem 5.1. With the notations from the preceding sections the following holds:

(i) If $p$ is a Wieferich prime to base $a$ then $\mathcal{O}_K = \mathbb{Z}[\beta'] \cdot \mathcal{O}^*$.
(ii) If $p$ is not a Wieferich prime to base $a$ then $\mathcal{O}_K = \mathcal{O}^*$.
(iii) The discriminant $\text{disc}(\mathcal{O}_K)$ equals $(-1)^{\frac{p-1}{2}} \cdot p^x \cdot \prod_{j=1}^m q_j^{p-1}$
with $x = p - 2$ in statement (i) and $x = p$ in statement (ii).
(iv) $\text{disc}(\mathcal{O}_K) = \{(\text{disc}(\mathbb{Z}[y_j]); 1 \leq j \leq m) \text{ in the non-Wieferich case.}
\text{disc}(\mathbb{Z}[\beta'] \cdot \mathcal{O}^*); 1 \leq j \leq m) \text{ in the Wieferich case.}

Proof. By Lemma 2.9 (i) $\mathcal{O}^*$ is a subring of $\mathcal{O}_K$, every $\mathbb{Z}[y_j]$ is contained in $\mathcal{O}^*$ and $\mathcal{O}^*$ is $q_j$-maximal for all $1 \leq j \leq m$ by Proposition 4.1 (v). As consequence from Lemma 2.5 (vi) it remains to show the $p$-maximality of $\mathcal{O}^*$ and $\mathcal{Z}[\beta'] \cdot \mathcal{O}^*$, respectively.

(i) If $\mathbb{Z}[\alpha]$ is not $p$-maximal then, by Proposition 3.1, $\mathbb{Z}[\beta']$ and $\mathbb{Z}[\beta'] \cdot \mathbb{Z}[\alpha]$ are $p$-maximal and 3-maximal, respectively. From $\mathbb{Z}[\alpha] \subseteq \mathcal{O}^*$ (Proposition 4.1 (vi)) it follows now that $\mathbb{Z}[\beta'] \cdot \mathcal{O}^*$ is $p$-maximal which proves (i).
(ii) Let $\mathbb{Z}[\alpha]$ be $p$-maximal. Then, by Proposition 4.1 (iv), $\mathbb{Z}[y_j]$ is $p$-maximal for all $1 \leq j \leq m$ hence $\mathcal{O}^*$ is also $p$-maximal which proves (ii).
(iii) and (iv) From Proposition 4.1 (ii) and, in the Wieferich case, Theorem 2.6 (ii) it follows immediately that $\{(\text{disc}(\mathbb{Z}[y_j]); 1 \leq j \leq m) = (-1)^{\frac{p-1}{2}} \cdot p^p \cdot \prod_{j=1}^m q_j^{p-1}\}$.
(disc(\(\mathbb{Z}[\beta']\)), disc(\(\mathbb{Z}[y_j]\)); 1 \leq j \leq m) = (-1)^{\frac{p-1}{2}} \cdot p^{p-2} \cdot \prod_{j=1}^{m} q_j^{p-1}. It remains to be shown that these numbers equal disc(\(O_K\)).

Firstly assume the non-Wieferich case. Then \(O_K = O^*\). From Lemma 2.9 (vi) we know that disc(\(O^*\)) divides (disc(\(\mathbb{Z}[y_i]\)); 1 \leq i \leq m). We also know that the only divisors of disc(\(O^*\)) are \(p, q_1, \ldots, q_m\) (Lemma 2.5 (vi) and Proposition 4.1 (iii)). Assume that there is \(1 \leq j \leq m\) such that \(q_j\) divides \((\text{disc}(\mathbb{Z}[y_i]): 1 \leq i \leq m)\). Then \(q_j\) divides every \(\frac{\text{disc}(\mathbb{Z}[y_i])}{\text{disc}(O^*)}\) (1 \(\leq i \leq m\)), in particular \(q_j\) divides \(\frac{\text{disc}(\mathbb{Z}[y_j])}{\text{disc}(O^*)} = \left[O^*: \mathbb{Z}[y_j]\right]^2\) by Lemma 2.9 (iv) which is a contradiction to the \(q_j\)-maximality of \(\mathbb{Z}[y_j]\). With the same argument it is shown that \(p\) does not divide \(\frac{\text{disc}(\mathbb{Z}[y_i]): 1 \leq i \leq m)\) disc(\(O^*)\)) because all \(\mathbb{Z}[y_i]\) are \(p\)-maximal by Proposition 4.1 (iv).

