ACTA ARITHMETICA
153.4 (2012)

On the indices of multiquadratic number fields

by

ATTILA PETHŐ (Debrecen) and MICHAEL E. POHST (Berlin)

1. Introduction. Let K be an algebraic number field with maximal order o_K. For $\alpha \in o_K$ the $\mathbb{Z}$-module index $I(\alpha) = (o_K : \mathbb{Z}[\alpha])$ is also said to be the index of the element α. The greatest common divisor of the indices of all integral elements of K is called the *field index* of K. (In older literature, see Hasse [4] for example, the field index is also referred to as *common inessential discriminant divisor*.) Problem 22 in the "Problems" chapter of Narkiewicz [8] asks for an explicit formula for the exact power of a prime number p dividing the field index.

The first result in this direction is due to T. Engstrom [2] who showed in 1930 that for number fields K of degree less than eight the exact power of a prime p dividing the field index is determined by the decomposition type of the prime ideal generated by p in K. He explicitly formulated that dependence. His results were generalized in the 1985 thesis of E. Nart [9] who developed a p-adic characterization of the field index.

Engstrom also showed that for quartic fields K the field index is of the form $2^\alpha 3^\beta$ with $\alpha \le 2$ and $\beta \le 1$. This result was reproved by T. Nakahara [7] in 1983 for biquadratic fields. Nakahara also showed that the field index is odd precisely when the discriminant of the field is even. The case of biquadratic fields was taken up again by Gaál, Pethő and Pohst [3] who showed in 1991 that each possible value $2^\alpha 3^\beta$ indeed occurs as the field index of a biquadratic field and presented infinite families of fields having the pertinent field index.

The results of Engstrom were explicitly extended to fields up to degree 12 by J. Śliwa [13] already in 1982, however only for non-ramified primes p. We note that our results for non-ramified primes p dividing the field index of $K = \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{c})$ together with Śliwa's tables determine the decomposition type of the principal ideal generated by p in terms of arithmetical properties of the generating elements a, b, c.

2010 *Mathematics Subject Classification*: 11Y40, 11R20.
Key words and phrases: index form equations, multiquadratic number fields.

Later G. Nyul [10] studied the case of multiquadratic number fields $K = K_r = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_r})$ of degree 2^r in 2002. He proved that fields K_r with odd discriminant do not have a power integral basis. For $r = 3$ he showed non-monogeneity under suitable conditions on the generators. His results were made more precise by Motoda and Nakahara [5] who showed in 2004 that multiquadratic number fields K_r are never monogenic for $r \geq 4$. Again two years later, Motoda, Nakahara and Park [6] proved that the cyclotomic field $K = \mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{2}, \sqrt{-1}, \sqrt{-3})$ is the only monogenic multiquadratic field for $r = 3$.

In this paper we generalize previous results for multiquadratic number fields K_r of degree 2^r in two respects. Starting from a suitable integral basis of such fields given in [11] and [12] we develop two versions of the corresponding index form, both of which split over $\mathbb{Z}$ into a product of $2^r - 1$ factors of degree 2^{r-1} each. Then we solve the problem of Narkiewicz for $r = 3$. We emphasize that our method is completely different from previous ones. In contrast to [3] no computer calculations are needed. Finally, we use the new method to show that the field index of K_r is divisible by any prime power p^k provided that r is large enough.

2. Multiquadratic number fields and their index forms. We shall consider multiquadratic number fields $K = K_r = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_r})$ for square-free rational integers $a_1, \dots, a_r$ which need to be chosen such that the field K has degree 2^r. The case $r = 1$ being trivial and the case $r = 2$ having been solved by Gaál, Pethő and Pohst [3], we concentrate on $r \in \mathbb{Z}^{\geq 3}$ in the remainder of this paper.

In order to make the presentation easier we adopt a normalization of the generating elements of $K/\mathbb{Q}$ introduced by B. Schmal in [11].

Step 1. Let p be a fixed prime number and let $i \in \{1, \dots, r\}$ be minimal such that p divides a_i. If there exists an index $i < j \leq r$ with $p \,|\, a_j$ then we replace the pair (a_i, a_j) by $(a_i, a_i a_j/\gcd(a_i, a_j)^2)$. For the new generators, only one of a_i, a_j will be divisible by p. Repeated application of this procedure yields elements $a_1, \dots, a_r$, only one of which, say a_1, is divisible by p.

Step 2. After Step 1 we may assume that there is at most one generating element which is divisible by 2, say a_1. Then all generating elements except maybe a_1 are odd. We claim that we can alter them in such a way that at most one odd generator is congruent to 3 modulo 4. Namely, if there exist $a_i \neq a_j$ which are both congruent to 3 modulo 4 we replace the pair (a_i, a_j) by $(a_i, (a_i a_j)/\gcd(a_i, a_j)^2)$.

After this procedure we obtain normalized generators.

LEMMA 2.1 (Schmal). *Generating square-free integers $a_1, \dots, a_r$ of a multiquadratic number field $K_r = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_r})$ can be chosen subject to the following conditions: $a_i \equiv 1 \bmod 4$ for $3 \le i \le r$, and the pair (a_1, a_2) belongs to one of three categories:*

(i) $a_1 \equiv 1 \bmod 4$, $a_2 \equiv 1 \bmod 4$;
(ii) $a_2 \equiv 1 \bmod 4$, $a_1 \equiv 3, 2 \bmod 4$;
(iii) $a_1 \equiv 2 \bmod 4$, $a_2 \equiv 3 \bmod 4$.

For this special form of the generators B. Schmal established integral bases for K_r. We follow his ideas but rather use the notation of Schmitt and Zimmer [12]. Let $n := 2^r$. For each integer $j \in \{1, \dots, n\}$ there is a unique 2-adic presentation

$$j - 1 = \sum_{i=1}^{r} \alpha_{ji} 2^{i-1}.$$

Accordingly, we put

$$\gamma_j = \prod_{i=1}^{r} \sqrt{a_i}^{\,\alpha_{ji}}. \tag{1}$$

Next we shall make the radicands

$$b_j := \prod_{i=1}^{r} a_i^{\alpha_{ji}}$$

square-free. For any prime number p we denote by ν_p the corresponding exponential valuation, i.e. $\nu_p(x)$ is the exact power of p dividing x for $x \in \mathbb{Z}$. We put

$$g_j := \prod_{p \mid b_j} p^{\mu_j} \quad \text{with} \quad \mu_j = \begin{cases} \nu_p(b_j)/2 & \text{for } \nu_p(b_j) \text{ even,} \\ (\nu_p(b_j) - 1)/2 & \text{for } \nu_p(b_j) \text{ odd.} \end{cases} \tag{2}$$

LEMMA 2.2 (Schmal). *An integral basis of K_r is given by*

$$\omega_j := \frac{1}{2^{\delta_j} g_j} \prod_{i=1}^{r} (\sqrt{a_i} - a_i)^{\alpha_{ji}} \qquad (i \le j \le 2^r)$$

where the α_{ji} are defined in (1), *the g_j in* (2) *and the δ_j satisfy*

$$\delta_1 = 0,\ \delta_2 = \begin{cases} 1 & \text{for } a_1 \equiv 1 \bmod 4, \\ 0 & \text{for } a_1 \equiv 2, 3 \bmod 4, \end{cases} \qquad \delta_j = \sum_{i=1}^{r} \alpha_{ji} - \beta_j \ (j > 2)$$

with

$$\beta_j = \begin{cases} 1 & \text{for } (a_1, a_2) \equiv (2, 1), (3, 1) \bmod 4,\ \alpha_{j1} = 1, \\ 1 & \text{for } (a_1, a_2) \equiv (2, 3) \bmod 4,\ \alpha_{j1} = 1 \text{ or } \alpha_{j2} = 1, \\ 0 & \text{else.} \end{cases}$$

If $p_1,\dots,p_s$ denote the different prime numbers dividing $a_1\cdots a_r$, the discriminant of $K=K_r$ becomes

$$d_K=(2^\ell p_1\cdots p_s)^{2^{r-1}}$$

with

$$\ell=\begin{cases}0 & \textit{for } (a_1,a_2)\equiv(1,1) \bmod 4, & \textit{case (i)},\\ 2 & \textit{for } (a_1,a_2)\equiv(3,1),(2,1) \bmod 4, & \textit{case (ii)},\\ 3 & \textit{for } (a_1,a_2)\equiv(2,3) \bmod 4, & \textit{case (iii)}.\end{cases}$$

Example. For $r=3$ we improve on the form of that integral basis. We follow the ideas in the proof of Satz 3.2 in [11]. For abbreviation we write $a=a_1$, $b=a_2$, $c=a_3$ and set

$$g=\gcd(a,b),\ h=\gcd(a,c),\ k=\gcd(b,c),\ l=ghk/\gcd(a,b,c)^2,\ f=l/g.$$

Then we obtain the following $\mathbb{Z}$-basis $\omega_1,\dots,\omega_8$ for the maximal order o_3 of K_3. (We remark that also in the case $r=2$ we need to consider only three cases instead of five in the earlier paper by K. S. Williams [14].)

