MATHEMATICS OF COMPUTATION
VOLUME 45, NUMBER 172
OCTOBER 1985, PAGES 591-611

On Real Cyclic Sextic Fields

By V. Ennola, S. Mäki and R. Turunen

Abstract. A table of units and class numbers of real cyclic sextic fields with conductor $f_6 \leqslant 2021$ has been given by the second author [13]. We first fill in the gaps in [13] and then construct an extended table for $2021 < f_6 < 4000$. The article contains results about Galois module structure of the unit group, relative norms of the units, and ideal classes of the subfields becoming principal in the sextic field. The connection with Leopoldt's theory [11] is described. A parametric family of fields containing exceptional units [14] is constructed. We give statistics referring to class numbers of fields with prime conductor, the appearance of units of different types if the relative class number is > 1, Leopoldt's unit index, and the signature rank of the unit group.

1. Introduction. A table of units and class numbers of the 1337 real cyclic sextic fields K_6 with conductor $f_6 \leqslant 2021$ has been given by the second author [13]. In this table there are 12 gaps (included in the cardinality 1337), the reason for the failure being in 6 cases similar gaps in M.-N. Gras's table of cyclic cubic fields [5], and in the 6 other cases, the appearance of too large numbers which the program could not handle. Since it seems to be of importance for many purposes to have a complete result reaching as far as possible, we have taken up the work and have constructed an extended table of the 1743 fields K_6 with $2021 < f_6 < 4000$. M.-N. Gras's table of real cyclic quartic fields, [6] and [7], and the main table in [5] also have the same range, i.e., conductor < 4000, but in [3] the first and third author have obtained the result in the cubic case up to conductor < 16000.

The efficient multiprecision routines developed in [2] and [3] enabled us first to fill in the gaps in [5] and then complete the computations in the 12 open sextic cases as well as in other difficult large cases. Hence, the table in [13] and the new one together provide a complete answer for all real cyclic sextic fields with conductor < 4000.

The gaps in [5] have independently been filled in by Godwin [4] whose method is entirely different from ours, the latter being based on the same adaptation of the Voronoi algorithm we used in [2].

The present paper should be regarded as a supplement to [13]. We use the same terminology and notation with one exception: the ambiguous term "f_6 is decomposable" is replaced by the more accurate "χ_6 is decomposable". See Section 2 for an explanation and for a list of additional notation.

In Section 3 we make a comparison between the terminology in [13] and the one of Leopoldt [11] applicable to any real abelian field. Although the latter is unnecessarily complicated in the cyclic case it has also been used there (e.g., in [6] and [7]) for the sake of uniformity. In addition, we give some supplementary remarks to [13].

Received August 8, 1984.
1980 *Mathematics Subject Classification*. Primary 12-04, 12A35, 12A45, 12A50.

Section 4 contains a description of the unit group as Galois module. This module structure is easily derived from known results about integral representations of the Galois group.

In the computations an important part is played by the relative norms of the unit ξ_A defined in [13]. In Section 5, we obtain rather precise information about these norms by a simple argument.

The next three sections are concerned with capitulation of ideal classes, i.e., nonprincipal ideal classes of subfields becoming principal in the sextic field. In the real cyclic quartic case the analogous question has been investigated by M.-N. Gras [6], [7]. For the quadratic and cubic subfield separately we prove practical criteria by means of which we have been able to verify that such a capitulation takes place for $f_6 < 4000$, provided that certain natural necessary conditions are satisfied. In the course of the investigation we need elements of K_6 satisfying Hilbert 90 for either subfield and for various units of K_6. In particular, for the quadratic subfield and for a generating relative unit ξ_R we define in a natural way such an element denoted by ω. An examination of the possibility $\omega = 0$ incidentally leads to a parametric family of fields K_6 containing exceptional units (in the sense of Nagell [14]) which do not belong to any of the proper subfields. The family can also be chosen so that four independent units have parametric representations but we have not been able to find such a representation for a missing (quadratic) unit.

In the new table the fields are listed in practically the same format as in [13]. The slight format changes are indicated at the outset of Section 9. The bulk of Section 9 consists of statistics. We first give a list of all fields K_6 such that the conductor f_6 is a prime < 4000 and the class number $h_6 > 1$. Next we divide all fields K_6 with relative class number $h_R > 1$ into 16 different types depending on the existence of units of different kinds, and we give the frequencies of fields belonging to each type. The fields belonging to scarce types are identified explicitly. The ensuing table contains statistics referring to the signature ranks for χ_6 decomposable or nondecomposable separately. In the next table we have gathered all cases in which the norm-positive cubic units are totally positive. A knowledge of these cases is of importance, e.g., in questions concerning the signature rank. Further, we consider the distribution of the values of Leopoldt's unit index Q_K. We conclude the paper by indicating a frequently occurring connection between the relative class numbers of distinct fields K_6 having the same conductor and the same quadratic or cubic subfield.

The bulk of the program is constructed for the UNIVAC 1108 system using FORTRAN V programming language. Some auxiliary computations have also been done on the DEC-20 computer. We express our appreciation for the cooperation we have received from the members of the staff of the Computer Centre at the University of Turku. We are particularly obliged to Mr. Jussi Salmela, M. Sc., for his generous help, and to Mrs. Marjo Henriksson for writing the data on a magnetic tape. The work has been supported financially by the Academy of Finland.

2. Notation. The present paper is a continuation of [13] and we use exactly the same terminology and notation throughout with one exception. The term "conductor f_6 is decomposable", adapted directly from [9, p. 60], is replaced by "the character

χ_6 is decomposable" used, e.g., in [11]. The reason for this is the following annoying fact. Let p be either 9 or a prime $\equiv 7 \bmod 12$. Then, in the old terminology the sextic conductor $f_6 = 8p$ is decomposable if $f_2 = 8$, but nondecomposable if $f_2 = 8p/(p,3)$. In both cases $f_3 = p$, and there are exactly 25 such values of $p < 500$. On the other hand, it is easily seen that these values of f_6 are the only ones for which such a dubious situation occurs.

First, we recall from [13] some of the most common notations. For $n \in \{1, 2, 3, 6\}$, K_n is a real cyclic extension of degree n over $\mathbf{Q}$ having conductor f_n, class number h_n, ring of integers $\mathcal{O}_n$, and unit group U_n. We write $f_2 = m$ or $4m$, where m is a square-free integer, and $f_3 = (a^2 + 3b^2)/4$, where a and b satisfy the normalization conditions [13, p. 6, (3)] introduced by Hasse [9]. $S_{n/q}$ and $N_{n/q}$ are the trace and norm from K_n to K_q. $G = \langle \sigma \rangle$ is the Galois group of K_6, and the conjugates of a number $\gamma \in K_6$ are $\gamma, \gamma' = \gamma^\sigma, \gamma'' = \gamma^{\sigma^2}$, etc. The fundamental unit of K_2 is denoted by μ, and τ is a norm-positive cubic unit such that $\langle -1, \tau, \tau' \rangle = U_3$. Finally, $U_R = \{\varepsilon \in U_6 \mid N_{6/3}(\varepsilon) = \pm 1, N_{6/2}(\varepsilon) = \pm 1\}$ is the group of relative units, and ξ_R is a generating relative unit, i.e., $\langle -1, \xi_R, \xi'_R \rangle = U_R$.

If $\mathfrak{a}$ is an integral ideal of any of the rings $\mathcal{O}_n$ then divisibility by $\mathfrak{a}$ and congruence modulo $\mathfrak{a}$ are defined in a natural way in the ring consisting of the numbers of the field K_n representable as a quotient of numbers of $\mathcal{O}_n$ with denominator prime to $\mathfrak{a}$. In particular, if $\mathfrak{p}$ is a prime ideal and γ is $\mathfrak{p}$-integral, then $\mathfrak{p}^k \parallel \gamma$ and $\nu_{\mathfrak{p}}(\gamma) = k$ both mean that $\gamma \equiv 0 \bmod \mathfrak{p}^k, \gamma \not\equiv 0 \bmod \mathfrak{p}^{k+1}$.

The cyclotomic field $\mathbf{Q}(\zeta_k) = \mathbf{Q}(\exp(2\pi i/k))$ is denoted by $C(k)$. In Section 4, R denotes the integral group ring $\mathbf{Z}[G]$. For any subgroup U of U_6 we write $|U| = \{|\varepsilon| \mid \varepsilon \in U\}$. The unit index from Leopoldt [11] is defined as $Q_K = [U_6 : U_2U_3U_R]$ and it is easy to see that

$$Q_K = \begin{cases} 12 & \text{if } N_{6/2}(U_6) = U_2 \text{ and } \langle -1 \rangle N_{6/3}(U_6) = U_3, \\ 3 & \text{if } N_{6/2}(U_6) = U_2 \text{ and } \langle -1 \rangle N_{6/3}(U_6) \neq U_3, \\ 4 & \text{if } N_{6/2}(U_6) \neq U_2 \text{ and } \langle -1 \rangle N_{6/3}(U_6) = U_3, \\ 1 & \text{if } N_{6/2}(U_6) \neq U_2 \text{ and } \langle -1 \rangle N_{6/3}(U_6) \neq U_3. \end{cases}$$

In Sections 6, 7, 8 we shall assume that $N_{6/2}(\xi_R) = 1$ which can be achieved by changing the sign of ξ_R if need be. This condition is not necessarily satisfied in the tables. We write $\xi_R = \alpha + \beta\sqrt{m}$, where $\alpha, \beta \in K_3$. We take $\omega = \tau^{-1} + \xi_R\tau''^{-1} + \xi'_R\tau'^{-1}$. For $n = 2$ or 3, $U_{Rn} = \{\varepsilon \in U_6 \mid N_{6/n}(\varepsilon) = 1\}$, $\mathrm{Cl}_n(\mathfrak{c})$ is the ideal class of K_n containing a given nonzero fractional ideal $\mathfrak{c}$, and $\mathscr{C}_{6/n} = \{\mathrm{Cl}_n(\mathfrak{c}) \mid \mathfrak{c}\mathcal{O}_6 = \gamma\mathcal{O}_6$ for some $\gamma \in K_6 \setminus \{0\}\}$ is the group of ideal classes of K_n becoming principal in K_6.

For any other undefined notations appearing in the text one should consult [13, pp. 196–198].

3. Connection with Leopoldt's Theory. For a unified theory of units and class numbers of real abelian fields, the concepts introduced by Leopoldt [11] are indispensable. In the cyclic case the situation is much less complicated, and it is enough to apply Satz 9 in Hasse [10, p. 40] as was also done in [13]. Anyway, it is useful to have an explicit list giving the translation of the basic concepts in [11] into our notation as follows:

Einheitengruppe von $\mathbf{K} = K_6$	$\mathbf{E_K}$	U_6
$\tilde{\chi}_n$-Relativeinheiten in $\mathbf{K}$	$\mathbf{E}^{\mathbf{K}}_{\tilde{\chi}_n} = \mathbf{E}^{+}_{\tilde{\chi}_n}$	U_R if $n = 6$ U_n if $n = 2$ or 3
Einheitenkern von $\mathbf{K}$	$\mathbf{E^K} = \mathbf{E^{K+}}$	$U_2U_3U_R$
Einheitenindex	$Q_{\mathbf{K}} = Q^{+}_{\mathbf{K}}$	Q_K defined in Section 2
Grenzindex	$Q_{\mathfrak{G}}$	12
Erzeugende $\tilde{\chi}_n$-Relativkreiseinheit	$\mathrm{H}_{\tilde{\chi}_n}$	$\eta^{(1+\sigma)(1-\sigma^3)}$ if $n = 6$ η_n if $n = 2$ or 3
Formaler Kreiseinheitenkern	$\mathbf{H^K}$	Y_6^*
Klassenzahlkomponenten	$h_{\tilde{\chi}_n}$	h_R^* if $n = 6$ h_n if $n = 2$ or 3

In this table, $\tilde{\chi}_n$ denotes the Frobenius division of the character group of K_6 containing χ_n; a generating character of the field K_n ($n = 2, 3, 6$), Y_6^* and h_R^* are new notations introduced here; and η_n is the cyclotomic unit of K_n ($\eta = \eta_6$) as defined in [10, p. 25].