Now assume the Wieferich case. Because \(\mathbb{Z}[\beta']\) is idempotent (which means \(\mathbb{Z}[\beta']^2 = \mathbb{Z}[\beta']\)) it follows that \(O_K = \mathbb{Z}[\beta'] \cdot O^* = \prod_{j=1}^{m} (\mathbb{Z}[\beta'] \cdot \mathbb{Z}[y_j])\) where every factor \(\mathbb{Z}[\beta'] \cdot \mathbb{Z}[y_j]\) is \(p\)-maximal and \(q_j\)-maximal. Furthermore \(\mathbb{Z}[\beta'] \cdot \mathbb{Z}[y_j] = \mathbb{Z}[y_j] + \beta' \mathbb{Z}[y_j]\) by Lemma 2.9 (iii) with disc(\(\mathbb{Z}[\beta'] \cdot \mathbb{Z}[y_j]\)) = \(\frac{\text{disc}(\mathbb{Z}[y_j])}{p^e}\) by Theorem 2.6 (ii). The statement in the Wieferich case now follows with the same argument as in the non-Wieferich case replacing \(\mathbb{Z}[y_j]\) by \(\mathbb{Z}[\beta'] \cdot \mathbb{Z}[y_j]\) (1 \(\leq j \leq m\)).

The proof of (iii) and (iv) is now complete. \(\square\)

Statement (iii) of Theorem 5.1 is well-known (Section 3 of [10] and a consequence of Theorem 1.1 of [5]). The proof given here is different from these approaches.

The first corollary shows that it is possible to integrate the factors of \(O_K\) if certain prerequisites are fulfilled.

**Corollary 5.2.**

(i) For \(1 \leq i, j \leq m\) with \(i \neq j\) assume that \(e_i = e_j\). Then

\[
\mathbb{Z}[y_i] \cdot \mathbb{Z}[y_j] = \mathbb{Z} \left[ \frac{a_i^{u_i}}{q_i^{v_i}, q_j^{v_j}} \right]
\]

and \(\mathbb{Z} \left[ \frac{a_i^{u_i}}{q_i^{v_i}, q_j^{v_j}} \right]\) is \(q_i\)- and \(q_j\)-maximal.

(ii) For \(1 \leq i \leq m\) denote \(a_i = \prod_{e_j = e_i}^{m} q_j\) and \(O_i = \prod_{e_j = e_i}^{m} \mathbb{Z}[y_j]\). Then

\[
O_i = \mathbb{Z} \left[ \frac{a_i^{u_i}}{\prod_{e_j = e_i}^{m} q_j^{v_j}} \right]
\]

(iii) Let \(\ell\) be the number of different \(e_i\) for \(1 \leq i \leq m\). Then \(O^* = \prod_{k=1}^{\ell} O_k\) where \(k\) runs over all different \(e_j\).

