Can. J. Math.Vol. **43** (5), 1991 pp. 1086–1097

THE NORMAL CLOSURE OF A QUADRATIC EXTENSION OF A CYCLIC QUARTIC FIELD

THERESA P. VAUGHAN

Pierre Barrucand asks the following question (Unsolved Problems, # ASI 88:04, Banff, May 1988, Richard K. Guy, Ed.; also [2, p. 594]). Let K be a cyclic quartic field, and let ξ be a non-square element of K. Let M be the Galois closure of $K\left(\sqrt{\xi}\right)$, and let G be the Galois group Gal(M/Q). Find (1) all possible G, (2) conditions on ξ to have such a G, and (3) a list of all possible subfields of M.

It is clear that the possible degrees for M over Q are 8, 16, 32, and 64. We shall see that only one G is possible for each $D > 8$, but if $D = 8$, there are two possibilities for G (Z_8 and $Z_2 \times Z_4$). For each group G of order D greater than 8, we give the following information:

(1) For $D \leq 32$, its *type,* according to the usage in the book *Group Tables,* by Thomas and Wood [4] (we call this the TW-type.);

(2) Its *type* according to the usage in the book *Groups of Order* 2^n ($n \leq 6$) by Hall and Senior [1] (called the HS-type);

(3) The fixed field $FF(C)$ of the center C of G, and Gal$\left(M/FF(C)\right)$;

(4) The fixed field $FF(G')$ of the commutator subgroup G' of G, and Gal$\left(M/FF(G')\right)$.

In addition, if $|G| = 64$, we also give a table of

(5) The number of elements of each order

(6) The number of subgroups of each order

(7) The number of normal subgroups of each order.

Finally, for $D = 16, 32$, we list all the subfields of M, and for $D = 64$, one representative of each of the classes of conjugate subfields (over Q, of course); indicating how many fields are in each conjugate class. Section 1 consists of definitions, notation, and preliminary results. Section 2 consists of tables summarizing the results about Gal(M/Q), except for the actual listing of subfields, which is in Section 4. The statements of the theorems are also in Section 2. The proofs of the theorems are in Section 3.

I would like to thank the referees for the references [1] and [2], and for their helpful suggestions.

Received by the editors February 7, 1990, revised: June 21, 1990 .
AMS subject classification: 12F05.
Key words and phrases: quadratic extension, cyclic quartic field.

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

1. In this paper, the degree of a field F means its degree over Q. If $x \in F$, then $N(x)$ denotes the absolute norm of x (the product of all the conjugates of x in F, over Q). If x is in a quadratic field, then its conjugate is denoted by x^*. The cyclic quartic field K is given by $Q\big(\sqrt{m}, \sqrt{\alpha}\big)$ (the meaning of m, α is fixed throughout.) We begin with some very elementary lemmas.

LEMMA 1.1. *$K = Q\big(\sqrt{m}, \sqrt{\alpha}\big)$, where m is a squarefree positive rational integer, and $\alpha \in Q(\sqrt{m}) - Q$ satisfies $N(\alpha) = ms^2$ where $s \in Q$.* ■

It is well-known that m must be a sum of two squares.

LEMMA 1.2. *If x, y, n, t are any quantities such that $x^2 - ny^2 = t^2$, then*

$$(ID1) \qquad 2(x \pm t)\big(x + y\sqrt{n}\big) = \big(x \pm t + y\sqrt{n}\big)^2$$

$$(ID2) \qquad \left(\sqrt{x + y\sqrt{n}} \pm \sqrt{x - y\sqrt{n}}\right)^2 = 2(x \pm t).$$ ■

LEMMA 1.3. *For any field F, and $x, y \in F$, $F(\sqrt{x}) = F(\sqrt{y})$ if and only if xy is a square in F.* ■

The following notation will be used throughout. Let ξ be a non-square element of K. Then ξ has four conjugates in K (not necessarily distinct), which we write as ξ_i ($i = 1, 2, 3, 4$) and we assume:

$$(A) \qquad \begin{aligned} &\xi = \xi_1, \text{ and } N(\xi) = nr^2 \quad (n \in Z, r \in Q, n \text{ squarefree}) \\ &\xi_1\xi_2 = x_1, \quad \xi_3\xi_4 = x_2 \in Q(\sqrt{m}) \\ &\xi_1\xi_3 = y_1, \quad \xi_2\xi_4 = y_2 \\ &\xi_1\xi_4 = z_1, \quad \xi_2\xi_3 = z_2 \end{aligned}$$

If $\xi \in Q(\sqrt{m})$, then so are all these quantities, and $y_1 = z_2$, $y_2 = z_1$. Otherwise, y_1, y_2, z_1, z_2 are not in $Q(\sqrt{m})$ and they are distinct; they are conjugates in K.

We also define the following fields:

$$\begin{aligned} H &= K(\sqrt{n}), \\ F &= H(\sqrt{x_1}), \\ L &= F(\sqrt{y_1}). \end{aligned}$$

LEMMA 1.4. *If any of y_1, y_2, z_1, z_2 is square in K, then they are all square in K, and x_1 and x_2 are also square in K.*

PROOF. Since y_1, y_2, z_1, z_2 are conjugates in K, then if one is square they all are. From the definition of these quantities, we have the relations :

$$x_1y_1 = \xi_1^2 z_2; \quad y_1z_1 = \xi_1^2 x_2, \quad x_1z_1 = \xi_1^2 y_2$$

and so on, and the result follows. ■

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

THEOREM 1.5. *H, F and L are normal fields (over Q), and $M = L(\sqrt{\xi_1})$.*

PROOF. Since K is normal, then $H = K(\sqrt{n})$ is also. Since x_1, x_2 are conjugates in $Q(\sqrt{m}) \subset H$, and $x_1x_2 = nr^2$ is square in H, then $F = H(\sqrt{x_1})$ is normal. From the relations (A), since n and x_1 are square in F, then all of the quantities y_1y_2, y_1z_2, y_1z_1 are square in F, and so $L = F(\sqrt{y_1})$ contains all the conjugates of $\sqrt{y_1}$, and is a normal field. Again from (A), $L(\sqrt{\xi_1})$ contains all the conjugates of $\sqrt{\xi_1}$, and so it is normal, and must be M. ■

THEOREM 1.6.