From [10, p. 40] and [13, p. 58], we have the central result

$$(3.1) \qquad h_6 = h_2h_3h_R = [U_6 : Y_6]$$

where $Y_6 = \langle -1, \eta_2, \eta_3, \eta_3', \eta, \eta' \rangle$ is the group of cyclotomic units in the sense of Hasse. By definition [11, p. 39],

$$Y_6^* = \langle -1, \eta_2, \eta_3, \eta_3', \eta^{(1+\sigma)(1-\sigma^3)}, \eta^{(\sigma+\sigma^2)(1-\sigma^3)} \rangle.$$

In accordance with [11, p. 41, Satz 20], we have

$$(3.2) \quad [U_6 : U_2U_3Y_6] = h_R, \quad [U_2U_3Y_6 : U_2U_3Y_6^*] = 12, \quad [U_2U_3Y_6^* : Y_6^*] = h_2h_3,$$

where the second equality can be deduced by direct computation, and the other equalities follow from (3.1) and the theorem of Hasse cited above. From [11, p. 40, Eq. (7)], we now have

$$(3.3) \qquad h_R^* = [U_2U_3U_R : U_2U_3Y_6^*] = 12h_R/Q_K.$$

In [13, p. 17; cf. also p. 59] the second author introduced the group $U_6^* = U_2U_3U_RY_6$. The index $[U_6 : U_6^*] = 1, 3, 4$ or 12 depending on the existence of certain units ξ_B, ξ_C. In order to compute the value of h_R from (3.2) one needs the index of $U_2U_3Y_6$ in U_6^*. It is not hard to infer from the considerations in [13] that, in fact,

$$(3.4) \qquad [U_6^* : U_2U_3Y_6] = 2^{2n}(K^2 + KL + L^2),$$

where n, K, L are determined by $\xi_1^{2^n} = \pm\xi_0$, $\xi_1 = \pm\xi_R^K\xi_R'^L$.

4. The Unit Group as G-Module. Let $R = \mathbf{Z}[G]$. The indecomposable R-modules have been computed by A. Matuljauskas [12], and, more generally, the question of integral representations of a cyclic group of square-free order has been investigated by J. H. Oppenheim in his thesis [15].

Let us first consider the R-module $M = R/(1 + \sigma + \cdots + \sigma^5)R$. Write $M_0 = \{x \in M \mid (1 + \sigma)(1 + \sigma + \sigma^2)x = 0\}$ and $M_1 = M/M_0$. It is easy to see that

$$M_0 = (1 - \sigma + \sigma^2)M \cong R/(1 + \sigma)R \oplus R/(1 + \sigma + \sigma^2)R,$$
$$M_1 \cong R/(1 - \sigma + \sigma^2)R.$$

Note that compared with Oppenheim [15], we have interchanged his s_0 and s_1 which causes a change in the definition of M_0 and M_1, but the main results remain unaffected. The module M is an extension of M_1 by M_0. Let $\Lambda\colon R \times M_1 \to M_0$ be a cocycle corresponding to this extension as defined in [15, p. 11]. If $\lambda \in \mathrm{Hom}_{\mathbf{Z}}(M_1, M)$ satisfies the condition $p \circ \lambda = 1$, where $p\colon M \to M_1$ is the natural projection, one can take

$$\Lambda(r, x) = r\lambda(x) - \lambda(rx) \quad \text{for } r \in R,\, x \in M_1. \tag{4.1}$$

If Λ is defined by (4.1), but with $\lambda \in \mathrm{Hom}_{\mathbf{Z}}(M_1, M_0)$, it is termed a coboundary. Then $\mathrm{Ext}^1_R(M_1, M_0)$ is the factor group cocycles modulo coboundaries. From [15, Corollary 3.17 and Theorem 4.1] it follows that

$$\begin{aligned}\mathrm{Ext}^1_R(M_1, M_0) \cong{} & \mathrm{Hom}_R\big(M_1/(1+\sigma)M_1, (1+\sigma+\sigma^2)M_0/(1+\sigma^2+\sigma^4)M_0\big)\\ & \oplus \mathrm{Hom}_R\big(M_1/(1+\sigma+\sigma^2)M_1, (1+\sigma)M_0/(1+\sigma^3)M_0\big).\end{aligned}$$

Let (f_Λ, g_Λ) be the image of the class represented by the cocycle Λ under this isomorphism. We have

$$\begin{aligned}M_1/(1+\sigma)M_1 &\cong (1+\sigma+\sigma^2)M_0/(1+\sigma^2+\sigma^4)M_0 \cong GF(3),\\ M_1/(1+\sigma+\sigma^2)M_1 &\cong (1+\sigma)M_0/(1+\sigma^3)M_0 \cong GF(4),\end{aligned}$$

the action of G on the finite fields being defined in an obvious way. It follows from the results of Oppenheim that, for any $x \in M_1$,

$$\begin{cases} f_\Lambda\big(x + (1+\sigma)M_1\big) = (1-\sigma)(1+\sigma^2+\sigma^4)\lambda(x) + (1+\sigma^2+\sigma^4)M_0,\\ g_\Lambda\big(x + (1+\sigma+\sigma^2)M_1\big) = (1-\sigma)(1+\sigma^3)\lambda(x) + (1+\sigma^3)M_0.\end{cases} \tag{4.2}$$

We can define λ by

$$\lambda\big(u + v\sigma + (1-\sigma+\sigma^2)R\big) = u + v\sigma + (1+\sigma+\cdots+\sigma^5)\mathbf{Z} \quad \text{for } u, v \in \mathbf{Z}.$$

From (4.2) we see that f_Λ and g_Λ are both nonzero. By [15, pp. 24–25], M is indecomposable and, on the other hand, any indecomposable extension of M_1 by M_0 is isomorphic to M.

Consider now the R-module $|U_6| = \{|\varepsilon| \mid \varepsilon \in U_6\}$. It is not hard to see that

$$\begin{aligned}|U_2U_3| &= \langle \mu, |\tau|, |\tau'|\rangle = \left\{x \in |U_6| \,\middle|\, x^{(1+\sigma)(1+\sigma+\sigma^2)} = 1\right\} \cong M_0,\\ |U_6|/|U_2U_3| &\cong |U_R| \cong M_1.\end{aligned}$$

Therefore, $|U_6|$ is also an extension of M_1 by M_0.

THEOREM 1. *The structure of the R-module $|U_6|$, in particular its decomposition into indecomposable direct summands, can be described as follows*:

$$|U_6| \cong \begin{cases} R/(1+\sigma+\cdots+\sigma^5)R & \text{if } Q_K = 12,\\ R/(1+\sigma+\sigma^2)R \oplus R/(1+\sigma^3)R & \text{if } Q_K = 3,\\ R/(1+\sigma)R \oplus R/(1+\sigma^2+\sigma^4)R & \text{if } Q_K = 4,\\ R/(1+\sigma)R \oplus R/(1+\sigma+\sigma^2)R \oplus R/(1-\sigma+\sigma^2)R & \text{if } Q_K = 1.\end{cases}$$

Proof. As stated above, we consider $|U_6|$ as an extension of $|U_6|/|U_2U_3|$ by $|U_2U_3|$. Let Λ be a cocycle corresponding to this extension and choose

$$\lambda \in \mathrm{Hom}_{\mathbf{Z}}\big(|U_6|/|U_2U_3|, |U_6|\big)$$

to satisfy $p \circ \lambda = 1$ and (4.1), mutatis mutandis. From the equations (4.2) we get

$$\begin{aligned} f_\Lambda = 0 &\Leftrightarrow \lambda(x)^{1+\sigma^2+\sigma^4} \in |U_2U_3|^3 \quad \text{for each } x \in |U_6|/|U_2U_3| \\ &\Leftrightarrow N_{6/2}(U_6) \neq U_2, \\ g_\Lambda = 0 &\Leftrightarrow \lambda(x)^{1+\sigma^3} \in |U_2U_3|^2 \quad \text{for each } x \in |U_6|/|U_2U_3| \\ &\Leftrightarrow \langle -1 \rangle N_{6/3}(U_6) \neq U_3. \end{aligned}$$

In the case $Q_K = 12$, we thus find immediately that $|U_6| \cong M$. Consider now, e.g., the case $Q_K = 4$, i.e.,

$$f_\Lambda = 0, \qquad g_\Lambda \neq 0.$$

Then $|U_6|$ is isomorphic to a direct sum of $R/(1+\sigma)R$ and an indecomposable extension of $R/(1-\sigma+\sigma^2)R$ by $R/(1+\sigma+\sigma^2)R$. The latter is necessarily isomorphic to $R/(1+\sigma^2+\sigma^4)R$. In the other two cases one can argue similarly. □

A unit ε of the ring $\mathcal{O}_6$ is called a *Minkowski unit* iff $|U_6|$ is a cyclic R-module and $|\varepsilon|$ is an R-generator of $|U_6|$. We thus see that a Minkowski unit exists if and only if $Q_K = 12$.

5. Unit Norms. Put

$$\kappa = \begin{cases} 0 & \text{if } \chi_6 \text{ is decomposable,} \\ 1 & \text{if } \chi_6 \text{ is nondecomposable.} \end{cases}$$

This notation enables one to state the results below in a compact form covering both the decomposable case and the nondecomposable ones.

The relative norms of the unit ξ_A to the fields K_2 and K_3 are important characteristics, and the numbers u, v, w defined by

$$N_{6/3}(\xi_A) = \pm\tau^u\tau'^v, \qquad N_{6/2}(\xi_A) = \pm\mu^w \tag{5.1}$$

are listed in the tables. We shall now derive rather precise results about these numbers. In the subsequent discussion $n = 2, 3$ or 6.

Let ξ_n be "die Basiszahl der Kreiseinheit" in Leopoldt's terminology. From [11, p. 37, (3)], we have

$$\xi_n^2 = \pm N_{C(f_n)/K_n}(1 - \zeta_{f_n}). \tag{5.2}$$

If η_n denotes the cyclotomic unit of K_n, then

$$\eta_n^2 = \xi_n^{2(1-\sigma)}. \tag{5.3}$$

The formula has been written with an extra factor 2 in the exponent in order to ensure that the number upon which $1-\sigma$ operates belongs to K_n. We also denote briefly $\xi = \xi_6$, $\eta = \eta_6$. Note that $\xi_A = \xi$ if χ_6 is decomposable, and $\xi_A = \eta$ otherwise.

From [9, p. 67, (6*)], we have

$$\eta_2 = \pm\mu^{-h_2}, \tag{5.4}$$

and from [10, p. 40, Satz 9],

$$h_3 = [U_3 : Y_3] = [\langle -1, \tau, \tau' \rangle : \langle -1, \eta_3, \eta_3' \rangle]. \tag{5.5}$$

The value of w is completely determined by the following result.