**Proof.** (i) From \(e_i = e_j\) it follows that \(u_i = u_j\) because \(1 \leq u_i \leq p - 1\). Then \(y_i = \frac{a_i^{u_i}}{q_i^{v_i}} = \frac{a_i^{u_i}}{q_i^{v_i}, q_j^{v_j}} \cdot q_j^{v_j}\) lies in the righthand side. The same argument applies to \(y_j\).
hence “⇐” follows. Because \( q_i \) and \( q_j \) are coprime there are integers \( r \) and \( s \) with
\[
1 = q_i^{v_i}r + q_j^{v_j}s \quad \text{hence} \quad \frac{a^{v_i}}{q_i^{v_i}q_j^{v_j}} = \frac{a^{v_i}q_i^{v_i}r + q_j^{v_j}s}{q_i^{v_i}q_j^{v_j}} = \frac{a^{v_i}r}{q_j^{v_j}} + \frac{a^{v_i}s}{q_i^{v_i}} \quad \text{which lies in the lefthand side, and}\n\]
then also “⇒” follows. An analogous argument as in Proposition 4.1 (v) shows that
\[
\mathbb{Z}\left[\frac{a^{v_i}}{q_i^{v_i}q_j^{v_j}}\right] \quad \text{is} \quad q_i- \text{and} \quad q_j-\text{maximal.}
\]
\[\text{(ii)} \quad \text{This is shown inductively from (i) because all distinct} \quad q_i, q_j \quad \text{with} \quad e_i = e_j \quad \text{are}\n\]
pairwise coprime.
\[\text{(iii)} \quad \text{This follows because all exponents of all prime factors of} \quad a \quad \text{are covered by}\n\]
each one \( O_k \).

Generally it is enough to assume in Corollary 5.2 that \( e_i \equiv e_j \pmod{p} \) but due to Remark 2.2 it is possible to assume that \( 1 \leq e_i \leq p - 1 \) hence \( e_i = e_j \).

The next corollary shows how, in the Wieferich case, \( \mathbb{Z}[\beta'] \) can be replaced by other rings.

**Corollary 5.3.** In the Wieferich case \( \mathbb{Z}[\beta'] \) can be replaced in Theorem 5.1 by any of the rings \( \mathbb{Z}\left[\frac{(\gamma_i - c_i)^{p-1}}{p}\right] \quad (1 \leq i \leq m) \).

**Proof.** The polynomial \( X^p - c_i \) is the minimal one for \( \gamma_i \) hence, by Lemma 2.3 (v), the situation for \( c_i \) is the same as for \( a \). From Proposition 3.1 it follows that also all rings \( \mathbb{Z}\left[\frac{(\gamma_i - c_i)^{p-1}}{p}\right] \) and \( \mathbb{Z}\left[\frac{(\gamma_i - c_i)^{2}}{3}\right] \cdot \mathbb{Z}[a] \) are \( p \)-maximal \( (p \geq 5) \) and 3-maximal subrings of \( O_K \), respectively. \( \square \)

6. EXAMPLES AND A CRITERION FOR MONOGENEITY

Firstly, we construct \( \mathbb{Z} \) bases of \( O_K \).

**Proposition 6.1.** With the notations from above the following holds:

1. For \( 0 \leq k \leq p - 1 \) and \( 1 \leq j \leq m \) there are \( t_{kj} \geq 0 \) and

   \[
   0 \leq e'_{kj} \leq p - 1 \quad \text{such that} \quad ke_i = pt_{ki} + e'_{ki} \quad \text{and} \quad \frac{a^k}{\prod_{j=1}^{m} q_j^{e'_{kj}}} = \prod_{j=1}^{m} a_j^{e'_{kj}} \in O_K.
   \]

   If \( k = 0 \) then \( t_{kj} = 0 \) else \( e'_{kj} \geq 1 \).

2. For \( 1 \leq j \leq m \) and \( 1 \leq k \leq p - 2 \) it holds that \( t_{k+1,j} \geq t_{kj} \), and for

   \[
   1 \leq k \leq p - 1 \quad \text{it holds that} \quad (p - 1 - k)e_j \geq t_{p-1,j} - t_{kj}.
   \]

3. If \( p \) is not a Wieferich prime to base \( a \) then

   \[
   B' = \left\{ \frac{a^k}{\prod_{j=1}^{m} q_j^{t_{kj}}}; \quad 0 \leq k \leq p - 1 \right\}
   \]

   is a \( \mathbb{Z} \) base of \( O_K \).
(iv) If \( p \) is a Wieferich prime to base \( a \) then

\[
B'' = \left\{ \frac{a^k}{\prod_{j=1}^{m} q_j^{t_{kj}}} \mid 0 \leq k \leq p-2 \right\} \cup \left\{ \frac{(a - a)^{p-1}}{p \cdot \prod_{j=1}^{m} q_j^{t_{p-1,j}}} \right\}
\]

is a \( \mathbb{Z} \) base of \( \mathcal{O}_K \).