	(i) $(a,b,c)\equiv(1,1,1) \bmod 4$	(ii) $a\equiv 3,2 \bmod 4$ $(b,c)\equiv(1,1) \bmod 4$	(iii) $(a,b,c)\equiv(2,3,1) \bmod 4$
ω_1	1	1	1
ω_2	$(1+\sqrt{a})/2$	$\sqrt{a}$	$\sqrt{a}$
ω_3	$(1+\sqrt{b})/2$	$(1+\sqrt{b})/2$	$\sqrt{b}$
ω_4	$(\sqrt{ab}/g+\sqrt{a}+\sqrt{b}+g)/4$	$(\sqrt{ab}/g+\sqrt{a})/2$	$(\sqrt{ab}/g+\sqrt{a})/2$
ω_5	$(1+\sqrt{c})/2$	$(1+\sqrt{c})/2$	$(1+\sqrt{c})/2$
ω_6	$(\sqrt{ac}/h+\sqrt{a}+\sqrt{c}+h)/4$	$(\sqrt{ac}/h+\sqrt{a})/2$	$(\sqrt{ac}/h+\sqrt{a})/2$
ω_7	$(\sqrt{bc}/k+\sqrt{b}+\sqrt{c}+k)/4$	$(\sqrt{bc}/k+\sqrt{b}+\sqrt{c}+k)/4$	$(\sqrt{bc}/k+\sqrt{b})/2$
ω_8	$(\sqrt{abc}/l+f(\sqrt{a}+\sqrt{b}+g\sqrt{c})$ $+f(\sqrt{ac}+\sqrt{bc}+\sqrt{ab}/g)+fg)\,/\,8$	$(\sqrt{abc}/l+f\sqrt{a}$ $+f\sqrt{ac}+f\sqrt{ab}/g)\,/\,4$	$(\sqrt{abc}/l+f\sqrt{a}$ $+f\sqrt{ac}+f\sqrt{ab}/g)\,/\,4$

Later we shall use the fact that this integral basis is obtained from the $\mathbb{Q}$-basis

$$(\gamma_1,\dots,\gamma_8)=(1,\sqrt{a},\sqrt{b},\sqrt{ab},\sqrt{c},\sqrt{ac},\sqrt{bc},\sqrt{abc})$$

of (1) upon multiplication by an upper triangular matrix $T=(t_{ij})\in\mathbb{Q}^{8\times 8}$:

$$(\omega_1,\dots,\omega_8)=(\gamma_1,\dots,\gamma_8)T. \tag{3}$$

The denominators of the t_{ij} are products of a power of 2 with exponent ≤ 3 and a divisor of abc. In particular, the diagonal elements t_{ii} are fractions with numerator 1. Their product equals the inverse of the index of the order generated by $\gamma_1,\dots,\gamma_8$ in the maximal order o_3 of‘K_3.

The conjugates of $K = K_r$ are denoted by $K^{(1)} = K, \dots, K^{(n)}$. We define linear forms

$$L_j(\mathbf{x}) := \sum_{i=1}^{n} x_i \omega_i^{(j)} \quad (1 \le j \le n). \tag{4}$$

Then the index form I of K becomes

$$I = I(x_2, \dots, x_n) = \frac{1}{\sqrt{d_K}} \prod_{1 \le \nu < \mu \le n} (L_\mu(\mathbf{x}) - L_\nu(\mathbf{x})). \tag{5}$$

It is a homogeneous polynomial in $x_2, \dots, x_n$ of degree $n(n-1)/2$. We will see that it factors over $\mathbb{Z}$ into polynomials of degree $n/2$. (For $r = 1$ this is trivial, for $r = 2$ it was shown in [3].)

It is well-known that $K_r/\mathbb{Q}$ is Galois with Galois group $G = G_r = \mathrm{Gal}(K_r/\mathbb{Q}) \cong C_2^r$. More precisely, we have

$$G = G_r = \langle \sigma_1 \rangle \times \dots \times \langle \sigma_r \rangle$$

with

$$\sigma_i(\sqrt{a_j}) = \begin{cases} \sqrt{a_j} & \text{for } j \ne i \\ -\sqrt{a_i} & \text{for } j = i \end{cases} \qquad (1 \le i, j \le r).$$

Any element $\sigma \in G$ has a presentation

$$\sigma = \prod_{i=1}^{r} \sigma_i^{n_i} \qquad \text{with } n_i \in \{0, 1\}.$$

If σ is not the identity then it generates a subgroup of order 2 in G. We choose a suitable system of residue class representatives for $G/\langle \sigma \rangle$ in the following way. There is a minimal index $k \in \{1, \dots, r\}$ with $n_k = 1$. As a set of residue class representatives we take

$$\mathcal{R} := \Big\{ \prod_{\substack{i=1 \\ i \ne k}}^{r} \sigma_i^{n_i} \;\Big|\; n_i \in \{0, 1\},\, 1 \le i \le r \Big\}.$$

We note that $\mathcal{R}$ is a subgroup of G of order $n/2$. We write $\mathcal{R} = \{\mu_1 = \mathrm{id}, \mu_2, \dots, \mu_{n/2}\}$ for abbreviation.

Lemma 2.3. *For* id $\ne \sigma \in G$ *the polynomial*

$$F_\sigma(x_2, \dots, x_r) := \prod_{i=1}^{n/2} \mu_i(L_1 - \sigma(L_1))$$

is in $\mathbb{Z}[x_2, \dots, x_r]$. *The index form* I *of* K *satisfies*

$$\sqrt{d_K}\, I = \prod_{\substack{\sigma \in G \\ \sigma \ne \mathrm{id}}} F_\sigma.$$

Proof. For fixed id $\neq \sigma \in G$ we show that F_σ is G-invariant. Clearly, $\sigma(F_\sigma) = F_\sigma$ since each of an even number of factors of F_σ is turned into its negative. It remains to prove that $\tau(F_\sigma) = F_\sigma$ also for all $\tau \in \mathcal{R}$. But this is obvious because $\mathcal{R}$ is a group.

We thus obtain $n-1$ polynomials F_σ, each being a homogeneous polynomial of degree $n/2$. Hence, their product is of degree $n(n-1)/2$, which coincides with the degree of I. The lemma will be proved when we show that any factor $L_i - L_j$ of I is also a factor of an F_σ for σ chosen appropriately. Let $\tau_i, \tau_j \in G$, $\tau_i \neq \tau_j$, subject to $L_i = \tau_i(L_1)$, $L_j = \tau_j(L_1)$. We put $\sigma = \tau_i^{-1}\tau_j$ and get $L_i - L_j = \tau_i(L_1 - \sigma(L_1))$. For $\tau_i \in \mathcal{R}$ this is clearly a factor of F_σ. If τ_i does not belong to $\mathcal{R}$, however, we have $\sigma\tau_i \in \mathcal{R}$ and $L_i - L_j$ becomes a factor of $\sigma(F_\sigma)$ which was shown to coincide with F_σ. ∎

3. Indices in K_3. The Galois group G of K_3 is generated by σ_1, σ_2, σ_3. We recall that σ_i maps $\sqrt{a_i}$ onto $-\sqrt{a_i}$ and leaves $\sqrt{a_j}$ invariant for $i, j \in \{1,2,3\}$ with $j \neq i$. The eight automorphisms of G are ordered as follows: $\tau_1 := \mathrm{id}, \tau_2 := \sigma_1, \tau_3 := \sigma_2, \tau_4 := \sigma_1\sigma_2$ and $\tau_j := \tau_{j-4}\sigma_3$ for $5 \leq j \leq 8$. Consequently, we put $K_3^{(j)} = \tau_j(K_3)$ $(1 \leq j \leq 8)$.

We recall that the index form I of K_3 was introduced in (4) and (5). It will turn out useful to rewrite the linear forms $L_j(\mathbf{x})$ involved in the form

$$(6)\quad L_j(\mathbf{x}) = \sum_{k=1}^{8} x_k \omega_k^{(j)} = (\omega_1^{(j)}, \ldots, \omega_8^{(j)})\mathbf{x} = (\gamma_1^{(j)}, \ldots, \gamma_8^{(j)})T\mathbf{x} =: M_j(\mathbf{y})$$

for $\mathbf{y} := T\mathbf{x}$. We remark that the transfer from $\mathbf{x}$ to $\mathbf{y}$ (and vice versa) is easy since T is an upper triangular matrix. But whereas the coordinates of $\mathbf{x}$ are integers, those of $\mathbf{y}$ are rationals with well-known bounded denominators.

In this section we will often choose the generators $a = a_1$, $b = a_2$, $c = a_3$ of K_3 in a different way which is less suitable for presenting integral bases but more appropriate for studying primes (and their powers) dividing the field index of K_3. The latter was defined to be the greatest common divisor of the module indices $(o_3 : \mathbb{Z}[\rho])$ for arbitrary $\rho \in o_3$ satisfying $K_3 = \mathbb{Q}(\rho)$. (We recall that o_3 denotes the maximal order of K_3.) It is a well known result of Żyliński [15] (see also [4, 8], for example) that any prime dividing the field index must be smaller than the degree of that field. Hence, for K_3 we just need to discuss the primes $2, 3, 5, 7$.

p **odd.** For a fixed odd prime p we shall consider the index form as a product of differences of $M_j(\mathbf{y})$ (see (5) and (6)). In order to transfer the results back to the $L_j(\mathbf{x})$, the entries of the transformation matrix T of (3) must be coprime to p. This can be achieved in the following way. From the beginning of the previous section we know that the generating elements a, b, c can be chosen so that at most one of them is divisible by p. That choice obviously guarantees that the numerators and denominators of non-zero entries of T are not divisible by p. We emphasize that the determinant of T is not divisible by p, i.e. p does not divide the index of $\mathbb{Z}[\sqrt{a}, \sqrt{b}, \sqrt{c}]$ in o_K.