THEOREM 2. *Denote* $f_6 = 3^\lambda p_1 \cdots p_\nu f_2$ *where* $\lambda \in \{0,1,2\}$, $\nu \geqslant 0$, *and the* p_i*'s are distinct primes* $\equiv 1 \bmod 6$.

(i) *If there exists an index* $i \in \{1,2,\ldots,\nu\}$ *such that* $(f_2/p_i) = 1$ *or if* $\lambda = 2$ *and* $f_2 \equiv 1 \bmod 3$, *then* $w = 0$.

(ii) *Otherwise*,

$$w = -2^{\nu+\kappa+\max\{1,\lambda\}-2}h_2.$$

Proof. For any prime p not dividing f_n, let $\sigma(n, p)$ denote the restriction to the field K_n of the automorphism of $C(f_n)$ induced by $\zeta_{f_n} \mapsto \zeta_{f_n}^p$. From [11, p. 38, (5)], we have

$$N_{6/n}(\xi^2) = \pm\xi_n^{2W_n}, \tag{5.6}$$

where

$$W_n = \prod_{p|f_6,\, p\nmid f_n} \left(1 - \sigma(n,p)^{-1}\right). \tag{5.7}$$

Here we take $n = 2$ in (5.6) and (5.7). Since $\sigma(2, p) = (f_2/p)$ the assertion (i) follows immediately. Suppose therefore that $(f_2/p_i) = -1$ for each i and consider first the case $\lambda \neq 2$. Then $p = 3$ does not appear in (5.7). If χ_6 is decomposable, we obtain from (5.1), (5.6), (5.3), (5.4),

$$\mu^{4w} = N_{6/2}(\xi^4) = \xi_2^{4W_2} = \xi_2^{2(1-\sigma)2^\nu} = \eta_2^{2^{\nu+1}} = \mu^{-2^{\nu+1}h_2}.$$

Hence $w = -2^{\nu-1}h_2$ as asserted. If χ_6 is nondecomposable, we obtain similarly

$$\mu^{2w} = N_{6/2}(\eta^2) = N_{6/2}\left(\xi^{2(1-\sigma)}\right) = \xi_2^{2(1-\sigma)W_2} = \eta_2^{2W_2} = \eta_2^{2^{\nu+1}} = \mu^{-2^{\nu+1}h_2},$$

whence $w = -2^\nu h_2$.

If $\lambda = 2$ and $f_2 \equiv 2 \bmod 3$ we have the same situation as above with the prime 3 added to the set $\{p_1,\ldots,p_\nu\}$. □

A corresponding result for the pair (u, v) is

THEOREM 3. *Denote* $f_6 = p_1^\lambda p_2 \cdots p_\nu f_3$, *where the* p_i*'s are distinct primes, and* $\lambda = 1$ *if* $\nu > 0$ *and* f_6 *is odd, while* $p_1 = 2$ *and* $\lambda \in \{2,3\}$ *if* f_6 *is even*.

(i) *If there exists an index* $i \in \{1,2,\ldots,\nu\}$ *such that* $\chi_3(p_i) = 1$, *then* $(u, v) = (0,0)$.

(ii) *Otherwise* $u^2 - uv + v^2 = 3^{\nu+\kappa-1}h_3$.

Proof. If $\gamma \neq \pm1$ is a unit in U_3, let $j(\gamma)$ denote the index $[U_3 : \langle -1, \gamma, \gamma' \rangle]$. Using this notation (5.5) takes the form $h_3 = j(\eta_3)$. A simple computation gives

$$j(\pm\gamma^{x+y\sigma}) = (x^2 - xy + y^2)j(\gamma) \quad \text{for } (x, y) \in \mathbf{Z}^2 \setminus \{(0,0)\}. \tag{5.8}$$

Take $n = 3$ in (5.6) and (5.7) and put $P = p_1^\lambda p_2 \cdots p_\nu = f_6/f_3$. Define $\delta(x)$ for any integer x prime to f_3 by

$$\delta(x) = \sigma^{2k} \quad \text{if } \chi_3(x) = \rho^k \quad (\rho = \exp(2\pi i/3),\ k \in \{0,1,2\}).$$

According to the agreement in [13, p. 9 and p. 12], the choice of σ and χ_3 was made so that for $(x, f_3) = 1$ the automorphism of $C(f_3)$ induced by $\zeta_{f_3} \mapsto \zeta_{f_3}^x$ and σ have the same restriction to the field K_3 if and only if $\chi_3(x) = \rho$. Therefore, the element W_3 in (5.7) is

$$W_3 = \prod_{p|P}(1 - \delta(p)).$$

If $\nu > 0$ and $\chi_3(p_i) = 1$ for some i then $W_3 = 0$ and the assertion (i) follows. Suppose the contrary. If χ_6 is decomposable, it follows from (5.1) and (5.6) that $\tau^{2u+2v\sigma} = \pm\xi_3^{2W_3}$, and thus (5.8), (5.3), (5.5) imply

$$4(u^2 - uv + v^2) = 3^{\nu-1}j\left(\xi_3^{2(1-\sigma)}\right) = 3^{\nu-1}j\left(\eta_3^2\right) = 4 \cdot 3^{\nu-1}h_3,$$

as asserted. Suppose, therefore, that χ_6 is nondecomposable. In this case $\tau^{2u+2v\sigma} = \xi_3^{2(1-\sigma)W_3}$ and we have the same computation with $3^{\nu-1}$ replaced by 3^ν. □

If K_6' and K_6'' have the same conductor f_6 and the same cubic subfield K_3, and if the corresponding characters χ_6', χ_6'' are both decomposable, it is obvious by (5.2), (5.3) (for $n = 6$) and by (5.1), that the pair (u, v) is the same for both fields K_6', K_6''. The same is trivially true if χ_6', χ_6'' are both nondecomposable, because in that case, $K_6' = K_6''$ as is easily seen.

6. Ideal classes of subfields becoming principal in K_6. Although the class number h_6 is divisible by the product h_2h_3, it is not always true that the ideal classes of the subfields are mapped injectively under the natural mapping induced by the inclusion. This phenomenon of capitulation has been studied by M.-N. Gras [6], [7] in the case of a real cyclic field of degree four. Here we shall carry out a similar investigation in the sextic case. We remind the reader of the notations introduced in Section 2. In particular, we shall assume that $N_{6/2}(\xi_R) = 1$. We note that $N_{6/3}(\varepsilon) = 1$ for each $\varepsilon \in U_R$ [13, p. 14, (22)]. In the following discussion $n = 2$ or 3, indicating that the subfield under consideration is K_n.

Suppose that $\mathrm{Cl}_n(\mathfrak{c}) \in \mathscr{C}_{6/n}$ and that $\mathfrak{c}\mathcal{O}_6 = \gamma\mathcal{O}_6$ for some $\gamma \in K_6 \setminus \{0\}$. It is obvious that the assignment $g_n(\mathrm{Cl}_n(\mathfrak{c})) = \gamma^{1-\sigma^n}U_6^{1-\sigma^n}$ gives a well-defined homomorphism $g_n\colon \mathscr{C}_{6/n} \to U_{Rn}/U_6^{1-\sigma^n}$. Further, it is easy to see that g_n is injective. Suppose, namely, that $\gamma^{1-\sigma^n} = \varepsilon^{1-\sigma^n}$, where $\varepsilon \in U_6$. We have $\gamma/\varepsilon = (\gamma/\varepsilon)^{\sigma^n}$ so that $\gamma/\varepsilon \in K_n$. Since $\mathfrak{c}\mathcal{O}_6 = (\gamma/\varepsilon)\mathcal{O}_6$ it follows that $\mathfrak{c} = (\gamma/\varepsilon)\mathcal{O}_n$ belongs to the principal class.

Suppose now that $\varepsilon U_6^{1-\sigma^n}$ is an arbitrary element of $U_{Rn}/U_6^{1-\sigma^n}$. By Theorem 90 of Hilbert there is a $\gamma \in \mathcal{O}_6 \setminus \{0\}$ such that $\varepsilon = \gamma^{1-\sigma^n}$. Since the automorphism σ^n leaves the ideal $\gamma\mathcal{O}_6$ fixed, we have

$$\gamma\mathcal{O}_6 = \mathfrak{c}\mathcal{O}_6 \times \mathfrak{p}_1^{\nu_1} \times \cdots \times \mathfrak{p}_h^{\nu_h},$$

where $\mathfrak{c}$ is an ideal of $\mathcal{O}_n$ and the $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_6$ which are ramified in K_6/K_n. We may assume that, for each i, $\mathfrak{p}_i \nmid \mathfrak{c}$ so that $\nu_i = \nu_{\mathfrak{p}_i}(\gamma)$.

LEMMA 1. *We have* $\varepsilon U_6^{1-\sigma^n} \in \mathrm{Im}(g_n)$ *if and only if* $n\nu_i \equiv 0 \bmod 6$ *for* $i = 1, 2, \ldots, h$.

Proof. Both conditions are clearly equivalent to the fact that $\gamma\mathcal{O}_6 = \mathfrak{c}_0\mathcal{O}_6$ for some ideal $\mathfrak{c}_0$ of $\mathcal{O}_n$. □

The number ω was defined as $\omega = \tau^{-1} + \xi_R\tau''^{-1} + \xi_R'\tau'^{-1}$. We have $\omega^{\sigma^2} = \xi_R^{-1}\omega$ so that ω satisfies Hilbert 90 in the extension K_6/K_2 for ξ_R provided that $\omega \neq 0$. Here we shall investigate the possibility $\omega = 0$ which incidentally leads to a parametric family of relative units in certain fields K_6. More generally, we shall prove the following result.

THEOREM 4. *Let $\delta \neq 1$ be a norm-positive unit in a cyclic cubic field K_3. Put $M = S_{3/1}(\delta^{-4} - 2\delta^2)$. Then, $M \geqslant 0$ with equality only when* $\mathrm{Irr}(\delta, \mathbf{Q}) = x^3 + 3x^2 - 1$. *Suppose that M is not a square in $\mathbf{Z}$ and write $M = c^2 m$, where $c \in \mathbf{Z}$ and m is a square-free positive integer.*

The number

$$\psi = (-\delta^{-2} + \delta'^{-2} - \delta''^{-2} + c\sqrt{m})/(2\delta') \tag{6.1}$$

is a unit in the field $K_3(\sqrt{m})$, such that

$$N_{6/2}(\psi) = N_{6/3}(\psi) = 1, \qquad \delta^{-1} + \psi\delta''^{-1} + \psi'\delta'^{-1} = 0. \tag{6.2}$$

Conversely, let K_6 be any real cyclic sextic field containing K_3 and let ψ be a unit in K_6 satisfying (6.2). *Then, $K_6 = K_3(\sqrt{m})$ and ψ is of the form* (6.1) *where both signs for c are permitted.*

Proof. We shall first prove the assertion concerning M. Let $\mathrm{Irr}(\delta, \mathbf{Q}) = x^3 - sx^2 + qx - 1$. Then, $M = q^4 - 4sq^2 + 8q$. Since the discriminant of $\mathrm{Irr}(\delta, \mathbf{Q})$ is a square $\geqslant 49$ in $\mathbf{Z}$, we have

$$s^2q^2 - 4q^3 - 4s^3 - 27 + 18sq = t^2 \tag{6.3}$$

for some integer $t \geqslant 7$. Consider first the possibility $q = 0$. Then, $-4s^3 - 27 = t^2$. Using a trick due to Fueter we can write this as a Fermat equation

$$(2s)^3 + (3 + t/3)^3 + (3 - t/3)^3 = 0.$$

The only solution is thus $t = 9$, $s = -3$, which is the exceptional case mentioned in the theorem. Suppose now that $q \neq 0$. We contend that $M > 0$. Write $N = M/(4q^2)$ so that

$$s = q^2/4 + 2/q - N.$$

Substituting this in (6.3), we obtain

$$4N^3 - (2q^2 + 24/q)N^2 + (q^4/4 - 10q + 48/q^2)N + 1 - 32/q^3 = t^2. \tag{6.4}$$

For $q \geqslant 4$ or $q = 1$ or $q \leqslant -3$ the expressions in parentheses in (6.4) are positive and therefore $t \geqslant 7$ implies $N > 0$. For the remaining values $q = -2, -1, 2, 3$ it is easy to verify by direct computation that $t \geqslant 7$ is possible only if $N > 0$. This proves the first assertion.