We omit the (lengthy but straightforward) proof because \( \mathbb{Z} \) bases of \( \mathcal{O}_K \) have already been constructed in [10] and, as a special case, in [6]. The methods used in our proof are quite similar to the one used in [10].

The following example illustrates the results developed here.

**Example 6.2.**

(i) Put \( p = 5 \) and let \( q_1, \ldots, q_5 \) be different primes. Set \( a' = q_1 q_2^2 q_3 q_4^2 q_5^5 \) and assume that \( 5 \) is not a Wieferich prime to base \( a' \). From Remark 2.2 and Lemma 2.3

(iii) it follows that \( \mathcal{O}_K \) is completely determined by \( a = q_1 q_2^2 q_3 q_4^2 \). Use the notations from above. Then:

\[ m = 4; \]
\[ e_1 = 1, \ e_2 = 2, \ e_3 = 4, \ e_4 = 2; \]
\[ \alpha = \frac{s}{a}, \ \alpha_i = \frac{s}{q_i} \] with \( \alpha = \alpha_1^2 \alpha_2 \alpha_3^2 ; \)
\[ (u_1, v_1) = (1, 0), \ (u_2, v_2) = (3, 1), \ (u_3, v_3) = (4, 3), \ (u_4, v_4) = (3, 1); \]
\[ c_1 = a, \ c_2 = \frac{a}{q_2}, \ c_3 = \frac{a}{q_3^2}, \ c_4 = \frac{a}{q_4^2}; \]
\[ \gamma_i = \frac{s}{c_i} \] (1 \( \leq i \leq 4 \)) with \( \gamma_1 = \alpha, \ \gamma_2 = \frac{a}{q_2}, \ \gamma_3 = \frac{a}{q_3^2}, \ \gamma_4 = \frac{a}{q_4^2}; \]
\[ \mathcal{O}_K = \mathbb{Z}[\alpha] \cdot \mathbb{Z}\left[\frac{\alpha}{q_2}\right] \cdot \mathbb{Z}\left[\frac{\alpha^2}{q_3}\right] \cdot \mathbb{Z}\left[\frac{\alpha^3}{q_4}\right] \] (Theorem 5.1 (i)) with
\[ \mathbb{Z}\left[\frac{\alpha^3}{q_2}\right] \cdot \mathbb{Z}\left[\frac{\alpha^2}{q_3}\right] = \mathbb{Z}\left[\frac{\alpha^3}{q_2 q_3}\right] \] (Corollary 5.2 (i)).

Next we compute a \( \mathbb{Z} \) base of \( \mathcal{O}_K \).

For \( 0 \leq k \leq 4 \) the \( k e_i = pt_{ki} + e_{ki}' \) from Proposition 6.1 (i) can be represented in the following matrix with entries \( (t_{ki}, e_{ki}') \) (5 columns numerated from 0 to 4, and 4 rows numerated from 1 to 4):

\[
\begin{pmatrix}
  k = 0 & k = 1 & k = 2 & k = 3 & k = 4 \\
  e_1 = 1 & (0, 0) & (0, 1) & (0, 2) & (0, 3) & (0, 4) \\
  e_2 = 2 & (0, 0) & (0, 2) & (0, 4) & (1, 1) & (1, 3) \\
  e_3 = 4 & (0, 0) & (0, 4) & (1, 3) & (2, 2) & (3, 1) \\
  e_4 = 2 & (0, 0) & (0, 2) & (0, 4) & (1, 1) & (1, 3)
\end{pmatrix}
\]

Then \( \prod_{i=1}^{4} q_i^{t_{i1}} = 1, \prod_{i=1}^{4} q_i^{t_{i2}} = q_3, \prod_{i=1}^{4} q_i^{t_{i3}} = q_2 q_3^2 q_4, \prod_{i=1}^{4} q_i^{t_{i4}} = q_2 q_3^2 q_4 \) hence \( B' = \{ 1, \alpha, \frac{\alpha^2}{q_3}, \frac{\alpha^3}{q_2 q_3 q_4}, \frac{\alpha^4}{q_2 q_3 q_4^2} \} \) is a \( \mathbb{Z} \) base of \( \mathcal{O}_K \).