(a) If $K \neq H$, then $H \neq F$

(b) If $H \neq F$, then $F \neq L$

(c) If $F \neq L$, then $L \neq M$

PROOF. (a). If $K \neq H$, then $N(\xi) = nr^2$ is not square in K, that is, $n \neq 1, m$. Then $H = Q(\sqrt{m}, \sqrt{\alpha}, \sqrt{n})$ has degree 8 and Galois group $Z_2 \times Z_4$. Since $x_1 \in Q(\sqrt{m})$ and $x_1x_2 = nr^2$, then $Q(\sqrt{m}, \sqrt{x_1}, \sqrt{n})$ has degree 8 and Galois group D_4. Then F is the composite of these fields, and has degree 16.

(b) Suppose that $H \neq F$, but $F = L$, that is, $H(\sqrt{x_1}) = H(\sqrt{x_1}, \sqrt{y_1})$. Since x_1 is not square in H, then none of the x_i, y_i, z_i are square in H (by Lemma 1.4 and the relations (A)), and so $H(\sqrt{y_1}) \neq H$. But then the hypothesis implies $H(\sqrt{y_1})$ and $H(\sqrt{x_1})$ must be the same field, and by Lemma 1.3, $x_1y_1 = \xi_1^2 z_2$ must be square in H. This contradicts the fact that z_2 is not square in H.

(c) Suppose to the contrary that $F \neq L$, but $L = M$. Clearly $\sqrt{\xi_i}$ is not in F, for $i = 1, 2, 3, 4$, since F is normal, and $F \neq F(\sqrt{y_1})$. Then $F(\sqrt{\xi_1})$ is not F, and we must have $F(\sqrt{\xi_1}) = F(\sqrt{y_1}) = L$. But then $\xi_1 y_1 = \xi_1^2 \xi_3$ must be square in F, a contradiction. ■

COROLLARY 1.7. *The degree D of M over Q is determined by the equalities holding among the fields K, H, F, and L, as follows:*

(a) $D = 8$ iff $K = H = F = L$

(b) $D = 16$ iff $K = H = F \neq L$

(c) $D = 32$ iff $K = H \neq F \neq L$

(d) $D = 64$ iff $K \neq H \neq F \neq L$

From this Corollary, we can read off the necessary and sufficient conditions on ξ for M to have given degree, since $K = H$ if and only if $n = 1$ or m, $H = F$ if and only if x_1 is square in H, and $F = L$ if and only if y_1 is square in F.

2. In this section we summarize the results in tables (except for the actual listing of subfields of M, which is in Section 4). The necessary theorems are stated first, and their proofs are given in the next section. The last statement in each theorem gives the TW-type (or HS type) of G; the preceding statements provide necessary and sufficient conditions for this type.

Let D be the degree of M over Q. We have $D \geq 8$ since ξ is not square in K. We use the notation of Section 1.

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

THEOREM 2.1. *If $D = 8$, then $n = 1$ or m, and $x_1, x_2, y_1, y_2, z_1, z_2$ are all square in K. If x_1 is square in $Q(\sqrt{m})$, then $G = Z_2 \times Z_4$, and otherwise $G = Z_8$.*

THEOREM 2.2. *Suppose that $D = 16$. Then*

(i) $n = 1$ or m, and x_1, x_2 are square in $K = H = F$.

(ii) The Galois group of L over Q is $Z_2 \times Z_4$, and the Galois group of M over $Q(\sqrt{m})$ is also $Z_2 \times Z_4$.

(iii) The TW-type is $16/11$.

THEOREM 2.3. *Suppose $D = 32$. Then*

(i) $n = 1$ or m, $K = H$, and x_1 and x_2 are not square in H.

(ii) $\mathrm{Gal}(F/Q) = Z_2 \times Z_4$.

(iii) M has seven subfields of degree 4 containing $\sqrt{m}$, eleven subfields of degree 8 containing $\sqrt{m}$, and seven subfields of degree 16 containing $\sqrt{m}$.

(iv) $\mathrm{Gal}\big(M/Q(\sqrt{m})\big) = Z_2 \times Z_2 \times Z_4$.

(v) $\mathrm{Gal}(L/Q)$ *has TW-type* $16/9$, *and G has precisely six subfields not containing $\sqrt{m}$.*

(vi) G has TW-type $32/20$.

For $D = 64$, it turned out to be simplest to give an explicit description of G, and use it to find the subfields.

If $\tau \in G$, then τ is determined by its action on $\{\sqrt{\xi_i} : i = 1,2,3,4\}$. Write

$$\tau(\sqrt{\xi_i}) = \delta_i\sqrt{\xi_{j(i)}} \quad (i = 1,2,3,4),$$

where each $\delta_i = \pm 1$, and $\big(j(1), j(2), j(3), j(4)\big)$ is a permutation of $(1,2,3,4)$. (This should not be confused with *cycle notation* for a permutation.) Define $S(\tau) = \Pi\delta_i$, and let $I(\tau) = \big(j(1), j(2), j(3), j(4)\big)$, and $D(\tau) = (\delta_1, \delta_2, \delta_3, \delta_4)$. There is a $1-1$ correspondence between the members of G, and the set of pairs $\{\big(D(\tau), I(\tau)\big) : \tau \in G\}$. Let $I(G)$ be the set of all possible $I(\tau)$, and $D(G)$ the set of all possible $D(\tau)$, for $\tau \in G$. The sets $I(G)$ and $D(G)$ may be equipped with natural binary operations: for $I(G)$, the usual composition of permutations, and for $D(G)$, the pointwise product. Given $I(\tau)$ and $D(\sigma)$, the permutation $I(\tau)$ acts on the 4-tuple $D(\sigma)$ in the obvious way; we denote this by $I(\tau)\big(D(\sigma)\big)$.