In what follows, we exclude the exceptional case and we assume further that M is not a square in $\mathbf{Z}$. We write $M = c^2 m$ as indicated and define ψ by (6.1). We have

$$\begin{aligned} 4\delta'^2\psi\psi''' &= S_{3/1}(\delta^{-4}) - 2\delta^2 + 2\delta'^2 - 2\delta''^2 - M \\ &= 2S_{3/1}(\delta^2) - 2\delta^2 + 2\delta'^2 - 2\delta''^2 = 4\delta'^2, \end{aligned}$$

whence $N_{6/3}(\psi) = \psi\psi''' = 1$. As $\psi + \psi''' \in \mathcal{O}_3$, ψ is an algebraic integer and, therefore, a unit in $K_6 = K_3(\sqrt{m})$. Put

$$h(x) = \mathrm{Irr}(\delta^{-2}, \mathbf{Q}) = x^3 - (q^2 - 2s)x^2 + (s^2 - 2q)x - 1.$$

We have

$$\begin{aligned} -N_{6/2}(\psi) = -N_{6/2}(\delta'\psi) &= N_{6/2}\big((q^2 - 2s - c\sqrt{m})/2 - \delta'^{-2}\big) \\ &= h\big((q^2 - 2s - c\sqrt{m})/2\big) = -1 \end{aligned}$$

and, finally,

$$\delta^{-1} + \psi\delta''^{-1} + \psi'\delta'^{-1} = \delta^{-1} + \tfrac{1}{2}\delta(-\delta^{-2} + \delta'^{-2} - \delta''^{-2} + c\sqrt{m}) + \tfrac{1}{2}\delta(-\delta'^{-2} + \delta''^{-2} - \delta^{-2} - c\sqrt{m}) = 0.$$

Hence (6.2) is satisfied.

Now, suppose, conversely, that ψ is a unit satisfying (6.2) in some real cyclic sextic field K_6 containing K_3. Combining the last condition (6.2) and the one obtained from it by applying the automorphism σ^3, we find

$$\delta'(\psi - \psi^{-1}) = -\delta''(\psi' - \psi'^{-1}). \tag{6.5}$$

Denote $c_* = \delta'(\psi - \psi^{-1})/\sqrt{m}$. It follows from (6.5) that σ leaves c_* fixed so that $c_* \in \mathbf{Q}$. Further,

$$\psi = (\gamma + c_*\sqrt{m})/(2\delta'),$$

where $\gamma \in K_3$, and the last condition (6.2) also gives

$$\delta^{-1} + \gamma\delta''^{-1} + \gamma'\delta'^{-1} = 0. \tag{6.6}$$

Applying the automorphism σ twice to (6.6), we get a system of three equations from which we can solve $\gamma, \gamma', \gamma''$. In that way we obtain $\gamma = (-\delta^{-2} + \delta'^{-2} - \delta''^{-2})/(2\delta')$ and the condition $N_{6/3}(\psi) = 1$ gives $c_*^2 m = M = c^2 m$, i.e., $c_* = \pm c$. □

Consider, in particular, the case $q = -s - 3$, i.e., $\operatorname{Irr}(\delta, \mathbf{Q}) = x^3 - sx^2 - (s+3)x - 1$. This polynomial is clearly irreducible in $\mathbf{Q}[x]$ for any integer s. The discriminant of the polynomial is $(s^2 + 3s + 9)^2$ so that $\mathbf{Q}(\delta)/\mathbf{Q}$ is cyclic. In this case, we have

$$M = q^4 - 4sq^2 + 8q = s^4 + 8s^3 + 30s^2 + 64s + 57.$$

E.g., for $s \equiv 1 \bmod 8$ it is easily seen that $M \equiv 32 \bmod 64$ so that, for these values of s, M is not a square in $\mathbf{Z}$. Further, it is not hard to see that $s^2 + 3s + 9$ is square-free for infinitely many $s \equiv 1 \bmod 8$, and, therefore, there are infinitely many different fields K_3. In the corresponding family of sextic fields we have an explicit system $\{\delta, \delta', \psi, \psi'\}$ of four independent units. Unfortunately, we have not been able to find an expression for a missing fifth unit in terms of the parameter s.

It is of interest to observe that if a unit ψ satisfying (6.2) exists in $K_3(\sqrt{m})$ then $\psi\delta\delta''^{-1}$ is an exceptional unit in the terminology of Nagell [14].

7. Classes of K_2 in K_6. In this section we shall assume that $\omega = \tau^{-1} + \xi_R\tau''^{-1} + \xi'_R\tau'^{-1} \neq 0$. Namely, by Theorem 4 it is obvious that if the original ω vanishes, we obtain a nonzero ω on replacing ξ_R by ξ'_R. We denote $\xi_R = \alpha + \beta\sqrt{m}$, where $\alpha, \beta \in K_3$. It follows easily from $N_{6/2}(\xi_R) = N_{6/3}(\xi_R) = 1$, that

$$\xi_R = \omega^{1-\sigma^2}, \tag{7.1}$$

$$\omega^{1+\sigma^3} = S_{3/1}(\tau^{-2} + 2\alpha\tau') \in \mathbf{Z}. \tag{7.2}$$

In the verification it is useful to note that, in particular, $\xi_R\xi''_R = \xi'_R$.

From [8, Ia, p. 92, Satz 12] we have

$$\left[U_{R2} : U_6^{1-\sigma^2}\right] = 3^{2-q}, \tag{7.3}$$

where

$$3^q = \left[N_{6/2}(U_6) : U_2^3\right] = \begin{cases} 3 & \text{if } N_{6/2}(U_6) = U_2, \\ 1 & \text{if } N_{6/2}(U_6) \neq U_2. \end{cases} \tag{7.4}$$

LEMMA 2. *A system of coset representatives of U_{R2} with respect to the subgroup $U_6^{1-\sigma^2}$ is*

$$\{\tau^i \mid i = 0, 1, 2\} \qquad \text{if } N_{6/2}(U_6) = U_2,$$
$$\{\tau^i \xi_R^j \mid i, j = 0, 1, 2\} \qquad \text{if } N_{6/2}(U_6) \neq U_2.$$

Proof. If $\tau \in U_6^{1-\sigma^2}$ there exists an $\varepsilon \in U_6$ such that $\tau = \varepsilon^{1-\sigma^2}$. Taking norms, we have $\tau^2 = \varepsilon^{(1+\sigma^3)(1-\sigma^2)}$, so that (5.8) implies

$$4 = j(\tau^2) = 3j(\varepsilon^{1+\sigma^3}),$$

which is impossible. In the case $N_{6/2}(U_6) = U_2$ the assertion therefore follows from (7.3) and (7.4).

Suppose now that $N_{6/2}(U_6) \neq U_2$ and that $\tau^i \xi_R = \varepsilon^{1-\sigma^2}$ for some $i \in \{0,1,2\}$ and some $\varepsilon \in U_6$. On multiplying ε by $\pm\mu^k$ for a suitable k, we may assume that $N_{6/2}(\varepsilon) = 1$. Taking norms, we have $\tau^{2i} = \varepsilon^{(1+\sigma^3)(1-\sigma^2)}$ which, for $i \neq 0$, leads to the same contradiction as above. Thus, $i = 0$, $\xi_R = \varepsilon^{1-\sigma^2}$ and $\varepsilon^{(1+\sigma^3)(1-\sigma^2)} = 1$. It follows that $\varepsilon^{1+\sigma^3} \in K_3 \cap K_2 = \mathbf{Q}$, i.e. $\varepsilon^{1+\sigma^3} = \pm 1$. Therefore, $\varepsilon \in U_R$. However, from $\xi_R = \varepsilon^{1-\sigma^2}$ it is easy to infer that

$$[\langle -1, \varepsilon, \varepsilon' \rangle : \langle -1, \xi_R, \xi_R' \rangle] = 3,$$

which is impossible. The assertion follows again from (7.3) and (7.4) □

THEOREM 5. *If $i \not\equiv 0 \bmod 3$ we have $\tau^i \xi_R^j U_6^{1-\sigma^2} \notin \mathrm{Im}(g_2)$ for each j. In particular, $\mathscr{C}_{6/2} = 1$ if $N_{6/2}(U_6) = U_2$.*

Proof. From Hilbert 90 we have $\tau^i \xi_R^j = \gamma^{1-\sigma^2}$ for some $\gamma \in \mathcal{O}_6 \setminus \{0\}$. If $\tau^i \xi_R^j U_6^{1-\sigma^2} \in \mathrm{Im}(g_2)$ there exists an ideal $\mathfrak{c}$ of $\mathcal{O}_2$ such that $\mathfrak{c}\mathcal{O}_6 = \gamma\mathcal{O}_6$. Applying the automorphism σ^3, we have $\gamma^{1+\sigma^3}\mathcal{O}_6 = \mathfrak{c}^{1+\sigma^3}\mathcal{O}_6 = c\mathcal{O}_6$, say, for some $c \in \mathbf{Z}$. Therefore, $\gamma^{1+\sigma^3} = c\varepsilon$, where $\varepsilon \in U_3$. We would have

$$\tau^{2i} = \left(\tau^i \xi_R^j\right)^{1+\sigma^3} = \varepsilon^{1-\sigma^2},$$

which leads to the same contradiction as in the proof of Lemma 2. The rest of the assertion is clear because g_2 is injective. □

From now on, in this section we shall assume that $N_{6/2}(U_6) \neq U_2$. From Lemma 2 and Theorem 5 we see that $\mathrm{Im}(g_2)$ is either 1 or $\langle \xi_R U_6^{1-\sigma^2} \rangle$, i.e., $\#\mathscr{C}_{6/2} = 1$ or 3. Our numerical results indicate that the latter alternative may always hold if $N_{6/2}(U_6) \neq U_2$ and $h_2 \equiv 0 \bmod 3$.

From Lemma 1 and (7.1) we have, immediately,

LEMMA 3. *If $N_{6/2}(U_6) \neq U_2$ and $h_2 \equiv 0 \bmod 3$, then $\#\mathscr{C}_{6/2} = 3$ if and only if $v_\mathfrak{p}(\omega) \equiv 0 \bmod 3$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_6$ which is ramified in the extension K_6/K_2.*

The following theorem gives a practical criterion by means of which we have been able to establish the truth of the above conjectural fact for every field K_6 up to $f_6 < 4000$.