(ii) Assume in (i) that \( 5 \) is a Wieferich prime to base \( a \). Then \( \beta' = \frac{(a-a)^4}{5} \) lies in \( \mathcal{O}_K \) and \( \mathbb{Z}[\beta'] \) is 5-maximal (Proposition 3.1 (i)). For
\[ O^* = \mathbb{Z}[\alpha] \cdot \mathbb{Z}[\frac{a^3}{q_3}] \cdot \mathbb{Z}[\frac{a^4}{q_4}] \cdot \mathbb{Z}[\frac{a^5}{q_5}] \cdot \mathbb{Z}[\frac{a^6}{q_6}] \cdot \mathbb{Z}[\frac{a^7}{q_7}] \cdot \mathbb{Z}[\frac{a^8}{q_8}] \cdot \mathbb{Z}[\frac{a^9}{q_9}] \] it follows that \( O_K = \mathbb{Z}[\beta'] \cdot O^* \), and a \( \mathbb{Z} \) base of \( O_K \) is \( B'' = \{ 1, \alpha, \frac{a^2}{q_3}, \frac{a^3}{q_4}, \frac{a^4}{q_5}, \frac{a^5}{q_6}, \frac{a^6}{q_7}, \frac{a^7}{q_8}, \frac{a^8}{q_9}, \frac{a^9}{q_9} \} \).

**Proposition 6.4.** If \( \mathbb{Z}[\alpha] \) is \( p \)-maximal and all exponents of the prime decomposition of \( \alpha \) which are not divided by \( p \) have the same congruence mod \( p \) then \( K \) is monogenic with \( O_K = \mathbb{Z}\left[ \frac{a^{u_i}}{\prod_{m=1}^{n_i} q_i^{v_i}} \right] \).

**Proof.** This is an immediate consequence from Remark 2.2 and Corollary 5.2 (iii) because \( \ell = 1 \) and \( \mathbb{Z}[\alpha] \) is \( p \)-maximal. \( \square \)

In particular this proposition can be applied if \( \alpha \) is squarefree which is Theorem 2.1 of [3] in the case of prime degree. In this case \( u_i = 1 \) and \( v_j = 0 \) in Lemma 2.3 (iv) hence \( c_j = a \) which yields \( O_K = \mathbb{Z}[\alpha] \) if \( \mathbb{Z}[\alpha] \) is \( p \)-maximal.

The other direction of this proposition is not true as the following example shows. It extends Exercise 10B to Chapter V of [8].
Example 6.5. Let $p = 3$ and $q_1, q_2$ be distinct primes. Put $a = q_1 q_2^2$. Then, with the notations of this paper, $\alpha_1 = 3\sqrt[3]{q_1}$, $\alpha_2 = 3\sqrt[3]{q_2}$ and $\alpha = \sqrt[3]{a} = a_1 a_2^2$. Additionally denote $\alpha' = a_1^2 a_2$. Then, from Theorem 5.1 (iii) and Proposition 6.1 (iii) and (iv), $\mathcal{O}_K$ has $\mathbb{Z}$ base $\{1, \alpha, \alpha'\}$ with $\text{disc}(\mathcal{O}_K) = -27(q_1 q_2)^2$ in the non-Wieferich case and $\mathbb{Z}$ base $\{1, \alpha, (\alpha - a_1)^2/3q_2\}$ with $\text{disc}(\mathcal{O}_K) = -3(q_1 q_2)^2$ in the Wieferich case (where 3 does not divide $a$), respectively. Note that the prerequisites of Proposition 6.4 are not fulfilled.