LEMMA 2.4.

(i) With the operations defined above, $I(G)$ and $D(G)$ are groups, with $D(G) = Z_2^4$; G is a semi-direct product of these groups.

(ii) The members of $I(G)$ are the permutations $(1,2,3,4)$, $(2,1,4,3)$, $(4,3,1,2)$, *and* $(3,4,2,1)$, *so that* $I(G) = Z_4$.

(iii) If $\sigma, \tau \in G$, then $I(\sigma\tau) = I(\sigma)I(\tau)$, and $D(\sigma\tau)$ is the pointwise product of $D(\tau)$ and $I(\tau)\big(D(\sigma)\big)$.

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

Define the following sets in G, of eight elements each:

$$
\begin{aligned}
\{a_i\} &= \{\tau \in G \mid I(\tau) = (1,2,3,4), \text{ and } S(\tau) = +1\}\\
\{c_i\} &= \{\tau \in G \mid I(\tau) = (1,2,3,4), \text{ and } S(\tau) = -1\}\\
\{b_i\} &= \{\tau \in G \mid I(\tau) = (2,1,4,3), \text{ and } S(\tau) = +1\}\\
\{d_i\} &= \{\tau \in G \mid I(\tau) = (2,1,4,3), \text{ and } S(\tau) = -1\}\\
\{e_i\} &= \{\tau \in G \mid I(\tau) = (3,4,2,1), \text{ and } S(\tau) = +1\}\\
\{g_i\} &= \{\tau \in G \mid I(\tau) = (3,4,2,1), \text{ and } S(\tau) = -1\}\\
\{f_i\} &= \{\tau \in G \mid I(\tau) = (4,3,1,2), \text{ and } S(\tau) = +1\}\\
\{h_i\} &= \{\tau \in G \mid I(\tau) = (4,3,1,2), \text{ and } S(\tau) = -1\}
\end{aligned}
$$

We arrange these (by indices) according to sign pattern, as follows:

$S(\tau) = +1$		$S(\tau) = -1$	
1. + + ++	5. + − +−	1. − + ++	5. + − −−
2. − − ++	6. − + −+	2. + − ++	6. − + −−
3. + + −−	7. + − −+	3. + + −+	7. − − +−
4. − − −−	8. − + +−	4. + + +−	8. − − −+

For example, h_7 has $I(h_7) = (4,3,1,2)$ and $D(h_7) = (-1,-1,+1,-1)$.

THEOREM 2.5. *(i) a_1 is the identity; $a_2 - a_7$, $b_1 - b_4$, $c_1 - c_8$ have order 2; $g_1 - g_8$, $h_1 - h_8$ have order 8, and the rest have order 4.*

(ii) $\{a_i\}$ is a subgroup (Z_2^3); and the other sets $\{b_i\}$, $\{c_i\}$, ... are its cosets.

(iii) $\{a_i\}$ is the commutator subgroup of G; its fixed field is H.

(iv) $\{a_1, a_4\}$ is the center of G; its fixed field is L.

(v) G has HS-type $(64)\Gamma_{22}a_1$

In Table I and Table II, we summarize the basic results about G, when $D > 8$. $FF(C)$ is the fixed field of the center C of G, and $FF(G')$ is the fixed field of the commutator subgroup G'. We give $\mathrm{Gal}\big(M/FF(C)\big)$ and $G\big(FF(G')/G\big)$, which are isomorphic, respectively, to C and to G'.

Table I

D	16	32	64
TW	$16/11$	$32/20$	$****$
HS	$(16)\Gamma_2 d$	$(32)\Gamma_2 j_1$	$(64)\Gamma_{22}a_1$
$FF(C)$	$Q(\sqrt{m}, \sqrt{j})$	$Q(\sqrt{m}, \sqrt{j\alpha})$	L
$\mathrm{Gal}\big(M/FF(C)\big)$	$Z_2 \times Z_2$	$Z_2 \times Z_4$	Z_2
$FF(G')$	$K(\sqrt{j})$	L	H
$\mathrm{Gal}\big(FF(G')\big)$	$Z_2 \times Z_4$	$16/9(TW)$ $\Gamma_2 c_1(HS)$	$Z_2 \times Z_4$

Table II gives the numbers of elements, subgroups, and normal subgroups, of a given order in G, for $D = 64$. Let $E(i)$ be the number of elements of G of order 2^i, $S(i)$ the

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

number of subgroups of G, of order 2^i, and $N(i)$ the number of normal subgroups of G, of order 2^i.