THEOREM 6. *Let* $\xi_R = \alpha + \beta\sqrt{m}$, *where* $\alpha, \beta \in K_3$. *Suppose that* $N_{6/2}(\xi_R) = 1$ *and that* $\omega = \tau^{-1} + \xi_R\tau''^{-1} + \xi'_R\tau'^{-1} \neq 0$. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathcal{O}_6$ *which is ramified in the extension* K_6/K_2. *Write* $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, *where* p *is a prime, and* $\omega = \varphi + \psi\sqrt{m}$, *where* $\varphi, \psi \in K_3$.

(i) *If* p *is ramified or inert in* $K_2/\mathbf{Q}$, *then* $\nu_\mathfrak{p}(\omega) \equiv 0 \bmod 3$.

(ii) *If* p *splits in* $K_2/\mathbf{Q}$ *and* $p \neq 3$, *then the following conditions are equivalent*:

$$\mathfrak{p} \mid \omega \Leftrightarrow \alpha \equiv -\tfrac{1}{2} \bmod \mathfrak{p} \Leftrightarrow \nu_\mathfrak{p}(\omega) \not\equiv 0 \bmod 3.$$

(iii) *Suppose that* $p = 3$ *splits in* $K_2/\mathbf{Q}$. *Let* $3^k \parallel S_{3/1}(\tau^{-1})$ ($\neq 0$; *cf.* [13, *p.* 64]) *and* $l = \nu_\mathfrak{p}(\beta)$.

If $3k \neq 2l$, *then*

$$\nu_\mathfrak{p}(\omega) \not\equiv 0 \bmod 3 \Leftrightarrow l = 1.$$

If $3k = 2l$, *then*

$$\nu_\mathfrak{p}(\omega) \not\equiv 0 \bmod 3 \Leftrightarrow \nu_\mathfrak{p}(\varphi) = \nu_\mathfrak{p}(\psi) \textit{ with common value } \not\equiv 0 \bmod 3.$$

Proof. (i) We have $p\mathcal{O}_6 = \mathfrak{p}^3$ or $\mathfrak{p}^6$. Since $\omega^{1+\sigma^3} \in \mathbf{Z}$ by (7.2), $\nu_\mathfrak{p}(\omega^{1+\sigma^3}) \equiv 0 \bmod 3$. Since σ^3 leaves $\mathfrak{p}$ fixed, the result follows.

(ii) Put $A = \omega^{1+\sigma^3}$. We have

$$\varphi = \tau^{-1} + \alpha\tau''^{-1} + \alpha'\tau'^{-1}, \qquad \psi = \beta\tau''^{-1} - \beta'\tau'^{-1}, \tag{7.5}$$

and from (7.5) and (7.2),

$$\varphi^2 - m\psi^2 = A = S_{3/1}(\varphi\tau^{-1}). \tag{7.6}$$

Since $p \nmid 2f_2$, the number β is $\mathfrak{p}$-integral so that (7.5) implies

$$\varphi \equiv (1 + 2\alpha)\tau^{-1} \bmod \mathfrak{p}, \qquad \psi \equiv 0 \bmod \mathfrak{p}. \tag{7.7}$$

It is clear by (7.7) that $\mathfrak{p} \mid \omega$ iff $\alpha \equiv -\frac{1}{2} \bmod \mathfrak{p}$ and that these conditions follow from $\nu_\mathfrak{p}(\omega) \not\equiv 0 \bmod 3$. We therefore assume that $\mathfrak{p} \mid \omega$ and contend that $\nu_\mathfrak{p}(\omega) \not\equiv 0 \bmod 3$.

We note that the following result holds:

$$\text{If } \gamma \in K_3 \text{ is } \mathfrak{p}\text{-integral, then } \mathfrak{p} \mid \gamma \text{ iff } p \mid S_{3/1}(\gamma). \tag{7.8}$$

This follows immediately from $S_{3/1}(\gamma) \equiv 3\gamma \bmod \mathfrak{p}$ and $\mathfrak{p} \nmid 3$.

We shall show first that $\nu_\mathfrak{p}(\psi) \not\equiv 0 \bmod 3$. Suppose, namely, that $\nu_\mathfrak{p}(\psi) = 3n$. Then $\tau^{-1}\psi p^{-n}$ is $\mathfrak{p}$-integral and not divisible by $\mathfrak{p}$. On the other hand, by (7.5),

$$S_{3/1}(\tau^{-1}\psi p^{-n}) = p^{-n}\big(S_{3/1}(\tau'\beta) - S_{3/1}(\tau''\beta')\big) = 0,$$

which contradicts (7.8).

We shall show next that $\nu_\mathfrak{p}(\varphi) \not\equiv 0 \bmod 3$. Suppose, on the contrary, that $\nu_\mathfrak{p}(\varphi) = 3n$. From (7.6), we have $\nu_\mathfrak{p}(A) = \nu_\mathfrak{p}(\varphi^2) = 6n$ and $S_{3/1}(\varphi\tau^{-1}) \equiv 0 \bmod p^{2n}$. On the other hand, $\varphi\tau^{-1}p^{-n}$ is $\mathfrak{p}$-integral and prime to p so that (7.8) implies $p^{-n}S_{3/1}(\varphi\tau^{-1}) \not\equiv 0 \bmod p$, a contradiction.

From (7.6) we now have $\nu_\mathfrak{p}(\varphi) = \nu_\mathfrak{p}(\psi) = n$, say, where $3 \nmid n$. Since $\omega = \varphi + \psi\sqrt{m}$ and $\omega + \omega''' = 2\varphi$, it follows that $\mathfrak{p}^n \parallel (\omega, \omega''')$. Since $\nu_\mathfrak{p}(\omega) + \nu_\mathfrak{p}(\omega''') = \nu_\mathfrak{p}(A) \equiv 0 \bmod 3$, it is clear that $\nu_\mathfrak{p}(\omega) \not\equiv 0 \bmod 3$.

(iii) The conditions (7.7) are plainly also true in the case $p = 3$. From $A = S_{3/1}(\varphi\tau^{-1}) \equiv 0 \bmod 3$ we have $\mathfrak{p} \mid \varphi$ whence by (7.7), $\alpha \equiv 1 \bmod \mathfrak{p}$. From the equation $(\alpha + 1)(\alpha - 1) = m\beta^2$ we find that $\mathfrak{p} \mid \beta$, i.e., $l > 0$ and then $\nu_\mathfrak{p}(\alpha - 1) = 2l$.

Case 1. $3k < 2l$. Since $k > 0$ we have $l > 1$ and we thus contend that $\nu_{\mathfrak{p}}(\omega) \equiv 0 \bmod 3$. Writing

$$\varphi = S_{3/1}(\tau^{-1}) + (\alpha - 1)\tau''^{-1} + (\alpha' - 1)\tau'^{-1} \tag{7.9}$$

we find that $\nu_{\mathfrak{p}}(\varphi) = 3k$. It is clear by (7.6) that if $\nu_{\mathfrak{p}}(\psi) \not\equiv 0 \bmod 3$, then necessarily $\nu_{\mathfrak{p}}(\psi) > 3k$. Using the same argument as at the end of (ii), we obtain first $\nu_{\mathfrak{p}}((\omega, \omega''')) \equiv 0 \bmod 3$ and then $\nu_{\mathfrak{p}}(\omega) \equiv 0 \bmod 3$ as asserted.

Case 2. $3k > 2l$. We shall use the following easily proved fact:

(7.10) If $\gamma \in K_3$ is $\mathfrak{p}$-integral, then $\mathfrak{p}^n \mid \gamma$ implies $\mathfrak{p}^{n+2} \mid S_{3/1}(\gamma)$.

From (7.9) we have

$$\varphi\tau^{-1} = \tau^{-1}S_{3/1}(\tau^{-1}) + S_{3/1}(\tau'(\alpha - 1)) - \tau(\alpha'' - 1) \tag{7.11}$$

so that $\nu_{\mathfrak{p}}(\varphi) = 2l$ by (7.10).

Suppose first that $l = 1$. From (7.11) and (7.10),

$$A = S_{3/1}(\varphi\tau^{-1}) = S_{3/1}(\tau^{-1})^2 + 2S_{3/1}(\tau'(\alpha - 1)) \equiv 0 \bmod 9.$$

In this case, we have $\nu_{\mathfrak{p}}(\varphi) = \nu_{\mathfrak{p}}(\psi) = \nu_{\mathfrak{p}}((\omega, \omega''')) = 2$, whence $\nu_{\mathfrak{p}}(\omega) \not\equiv 0 \bmod 3$ as asserted.

Suppose next that $l \geqslant 2$. From $N_{6/2}(\alpha + \beta\sqrt{m}) = 1$ we have, by computing the coefficient of $\sqrt{m}$,

$$S_{3/1}(\beta) + S_{3/1}((\alpha\alpha' - 1)\beta'') + N_{3/1}(\beta)m = 0.$$

In this equation, $\nu_{\mathfrak{p}}(N_{3/1}(\beta)m) = 3l$ and $(\alpha\alpha' - 1)\beta'' \equiv 0 \bmod \mathfrak{p}^{3l}$ so that $\nu_{\mathfrak{p}}(S_{3/1}(\beta)) = 3l$ by (7.10).

Denote $\beta = c_0 + c_1\theta + c_2\theta'$, where the c_i's are 3-integral rational numbers. Since $S_{3/1}(\beta) = 3c_0$, we have $3^{l-1} \| c_0$. As 3 is ramified in $K_3/\mathbf{Q}$, $\mathrm{Irr}(\theta, \mathbf{Q}) = x^3 - (f_3/3)x - f_3a/27$ [13, p.9]. Clearly, $\theta \equiv -1 \bmod \mathfrak{p}$ and, further, $\nu_{\mathfrak{p}}(\theta - \theta') = 2$ because

$$N_{3/1}(\theta - \theta')^2 = 4(f_3/3)^3 - 27(f_3a/27)^2 = f_3^2(b/3)^2,$$

where $3^1 \| b$. Writing

$$\beta = c_0 + (c_1 + c_2)\theta - c_2(\theta - \theta') = c_0 + (c_1 + c_2)\theta' + c_1(\theta - \theta')$$

and taking into account that $\nu_{\mathfrak{p}}(c_0) = 3l - 3 > l = \nu_{\mathfrak{p}}(\beta)$, we find that there are two possibilities: either

$$l \equiv 0 \bmod 3, \quad \nu_{\mathfrak{p}}(c_1 + c_2) = l, \quad \nu_{\mathfrak{p}}(c_i) \geqslant l \qquad (i = 1, 2), \tag{7.12}$$

or

$$l \equiv 2 \bmod 3, \quad \nu_{\mathfrak{p}}(c_1) = \nu_{\mathfrak{p}}(c_2) = l - 2, \qquad c_1 + c_2 \equiv 0 \bmod \mathfrak{p}^{l+1}. \tag{7.13}$$

In the case (7.12) we have $\nu_{\mathfrak{p}}(A) \equiv \nu_{\mathfrak{p}}(\varphi) \equiv 0 \bmod 3$ in the equation $A = \varphi^2 - m\psi^2$ whence, either $\nu_{\mathfrak{p}}(\psi) > \nu_{\mathfrak{p}}(\varphi)$ or $\nu_{\mathfrak{p}}(\psi) \equiv 0 \bmod 3$, and the same argument as above gives $\nu_{\mathfrak{p}}(\omega) \equiv 0 \bmod 3$.