Let $\eta = t_0 + t_1 \alpha + t_2 \alpha' \in \mathcal{O}_K$ with $t_0, t_1, t_2 \in \mathbb{Z}$. In the non-Wieferich case $\eta$ is an arbitrary element from $\mathcal{O}_K$, in the Wieferich case there are further elements in $\mathcal{O}_K$.

Firstly, we assume the non-Wieferich case. Using $\alpha^2 = q_2 \alpha'$, $\alpha'^2 = q_1 \alpha$ and $\alpha \alpha' = q_1 q_2$ it follows that $\eta^2 = t_0^2 + 2t_1 t_2 q_1 q_2 + (t_2^2 q_1 + 2t_0 t_1 + t_1^2 q_2 + 2t_0 t_2) \alpha'$. Hence the base change matrix from $\{1, \alpha, \alpha'\}$ to $\{1, \eta, \eta^2\}$ is

$$
\begin{pmatrix}
1 & 0 & 0 \\
0 & t_0 & t_1 \\
t_0 + 2t_1 t_2 q_1 q_2 & t_2 q_1 + 2t_0 t_1 & t_1^2 q_2 + 2t_0 t_2
\end{pmatrix}
$$

with determinant $t_3 q_2 - t_3 q_1$. Then $\text{disc}(\mathbb{Z}[\eta]) = -27(q_1 q_2)^2 \cdot (t_3 q_2 - t_3 q_1)^2$ (see Proposition 1 in §2.7 of [8]) which corrects statement (e) of the mentioned exercise. From $\text{disc}(\mathcal{O}_K) = -27(q_1 q_2)^2$ it follows that that $\mathcal{O}_K = \mathbb{Z}[\eta]$ if and only if there is a solution $(t_1, t_2)$ such that $(t_3 q_2 - t_3 q_1)^2 = 1$. Solutions for $(q_1, q_2, t_1, t_2)$ are, for example, $x_1 = (2, 17, 1, 2)$, $x_2 = (5, 41, 1, 2)$, $x_3 = (11, 19, -5, -6)$. Because 3 is a Wieferich prime to base $5 \cdot 41^2$ and not in the other cases it follows that $\mathcal{O}_K = \mathbb{Z}[\eta]$ for $(q_1, q_2) = (2, 17)$ and $(11, 19)$ but not for $(q_1, q_2) = (5, 41)$.

Now we assume the Wieferich case. Denote $\beta'' = (\alpha - a_1)^2/3q_2$ and note that $\frac{4 + 5a^2}{9}, \frac{1 + 8a^2}{9}$ are integers because we are in the Wieferich case. Also $\frac{1 + 2a^2}{3}$ is an integer because 3 and $a$ are coprime. Then straightforward calculations show:

$$
\alpha^2 = -a^2 + 2aa + 3q_2 \beta''
$$

$$
\alpha \beta'' = q_1 q_2 \frac{1 + 2a^2}{3} = q_1 q_2 a \alpha - 2a \beta''
$$

$$
\beta''^2 = -a \frac{4 + 5a^2}{9} + \frac{1 + 8a^2}{9} a + 2q_1 q_2 a \beta''
$$

Now let $\vartheta = s_0 + s_1 \alpha + s_2 \beta''$ $(s_0, s_1, s_2 \in \mathbb{Z})$ be an arbitrary element from $\mathcal{O}_K$. Then $\vartheta^2 = s_0' + s_1' \alpha + s_2' \beta''$ with

$$
\begin{align*}
\vartheta_0 &= s_0^2 - s_2^2 q_1 a^2 - s_2^2 q_1 a \frac{4 + 5a^2}{9} + 2s_1 s_2 q_1 q_2 \frac{1 + 2a^2}{3}, \\
\vartheta_1 &= 2s_1 a + s_2 q_1 \frac{1 + 8a^2}{9} + 2s_0 s_1 - 2s_1 s_2 q_1 q_2 a, \\
\vartheta_2 &= 3s_2^2 q_2 + 2s_2^2 q_1 q_2 a + 2s_0 s_2 - 4s_1 s_2 a.
\end{align*}
$$