Table II (D = 64)

i	1	2	3	4	5
$E(i)$	19	28	16	0	0
$S(i)$	19	55	43	11	3
$N(i)$	1	1	3	3	3

3. In this section, we prove the results stated in Section 2.

PROOF OF THEOREM 2.1. The first statement follows from Theorem 1.6: since $H = K$, then $n = 1$ or m; since $F = H = K$, then x_1 and x_2 are square in K; and so on. Since $K \subset M$, the only possibilities for G are $Z_2 \times Z_4$ and Z_8. Now write $\xi = u + v\sqrt{\alpha}$, for some $u, v \in Q(\sqrt{m})$. Then $x_1 = \xi_1\xi_2 = u^2 - v^2\alpha = s^2$ for some $s \in K$. Suppose first that $s \in Q(\sqrt{m})$. Then by $(ID1)$ and Lemma 1.3,

$$M = K(\sqrt{\xi_1}) = K\big(\sqrt{2(u-s)}\big)$$

and so M contains the quartic subfield $Q\big(\sqrt{m}, \sqrt{2(u-s)}\big)$, which is different from K. So G cannot be Z_8. Conversely, if G is $Z_2 \times Z_4$, then there must be some $j \in Z$ such that$K(\sqrt{\xi_1}) = K(\sqrt{j})$, so that $j\xi_1$ is square in K. But then x_1 is square in $Q(\sqrt{m})$, since we can write $x_1 = (j\xi_1)(j\xi_2)/j^2$. ■

PROOF OF THEOREM 2.2. The first statement follows as before. The field L is normal of degree 8, and since $K \subset L$, $\mathrm{Gal}(L/Q)$ must be $Z_2 \times Z_4$ or Z_8. Write $y_1 = A + B\sqrt{\alpha}$ for some A, B in $Q(\sqrt{m})$. Then $y_2 = A - B\sqrt{\alpha}$, and (since $n = 1$ or m)

$$A^2 - B^2\alpha = N(\xi_1) = nr^2 = t^2$$

for some $t \in Q(\sqrt{m})$. Then by $(ID1)$, we have $K(\sqrt{y_1}) = K\big(\sqrt{2(A-t)}\big)$. Then $Q\big(\sqrt{m}, \sqrt{2(A-t)}\big)$ is a quartic subfield of L, different from K. Then $\mathrm{Gal}(L/Q) = Z_2 \times Z_4$.

Now there must be some $j \in Z$ such that $L = K(\sqrt{j})$, that is, jy_1 is square in K. We have $M = L(\sqrt{\xi})$, and since $jy_1 = j\xi_1\xi_3$ is square in K (and $x_1 = \xi_1\xi_2$ is square in K) then there are three fields between M and K: L, $K(\sqrt{\xi_1})$, and $K(\sqrt{\xi_3})$. Then $\mathrm{Gal}(M/K) = Z_2 \times Z_2$. Since L and M are normal, there are no other fields of degree 8 in M, and then $\mathrm{Gal}(M/Q(\sqrt{m}) = Z_2 \times Z_4$.

Then $G = \mathrm{Gal}(M/Q)$ can only be of TW-type $16/11$. ■

PROOF OF THEOREM 2.3. (i) By Corollary 1.7, $n = 1$ or m, and $K = H$. So $H \neq F = H(\sqrt{x_1})$, and so x_1 and x_2 are not square in H.

(ii) From (i), $\mathrm{Gal}(F/Q)$ is either $Z_2 \times Z_4$ or Z_8 and since $x_1 \in Q(\sqrt{m}) \subset K$, F has more than one quartic subfield; hence $\mathrm{Gal}(F/Q) = Z_2 \times Z_4$.

(iii) From (ii), there is some $j \in Z$ such that $F = H(\sqrt{j})$, and jx_1 is square in H. As in the proof of Theorem 2.2, there is an integer $\delta = 2(A-t)$ in $Q(\sqrt{m})$ such that δy_1 is square in K. We need to show first that $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta})$ is a dihedral field. Since δy_1 is square in K, then its conjugate $\delta^* z_1$ is also square in K, and so we have that $(\delta\delta^*)y_1 z_1 = (\delta\delta^*)\xi_1^2 x_2$ is square in K. Since jx_2 is square in K, then the rational integer $j(\delta\delta^*)$ is square in K, and it follows that $(\delta\delta^*)$ is a rational square multiple of either j or mj. Hence, both $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta})$ and $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta\alpha})$ are dihedral fields. Then M must contain the following subfields:

$$\begin{aligned}
&Q(\sqrt{m}, \sqrt{\alpha}), Q(\sqrt{m}, \sqrt{j\alpha}), Q(\sqrt{m}, \sqrt{j}),\\
&Q(\sqrt{m}, \sqrt{\delta}), Q(\sqrt{m}, \sqrt{\delta^*}), Q(\sqrt{m}, \sqrt{\delta\alpha}), Q(\sqrt{m}, \sqrt{\delta^*\alpha^*}),\\
&Q(\sqrt{m}, \sqrt{\alpha}, \sqrt{j}), Q(\sqrt{m}, \sqrt{\delta}, \sqrt{j}), Q(\sqrt{m}, \sqrt{\delta\alpha}, \sqrt{j}),\\
&Q(\sqrt{m}, \sqrt{j\alpha}, \sqrt{\delta}), Q(\sqrt{m}, \sqrt{j\alpha}, \sqrt{\delta^*}), K(\sqrt{\delta}),\\
&K(\sqrt{\delta^*}), K(\sqrt{\xi_1}), K(\sqrt{\xi_2}), K(\sqrt{\xi_3}), K(\sqrt{\xi_4}),\\
&L = K(\sqrt{j}, \sqrt{\delta}), K(\sqrt{\xi_i}, \sqrt{\xi_k}), \big((i,k) = (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\big)
\end{aligned}$$

It is straightforward, if tedious, to check that these fields are all distinct, using such things as Lemma 1.3, relations on x_i, y_i, z_i as in Lemma 1.4, and the fact that none of them is square in H. Then (iii) follows.

(iv) $\mathrm{Gal}\big(M/Q(\sqrt{m}\big)$ has order 16, and it has seven subgroups of order 2, eleven of order 4, and seven of order 8. From the TW-types for groups of order 16, it can only be $Z_2 \times Z_2 \times Z_4$.