According to our considerations at the beginning of the previous section, we can choose a, b, c such that

- a, b, c are quadratic residues modulo p (Case (i));
- a, b are quadratic residues modulo p, but c is not (including the case $p \mid c$) (Case (ii));
- a is a quadratic residue modulo p, $b \not\equiv x^2 \bmod p$, and $p \mid c$ (Case (iii)).

As outlined above, this choice guarantees that a fixed odd prime number p neither divides the numerators nor the denominators of the non-zero entries of T.

We briefly describe our strategy for the different cases. The index form $I = I(\mathbf{y})$ of K satisfies

$$\sqrt{d_K}\, I(y_1, \ldots, y_n) = \prod_{1 \le \nu < \mu \le n} (M_\mu(\mathbf{y}) - M_\nu(\mathbf{y})). \tag{7}$$

If a, b, c are all squares modulo p then each linear form $M_j(\mathbf{y})$ can be mapped into $\mathbb{F}_p^8$ by reducing coefficients modulo p and choosing $y_j \in \mathbb{F}_p$ $(1 \le j \le 8)$. If c, say, is a quadratic non-residue modulo p we need to combine suitable factors of the right-hand side of (7) in order to remove all terms of I in which $\sqrt{c}$ occurs before we can carry out reduction modulo p. This can be easily achieved by the action of the Galois group. Since

$$(M_1(\mathbf{y}), \ldots, M_8(\mathbf{y}))^{\mathrm{tr}} = (\tau_i(\gamma_j))_{1 \le i,j \le 8} (y_1, \ldots, y_8)^{\mathrm{tr}},$$

the matrix $\Gamma = (\tau_i(\gamma_j))$ is invertible modulo p if p does not divide its determinant. The latter differs from the square root of the discriminant of K_3 by a factor $\det(T)$. Hence, if p^2 does not divide abc the matrix T is invertible modulo p and for each tuple $\mathbf{m} = (m_1, \ldots, m_8)^{\mathrm{tr}} \in \mathbb{F}_p^8$ we get unique corresponding values $M_j(\mathbf{m})$ and also $L_j(\mathbf{x})$. Choosing the $\mathbf{m}$ appropriately we can deduce divisibility conditions for I by powers of p.

Case (i): *a, b, c are quadratic residues modulo p.* For $p = 7$ we choose $m_1 \equiv m_2 \bmod p$ with $m_1 \not\equiv m_2 \bmod p^2$ and $m_i \not\equiv m_j \bmod p$ $(2 \le i < j \le 8)$, for example. (At least two values m_i must belong to the same residue class modulo 7.) This immediately implies that the field index is divisible by 7. Choosing $m_1 \not\equiv m_2 \bmod 49$ we see that the field index is exactly divisible by 7.

Now let $p = 5$. Then we distribute the eight values $L_i(\mathbf{x})$ into five residue classes modulo 5. First we assume that each residue class contains at most two values. Reordering the linear forms if necessary we get

$$L_1(\mathbf{x}) \equiv L_2(\mathbf{x}) \bmod 5, \quad L_3(\mathbf{x}) \equiv L_4(\mathbf{x}) \bmod 5, \quad L_5(\mathbf{x}) \equiv L_6(\mathbf{x}) \bmod 5,$$

implying that the field index is divisible by 5^3. (We can choose the $L_i(\mathbf{x})$ so that they are pairwise incongruent modulo 5 for $i \in \{1,3,5,7,8\}$ and the differences $L_i(\mathbf{x}) - L_{i+1}(\mathbf{x})$ are not divisible by 25 for $i \in \{1,3,5\}$.) If there is a residue class containing three values $L_i(\mathbf{x})$, however, it is straightforward that the field index is divisible by 5^3, too. As we remarked for $p = 7$ already, this also shows that the field index is exactly divisible by 5^3.

Finally, we consider $p = 3$. If each residue class modulo 3 contains at most three values $L_i(\mathbf{x})$, a suitable ordering yields

$$\begin{aligned} &L_1(\mathbf{x}) \equiv L_2(\mathbf{x}) \equiv L_3(\mathbf{x}) \bmod 3,\\ &L_4(\mathbf{x}) \equiv L_5(\mathbf{x}) \equiv L_6(\mathbf{x}) \bmod 3,\\ &L_7(\mathbf{x}) \equiv L_8(\mathbf{x}) \bmod 3, \end{aligned}$$

with L_1, L_4, L_7 pairwise incongruent modulo 3. For this choice we clearly obtain the divisibility of the field index by 3^7. We can choose the values so that the differences $L_i(\mathbf{x}) - L_j(\mathbf{x})$ are not divisible by 9 for the indices $1 \le i < j \le 3$, $1 \le i < j \le 6$, and $(i,j) = (7,8)$. It is easily seen that this divisibility is also satisfied if there exist residue classes containing four or more values. As before, we conclude that the field index is exactly divisible by 3^7.

Case (ii): *a, b are quadratic residues modulo p.*

Subcase (ii)(a): *c is a quadratic non-residue modulo p.* We order the linear factors of I in a suitable way. We have

$$M_j = M_{1j} + \sqrt{c}\, M_{2j} \quad (1 \le j \le 4)$$

with

$$M_{1j} = \sum_{i=1}^{4} y_i \gamma_i^{(j)} \quad \text{and} \quad M_{2j} = \sum_{i=1}^{4} y_{i+4} \gamma_i^{(j)},$$

implying

$$M_{4+j} = M_{1j} - \sqrt{c}\, M_{2j} \quad (1 \le j \le 4).$$

We remark that M_{1j} $(1 \le j \le 4)$ depends only on $y_1, \ldots, y_4$, whereas M_{2j} $(1 \le j \le 4)$ depends only on $y_5, \ldots, y_8$. We combine suitable factors of the index form $I = I(\mathbf{y})$, namely,

$$\begin{aligned} (M_i - M_j)(M_{i+4} - M_{j+4}) &= (M_{1i} - M_{1j})^2 - c(M_{2i} - M_{2j})^2 \\ &\qquad\qquad \text{for } 1 \le i < j \le 4,\\ (M_i - M_{j+4})(M_{i+4} - M_j) &= (M_{1i} - M_{1j})^2 - c(M_{2i} + M_{2j})^2 \\ &\qquad\qquad \text{for } 1 \le i \le 4,\ j+4 \ge 5,\ i \ne j,\\ M_i - M_{i+4} &= 2\sqrt{c} M_{2i} \quad \text{for } 1 \le i \le 4. \end{aligned}$$

For abbreviation we set

$$\tilde{M}_{ij} = ((M_{1i} - M_{1j})^2 - c(M_{2i} - M_{2j})^2)((M_{1i} - M_{1j})^2 - c(M_{2i} + M_{2j})^2)$$

for $1 \le i < j \le 4$ and obtain

$$\sqrt{d_{K_3}}\, I(\mathbf{y}) = 2^4 c^2 \prod_{i=1}^{4} M_{2i} \prod_{1\le i<j\le 4} \tilde{M}_{ij}. \tag{8}$$

The determinants of the coefficient matrices of $M_{11}, \ldots, M_{14}$ and of $M_{21}, \ldots, M_{24}$, respectively, are not divisible by p, hence they correspond to invertible endomorphisms of $\mathbb{F}_p^4$.

For $p \ge 5$ we choose non-zero $m_{2j} \in \mathbb{F}_p$ $(1 \le j \le 4)$ pairwise incongruent modulo p. We also choose $m_{1j} \in \mathbb{F}_p$ $(1 \le j \le 4)$ pairwise incongruent modulo p. For this choice there exist $y_1, \ldots, y_8 \in \mathbb{F}_p$ with

$$M_{1j} \equiv m_{1j} \bmod p \quad \text{and} \quad M_{2j} \equiv m_{2j} \bmod p \quad (1 \le j \le 4).$$

Then the product $M_{21} \cdots M_{24}$ is not divisible by p. Now we assume that p divides $\tilde{M}_{ij}$ for some indices $1 \le i < j \le 4$. This implies

$$(m_{1i} - m_{1j})^2 - c(m_{2i} - \varepsilon m_{2j})^2 \equiv 0 \bmod p$$

for $\varepsilon \in \{\pm 1\}$. Since c is a quadratic non-residue in this case, the latter would be possible only for $m_{1i} \equiv m_{1j} \bmod p$, which we excluded. We conclude that the field index is divisible neither by 5 nor by 7.