Suppose now that (7.13) holds. In the equation

$$\psi\tau^{-1} = \tau'\beta - \tau''\beta' = (\tau' - \tau'')\beta + \tau''(c_1 + c_2)(\theta - \theta') + 3c_2\tau''\theta'$$

we have $\nu_{\mathfrak{p}}(3c_2\tau''\theta') = l + 1$ while the other terms on the right-hand side are divisible by a higher power of $\mathfrak{p}$. Hence $\nu_{\mathfrak{p}}(\psi) = l + 1$ and the assertion $\nu_{\mathfrak{p}}(\omega) \equiv 0 \bmod 3$ follows by the standard argument.

Case 3. $3k = 2l$. If $\nu_{\mathfrak{p}}(\varphi) \neq \nu_{\mathfrak{p}}(\psi)$, then $\nu_{\mathfrak{p}}(A) = \min\{\nu_{\mathfrak{p}}(\varphi^2), \nu_{\mathfrak{p}}(\psi^2)\}$ and $\nu_{\mathfrak{p}}(\omega) \equiv 0 \bmod 3$ as before. Suppose that $\nu_{\mathfrak{p}}(\varphi) = \nu_{\mathfrak{p}}(\psi) = n$, say. In this case we have $\nu_{\mathfrak{p}}(\omega) \equiv 0 \bmod 3$ iff $n \equiv 0 \bmod 3$. □

For $N_{6/2}(U_6) \neq U_2$ and $h_2 \equiv 0 \bmod 3$ it follows immediately from Lemma 3 and Theorem 6(i), that $\#\mathscr{C}_{6/2} = 3$ if $f_3 \mid 3f_2$. Otherwise, one has to check that the prime factors of f_3 not dividing f_2 are inert in $K_2/\mathbf{Q}$ or that the conditions in (ii) and (iii) are not satisfied. This verification is most arduous in the very last case $p = 3$, $3k = 2l$, but this case seems to be scarce; we have encountered it only once.

8. Classes of K_3 in K_6. From [8, Ia, p. 92, Satz 12], we have

$$[U_{R3} : U_6^{1-\sigma^3}] = 2^{4-q}, \tag{8.1}$$

where

$$2^q = [N_{6/3}(U_6) : U_3^2] = \begin{cases} 8 & \text{if } N_{6/3}(U_6) = \langle -1, \tau, \tau' \rangle = U_3, \\ 4 & \text{if } N_{6/3}(U_6) = \langle \tau, \tau' \rangle, \\ 2 & \text{if } N_{6/3}(U_6) = \langle -1, \tau^2, \tau'^2 \rangle, \\ 1 & \text{if } N_{6/3}(U_6) = \langle \tau^2, \tau'^2 \rangle = U_3^2. \end{cases} \tag{8.2}$$

LEMMA 4. *A system of coset representatives of U_{R3} with respect to the subgroup $U_6^{1-\sigma^3}$ is*

$$\begin{array}{ll} \{(-1)^i \mid i = 0, 1\} & \text{if } q = 3, \\ \{(-1)^i \mu^j \mid i, j = 0, 1\} & \text{if } q = 2, \\ \{(-1)^i \xi_R^j \xi_R'^k \mid i, j, k = 0, 1\} & \text{if } q = 1, \\ \{(-1)^i \mu^j \xi_R^k \xi_R'^l \mid i, j, k, l = 0, 1\} & \text{if } q = 0. \end{array}$$

Proof. Suppose that there exists an $\varepsilon_2 \in U_2 \cap U_6^{1-\sigma^3}$. Write $\varepsilon_2 = \varepsilon^{1-\sigma^3}$, where $\varepsilon \in U_6$. We have

$$(\varepsilon^4 \varepsilon_2^{-2})^{1-\sigma^3} = \varepsilon_2^{2(1+\sigma^3)} = 1,$$

so that $\varepsilon^4 \varepsilon_2^{-2} \in U_3$. From [13, p. 15, Theorem 2] we get $\varepsilon^2 \varepsilon_2^{-1} = \varepsilon_3$, say, where $\varepsilon_3 \in U_3$. From [13, p. 21, Theorem 9] we know that $\mathscr{O}_6$ has a system of fundamental units containing $\{\mu, \tau, \tau'\}$. Since $\varepsilon_2 \varepsilon_3$ is a square in U_6, $\pm\varepsilon_2$ is a square in U_2 and $\pm\varepsilon_3$ is a square in U_3. If, in particular, $\varepsilon_2 = -1$, then $\varepsilon \in U_3$ which leads to the contradiction $-1 = \varepsilon_2 = \varepsilon^{1-\sigma^3} = 1$. Since $\mu \in U_{R3}$ if $q = 2$, the assertion is plainly true for $q = 3$ or 2 by (8.1) and (8.2).

Suppose, therefore, that $q = 1$ or 0 so that $N_{6/3}(U_6) = \langle -1 \rangle U_3^2$ or U_3^2. Let $\varepsilon_2 \in U_2$ and $\varepsilon_R \in U_R$ and suppose that $\varepsilon_2 \varepsilon_R \in U_2 U_R \cap U_6^{1-\sigma^3}$. Denote $\varepsilon_2 \varepsilon_R = \varepsilon^{1-\sigma^3}$ where $\varepsilon \in U_6$. As above, we have first

$$(\varepsilon^4 \varepsilon_2^{-2} \varepsilon_R^{-2})^{1-\sigma^3} = 1$$

and then $\varepsilon^2 \varepsilon_2^{-1} \varepsilon_R^{-1} = \varepsilon_3$, where $\varepsilon_3 \in U_3$. Hence $\varepsilon_3^2 = N_{6/3}(\varepsilon)^2$ so that

$$\varepsilon_3 = \pm N_{6/3}(\varepsilon) \in \langle -1 \rangle N_{6/3}(U_6) = \langle -1 \rangle U_3^2.$$

Therefore, $\pm\varepsilon_3$ is a square in U_3. Further, $N_{6/2}(\varepsilon)^2 \varepsilon_2^{-3} = \pm 1$ so that $\pm\varepsilon_2$ is a square in U_2. Finally, of course, $\pm\varepsilon_R$ is also a square in U_R. It is now easy to deduce the assertion from (8.1), (8.2) and the results in the first part of the proof. □

THEOREM 7. *If* $\varepsilon_2 \in U_2 \cap U_{R3} \setminus U_6^{1-\sigma^3}$ *and* $\varepsilon_R \in U_R \cap U_{R2}$, *then* $\varepsilon_2 \varepsilon_R U_6^{1-\sigma^3} \notin \mathrm{Im}(g_3)$. *In particular,* $\mathscr{C}_{6/3} = 1$ *if* $\langle -1 \rangle N_{6/3}(U_6) = U_3$.

Proof. The proof is similar in structure to that of Theorem 5. From Hilbert 90 we have $\varepsilon_2 \varepsilon_R = \gamma^{1-\sigma^3}$ for some $\gamma \in \mathcal{O}_6 \setminus \{0\}$. If $\varepsilon_2 \varepsilon_R U_6^{1-\sigma^3} \in \mathrm{Im}(g_3)$, there exists an ideal $\mathfrak{c}$ of $\mathcal{O}_3$ such that $\gamma \mathcal{O}_6 = \mathfrak{c}\mathcal{O}_6$. Taking norms, we have $N_{6/2}(\gamma)\mathcal{O}_6 = N_{3/1}(\mathfrak{c})\mathcal{O}_6 = c\mathcal{O}_6$, say, for some $c \in \mathbf{Z}$. Therefore, $N_{6/2}(\gamma) = c\varepsilon$, where $\varepsilon \in U_2$. Hence, $\varepsilon_2^3 = N_{6/2}(\varepsilon_2 \varepsilon_R) = \varepsilon^{1-\sigma^3}$. It follows from $\varepsilon_2 \in U_{R3}$ that $\varepsilon_2^2 \in U_6^{1-\sigma^3}$ and thus, also, $\varepsilon_2 \in U_6^{1-\sigma^3}$, contrary to the hypothesis. The rest of the assertion is clearly true. □

From now on, in this section, we shall assume that $\langle -1 \rangle N_{6/3}(U_6) \neq U_3$, i.e., $q = 1$ or 0. It is clear from Lemma 4 and Theorem 7, that $\mathrm{Im}(g_3)$ is either 1 or $\{\xi_R^k \xi_R'^l U_6^{1-\sigma^3} \mid k, l = 0, 1\}$, i.e., $\#\mathscr{C}_{6/3} = 1$ or 4. The latter alternative holds true for every such field K_6 with $h_3 \equiv 0 \bmod 4$ up to $f_6 < 4000$.

A number satisfying Hilbert 90 for ξ_R is $1 + \xi_R$, i.e.,

$$\xi_R = (1 + \xi_R)^{1-\sigma^3}. \tag{8.3}$$

Further,

$$(1 + \xi_R)^{1+\sigma^3} = 2(\alpha + 1). \tag{8.4}$$

From Lemma 1 and (8.3), we have

LEMMA 5. *If* $\langle -1 \rangle N_{6/3}(U_6) \neq U_3$ *and* $h_3 \equiv 0 \bmod 4$, *then* $\#\mathscr{C}_{6/3} = 4$ *if and only if* $v_{\mathfrak{p}}(1 + \xi_R) \equiv 0 \bmod 2$ *for every prime ideal* $\mathfrak{p}$ *of* $\mathcal{O}_6$ *which is ramified in the extension* K_6/K_3.

Our aim is to construct a criterion analogous to Theorem 6 which, however, will be of somewhat different type. For that purpose we need some auxiliary results.

LEMMA 6. *Suppose that* $N_{6/2}(\xi_R) = 1$ *and that* $4 \mid f_2$.

(i) *If* $\alpha \not\equiv 1 \bmod 2$, *then* $a \equiv b \equiv 0 \bmod 2$ *and* $8 \nmid f_2$.

(ii) *If* $a \equiv b \equiv 1 \bmod 2$, *then* $2 \mid 1 + \xi_R$ *and* $((1 + \xi_R)/2, 2) = 1$.

Proof. We shall use the following well-known fact:

(8.5) The prime 2 is inert in $K_3/\mathbf{Q}$ if and only if $a \equiv b \equiv 1 \bmod 2$.

We prove (i) first. If $2 \mid m\beta$ it follows from $(\alpha - 1)(\alpha + 1) = m\beta^2$ that $\alpha \equiv 1 \bmod 2$. We shall therefore assume that $m \equiv 3 \bmod 4$, $a \equiv b \equiv 1 \bmod 2$ (i.e., 2 is inert in $K_3/\mathbf{Q}$), $2 \nmid \beta$, and show that these assumptions lead to a contradiction.

Since $\{1, \theta, \theta'\}$ is an integral basis for $\mathcal{O}_3$ and b is odd, it follows from the expression of θ' [13, pp. 8–9], that $\{1, \theta, \theta^2\}$ is a local integral basis at the prime 2. Replacing θ by one of its conjugates if need be, we may assume that $\beta \equiv h + k\theta \bmod 2$, where $h, k \in \{0, 1\}$. Let $\alpha \equiv q + r\theta + s\theta^2 \bmod 2$, where $q, r, s \in \{0, 1\}$.