(v) It was shown above that M contains two distinct dihedral subfields. If $\delta\delta^*$ is a square multiple of j, then $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta})$ is cyclic over $Q(\sqrt{mj}$, and $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta\alpha})$ is cyclic over $Q(\sqrt{j})$; if $\delta\delta^*$ is a square multiple of mj, it's the other way around. Either way, each of $Q(\sqrt{j})$ and $Q(\sqrt{mj}$ has precisely two quadratic extensions not containing $Q(\sqrt{m})$. From this, and the list of fields in (iii), $\mathrm{Gal}(L/Q)$ has three subgroups of order 8, eleven subgroups of order 4, and seven subgroups of order 2. The only group of order 16 satisfying this, is TW-type 16/9. From the above, the subfields of M not containing $\sqrt{m}$ are:

$$Q(\sqrt{j}), Q(\sqrt{mj}), Q(\sqrt{j}, \sqrt{\beta}), Q(\sqrt{j}, \sqrt{\beta^*}), Q(\sqrt{j}, \sqrt{\gamma}), Q(\sqrt{j}, \sqrt{\gamma^*}),$$

where $\beta = (\sqrt{\delta} + \sqrt{\delta^*})^2$ and $\gamma = (\sqrt{\delta\alpha} + \sqrt{\delta^*\alpha^*})^2$

(vi) Let N_i $(i = 1, 2, 3, 4)$ denote the four quartic subfields which do not contain $\sqrt{m}$. It is clear from the listing in (iii), that $\mathrm{Gal}(M/N_i) = Z_8$, and that this is not true for any other quartic subfield of M. Similarly, if X is one of $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta})$, $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta\alpha})$, $Q(\sqrt{m}, \sqrt{j\alpha}, \sqrt{\delta})$, or $Q(\sqrt{m}, \sqrt{j\alpha}, \sqrt{\delta^*})$, then $\mathrm{Gal}(M/X)$ is Z_4, and this is not true for any other subfield of degree 8. Since there is only one normal subfield of degree 16, G has only one normal subgroup of order 2. From these facts, the only possibilities for the TW-type of G are 32/17 and 32/20. Then the center of G must have order 8. The only normal quartic subfields of M are K itself, $Q(\sqrt{m}, \sqrt{j})$, and $Q(\sqrt{m}, \sqrt{j\alpha})$; and none of the corresponding subgroups of G is cyclic. Thus the center of G is not cyclic, and G must have TW-type 32/20. ■

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

PROOF OF LEMMA 2.4. The first statement is obvious. For (ii), since $\xi_1\xi_2 = x_1$ and $\xi_3\xi_4 = x_2$ are in $Q(\sqrt{m})$, then if $(a,b,c,d) \in I(G)$, we must have either $\{a,b\} = \{1,2\}$ or $\{a,b\} = \{3,4\}$. If $\{a,b\} = \{1,2\}$, then the corresponding τ fixes $Q(\sqrt{m})$, and then we must have $\tau(y_1) = y_1$ or y_2, so that $\{a,c\} = \{1,3\}$ or $\{2,4\}$. If $\{a,b\} = \{3,4\}$, then $\tau(y_1) = z_1$ or z_2, and then $\{a,c\} = \{2,3\}$ or $\{1,4\}$. Only four permutations satisfy all these conditions, and this gives $I(G)$. The last statement is clear from the definition.

PROOF OF THEOREM 2.5. (i) The orders of the elements are easily computed, using Lemma 2.4.

(ii) $\{a_i\}$ is the subgroup of G consisting of all σ such that $I(\sigma)$ is the identity permutation $(1,2,3,4)$. Since all the elements of $\{a_i\}$ have order 2, then $\{a_i\} = Z_2^3$. The other sets $\{b_i\}$, $\{c_i\}$, etc. are clearly its cosets.

(iii) From Lemma 2.4 (iii), $I(\sigma\tau\sigma^{-1}\tau^{-1}) = (1,2,3,4)$, and so the commutator subgroup is contained in $\{a_i\}$. Computing commutators, we get $[a_2, g_1] = a_4$, $[a_7, g_1] = a_2$, and $[a_5, g_1] = a_3$, so the commutator subgroup contains three elements of order 2, and must be all of $\{a_i\}$. It is clear from the definition that its fixed field is H.

(iv) From Lemma 2.4(iii), if σ, τ are in G, then $D(\sigma\tau)$ is the pointwise product $D(\tau)^*I(\tau)\big(D(\sigma)\big)$, and $D(\tau\sigma) = D(\sigma)^*I(\sigma)\big(D(\tau)\big)$. Suppose for some fixed σ, these two quantities are equal for all τ in G. Then (considering e.g. $\tau \in \{a_i\}$) it follows that $I(\sigma)$ must be the identity, and the sign-pattern $D(\sigma)$ must be invariant under all possible $I(\tau)$. So $D(\sigma)$ is either $(1,1,1,1)$ or $(-1,-1,-1,-1)$, and then σ is either a_1 or a_4. From the definition of the a_i, the fixed field is L.

(v) The properties of G established in (i)–(iv) determine a unique group of order 64 in the tables of Hall and Senior [1]. (The tables of Thomas and Wood [3] only go up to order 32). This group is $(64)\Gamma_{22}a_1$.

4. In this section, we list the subfields of M, for $D = 16$, 32, and 64. In the table for $D = 64$, we list only one representative from each class of conjugate fields (over Q), and indicate the number of fields in each class by a number in parentheses on the left. Beside each field in the list for $D = 64$, we also give the subgroup of the Galois group for which it is the fixed field.