It remains to consider $p = 3$. For $\mathbf{y} \in \mathbb{F}_p^4$ with $M_{2j}(\mathbf{y}) \equiv 0 \bmod 3$ the field index is clearly divisible by 3. If we choose $\mathbf{y}_i \in \mathbb{F}_p^4$ for $i = 1, 2$ subject to

$$(M_{11}(\mathbf{y}_1), (M_{12}(\mathbf{y}_1), (M_{13}(\mathbf{y}_1), (M_{14}(\mathbf{y}_1)) \equiv (1, 1, 3, 2) \bmod 9,$$
$$(M_{21}(\mathbf{y}_2), (M_{22}(\mathbf{y}_2), (M_{23}(\mathbf{y}_2), (M_{24}(\mathbf{y}_2)) \equiv (3, 1, 2, 2) \bmod 9,$$

we obtain elements whose index is exactly divisible by 3. Finally, if none of the $M_{2j}(\mathbf{y})$ $(1 \le j \le 4)$ is divisible by 3, their values are congruent to 1 or 2 modulo 3. For any $\mathbf{y} \in \mathbb{F}_3^8$ there exists a pair (i, j) with $M_{1i}(\mathbf{y}) \equiv M_{1j}(\mathbf{y}) \bmod 3$. For these indices we obtain either $M_{2i} \equiv M_{2j} \bmod 3$ or $M_{2i} + M_{2j} \equiv 0 \bmod 3$. In both cases the index $I(\mathbf{y})$ is divisible by 9 (compare (8)). Hence, we have proven that the field index is exactly divisible by 3.

Subcase (ii)(b): *p divides c.* For prime numbers $p \ge 5$ the arguments of the previous subcase remain valid. We only need to consider $p = 3$. For any $\mathbf{y} \in \mathbb{F}_p^8$ there exists a pair (i, j) with $M_{1i}(\mathbf{y}) \equiv M_{1j}(\mathbf{y}) \bmod 3$ $(1 \le j \le 4)$. But then $\tilde{M}_{ij}(\mathbf{y})$ is divisible by 9. If additionally one of the M_{2j} is divisible by 3 then the field index is divisible by 3^3. If no M_{2j} is divisible by 3, they belong to only two residue classes modulo 3 and—as in the previous subcase—either $M_{2i}(\mathbf{y}) - M_{2j}(\mathbf{y})$ or $M_{2i}(\mathbf{y}) + M_{2j}(\mathbf{y})$ is divisible by 3 for suitable (i, j). Hence, the field index is divisible by 3^3 in any case. Finally, if we choose $\mathbf{y} \in \mathbb{F}_3^8$ subject to

$$(M_{11}(\mathbf{y}), (M_{12}(\mathbf{y}), (M_{13}(\mathbf{y}), (M_{14}(\mathbf{y})) \equiv (1,4,3,2) \bmod 9,$$
$$(M_{21}(\mathbf{y}), (M_{22}(\mathbf{y}), (M_{23}(\mathbf{y}), (M_{24}(\mathbf{y})) \equiv (1,2,2,2) \bmod 9,$$

an easy calculation shows that the field index is exactly divisible by the third power of 3.

Case (iii): *a is a quadratic residue modulo p, b is a quadratic non-residue modulo p, and p divides c.* With the notation of the previous case we further split the M_{1j}, M_{2j} into

$$\begin{aligned} M_{11} &= M_{111} + \sqrt{b}\, M_{211}, & M_{21} &= M_{121} + \sqrt{b}\, M_{221},\\ M_{12} &= M_{112} + \sqrt{b}\, M_{212}, & M_{22} &= M_{122} + \sqrt{b}\, M_{222},\\ M_{13} &= M_{111} - \sqrt{b}\, M_{211}, & M_{23} &= M_{121} - \sqrt{b}\, M_{221},\\ M_{14} &= M_{112} - \sqrt{b}\, M_{212}, & M_{24} &= M_{122} - \sqrt{b}\, M_{222}. \end{aligned}$$

If we set

$$\begin{aligned} M = {}& 4bM_{211}M_{212}((M_{111} - M_{112})^2 - b(M_{211} - M_{212})^2)\\ & \times ((M_{111} - M_{112})^2 - b(M_{211} + M_{212})^2) \end{aligned}$$

for abbreviation, then the index form satisfies

$$I(\mathbf{y}) \equiv (M_{121}^2 - bM_{221}^2)(M_{122}^2 - bM_{222}^2)M^4 \bmod p. \tag{9}$$

Because $p \geq 3$ we can choose $M_{111} \not\equiv M_{112} \bmod p$ so that the last two factors of M are not divisible by p. If additionally p does not divide $M_{211}M_{212}M_{121}M_{112}$ we even obtain

$$M \not\equiv 0 \bmod p, \quad (M_{121}^2 - bM_{221}^2) \not\equiv 0 \bmod p, \quad (M_{122}^2 - bM_{222}^2) \not\equiv 0 \bmod p.$$

Putting things together, we have proved the following theorem.

Theorem 3.1. *Let p be one of the primes $3, 5, 7$ and denote by $\alpha(p)$ the ν_p-value of the field index of K_3.*

1. *If a, b, c are quadratic residues modulo p, then*
$$\alpha(p) = \begin{cases} 7 & \text{if } p = 3,\\ 3 & \text{if } p = 5,\\ 1 & \text{if } p = 7. \end{cases}$$
2. *If a, b are quadratic residues modulo p, and c is a quadratic non-residue modulo p, then*
$$\alpha(p) = \begin{cases} 1 & \text{if } p = 3,\\ 0 & \text{if } p = 5,\\ 0 & \text{if } p = 7. \end{cases}$$

3. *If a, b are quadratic residues modulo p and $p \mid c$, then*

$$\alpha(p) = \begin{cases} 3 & \text{if } p = 3, \\ 0 & \text{if } p = 5, \\ 0 & \text{if } p = 7. \end{cases}$$

4. *If a is a quadratic residue modulo p, b is a quadratic-non-residue modulo p, and $p \mid c$, then $\alpha(p) = 0$.*

This finishes the consideration of the odd part of the field index.

p **even.** Since 2 is certainly not coprime to the non-zero entries of the transformation matrix T, we must now work with the integral bases $\omega_1, \dots, \omega_8$ introduced in the previous section (see Lemma 2.2 and the subsequent example).

This motivates us to distinguish the following main cases:

- b, c are quadratic residues modulo 8 and $a \equiv 1, 5 \bmod 8$ (Case (i));
- $a \equiv 3 \bmod 4$, $b \equiv 1, 5 \bmod 8$, $c \equiv 1 \bmod 8$ (Case (ii));
- $a \equiv 2 \bmod 4$ (Case (iii)).

Each of them must still be split into subcases below.

We note that 1 is the only quadratic residue modulo 2, 4, 8. Hence, it will be helpful if we can map (parts of) the linear forms considered into $\mathbb{Z}/8\mathbb{Z}$. The next lemma is useful in this context.

Let b, c be congruent to 1 modulo 8. According to Lemma 2.2 the ring of integers o_E of the extension $E = \mathbb{Q}(\sqrt{b}, \sqrt{c})$ has an integral basis

$$\omega_1 = 1, \qquad \omega_2 = \frac{\sqrt{b} + b}{2}, \qquad \omega_3 = \frac{\sqrt{c} + c}{2}, \qquad \omega_4 = \frac{1}{k}\omega_2\omega_3,$$

where k denotes the greatest common divisor of b and c.

Lemma 3.2. *For b, c congruent to 1 modulo 8 there exists a surjective $\mathbb{Z}$-module homomorphism ψ from o_E to $\mathbb{Z}/8\mathbb{Z}$. For $L_{1j}(\mathbf{x}) := \sum_{i=1}^{4} x_i \omega_i^{(j)}$ and arbitrary $(z_1, \dots, z_4) \in \mathbb{Z}/8\mathbb{Z}$ there exist $x_1, \dots, x_4 \in \mathbb{Z}$ satisfying*

$$\psi(L_{1j}(x_1, \dots, x_4)) = z_j \qquad (1 \le j \le 4).$$

Proof. We consider the system of congruences

$$u + v \equiv 1 \bmod 8 \quad \text{and} \quad uv \equiv 2d \bmod 8$$

for given $d \in \mathbb{Z}$. Clearly, exactly one of u, v must be even; assume that $u \in 2\mathbb{Z}$. Then necessarily $\nu_2(u) = \nu_2(2d)$. An easy calculation shows that there is a unique solution (u, v) for each d. To define a $\mathbb{Z}$-homomorphism $\psi : o_E \to \mathbb{Z}/8\mathbb{Z}$ we just need to prescribe the images of the basis elements.