Suppose first that $s = 1$. We have $\theta^4 \equiv e + \theta + \theta^2 \bmod 2$, where $e = 1$ if $3 \nmid f_3$ and $e = 0$ if $3 \mid f_3$. From $\alpha^2 - m\beta^2 = 1$ we get

$$h + q + e + \theta + (k + r + 1)\theta^2 \equiv 1 \bmod 2,$$

a contradiction. Hence $s = 0$ and we have similarly

$$q^2 - mh^2 + 2(qr + hk)\theta + (r^2 - mk^2)\theta^2 \equiv 1 \bmod 4. \tag{8.6}$$

In particular, $r^2 - mk^2 \equiv 0 \bmod 4$ whence $r = k = 0$ because of the assumption $m \equiv 3 \bmod 4$. Since $2 \nmid \beta$, we have $h = 1$ so that $q = 0$ by (8.6). Then $2 \mid \alpha$, so that $N_{6/2}(\xi_R) = 1$ implies $mN_{3/1}(\beta)\sqrt{m} \equiv 1 \bmod 2$, a contradiction because $m \equiv 3 \bmod 4$. This completes the proof of (i).

To prove (ii) we still assume that $a \equiv b \equiv 1 \bmod 2$. From (i) we know that $\alpha \equiv 1 \bmod 2$. From (8.4) we have

$$\mathrm{Irr}(1 + \xi_R, K_3) = x^2 - 2(\alpha + 1)x + 2(\alpha + 1)$$

so that $2 \mid 1 + \xi_R$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_6$ dividing 2. Then by (8.5), $2\mathcal{O}_6 = \mathfrak{p}^2$. If $((1 + \xi_R)/2, 2) \neq 1$, then $4 \mid \alpha + 1$. From $m\beta^2 = (\alpha - 1)(\alpha + 1)$, we obtain $8 \mid m\beta^2$ so that either $m \equiv \beta \equiv 0 \bmod 2$ or $\beta \equiv 0 \bmod 4$. In both cases,

$$1 = N_{6/2}(\xi_R) \equiv \alpha\alpha'\alpha'' \equiv -1 \bmod \mathfrak{p}^3$$

which is impossible. □

LEMMA 7. *Suppose that* $N_{6/2}(\xi_R) = 1$. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathcal{O}_6$ *which is ramified in* K_6/K_3. *Write* $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. *If* p *is ramified or inert in* $K_3/\mathbf{Q}$, *then*

$$\nu_{\mathfrak{p}}(1 + \xi_R) = \begin{cases} 0 & \text{if } p \neq 2, \\ 2 & \text{if } p = 2. \end{cases}$$

Proof. If $p = 2$ then p is inert in $K_3/\mathbf{Q}$ and the result follows immediately from Lemma 6(ii). Suppose that $p \neq 2$. Then $\beta\sqrt{m}$ is a $\mathfrak{p}$-integer divisible by $\mathfrak{p}$ because $\nu_{\mathfrak{p}}(\beta)$ is even and $\nu_{\mathfrak{p}}(\sqrt{m})$ is odd. Suppose that, contrary to the assertion, $\alpha \equiv -1 \bmod \mathfrak{p}$. It would follow that $1 = N_{6/2}(\xi_R) \equiv \alpha\alpha'\alpha'' \equiv -1 \bmod \mathfrak{p}$, a contradiction. □

We are now ready to state the main criterion.

THEOREM 8. *Let* $\xi_R = \alpha + \beta\sqrt{m}$, *where* $\alpha, \beta \in K_3$. *Suppose that* $N_{6/2}(\xi_R) = 1$. *Denote*

$$P = 2^{\lambda}\prod p$$

where the product is to be taken over all odd primes p *dividing* f_2 *which split in* K_3, *and*

$$\lambda = \begin{cases} 2 & \text{if } a \equiv b \equiv 0 \bmod 2 \text{ and } m \equiv 2 \bmod 4, \\ 1 & \text{if } a \equiv b \equiv 0 \bmod 2 \text{ and } m \equiv 3 \bmod 4, \\ 0 & \text{otherwise}. \end{cases}$$

Then the following conditions are equivalent:

(i) *We have* $\nu_{\mathfrak{p}}(1 + \xi_R) \equiv 0 \bmod 2$ *for every prime ideal* $\mathfrak{p}$ *of* $\mathcal{O}_6$ *which is ramified in* K_6/K_3.

(ii) *The number* α *is congruent to a rational integer* mod P.

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_6$ which is ramified in K_6/K_3. Write $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. If p is ramified or inert in $K_3/\mathbf{Q}$, then $\nu_{\mathfrak{p}}(1 + \xi_R) \equiv 0 \bmod 2$ by Lemma 7, and, on the other hand, no condition upon $\alpha \bmod p$ is imposed in (ii). It is therefore enough to assume that p splits in K_3.

We consider first the case $p \neq 2$. As in the proof of Lemma 7 we have $\beta\sqrt{m} \equiv \beta'\sqrt{m} \equiv \beta''\sqrt{m} \equiv 0 \bmod \mathfrak{p}$. If $\alpha \equiv c \bmod p$, where $c \in \mathbf{Z}$, it follows from $\alpha^2 - m\beta^2 = 1$ that $c^2 \equiv 1 \bmod p$, and from $1 = N_{6/2}(\xi_R) \equiv \alpha\alpha'\alpha'' \bmod \mathfrak{p}$ that $c^3 \equiv 1 \bmod p$. Thus $c \equiv 1 \bmod p$ and $2(\alpha + 1) \equiv 4 \bmod p$. Hence, none of the conjugates of $\mathfrak{p}$ divides $1 + \xi_R$ by (8.4). Suppose, on the contrary, that α is not congruent to a rational integer mod p. It follows from $(\alpha - 1)(\alpha + 1) = m\beta^2 \equiv 0 \bmod p$ that for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_6$ dividing p we must have $\mathfrak{p} \mid \alpha + 1$, because otherwise $\alpha \equiv 1 \bmod p$ contrary to the hypothesis. Furthermore, by (8.4),

$$2\nu_{\mathfrak{p}}(1 + \xi_R) = \nu_{\mathfrak{p}}(\alpha + 1) = \nu_{\mathfrak{p}}(m) + 2\nu_{\mathfrak{p}}(\beta),$$

implying that $\nu_{\mathfrak{p}}(1 + \xi_R)$ is odd. We have thus proved the equivalence (i) and (ii) locally at the prime p.

Consider next the case $p = 2$. We have $a \equiv b \equiv 0 \bmod 2$ by (8.5) and $m \equiv 2$ or $3 \bmod 4$ because 2 is ramified in $K_2/\mathbf{Q}$. First let $m \equiv 2 \bmod 4$. From Lemma 6(i) we have $\alpha \equiv 1 \bmod 2$. We write

$$((\alpha - 1)/2)((\alpha + 1)/2) = m(\beta/2)^2 \tag{8.7}$$

because, obviously, $2 \mid \beta$. If $\alpha \equiv c \bmod 4$ for some $c \in \mathbf{Z}$, one can conclude in the same way as in the first part of the proof that $c \equiv 1 \bmod 4$. Then, $((\alpha + 1)/2, 2) = 1$ so that from (8.4),

$$2\nu_{\mathfrak{p}}(1 + \xi_R) = \nu_{\mathfrak{p}}(4) = 4.$$

On the other hand, if α is not congruent to a rational integer mod 4, it follows from (8.7) that for some prime ideal factor $\mathfrak{p}$ of 2 in $\mathcal{O}_6$ we must have $(\alpha + 1)/2 \equiv 0 \bmod \mathfrak{p}$, $(\alpha - 1)/2 \not\equiv 0 \bmod \mathfrak{p}$. For this $\mathfrak{p}$ we have, by (8.4) and (8.7),

$$2\nu_{\mathfrak{p}}(1 + \xi_R) = \nu_{\mathfrak{p}}(4) + \nu_{\mathfrak{p}}((\alpha + 1)/2) = 4 + \nu_{\mathfrak{p}}(m) + 2\nu_{\mathfrak{p}}(\beta/2),$$

whence

$$\nu_{\mathfrak{p}}(1 + \xi_R) = 3 + \nu_{\mathfrak{p}}(\beta/2) \equiv 1 \bmod 2.$$

This proves the equivalence of (i) and (ii) at the prime 2 in the case $m \equiv 2 \bmod 4$.

Suppose, finally, that $m \equiv 3 \bmod 4$. If $\alpha \equiv c \bmod 2$ for some $c \in \mathbf{Z}$, the same argument as at the end of the proof of Lemma 6(i) shows that c cannot be even. Hence, $\alpha \equiv 1 \bmod 2$ and the numbers appearing in (8.7) are algebraic integers. For any $\mathfrak{p}$ dividing 2 we have $\nu_{\mathfrak{p}}((\alpha + 1)/2) = 0$ or $2\nu_{\mathfrak{p}}(\beta/2)$, both of which are $\equiv 0 \bmod 4$. From (8.4), $\nu_{\mathfrak{p}}(1 + \xi_R) \equiv 0 \bmod 2$.

If α is not congruent to a rational integer mod 2, then for some $\mathfrak{p}$ dividing 2, we have $\mathfrak{p} \nmid \alpha + 1$. For this $\mathfrak{p}$, $\nu_{\mathfrak{p}}(1 + \xi_R) = 1$ by (8.4). This concludes the proof of Theorem 8. □

If $\langle -1 \rangle N_{6/3}(U_6) \neq U_3$ and $h_3 \equiv 0 \bmod 4$, it follows from Lemma 5 and Theorem 8 that $\#\mathscr{C}_{6/3} = 4$ in the case $f_2 \mid f_3$. Otherwise, Theorem 8 provides a very convenient tool for establishing the truth of that conjectural fact.

9. Tables and Statistics. The table containing the 12 cases missing from [13] and the 1743 fields with $2021 < f_6 < 4000$ has been deposited in the Mathematics of Computation's UMT-depository. The data in the table are listed in the same format as in [13] with the following slight changes. Firstly, no distinction is made between the cases $r1$ and $r2$ when $h_R = 7$. Secondly, let ξ_* be any of the units whose coordinates multiplied by k [13, p. 68] are listed in the table. Here $*$ stands for any of the letters A, R, B, C. Denote $k\xi_* = c_0 + c_1\theta + c_2\theta' + (d_0 + d_1\theta + d_2\theta')\sqrt{m}$, where $c_i, d_i \in \mathbf{Z}$. These numbers are arranged in the form of the matrix

$$\begin{pmatrix} c_0 & c_1 & c_2 \\ d_0 & d_1 & d_2 \end{pmatrix}$$

as in [13] if there is enough space for that. If not, they are written one underneath the other in the natural order $c_0, c_1, c_2, d_0, d_1, d_2$.

In each of the 12 cases missing from [13] the relative class number $h_R = 1$. The corresponding values of f_6 are 997, 1021, 1093, 1561, 1597, 1657, 1753, 1777, 1801, 1933, 1981, 2017. Of these, $1561 = 7 \times 223$, $1981 = 7 \times 283$, and the other 10 numbers are primes.