In these tables, we use the following notation. $K = Q(\sqrt{m}, \sqrt{\alpha})$, where m is a squarefree positive rational integer, and $\alpha \in Q(\sqrt{m}) - Q$ satisfies $N(\alpha) = ms^2$ where $s \in Q$.

$$\xi = \xi_1, \text{ and } N(\xi) = nr^2 \quad (n \in Z, r \in Q, n \text{ squarefree})$$

$$(A)\qquad \begin{aligned} &\xi_1\xi_2 = x_1, \quad \xi_3\xi_4 = x_2 \in Q(\sqrt{m}) \\ &\xi_1\xi_3 = y_1 \quad \xi_2\xi_4 = y_2 \\ &\xi_1\xi_4 = z_1 \quad \xi_2\xi_3 = z_2 \\ &H = K(\sqrt{n}); \quad F = H(\sqrt{x_1}); L = F(\sqrt{y_1}) \end{aligned}$$

For $D = 16$, we know that $\mathrm{Gal}(L/Q) = Z_2 \times Z_4$; there must be some $j \in Z$ such that

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

$L = K(\sqrt{j})$, that is, jy_1 is square in K. This j appears in the table below.

Subfields of M, for $D = 16$

$$
\begin{aligned}
&Q(\sqrt{m}), Q(\sqrt{j}), Q(\sqrt{mj}),\\
&Q(\sqrt{m}, \sqrt{j}), Q(\sqrt{m}, \sqrt{\alpha}), Q(\sqrt{m}, \sqrt{j\alpha}),\\
&Q(\sqrt{m}, \sqrt{\alpha}, \sqrt{j}), Q(\sqrt{m}, \sqrt{\alpha}, \sqrt{\xi_1}),\\
&Q(\sqrt{m}, \sqrt{\alpha}, \sqrt{\xi_3}).
\end{aligned}
$$

For $D = 32$, we know that $\mathrm{Gal}(F/Q) = Z_2 \times Z_4$, and so there is some $j \in Z$ such that $F = H(\sqrt{j})$, and jx_1 is square in H. Let $\delta = (\sqrt{y_1} + \sqrt{y_2})^2$ (in $Q(\sqrt{m})$); then δy_1 is square in K and $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta})$ is a dihedral field. $Q(\sqrt{m}, \sqrt{j}, \sqrt{\delta\,\alpha})$ is also dihedral.

Subfields of M, for $D = 32$

$$
\begin{aligned}
&Q(\sqrt{m}, \sqrt{\alpha}), Q(\sqrt{m}, \sqrt{j\alpha}), Q(\sqrt{m}, \sqrt{j}),\\
&Q(\sqrt{m}, \sqrt{\delta}), Q(\sqrt{m}, \sqrt{\delta^*}), Q(\sqrt{m}, \sqrt{\delta\,\alpha}), Q(\sqrt{m}, \sqrt{\delta^*\alpha^*}),\\
&Q(\sqrt{m}, \sqrt{\alpha}, \sqrt{j}), Q(\sqrt{m}, \sqrt{\delta}, \sqrt{j}), Q(\sqrt{m}, \sqrt{\delta\,\alpha}, \sqrt{j}),\\
&Q(\sqrt{m}, \sqrt{j\alpha}, \sqrt{\delta}), Q(\sqrt{m}, \sqrt{j\alpha}, \sqrt{\delta^*}), K(\sqrt{\delta}),\\
&K(\sqrt{\delta^*}), K(\sqrt{\xi_1}), K(\sqrt{\xi_2}), K(\sqrt{\xi_3}), K(\sqrt{\xi_4}),\\
&L = K(\sqrt{j}, \sqrt{\delta}), K(\sqrt{\xi_i}, \sqrt{\xi_k}), \big((i,k) = (1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\big)\\
&Q(\sqrt{j}), Q(\sqrt{mj}), Q(\sqrt{j}, \sqrt{\beta}), Q(\sqrt{j}, \sqrt{\beta^*}), Q(\sqrt{j}, \sqrt{\gamma}), Q(\sqrt{j}, \sqrt{\gamma^*}),
\end{aligned}
$$

where $\beta = (\sqrt{\delta} + \sqrt{\delta^*})^2$ and $\gamma = (\sqrt{\delta\,\alpha} + \sqrt{\delta^*\alpha^*})^2$

For $D = 64$, we define the following quantities:

$$
\begin{aligned}
\delta &= (\sqrt{x_1} + \sqrt{x_2})^2 \in Q(\sqrt{n})\\
\gamma &= (\sqrt{\alpha x_1} + \sqrt{\alpha^* x_2})^2 \in Q(\sqrt{mn})\\
\beta_1 &= (\sqrt{\xi_1} + \sqrt{\xi_2})^2 \text{ and } \beta_2 = (\sqrt{\xi_1} - \sqrt{\xi_2})^2 \in Q(\sqrt{m}, \sqrt{x_1})\\
\beta_3 &= (\sqrt{\xi_3} + \sqrt{\xi_4})^2 \text{ and } \beta_4 = (\sqrt{\xi_3} - \sqrt{\xi_4})^2 \in Q(\sqrt{m}, \sqrt{x_2})\\
\varepsilon_1 &= (\sqrt{y_1} + \sqrt{y_2})^2 \text{ and } \varepsilon_2 = (\sqrt{y_1} - \sqrt{y_2})^2 \in Q(\sqrt{m}, \sqrt{n})\\
\varepsilon_3 &= (\sqrt{z_1} + \sqrt{z_2})^2 \text{ and } \varepsilon_4 = (\sqrt{z_1} - \sqrt{z_2})^2 \in Q(\sqrt{m}, \sqrt{n})
\end{aligned}
$$

The subfields T of M for $D = 64$ are given in separate tables, one for degree 2, one for degree 4, and for higher degrees, one for each group-type for $\mathrm{Gal}(M/T)$. To the left of each field, in parentheses, is the number of its conjugate fields (over Q). We list only one member of each conjugate class. To the right of the field, we give the subgroup of

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

G of which it is the fixed field, and some information about it. At the beginning of each table, we indicate the total number of subfields of M in that table. For the fields of degree 2, we give a set of generators for the corresponding group, and relations for it, except for the orders of the elements.