Considering traces and norms of ω_2, ω_3 we get

$$b \equiv 1 \bmod 8, \quad (b^2-b)/4 \equiv 2d_b \bmod 8,$$
$$c \equiv 1 \bmod 8, \quad (c^2-c)/4 \equiv 2d_c \bmod 8.$$

Let the solutions of these two systems of congruences be (b_1, b_2) and (c_1, c_2) with odd integers b_2, c_2. We set

$$\psi(\omega_2) = \psi\left(\frac{b+\sqrt{b}}{2}\right) = b_1, \quad \psi\left(\frac{b-\sqrt{b}}{2}\right) = b_2,$$
$$\psi(\omega_3) = \psi\left(\frac{c+\sqrt{c}}{2}\right) = c_1, \quad \psi\left(\frac{c-\sqrt{c}}{2}\right) = c_2.$$

The remaining images are straightforward:

$$\psi(1) = 1, \quad \psi(\omega_4) \equiv b_1c_1/k \bmod 8.$$

We remark that ψ is surjective (according to its definition) and compatible with the action of the Galois group. The matrix $M_1 := (\psi(\omega_i^{(j)}))_{1\le i,j\le 4}$ has a non-zero determinant in $\mathbb{Z}/8\mathbb{Z}$. Hence, for any $(z_1, \dots, z_4) \in (\mathbb{Z}/8\mathbb{Z})^4$ there exist $x_1, \dots, x_4 \in \mathbb{Z}$ such that $\psi(L_{1j}(x_1, \dots, x_4)) = z_j$ for $1 \le j \le 4$. ∎

Case (i): *b, c are quadratic residues modulo 8.*

Subcase (i)(a): *a is a quadratic residue modulo 8.* Here the linear forms $L_j(\mathbf{x})$ $(1 \le j \le 8)$ can be directly mapped onto $(\mathbb{Z}/8\mathbb{Z})^8$ since the discriminant of K_3 is not divisible by 2 according to Lemma 2.2. We choose $j-1$ as the value of the linear form $L_j(\mathbf{x})$ $(1 \le j \le 8)$. Then it is easily seen that the product on the right-hand side of (7) becomes divisible by 2^{16}. (For example, the differences of $L_1(\mathbf{x})$ with the other $L_j(\mathbf{x})$ for odd j yield a factor of 2^{1+2+1}.) If we put more than one $L_j(\mathbf{x})$ into the same residue class the power of 2 in that product obviously increases.

Subcase (i)(b): $a \equiv 5 \bmod 8$. We take up the ideas of Subcase (ii)(a) for odd p (see (8)) to split the linear forms $L_j(\mathbf{x})$ of the index form I as follows. According to Lemma 2.2 we put $\eta_1 = (a+\sqrt{a})/2$, $\eta_2 = (b+\sqrt{b})/2$, $\eta_3 = (c+\sqrt{c})/2$ to get

$$\omega_j := \frac{1}{g_j}\prod_{i=1}^{r}\eta_i^{\alpha_{ji}} \quad (i \le j \le 8)$$

where the α_{ji} were defined in (1) and the g_j in (2).

Reordering the conjugates appropriately we can write the linear forms

$$L_j = L_{1j} + \frac{a+\sqrt{a}}{2}L_{2j} \quad \text{and} \quad L_{4+j} = L_{1j} + \frac{a-\sqrt{a}}{2}L_{2j} \quad (1 \le j \le 4).$$

We note that the L_{1j}, L_{2j} are linear forms in $1, \eta_2, \eta_3, \eta_2\eta_3$ and their conjugates, with the coefficients being fractions with odd denominators. Also, the L_{1j} $(1 \le j \le 4)$ only depend on $x_1, \dots, x_4$, whereas the L_{2j} $(1 \le j \le 4)$ only depend on $x_5, \dots, x_8$. Combining suitable factors of the index form $I = I(\mathbf{x})$ we obtain

$$\sqrt{d_{K_3}}\, I(\mathbf{x}) = a^2 \prod_{i=1}^{4} L_{2i} \prod_{1\le i<j\le 4} (\tilde{L}_{ij1}\tilde{L}_{ij2}) \tag{10}$$

with

$$\tilde{L}_{ij1} = \left((L_{1i} - L_{1j}) + \frac{1}{2}(L_{2i} - L_{2j})\right)^2 - \frac{a}{4}(L_{2i} - L_{2j})^2,$$
$$\tilde{L}_{ij2} = \left((L_{1i} - L_{1j}) + \frac{1}{2}(L_{2i} - L_{2j})\right)^2 - \frac{a}{4}(L_{2i} + L_{2j})^2.$$

A simple calculation yields

$$\tilde{L}_{ij2} - \tilde{L}_{ij1} = \frac{a}{4}((L_{2i} - L_{2j})^2 - (L_{2i} + L_{2j})^2) = -aL_{2i}L_{2j}.$$

Hence, $\tilde{L}_{ij1}$ and $\tilde{L}_{ij2}$ have different parity if and only if L_{2i} and L_{2j} are both odd.

Now we substitute $a = 8\alpha + 5$ into $\tilde{L}_{ij1}$ to get

$$\begin{aligned}\tilde{L}_{ij1} &= (L_{1i} - L_{1j})^2 + (L_{1i} - L_{1j})(L_{2i} - L_{2j}) - \frac{a-1}{4}(L_{2i} - L_{2j})^2\\ &= (L_{1i} - L_{1j})^2 + (L_{1i} - L_{1j})(L_{2i} - L_{2j}) - (2\alpha + 1)(L_{2i} - L_{2j})^2.\end{aligned}$$

We observe that $\tilde{L}_{ij1}(\mathbf{x})$ is even exactly if

$$L_{1i}(\mathbf{x}) \equiv L_{1j}(\mathbf{x}) \bmod 2 \quad \text{and} \quad L_{2i}(\mathbf{x}) \equiv L_{2j}(\mathbf{x}) \bmod 2,$$

and in this case $\tilde{L}_{ij1}(\mathbf{x})$ is at least divisible by 4.

Now we apply the map ψ of Lemma 3.2 to the linear forms L_{1j}, L_{2j}. We can choose $\mathbf{x} \in \mathbb{Z}^8$ such that

$$\begin{aligned}(L_{21}(\mathbf{x}), \dots, L_{24}(\mathbf{x})) &\equiv (2, 1, 5, 6) \bmod 8,\\ (L_{11}(\mathbf{x}), \dots, L_{14}(\mathbf{x})) &\equiv (1, 2, 3, 6) \bmod 8.\end{aligned}$$

Then $\prod_{i=1}^4 L_{2i}(\mathbf{x})$ is exactly divisible by 4. Also, according to the discussion above, $\tilde{L}_{ij1}$ is odd for $(i, j) \neq (2, 3)$. For $(i, j) = (2, 3)$ the values $\tilde{L}_{ij1}$ and $\tilde{L}_{ij2}$ have different parities. While $\tilde{L}_{231}$ is still odd we obtain

$$\begin{aligned}\tilde{L}_{232} &\equiv (L_{12} - L_{13})^2 + (L_{12} - L_{13})(L_{22} - L_{23})\\ &\quad - (2\alpha + 1)(L_{22} - L_{23})^2 - (8\alpha + 5)L_{22}L_{33} \bmod 8\\ &\equiv 1 + 4 - (2\alpha + 1)4^2 - 5^2 \bmod 8\\ &\equiv -20 \bmod 8.\end{aligned}$$

Hence, $\tilde{L}_{232}$ is exactly divisible by 4, and $I(\mathbf{x})$ is exactly divisible by 2^4.

It remains to show that $I(\mathbf{x})$ is at least divisible by 2^4 in all other cases. If all L_{2i}-values are odd then there are at least two pairs (i, j) for which

L_{1i} and L_{1j} have the same parity. This implies $16 \mid I(\mathbf{x})$. If exactly one value L_{2i} is even we can assume that this is L_{21}. Among the pairs (i,j) for $2 \le i < j \le 4$ there is at least one for which L_{1i} and L_{1j} have the same parity. (If two such pairs exist we necessarily have $2^5 \mid I(\mathbf{x})$.) Again, we can assume that $L_{12}(\mathbf{x}) \equiv L_{13}(\mathbf{x}) \bmod 2$. Then $\tilde{L}_{231}(\mathbf{x})$ is divisible at least by 4. Now, $L_{22}, L_{24}, \tilde{L}_{241}$ are all odd and the parity of $\tilde{L}_{241}$ is different from that of $\tilde{L}_{242}$. Since $\tilde{L}_{242}$ is even we see that 2^4 divides $I(\mathbf{x})$. If more than two values L_{2i} are even it is obvious that 2^4 divides $I(\mathbf{x})$.

Case (ii): *a is a quadratic non-residue modulo* 4. We observe that the elements ω_2, ω_4, ω_6, ω_8 of the integral basis are of the form $\omega_{2j} = \sqrt{a}\,\tilde{\omega}_{2j}$ $(1 \le j \le 4)$, where the $\tilde{\omega}_{2j}$ are not necessarily integral. Any occurring denominators are odd, however. We reorder the L_j into $L_1, L_3, L_5, L_7, L_2, L_4, L_6, L_8$. Thus we get

$$L_j(\mathbf{x}) = L_{1j} + \sqrt{a}\,L_{2j} \qquad (1 \le j \le 4)$$

with

$$L_{1j} = \sum_{i=1}^{4} x_i \omega_i^{(j)} \quad \text{and} \quad L_{2j} = \sum_{i=1}^{4} x_{i+4} \tilde{\omega}_i^{(j)},$$

implying

$$L_{4+j} = L_{1j} - \sqrt{a}\,L_{2j} \qquad (1 \le j \le 4).$$

We remark that L_{1j} $(1 \le j \le 4)$ depends only on $x_1, \ldots, x_4$, whereas L_{2j} $(1 \le j \le 4)$ depends only on $x_5, \ldots, x_8$. We combine suitable factors of the index form $I = I(\mathbf{x})$. For abbreviation we set

$$\tilde{L}_{ij} = ((L_{1i} - L_{1j})^2 - a(L_{2i} - L_{2j})^2)((L_{1i} - L_{1j})^2 - a(L_{2i} + L_{2j})^2)$$

for $1 \le i < j \le 4$ to obtain

$$\sqrt{d_{K_3}}\, I(\mathbf{x}) = 2^4\, a^2 \prod_{i=1}^{4} L_{2i} \prod_{1 \le i < j \le 4} \tilde{L}_{ij}. \tag{11}$$

Subcase (ii)(a): *b, c are quadratic residues modulo* 8. The determinants of the coefficient matrices of $L_{11}, \ldots, L_{14}$ and of $L_{21}, \ldots, L_{24}$, respectively, are not divisible by 2, hence these matrices correspond to invertible endomorphisms from $\mathbb{Z}^4$ onto $(\mathbb{Z}/8\mathbb{Z})^4$ (cf. Lemma 3.2).