TABLE 1

f_6	h_R	h_2	h_3	f_6	h_R	h_2	h_3	f_6	h_R	h_2	h_3
229	1	3	1	277	1	1	4	313	1	1	7
349	4	1	4	397	1	1	4	577	1	7	1
709	4	1	4	733	1	3	1	853	1	1	4
877	7	1	7	937	4	1	4	1009	1	7	4
1069	7	1	1	1093	1	5	1	1129	1	9	7
1297	1	11	1	1381	7	1	1	1429	1	5	1
1489	1	3	19	1777	1	1	16	1789	1	1	4
2029	1	7	1	2089	3	3	1	2437	1	1	7
2557	7	3	7	2677	1	3	1	2689	1	1	4
2713	1	3	1	2797	1	1	4	2857	1	3	1
2917	7	3	1	3037	1	1	4	3121	1	5	1
3181	1	5	1	3217	1	1	7	3229	3	3	1
3253	1	5	1	3313	7	1	19	3469	13	1	1
3517	1	1	4	3529	1	1	19	3877	1	3	1
3889	1	3	1								

TABLE 2

Type		h_R	No
1	$\xi_R^2 = \pm\xi_0$	4	42
2	$\xi_R^3 = \xi_0$	9	1
3	$\xi_R^5 = \xi_0$	25	1
4	$\xi_R^3 = \xi_0\xi_0'$	3	40
5	$\xi_R^7 = \xi_0^2\xi_0'$ or $\xi_0\xi_0'^2$	7	72
6	$\xi_R^{13} = \xi_0^3\xi_0'$ or $\xi_0\xi_0'^3$	13	17
7	$\xi_R^{19} = \xi_0^3\xi_0'^2$	19	2
8	$\xi_R^{61} = \xi_0^5\xi_0'^4$	61	1
9	$\xi_R = \xi_0$, ξ_B exists	3	94
10	$\xi_R = \xi_0$, ξ_C exists	4	130
11	$\xi_R^2 = \xi_0$, ξ_B exists	12	1
12	$\xi_R^3 = \xi_0\xi_0'$, ξ_B exists	9	6
13	$\xi_R^7 = \xi_0^2\xi_0'$, ξ_B exists	21	1
14	$\xi_R^2 = \pm\xi_0$, ξ_C exists	16	6
15	$\xi_R^3 = \xi_0\xi_0'$, ξ_C exists	12	2
16	$\xi_R = \xi_0$, ξ_B and ξ_C exist	12	3

There are 131 prime sextic conductors f_6 less that 4000. They are of particular interest for a number of reasons, especially because of the following well-known fact: If f_6 is prime and L is any subfield of $C(f_6)$ containing K_6, then the class number of L is divisible by h_6. For an interesting historical remark concerning a closely related result see [1, p. 219, Footnote 3]. There are exactly 43 prime sextic conductors f_6 less than 4000 such that the class number $h_6 = h_R h_2 h_3 > 1$. These conductors and the class numbers h_R, h_2, h_3 are listed in Table 1.

We note that all statistics we give in this paper concern the total range $1 < f_6 < 4000$ and thus include the statistics in [13]. There are altogether 419 fields K_6 with $f_6 < 4000$ such that $h_R > 1$. These fields can be divided into 16 different types depending on the expression of ξ_R in terms of ξ_0 and ξ_0' and on the existence of ξ_B or ξ_C. A similar division was exercised in [13] but only 8 types emerged there. In Table 2 we give for each type the relative class number h_R and the number of fields

TABLE 3

f_6	f_2	f_3	a	b	Type	f_6	f_2	f_3	a	b	Type
995	5	199	11	15	16	1143	381	1143	−3	39	14
1548	172	387	−39	3	2	2077	2077	2077	−91	3	14
2135	305	427	−40	6	16	2289	21	763	53	9	15
2428	2428	607	−49	3	14	2439	813	2439	−3	57	3
2669	17	157	14	12	13	2812	76	703	−25	27	14
2844	316	711	−12	30	16	2869	2869	2869	107	3	7
2921	2921	127	20	6	8	2945	5	589	41	15	15
3003	429	91	11	9	11	3052	3052	763	−55	3	14
3155	5	631	−43	15	14	3339	53	63	15	3	12
3339	1113	63	−12	6	7	3432	264	13	5	3	12
3572	188	19	−7	3	12	3708	412	9	−3	3	12
3981	3981	1327	−4	42	12	3983	569	7	−1	3	12

TABLE 4

	χ_6 decomposable					χ_6 nondecomposable				
	3	4	5	6	Σ	3	4	5	6	Σ
$1 < f_6 \leqslant 1000$	60	45	155	146	406	20	3	106	33	162
$1000 < f_6 \leqslant 2000$	131	57	252	168	608	26	3	89	31	149
$2000 < f_6 \leqslant 3000$	155	61	303	208	727	28	2	77	27	134
$3000 < f_6 \leqslant 4000$	156	79	301	215	751	21	2	90	30	143
Σ	502	242	1011	737	2492	95	10	362	121	588

belonging to that type. In Table 3 we list the parameters f_6, f_2, f_3, a, b of the fields belonging to the less frequent and perhaps more interesting types 2, 3, 7, 8, 11-16.

Statistics referring to the signature rank Sr of the unit group U_6 are given in Table 4 in the decomposable and nondecomposable cases separately. The numbers at the top of the columns are the values of Sr.

There are 14 fields K_6 with $f_6 < 4000$ such that the norm-positive cubic units in U_3 are totally positive. As noted in [13, p. 70] it is of importance to be able to recognize these cases. These fields and the class numbers h_R, h_2, h_3 are listed below.

f_6	f_2	f_3	a	b	h_R	h_2	h_3
703	37	703	−25	27	1	1	12
711	237	711	−12	30	1	1	12
1009	1009	1009	−43	27	1	7	4
2109	57	703	−25	27	1	1	12
2109	2109	703	−25	27	1	2	12
2812	76	703	−25	27	16	1	12
2812	2812	703	−25	27	1	2	12
2844	12	711	−12	30	4	1	12
2844	316	711	−12	30	12	3	12
3193	3193	3193	−55	57	4	1	12
3515	5	703	−25	27	1	1	12
3515	185	703	−25	27	1	2	12
3555	5	711	−12	30	1	1	12
3555	1185	711	−12	30	1	2	12

The unit index Q_K is not listed in the tables but it is easily determined by means of the following two rules:

$$N_{6/2}(U_6) \neq U_2 \Leftrightarrow 3 \mid w \quad \text{and} \quad \xi_B \text{ does not exist,}$$

$$\langle -1 \rangle N_{6/3}(U_6) \neq U_3 \Leftrightarrow 2 \mid u, 2 \mid v \quad \text{and} \quad \xi_C \text{ does not exist.}$$

The distribution of the values of Q_K is as follows:

	12	3	4	1	Σ
$1 < f_6 \leqslant 1000$	347	100	93	28	568
$1000 < f_6 \leqslant 2000$	394	152	146	65	757
$2000 < f_6 \leqslant 3000$	443	179	175	64	861
$3000 < f_6 \leqslant 4000$	462	185	175	72	894
Σ	1646	616	589	229	3080

In conclusion, we would like to draw attention to a rather frequently occurring connection between the relative class numbers h_R of distinct fields K_6 having the same conductor f_6 and the same subfield K_2 or K_3. Consider values of f such that for $n = 2$ or 3 there is a quadratic (resp. cubic) field K_n contained in more than one sextic field K_6 having conductor $f_6 = f$ at least one of these fields K_6 having relative class number h_R divisible by $6/n$. Let $P(f, n)$ denote the following property:

For any given quadratic (resp. cubic) field K_n the relative class numbers h_R of the sextic fields K_6 having conductor $f_6 = f$ and containing K_n are either all prime to $6/n$ or all divisible by $6/n$.

The values of f satisfying the preliminary requirement above are the following ones:

$n = 2$, $P(f, 2)$ is true

793, 981, 1027, 1548, 1629, 1736, 2135, 2163, 2184, 2289, 2331, 2405, 2412, 2639, 2701, 2844, 2945, 2983, 3003, 3007, 3033, 3339, 3416, 3492, 3573, 3601, 3708, 3892, 3999

$n = 2$, $P(f, 2)$ is false

469, 1603, 1708, 1957, 2977, 3303

$n = 3$, $P(f, 3)$ is true

651, 732, 741, 1073, 1221, 1281, 1449, 1464, 1533, 1628, 1729, 1833, 1935, 2013, 2044, 2135, 2289, 2444, 2604, 2660, 2821, 2844, 2849, 2945, 2964, 3003, 3059, 3069, 3081, 3108, 3233, 3255, 3256, 3445, 3464, 3465, 3477, 3601, 3627, 3660, 3705, 3717, 3784

$n = 3$, $P(f, 3)$ is false

248, 744, 936, 1064, 1240, 1368, 1736, 2072, 2456, 2709, 2728, 2812, 3052, 3192, 3224, 3512, 3720, 3752, 3913, 3992, 3999

Department of Mathematics
University of Turku
SF-20500 Turku 50, Finland

1. N. C. ANKENY, S. CHOWLA & H. HASSE, "On the class-number of the maximal real subfield of a cyclotomic field," *J. Reine Angew. Math.*, v. 217, 1965, pp. 217–220. MR **30** #3078.

2. VEIKKO ENNOLA & REINO TURUNEN, "On totally real cubic fields," *Math. Comp.*, v. 44, 1985, pp. 495–518.

3. VEIKKO ENNOLA & REINO TURUNEN, "On cyclic cubic fields," *Math. Comp.*, v. 45, 1985, pp. 585–589.

4. H. J. GODWIN, "The calculation of large units in cyclic cubic fields," *J. Reine Angew. Math.*, v. 338, 1983, pp. 216–220. MR **84e**:12003.

5. MARIE-NICOLE GRAS, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de **Q**," *J. Reine Angew. Math.*, v. 277, 1975, pp. 89–116. MR **52** #10675.

6. MARIE-NICOLE GRAS, "Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de **Q**," *Publ. Math. Univ. Besançon*, 1977/78, fasc. 2.

7. MARIE-NICOLE GRAS, "Classes et unités des extensions cycliques réelles de degré 4 de **Q**," *Ann. Inst. Fourier (Grenoble)*, v. 29, no. 1, 1979, pp. 107–124. MR **81f**: 12003.

8. HELMUT HASSE, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil* I: *Klassenkörpertheorie. Teil* Ia: *Beweise zu Teil* I. *Teil* II: *Reziprozitätsgesetz*, Dritte Auflage, Physica-Verlag, Würzburg-Vienna, 1970. MR **42** #1795.

9. HELMUT HASSE, "Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern," *Abh. Deutsch. Akad. Wiss. Berlin, Math.-Nat. Kl.*, **1948**, No 2, 1950. MR **11**, 503.

10. HELMUT HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952. MR **14**, 141.

11. H. W. LEOPOLDT, "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper," *Abh. Deutsch. Akad. Wiss. Berlin, Math.-Nat. Kl.*, **1953**, No 2, 1954. MR **16**, 799.

12. A. MATULJAUSKAS, "Integral representations of the cyclic group of order six," *Litovsk. Mat. Sb.*, v. 2, no. 2, 1962, pp. 149–157. (Russian) MR **27** #5835.

13. SIRPA MÄKI, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math., vol. 797, Springer-Verlag, Berlin and New York, 1980. MR **82a**: 12004.

14. TRYGVE NAGELL, "Sur un type particulier d'unités algébriques," *Ark. Mat.*, v. 8, 1969, pp. 163–184. MR **42** #3064.

15. J. H. OPPENHEIM, *Integral Representations of Cyclic Groups of Square-Free Order*, Ph.D. Thesis, Univ. of Illinois, Urbana, Ill., 1962.