Subfields of M, $D = 64$

I. Subfields of degree 2 (3)

$Q(\sqrt{m})$	$\{a_i, b_i, c_i, d_i\}$ type 32/33 generators $\langle a_2, a_3, c_1, c_3, b_1\rangle$ relations $c_1b_1 = b_1a_2c_1$ and $c_3b_1 = b_1a_3c_3$
$Q(\sqrt{n})$	$\{a_i, b_i, e_i, f_i\}$ type 32/46 generators $\langle a_2, a_4, a_7, e_1\rangle$ relations $a_2e_1 = e_1a_4a_2$ and $a_7e_1 = e_1a_4a_2a_7$
$Q(\sqrt{mn})$	$\{a_i, b_i, g_i, h_i\}$ type 32/47 generators $\langle a_2, a_7, g_1\rangle$ relations $g_1a_2 = a_2g_1^5$ and $g_1a_7 = a_7a_2g_1$

II. Subfields of degree 4 (11)

	$Q(\sqrt{m}, \sqrt{\alpha})$	$\{a_i, c_i\}$; type Z_2^4; normal
	$Q(\sqrt{m}, \sqrt{n})$	$\{a_i, b_i\}$; type 16/6 ; normal
	$Q(\sqrt{m}, \sqrt{n\alpha})$	$\{a_i, d_i\}$; type 16/9 ; normal,
(2)	$Q(\sqrt{m}, \sqrt{\alpha x_1})$	$\{a_1 - a_4, b_5 - b_8, c_3, c_4, c_7, c_8, d_1, d_2, d_5, d_6\}$ type 16/9,
(2)	$Q(\sqrt{m}, \sqrt{x_1})$	$\{a_1 - a_4, b_1 - b_4, c_3, c_4, c_7, c_8, d_3, d_4, d_7, d_8\}$ type 16/6,
(2)	$Q(\sqrt{mn}, \sqrt{\gamma})$	$\{a_1 - a_4, b_5 - b_8, g_3, g_4, g_7, g_8, h_1, h_2, h_5, h_6\}$ type 16/11
(2)	$Q(\sqrt{n}, \sqrt{\delta}))$	$\{a_1 - a_4, b_1 - b_4, e_1 - e_4, f_1 - f_4\}$ type 16/9

III. Subfields T of degree 8, Gal$(M/T) = Z_2^3$ (16)

$Q(\sqrt{m}, \sqrt{n}), \sqrt{\alpha})$	$\{a_i\}$; commutator subgroup; normal
$Q(\sqrt{m}, \sqrt{n}, \sqrt{x_1})$	$\{a_1 - a_4, b_1 - b_4\}$; normal

For the 14 remaining fields in this table, the corresponding subgroup of G consists of four elements of $\{a_i\}$ and four elements of $\{c_i\}$.

(2)	$K(\sqrt{x_1})$	$\{a_1, a_2, a_3, a_4, c_3, c_4, c_7, c_8\}$
(4)	$K(\sqrt{y_1})$	$\{a_1, a_4, a_5, a_6, c_2, c_4, c_6, c_8\}$
(4)	$K(\sqrt{n\xi_1})$	$\{a_1, a_3, a_5, a_7, c_1, c_6, c_7, c_8\}$
(4)	$K(\sqrt{\xi_1})$	$\{a_1, a_3, a_5, a_7, c_2, c_3, c_4, c_5\}$

IV. Subfields T of degree 8, Gal$(M/T) = Z_2 \times Z_4$ (7)

$Q(\sqrt{m}, \sqrt{n}, \sqrt{\alpha x_1})$	$\{a_1 - a_4, b_5 - b_8\}$; normal

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

(2)	$Q(\sqrt{m}, \sqrt{n\alpha}, \sqrt{x_1})$	$\{a_1 - a_4, d_3, d_4, d_7, d_8\}$
(4)	$Q(\sqrt{n}, \sqrt{\delta}, \sqrt{y_1} + \sqrt{y_2} + \sqrt{z_1} + \sqrt{z_2})$	$\{a_1, a_4, b_1, b_4, e_1, e_4, f_1, f_4\}$

V. Subfields T of degree 8, $\mathrm{Gal}(M/T) = D_4$ (12)

(4)	$Q(\sqrt{m}, \sqrt{x_1}, \sqrt{\beta_1})$	$\{a_1, a_3, b_1, b_3, c_3, c_4, d_3, d_4\}$
(4)	$Q(\sqrt{m}, \sqrt{x_1}, \sqrt{n\beta_1}))$	$\{a_1, a_3, b_1, b_3, c_7, c_8, d_7, d_8\}$
(4)	$Q(\sqrt{m}, \sqrt{n}, \sqrt{y_1} + \sqrt{y_2}))$	$\{a_1, a_4, a_5, a_6, b_1, b_4, b_5, b_6\}$

VI. Subfields T of degree 8, $\mathrm{Gal}(M/T) = Z_8$ (4)

These are all conjugate, but are listed separately because knowledge of these cyclic subgroups is helpful.