If we choose

$$(L_{21}(\mathbf{x}), \ldots, L_{24}(\mathbf{x})) \equiv (2,1,3,6) \bmod 8,$$
$$(L_{11}(\mathbf{x}), \ldots, L_{14}(\mathbf{x})) \equiv (1,2,3,6) \bmod 8,$$

the products on the right-hand side of (11) contain a factor of 2^{10}. We note that even values of $\tilde{L}_{ij}$ are necessarily divisible by 2^4. Hence, for any other choice of the $L_{ij}(\mathbf{x})$ $(i = 1, 2,\ 1 \le j \le 4)$ the products on the right-hand side of (11) are at least divisible by 2^{10}.

We conclude that the field index is exactly divisible by 2^6. This is because we have an additional factor of 2^4 in the square root of the discriminant of K_3.

Subcase (ii)(b): *c is a quadratic residue modulo* 8 *and* $b \equiv 5 \bmod 8$. In this case the terms of $\tilde{L}_{ij}$ can be viewed as elements in $F := \mathbb{Q}(\sqrt{b})$, more precisely we study them in $o_F/2o_F$, where o_F denotes the maximal order of F. Since $b \equiv 5 \bmod 8$, the prime 2 stays inert in F. The factor ring (finite field) $o_F/2o_F$ consists of four residue classes represented by $2, 1, \zeta := (1+\sqrt{b})/2, \zeta^2$. If we distribute the values $L_{1j}(\mathbf{x})$ into all four residue classes in the given order then only the difference $L_{13} - L_{14}$ is divisible by 2. If we also choose all L_{2j} odd so that their differences are at least divisible by 2 then exactly one $\tilde{L}_{ij}$ becomes divisible by exactly 4 and the others stay odd. Hence, the products on the right-hand side of (11) are exactly divisible by 2^2. All other choices of the L_{ij}-values lead at least to that divisibility condition.

Case (iii): *a is exactly divisible by* 2. Again, the index form can be written as in (11).

Subcase (iii)(a): *b, c are quadratic residues modulo* 8. If we choose

$$(L_{21}(\mathbf{x}), \dots, L_{24}(\mathbf{x})) \equiv (1, 5, 2, 6) \bmod 8,$$
$$(L_{11}(\mathbf{x}), \dots, L_{14}(\mathbf{x})) \equiv (1, 2, 3, 4) \bmod 8,$$

the products on the right-hand side of (11) are exactly divisible by 2^{10}. Any other choice of the $L_{ij}(\mathbf{x})$ ($i = 1, 2$, $1 \le j \le 4$) yields divisibility by at least 2^{10}. Since an additional factor 2^4 is contained in the square root of the discriminant in this case, the even part of the field index is 2^6.

Subcase (iii)(b): *c is a quadratic residue modulo* 8 *and* $b \equiv 5 \bmod 8$. We take up our considerations of Subcase (ii)(b). There are only two new aspects: the square root of the discriminant of K_3 gets an additional factor 2^2 and the generating element a is now exactly divisible by 2. Then the same analysis as in the previous case shows that the field index is always divisible by 2^2, and there are elements in K_3 for which this index is not divisible by 2^3, for example $\omega_4 + \omega_7$.

Subcase (iii)(c): *c is a quadratic residue modulo* 4 *and b is a quadratic non-residue modulo* 4. As we know from the introduction, the field $\mathbb{Q}(\zeta_{24})$ has a power integral basis. Hence, we need to show that the field index is odd and therefore 1.

We conclude as in Subcases (ii)(b) and (iii)(b). But we need to point out that the second and fourth summands of L_{2j} are not necessarily algebraic integers anymore, only their product with $\sqrt{a}$ is.

We show that the element $\eta := \omega_4 + \omega_5$ (notation as in the example in the previous section) has index not divisible by 2. We have $L_{11} = (1+\sqrt{c})/2$ and $L_{21} = (\sqrt{b}/g + 1)/2$. Accordingly, the differences $L_{1ij} := L_{1i} - L_{1j}$ become 0 for $(i,j) = (1,2),(3,4)$ and $\sqrt{c}$ in the remaining four cases. We also calculate $L_{2ij} := L_{2i} - L_{2j}$. The values are 0 for $(i,j) = (1,3),(2,4)$ and $\sqrt{b}/g$ otherwise. From this we obtain, for the factors on the right-hand side of (11),

$$2^4 a^2 \prod_{i=1}^{4} L_{2i} = 2^4 a^2 \left(1 - \frac{b}{g^2}\right)^2 \frac{1}{16},$$

which is exactly divisible by 2^4, and

$$\tilde{L}_{ij} \begin{cases} \text{odd} & \text{for } (i,j) \in \{(1,3),(1,4),(2,3),(2,4)\}, \\ \text{exactly divisible by 4} & \text{for } (i,j) \in \{(1,2),(3,4)\}. \end{cases}$$

Since the square root of the discriminant of K_3 is exactly divisible by 2^8, the index of η is odd.

Putting these results together we obtain:

Theorem 3.3. *The* 2*-part of the field index of* K_3 *is*

- 2^{16} *for* $(a,b,c) \equiv (1,1,1) \bmod 8$*;*
- 2^4 *for* $a \equiv 5 \bmod 8$ *and* $(b,c) \equiv (1,1) \bmod 8$;
- 2^6 *for* $a \equiv 3 \bmod 4$ *and* $(b,c) \equiv (1,1) \bmod 8$;
- 2^2 *for* $a \equiv 3 \bmod 4$ *and* $(b,c) \equiv (5,1) \bmod 8$;
- 2^6 *for* $a \equiv 2 \bmod 4$ *and* $(b,c) \equiv (1,1) \bmod 8$;
- 2^2 *for* $a \equiv 2 \bmod 4$ *and* $(b,c) \equiv (5,1) \bmod 8$;
- 2^0 *for* $a \equiv 2 \bmod 4$ *and* $(b,c) \equiv (3,1) \bmod 4$.

Remark. We note that our results include those of [10] without any restrictions on the generating elements a, b, c.

4. Field indices of K_r for higher r. Let r be a positive integer and $a_1, \ldots, a_r$ be integers such that the field $K := K_r = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r})$ has degree 2^r. Let o_K denote the maximal order of K as before. The aim of this section is to prove the following theorem.

Theorem 4.1. *Let p be a prime number and n be a positive integer. Then there exists $N_0 = N_0(p,n)$ such that $N \geq N_0$ implies that the field index of K_N is divisible by p^n.*

Proof. Case of p odd. Let p be an odd prime. We denote by $\left(\frac{\cdot}{p}\right)$ the Legendre symbol. As we showed in Section 3, Subsection "p odd", we need to discuss three cases for K_r:

1. $\left(\frac{a_i}{p}\right) = 1$ for all $i = 1, \ldots, r$;
2. $\left(\frac{a_1}{p}\right) = -1$ or p divides a_1 and $\left(\frac{a_i}{p}\right) = 1$ for all $i = 2, \ldots, r$;
3. a_1 is divisible by p, $\left(\frac{a_2}{p}\right) = -1$ and $\left(\frac{a_i}{p}\right) = 1$ for all $i = 3, \ldots, r$.

In case $\left(\frac{a_i}{p}\right) = 1$ $(1 \le i \le r)$ we fix $b_i \in \mathbb{F}_p$ such that $b_i^2 = a_i$. Then we define $\psi(\varepsilon\sqrt{a_i}) = \varepsilon b_i$ for all allowed indices, where $\varepsilon = \pm 1$. One can extend ψ in a straightforward way to a homomorphism $\psi : o_K \to \mathbb{F}_p$. See the discussion about the correspondence between the linear forms $L_i(\mathbf{x})$ and $M_j(\mathbf{y})$ in Section 3.

CASE 1. We choose r so large that $2^r > p^{n+1}$. Let $\mathbf{y} \in \mathbb{Z}^{2^r}$. Because $\psi(M_j(\mathbf{y})) \in \mathbb{F}_p$ for all $j = 1, \ldots, 2^r$, there exists $u \in \mathbb{F}_p$ which appears as the value of at least $2^r/p > p^n$ linear forms. Let $J = \{j \mid \psi(M_j(\mathbf{y})) = u\}$. Then $M_{j_1}(\mathbf{y}) - M_{j_2}(\mathbf{y})$ is divisible by p for all $j_1, j_2 \in J$, with $j_1 < j_2$. The number of such pairs of indices is $|J|(|J|-1)/2 > |J| > p^n$. Thus p^n divides $I_{K_r}(M(\mathbf{y}))$ for all $\mathbf{y} \in \mathbb{Z}^{2^r}$, i.e. p^n divides the index of all integral elements of K_r.