Then the base change matrix from $\{1, \alpha, \beta''\}$ to $\{1, \vartheta, \vartheta^2\}$ is

$$
\begin{pmatrix}
1 & 0 & 0 \\
s_0 & s_1 & s_2 \\
s_0' & s_1' & s_2'
\end{pmatrix}
$$

with determinant
\[ \Delta = s_1s'_2 - s_2s'_1 = 3s_1^3q_2 + 4s_1s_2^2q_1q_2a - 6s_1^2s_2a - s_2^3q_1 \frac{1 + 8a^2}{9} \]

hence \( 9\Delta = (3s_1 - 2s_2q_1q_2)^3q_2 - s_2^2q_1 \). With the same argument as in the non-Wieferich case it follows that that \( O_K = \mathbb{Z}[\theta] \) if and only if there is a solution \((s_1, s_2)\) such that \( \Delta = 1 \). A solution is, for example, \((q_1, q_2, s_1, s_2) = (2, 11, 15, 1)\) as is easily calculated. □

The results of Example 6.5 can be summarized as follows:

**Remark 6.6.** In the situation of Example 6.5 the following holds:

(i) If 3 is not a Wieferich prime to base a then \( K \) is monogenic if and only if the equation \( t_1^3q_2 - t_2^3q_1 = 1 \) has a solution with integers \( t_1, t_2 \). If \( K \) is monogenic then \( O_K = \mathbb{Z}[t_1a + t_2a'] \).

(ii) If 3 is a Wieferich prime to base a then \( K \) is monogenic if and only if the equation \( (3s_1 - 2s_2q_1q_2)^3q_2 - s_2^3q_1 = 9 \) has a solution with integers \( s_1, s_2 \). If \( K \) is monogenic then \( O_K = \mathbb{Z}[s_1\alpha + s_2\left(\frac{\alpha-a)^2}{3q_2} \right) \). □

**REFERENCES**

[1] S. I. Borevicz, I. R. Šafarevič, „Zahlentheorie“, Birkhäuser Verlag Basel (1966)
[2] H. Cohen, „A Course in Computational Algebraic Number Theory“ (Graduate texts in mathematics 138), 3. corr. print, Springer Verlag Berlin, Heidelberg, New York (1996)
[3] K. Conrad, „The Ring of Integers in a Radical Extension“, [https://kconrad.math.uconn.edu/blurbs/gradnumthy/integersradical.pdf](https://kconrad.math.uconn.edu/blurbs/gradnumthy/integersradical.pdf) (no date)
[4] A. Fröhlich, M. J. Taylor, „Algebraic number theory“ (volume 27 of Cambridge studies in advanced mathematics), Cambridge University Press (1993)
[5] A. Jakhar, S. K. Khanduja, N. Sangwan, „On the discriminant of pure number fields“, Colloq. Math. 167 (2022), 149-157
[6] A. Jakhar, S. K. Khanduja, N. Sangwan, „On Integral Basis of Pure Number fields“, Mathematika 67 (2021), 187-195
[7] H.-J. Reiffen, G. Scheja, U. Vetter, „Algebra“ (B.I. Hochschultaschenbücher Band 110), Bibliographisches Institut Mannheim, Wien, Zürich (1969)
[8] P. Samuel, „Algebraic Theory of Numbers“, Hermann Paris (1970)
[9] H. Smith, „The Monogeneity of Radical Extensions“, Acta Arithmetica 198 (2021), 313-327
[10] J. Westlund, „On the Fundamental Number of the Algebraic Number Field \( k(\sqrt{m}) \)“, Trans. Amer. Math. Soc. 11 (1910), 388-392.
INTEGERS FOR RADICAL EXTENSIONS OF ODD PRIME DEGREE AS PRODUCT OF SUBRINGS

Julius_Kraemer@gmx.de

MATHEMATISCHES INSTITUT DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN FROM 1972 UNTIL 1988