$Q(\sqrt{mn}, \sqrt{\gamma}, \sqrt{y_1} + \sqrt{y_2} - \sqrt{z_1} + \sqrt{z_2})$
$\langle h_1 \rangle = \{h_1, b_6, g_8, a_4, h_5, b_5, g_4, a_1\}$

$Q(\sqrt{mn}, \sqrt{\gamma}, \sqrt{y_1} + \sqrt{y_2} + \sqrt{z_1} - \sqrt{z_2})$
$\langle h_2 \rangle = \{h_2, b_5, g_7, a_4, h_6, b_6, g_3, a_1\}$

$Q(\sqrt{mn}, \sqrt{\gamma^*}, \sqrt{y_1} - \sqrt{y_2} - \sqrt{z_1} - \sqrt{z_2})$
$\langle h_3 \rangle = \{h_3, b_7, g_5, a_4, h_7, b_8, g_1, a_1\}$

$Q(\sqrt{mn}, \sqrt{\gamma^*}, \sqrt{y_1} - \sqrt{y_2} + \sqrt{z_1} + \sqrt{z_2})$
$\langle h_4 \rangle = \{h_4, b_8, g_6, a_4, h_8, b_7, g_2, a_1\}$

VII. Subfields T of degree 16, $\mathrm{Gal}(M/T) = Z_2 \times Z_2$ (41)

Put $J = Q(\sqrt{m}, \sqrt{n})$.

	$J(\sqrt{\alpha}, \sqrt{x_1})$	$\{a_1, a_2, a_3, a_4\}$; normal
(4)	$K(\sqrt{n}, \sqrt{\xi_1})$	$\{a_1, a_3, a_5, a_7\}$
(2)	$J(\sqrt{\alpha}, \sqrt{y_1})$	$\{a_1, a_4, a_5, a_6\}$
(4)	$J(\sqrt{x_1}, \sqrt{\beta_1})$	$\{a_1, a_3, b_1, b_3\}$
(2)	$J(\sqrt{x_1}, \sqrt{\varepsilon_1})$	$\{a_1, a_4, b_1, b_4\}$
(4)	$K(\sqrt{\xi_1}, \sqrt{n\xi_2})$	$\{a_1, a_3, c_2, c_5\}$
(8)	$K(\sqrt{n\xi_1}, \sqrt{\xi_3})$	$\{a_1, a_5, c_1, c_7\}$
(2)	$K(\sqrt{n\xi_1}, \sqrt{n\xi_2})$	$\{a_1, a_3, c_7, c_8\}$
(4)	$K(\sqrt{n\xi_1}, \sqrt{n\xi_3})$	$\{a_1, a_5, c_6, c_8\}$
(4)	$K(\sqrt{x_1}, \sqrt{y_1})$	$\{a_1, a_4, c_4, c_8\}$
(4)	$K(\sqrt{\xi_1}, \sqrt{\xi_3})$	$\{a_1, a_5, c_2, c_4\}$
(2)	$K(\sqrt{\xi_1}, \sqrt{\xi_2})$	$\{a_1, a_3, c_3, c_4\}$

VIII. Subfields T of degree 16, $\mathrm{Gal}(M/T) = Z_4$ (14)

Put $U = Q(\sqrt{m}, \sqrt{n\alpha})$.

(2)	$J(\sqrt{\alpha x_1}, \sqrt{\varepsilon_1})$	$\langle b_5 \rangle = \{b_5, a_4, b_6, a_1\}$ (conj. $\langle b_7 \rangle$)

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press

(2)	$U(\sqrt{x_2}, \sqrt{\beta_3})$	$\langle d_1 \rangle = \{d_1, a_2, d_2, a_1\}$ (conj. $\langle d_3 \rangle$)
(2)	$U(\sqrt{x_1}, \sqrt{n\beta_1})$	$\langle d_7 \rangle = \{d_7, a_3, d_8, a_1\}$ (conj. $\langle d_5 \rangle$)

Put $S = Q(\sqrt{n}, \sqrt{x_1} + \sqrt{x_2})$.

(8)	$S(\sqrt{y_1} + \sqrt{y_2} + \sqrt{z_1} + \sqrt{z_2}, \sqrt{\beta_1} + \sqrt{\beta_3})$	
		$\langle e_1 \rangle = \{e_1, b_1, f_1, a_1\}$ (conj. $\langle e_i \rangle$, $i = 2, 3, \ldots, 8$).

IX. Subfields of degree 32 (19)

	$L = K(\sqrt{n}, \sqrt{x_1}, \sqrt{y_1})$	$\{a_1, a_4\}$ (center of G)
(2)	$K(\sqrt{\xi_1}, \sqrt{\xi_2}, \sqrt{n})$	$\{a_1, a_3\}$
(4)	$J(\sqrt{x_1}, \sqrt{\beta_1}, \sqrt{\beta_3})$	$\{a_1, b_1\}$
(4)	$K(\sqrt{\xi_1}, \sqrt{\xi_3}, \sqrt{n})$	$\{a_1, a_5\}$
(4)	$K(\sqrt{\xi_1}, \sqrt{\xi_2}, \sqrt{\xi_3})$	$\{a_1, c_4\}$
(4)	$K(\sqrt{n\xi_1}, \sqrt{n\xi_2}, \sqrt{n\xi_3})$	$\{a_1, c_8\}$

References

1. M. Hall, Jr. and J. K. Senior, *The groups of order* $2^n (n \geq 6)$. Macmillan, 1964.

2. R. A. Mollin, *Number Theory and Applications*. Kluwer, 1989.

3. B. L. van der Waerden, *Modern Algebra*. Frederick Ungar Publishing, New York, 1950.

4. A. D. Thomas and G. V. Wood, *Group Tables*. Shiva Publishing Ltd., Orpington, Kent, UK, 1980.

Department of Mathematics
University of North Carolina at Greensboro
Greensboro, NC 27412
USA

https://doi.org/10.4153/CJM-1991-063-4 Published online by Cambridge University Press