CASE 2. Now we write

$$\begin{aligned} M_j(\mathbf{y}) &= M_{1j}(\mathbf{y}) + \sqrt{a_1}\, M_{2j}(\mathbf{y}) \quad (j = 1, \ldots, 2^{r-1}), \\ M_{j+2^{r-1}}(\mathbf{y}) &= M_{1j}(\mathbf{y}) - \sqrt{a_1}\, M_{2j}(\mathbf{y}) \quad (j = 1, \ldots, 2^{r-1}). \end{aligned}$$

We put

$$\tilde{M}_{ij} = ((M_{1i}-M_{1j})^2 - a_1(M_{2i}-M_{2j})^2)((M_{1i}-M_{1j})^2 - a_1(M_{2i}+M_{2j})^2) \tag{12}$$

for $1 \le i < j \le 2^{r-1}$. Then we get as before

$$\sqrt{D_{K_r}}\, I_{K_r}(\mathbf{y}) = (2a_1)^{2^{r-1}} \prod_{j=1}^{2^{r-1}} M_{2j} \prod_{1 \le i < j \le 2^{r-1}} \tilde{M}_{ij}.$$

We choose r so large that $2^{r-1} > p^{n+2}$. Because $\psi(M_{1j}(\mathbf{y})) \in \mathbb{F}_p$ for all $j = 1, \ldots, 2^{r-1}$, there exists $u \in \mathbb{F}_p$ which appears as the value of at least $2^{r-1}/p$ linear forms. Let $J_1 = \{j \mid \psi(M_{1j}(\mathbf{y})) = u\}$. As $\psi(M_{2j}(\mathbf{y})) \in \mathbb{F}_p$ for all $j \in J_1$ (actually for all $j = 1, \ldots, 2^{r-1}$) there exists $v \in \mathbb{F}_p$ which appears as the value of at least $|J_1|/p \ge 2^{r-1}/p^2$ linear forms. Let $J_2 = \{j \mid \psi(M_{2j}(\mathbf{y})) = v\}$. Then $\psi(M_{1i} - M_{1j}) = \psi(M_{2i} - M_{2j}) = 0$ for all $i, j \in J_2$, $i < j$. This means that the exponent of p in $I_{K_r}(\mathbf{y})$ is at least

$$2|J_2|(|J_2|-1)/2 > 2^{r-1}/p^2 > p^n.$$

CASE 3. Now we have to split the linear forms M_{1j}, M_{2j} further. We write

$$\begin{aligned} M_{1j}(\mathbf{y}) &= M_{11j}(\mathbf{y}) + \sqrt{a_2}\, M_{12j}(\mathbf{y}) \quad (j = 1, \ldots, 2^{r-2}), \\ M_{2j}(\mathbf{y}) &= M_{21j}(\mathbf{y}) + \sqrt{a_2}\, M_{22j}(\mathbf{y}) \quad (j = 1, \ldots, 2^{r-2}), \\ M_{1,j+2^{r-2}}(\mathbf{y}) &= M_{11j}(\mathbf{y}) - \sqrt{a_2}\, M_{12j}(\mathbf{y}) \quad (j = 1, \ldots, 2^{r-2}), \\ M_{2,j+2^{r-2}}(\mathbf{y}) &= M_{21j}(\mathbf{y}) - \sqrt{a_2}\, M_{22j}(\mathbf{y}) \quad (j = 1, \ldots, 2^{r-2}). \end{aligned}$$

Then we obtain

$$\begin{aligned}\tilde{M}_{ij}\tilde{M}_{i,j+2^{r-2}} &= (((M_{11i}-M_{11j})-\sqrt{a_2}(M_{21i}-M_{21j}))^4-a_1A_1)\\ &\quad\times(((M_{11i}-M_{11j})+\sqrt{a_2}(M_{21i}-M_{21j}))^4-a_1A_2)\\ &= ((M_{11i}-M_{11j})^2-a_2(M_{21i}-M_{21j})^2)^4-a_1A_3,\end{aligned}$$

with integers A_1, A_2, A_3 of K_r.

Now we repeat the argument of the previous cases. Firstly, there is a $J_1 \subseteq \{1,\dots,2^{r-2}\}$ such that $|J_1| \geq 2^{r-2}/p$ and the values $\psi(M_{11i})(\mathbf{y})$ are the same for all $i \in J_1$. Then there exists $J_2 \subseteq J_1$ such that $|J_2| \geq |J_1|/p$ and the values $\psi(M_{21i})(\mathbf{y})$ are the same for all $i \in J_2$. Consequently, $\tilde{M}_{ij}\tilde{M}_{i,j+2^{r-2}}$ is divisible by p. Thus the exponent of p in $I_{K_r}(\mathbf{y})$ is at least

$$2|J_2|(|J_2|-1)/2 > 2^{r-2}/p^2 > p^n.$$

Hence, for $2^{r-2} > p^{n+2}$ the field index is divisible by p^n.

Case of p even. The case $p = 2$ is dealt with similarly. The generalization from $r = 3$ to higher exponents r follows an analogous pattern to that for odd p. Since the number of subcases to be considered is 7 (as for $r = 3$) the proof requires arguments as in the previous section. We therefore omit the details. ∎

However, we still give an explicit proof in the most interesting case $a_1 \equiv 2 \bmod 4$, $a_2 \equiv 3 \bmod 4$, $a_i \equiv 1 \bmod 4$ $(i = 3,\dots,r)$ and $p = 2$. We consider it most interesting since the result below also shows that the field index is even for $r > 3$. For the proof we will introduce some new ideas particularly for this case. We shall use the linear forms L_i from (4) and the integral basis $\omega_1,\dots,\omega_{2^r}$ of Lemma 2.2.

LEMMA 4.2. *Let $r \geq 4$. For $a_1 \equiv 2 \bmod 4$, $a_2 \equiv 3 \bmod 4$, $a_3 \equiv 1 \bmod 4$ and $a_i \equiv 1 \bmod 8$ $(4 \leq i \leq r)$ the field index of K_r is divisible by 2^{r-2}.*

We remark that the lemma implies that the field index of K_r is even for $r > 3$ and tends to infinity for large values of r.

Proof. By Lemma 2.2 the ν_2-value of the square root of the discriminant is 2^r in this case. Similar to our considerations at the beginning of Section 2 we can further normalize the generators when we consider $p = 2$. It is easy to see that we can additionally choose $a_1,\dots,a_r$ subject to $a_i \equiv 1 \bmod 8$ for $r \geq 4$.

We shall show the result by induction on r.

Although the result of the lemma is not true for $r = 3$ we need that case for our induction hypothesis. We recall part of the results from the previous section, but we need a more precise premise for the induction step. We make use of the basis given in Lemma 2.2, but in a different ordering:

$$\omega_1 = 1, \qquad \omega_2 = \sqrt{a_2} - a_2,$$
$$\omega_3 = \frac{\sqrt{a_3} - a_3}{2}, \qquad \omega_4 = \frac{1}{2g_4}(\sqrt{a_2} - a_2)(\sqrt{a_3} - a_3),$$
$$\omega_5 = \sqrt{a_1} - a_1, \qquad \omega_6 = \frac{1}{2}(\sqrt{a_1} - a_1)(\sqrt{a_2} - a_2),$$
$$\omega_7 = \frac{1}{2g_7}(\sqrt{a_1} - a_1)(\sqrt{a_3} - a_3), \quad \omega_8 = \frac{1}{4g_8}\prod_{i=1}^{3}(\sqrt{a_i} - a_i).$$

We note that the elements g_i are odd natural numbers. The conjugates are chosen in the order

$$\mathrm{id}, \sigma_2, \sigma_3, \sigma_2\sigma_3, \sigma_1, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_1\sigma_2\sigma_3.$$

We decompose the linear forms $L_j(\mathbf{x})$ of (4) into

$$L_j(\mathbf{x}) = L_{1j} + L_{2j} \qquad (1 \le j \le 4)$$

with

$$L_{1j} = \sum_{i=1}^{4} x_i\omega_i^{(j)} \quad \text{and} \quad L_{2j} = \sum_{i=1}^{4} x_{4+i}\omega_{4+i}^{(j)}.$$

We note that $L_{2j} = \tilde{L}_{2j}(\sqrt{a_1} - a_1)/2$, implying

$$L_{4+j} = L_{1j} + \frac{-\sqrt{a_1} - a_1}{2}\tilde{L}_{2j} \qquad (1 \le j \le 4).$$

A straightforward calculation shows that for $(i,j) = (1,2),(3,4)$ the differences $L_{1i} - L_{1j}$ are multiples of 2, and those of $L_{2i} - L_{2j}$ are multiples of $\sqrt{2}$ by algebraic integers. That property remains valid for all pairs (i,j) in

$$J_3 := \{(1,2),(1,6),(5,2),(5,6),(3,4),(3,8),(7,4),(7,8)\}.$$

Also, we put

$$\hat{J}_3 := \{(i, 4+i) \mid 1 \le i \le 4\}$$

and observe that the values $L_j - L_{4+j}$ for $(j, 4+j) \in \hat{J}_3$ are multiples of 2 by algebraic integers. Hence, the index form multiplied by the square root of the discriminant of K_3 is divisible at least by $2^{4+4} = 2^8$.

Now we carry out the induction step. We put $\kappa := 2^{r-2}$ and we assume that on level $r-1$ we have an integral basis $\omega_1, \ldots, \omega_{2\kappa}$. These basis elements are ordered in such a way that the index form decomposes into two linear forms, say

$$L_j^{(r-1)} = L_{1j}^{(r-1)} + L_{2j}^{(r-1)}, \tag{13}$$

such that

$$L_{1i}^{(r-1)} - L_{1j}^{(r-1)} \in 2\bar{\mathbb{Z}},\ L_{2i}^{(r-1)} - L_{2j}^{(r-1)} \in \sqrt{2}\,\bar{\mathbb{Z}} \tag{14}$$

for each of the 2^{r-1} pairs of indices $(i,j) \in J_{r-1}$. According to Lemma 2.2 there exists an integral basis on level r in the form

$$\omega_1, \dots, \omega_{2\kappa},$$
$$\omega_{2\kappa+\mu} = \frac{\sqrt{a_r} - a_r}{2} \frac{1}{g_{\kappa,\mu}} \omega_\mu \qquad (1 \le \mu \le 2\kappa)$$

with odd integers $g_{\kappa,\mu}$. (We consider $r \ge 4$, which implies $a_r \equiv 1 \bmod 8$.)

On level r the index form $L_j^{(r)}$ decomposes as

$$L_j^{(r)} = L_j^{(r-1)} + \frac{\sqrt{a_r} - a_r}{2} \tilde{L}_j^{(r-1)} \qquad (1 \le j \le 2^r) \tag{15}$$

where the coefficients of the basis elements in $L_j^{(r-1)}$ and in $\tilde{L}_j^{(r-1)}$ just differ by the rational factors $1/g_{\kappa,\mu}$. The conjugates are ordered so the first 2κ correspond to $\langle \sigma_1, \dots, \sigma_{r-1} \rangle = G_{r-1}$ and the last 2κ correspond to $\sigma_r G_{r-1}$. This means that

$$L_{2\kappa+j}^{(r)} = L_j^{(r-1)} + \frac{-\sqrt{a_r} - a_r}{2} \tilde{L}_j^{(r-1)} \qquad (1 \le j \le 2^{r-1}). \tag{16}$$

Now we let $(i,j) \in J_{r-1}$, i.e. $L_i^{(r-1)} - L_j^{(r-1)} \in \sqrt{2}\,\bar{\mathbb{Z}}$. Then also $L_i^{(r)} - L_j^{(r)}$ and $L_{2\kappa+i}^{(r)} - L_{2\kappa+j}^{(r)}$ have this property. Therefore we get 2^r pairs of indices for which the corresponding differences of linear forms are divisible by $\sqrt{2}$.

By induction hypothesis, on level $r-1$ we have the 2^{r-2} differences $L_i^{(r-1)} - L_j^{(r-1)}$ ($(i,j) \in \hat{J}_{r-1}$) which are multiples of 2. On level r we therefore obtain twice as many such differences, namely $L_i^{(r)} - L_j^{(r)}$ and $L_{2\kappa+i}^{(r)} - L_{2\kappa+j}^{(r)}$.

It is now straightforward how to update the information from level $r-1$ to level r. We have explicitly constructed J_r from J_{r-1} containing twice as many, i.e. 2^r, pairs (i,j) for which (13) and (14) are satisfied on level r. Each of the corresponding differences of linear forms is divisible by $\sqrt{2}$. Also from the pairs $(i,j) \in \hat{J}_{r-1}$ on level $r-1$ we have obtained twice as many, i.e. 2^{r-1}, pairs (i,j) and $(2\kappa+i, 2\kappa+j)$ forming $\hat{J}_r$ for which the corresponding differences of linear forms are divisible by 2. We still remark that $J_{r-1} \cap \hat{J}_{r-1} = \emptyset$ implies $J_r \cap \hat{J}_r = \emptyset$.

Hence, the ν_2-value of the product of all these differences is $2^{r-1} + 2^{r-1} = 2^r$ which equals the ν_2-value of the square root of the discriminant of K_r. To prove the lemma we still need to exhibit additional factors of 2 in the product of differences of linear forms. They come from the fact that $a_r \equiv 1 \bmod 8$, i.e. the norm of $(\sqrt{a_r} - a_r)/2$ is even.

We consider the products $P_{ij} := (L_i^{(r)} - L_j^{(r)})(L_{2\kappa+i}^{(r)} - L_{2\kappa+j}^{(r)})$ for $(i,j) \in J_{r-1}$. We already know that P_{ij} is an integral multiple of 2. We shall prove that it is even an integral multiple of $2\sqrt{2}$. Obviously, we have 2^{r-1}

factors P_{ij}. By (13)–(16) we conclude that

$$\begin{aligned} P_{ij} &= 2\sqrt{2}\,\lambda_1 + (L_{2i}^{(r-1)} - L_{2j}^{(r-1)})^2 \\ &\quad + \frac{-\sqrt{a_r} - a_r}{2}(L_{2i}^{(r-1)} - L_{2j}^{(r-1)})(\tilde{L}_{2i}^{(r-1)} - \tilde{L}_{2j}^{(r-1)}) \\ &\quad + \frac{\sqrt{a_r} - a_r}{2}(L_{2i}^{(r-1)} - L_{2j}^{(r-1)})(\tilde{L}_{2i}^{(r-1)} - \tilde{L}_{2j}^{(r-1)}) \\ &\quad + \frac{a_r^2 - a_r}{2}(\tilde{L}_{2i}^{(r-1)} - \tilde{L}_{2j}^{(r-1)})^2, \end{aligned}$$

hence

$$P_{ij} = 2\sqrt{2}\,\lambda_2 + (L_{2i}^{(r-1)} - L_{2j}^{(r-1)})(L_{2i}^{(r-1)} - L_{2j}^{(r-1)} - a_r(\tilde{L}_{2i}^{(r-1)} - \tilde{L}_{2i}^{(r-1)})) \tag{17}$$

with algebraic integers λ_1, λ_2. Since a_r is odd and the coefficients of the basis elements in $L, \tilde{L}$ differ only by odd fractions, the last factor on the right-hand side of (17) is divisible by 2. Therefore P_{ij} is an integral multiple of $2\sqrt{2}$. Since we have 2^{r-1} such pairs $(i,j), (2\kappa+i, 2\kappa+j)$ in J_r, the ν_2-value of those products is $2^{r-1} + 2^{r-2}$. Together with the contribution of the 2^{r-1} factors $L_i^{(r)} - L_j^{(r)}$ $((i,j) \in \hat{J}_r)$ this proves the lemma. ∎

Acknowledgments. We thank the referee for his careful reading of our manuscript and important references to previous literature. His remarks helped to improve the quality of our paper considerably.

The first author was supported by the Hungarian National Foundation for Scientific Research Grant No. T67580.

Both authors were supported by the TÁMOP 4.2.1/B-09/1/KONV-2010-0007 project, which is implemented through the New Hungary Development Plan co-financed by the European Social Fund, and the European Regional Development Fund.

References

[1] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, *KANT V4*, J. Symbolic Comput. 24 (1997), 267–283.

[2] H. T. Engstrom, *On the common index divisor of an algebraic field*, Trans. Amer. Math. Soc. 32 (1930), 223–237.

[3] I. Gaál, A. Pethő and M. Pohst, *On the indices of biquadratic number fields having Galois group V_4*, Arch. Math. (Basel) 57 (1991), 357–361.

[4] H. Hasse, *Number Theory*, Springer, 1980.

[5] Y. Motoda and T. Nakahara, *Power integral bases in algebraic number fields whose Galois groups are 2-elementary abelian*, Arch. Math. (Basel) 83 (2004), 309–316.

[6] Y. Motoda, T. Nakahara and K. H. Park, *On power integral bases of the 2-elementary abelian extension fields*, Trends in Math., Information Center for Mathematical Sciences 8 (2006), 55–63.

[7] T. Nakahara, *On the indices and integral bases of non-cyclic but abelian biquadratic number fields*, Arch. Math. (Basel) 41 (1983), 504–508.
[8] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, 2004.
[9] E. Nart, *On the index of a number field*, Trans. Amer. Math. Soc. 289 (1985), 171–183.
[10] G. Nyul, *Non-monogeneity of multiquadratic number fields*, Acta Math. Inform. Univ. Ostraviensis 10 (2002), 85–93.
[11] B. Schmal, *Diskriminanten, $\mathbb{Z}$-Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern*, Arch. Math. (Basel) 52 (1989), 245–257.
[12] S. Schmitt and H. G. Zimmer, *Elliptic Curves: A Computational Approach*, de Gruyter, 2003.
[13] J. Śliwa, *On the nonessential discriminant divisor of an algebraic number field*, Acta Arith. 42 (1982), 57–72.
[14] K. S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull. 13 (1970), 519–526.
[15] E. Żyliński, *Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Körper*, Math. Ann. 73 (1913), 273–274.

Attila Pethő
Department of Computer Science
University of Debrecen
Number Theory Research Group
Hungarian Academy of Sciences
and University of Debrecen
P.O. Box 12
H-4010 Debrecen, Hungary
E-mail: petho.attila@inf.unideb.hu

Michael E. Pohst
Technische Universtät Berlin
Institut für Mathematik, MA 8-1
Straße des 17. Juni 136
10623 Berlin, Germany
E-mail: pohst@math.tu-berlin.de

Received on 13.5.2011
and in revised form on 2.10.2011 (6696)