JOURNAL OF ALGEBRA 43, 155–167 (1976)

Uniform Distribution and Real Fields

R. MOLLIN*

Department of Mathematics, Queen's University, Kingston, Ontario, Canada K71 3N6

Communicated by I. N. Herstein

Received June 16, 1975

INTRODUCTION

In this paper we continue the investigation into the *group of algebras with uniformly distributed invariants*, $U(K)$, and its relation to the *Schur subgroup* $S(K)$, undertaken in [6, 7]. We maintain the notation of [6, 7].

In the first section we investigate $U(K)$ for a real quadratic field K. We calculate generators of $U(K)$ explicitly.

In the second section we investigate $U(K)$ for other real fields K. We use a recent result by Yamada to show that $| U(K) : S(K)|$ is infinite for real fields K subject to the restrictions:

(1) $\mathbf{Q}(\epsilon_n)/K$ is cyclic where $\mathbf{Q}(\epsilon_n)$ is the least root of unity field containing K.

(2) $n \not\equiv 2 \pmod 4$, and is divisible by at least two distinct primes.

We note that a special case of the above result is for $K = \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})$. In the case where n is odd and divisible by at least two distinct primes then we obtain: $S(\mathbf{Q}(\epsilon_n + \epsilon_n^{-1})) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$ if and only if n is divisible by a prime congruent to 3 modulo 4. This condition is the exact analog of Yamada's result on real quadratic fields $\mathbf{Q}(d^{1/2})$ [9, Theorem 7.14, p. 112; 13], viz.: $S(\mathbf{Q}(d^{1/2})) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{Q}(d^{1/2})$ if and only if d is divisible by a prime congruent to 3 modulo 4. In the case where d is not divisible by any prime congruent to 3 modulo 4 then $S(K) = U(K)$ [9, Theorem 7.8, p. 107; 12].

As a corollary of the above result we obtain: If

(1) $K/\mathbf{Q}$ is real of even degree, and

(2) the least root of unity field $\mathbf{Q}(\epsilon_n)$ containing K has the property that n is odd, divisible by at least 2 distinct primes, and no prime congruent to 1 modulo 4 divides n, then

$$S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K.$$

---

[*] Present address: Department of Mathematics, University of Victoria, P.O. Box 1700, Victoria, British Columbia, Canada, V8W 2Y2.

When K is a quadratic field subject to these conditions then we get a special case of Yamada's aforementioned result for real quadratic fields [9, Theorem 7.8, p. 107]. Finally, for K subject to these conditions we obtain that $|U(K):S(K)|$ is infinite.

1. Real Quadratic Fields

Before we proceed with the task of calculating generators of $U(K)$ where K is a real quadratic field we need some notation and class field theoretic concepts most of which can be found in [5].

K = algebraic number field with ring of integers R.

$K^{(1)}$ = Hilbert class field of K [5, p. 191].

$K^{(+)}$ = extended Hilbert class field of K [5, p. 203].

$m = m_0 m_\infty$ = a K-modulus [5, p. 107], where

m_0 = modulus which is the product of the finite primes appearing with positive exponent in m, and

m_∞ = the product of the real primes in m.

I_K = group of fractional R-ideals of K.

$I_K{}^m$ = subgroup of I_K generated by primes not dividing m_0.

$K_m = \{a/b\colon a, b \in R;\ aR, bR$ relatively prime to $m_0\}$ [5, p. 108].

$K_{m,1} = \{\alpha \in K_m\colon \alpha \equiv 1 \pmod{m}\}$ [5, p. 108]. (The group $K_{m,1}$ is called the *ray mod m*.)

i = the map from K^* to I_K where $i(\alpha)$ is the principal ideal $(\alpha) = \alpha R = i(\alpha)$. (We observe that $i(K_{m,1}) \subseteq I^m$.)

Now we need a lemma.

Lemma 1.1. *Let $K = \mathbf{Q}(d^{1/2})$ where d is a positive square-free integer. Let q be a prime dividing d, and p an odd prime not dividing d such that $(q/p) = -1$ (where $(/)$ denotes the Legendre symbol). Then there exists a prime r such that $(r/p) = 1$ and $a^2 - db^2 = rq$ where $a + b(d^{1/2})$ is an algebraic integer in K (so that $2a$, $2b$ are rational integers).*

Proof. First we need some notation.

$L = K^{(+)}((\delta(p)\cdot p)^{1/2})$, where $\delta(p) = (-1)^{(p-1)/2}$.

$\mathscr{P}$ = a K-prime above p.

m = a modulus which is a product of the real K-primes.

$(n) = m \cdot \mathscr{P}^{a(\mathscr{P})}$ = modulus, where $\mathscr{P}$ appears to a sufficiently high power $a(\mathscr{P})$.

Now, the Artin reciprocity theorem [5, Theorem 5.7, p. 164] says that the Artin map, $\phi_{L/K}^{(n)}$ [5, p. 103], maps $I_K^{(n)}$ onto $\mathrm{Gal}(L/K)$ and $\phi_{K^{(+)}/K}^{(n)}$ maps $I_K^{(n)}$ onto $\mathrm{Gal}(K^{(+)}/K)$.

Since $K^{(+)} \subseteq L$ then clearly $\ker \phi_{L/K}^{(n)} \subseteq \ker \phi_{K^{(+)}/K}^{(n)}$. The first step is to show that $\ker \phi_{L/K}^{(n)} \neq \ker \phi_{K^{(+)}/K}^{(n)}$. Then we choose a suitable element (y) in $\ker \phi_{K^{(+)}/K}^{(n)}$ not in $\ker \phi_{L/K}^{(n)}$, and choose a suitable prime $\mathscr{R}$ in $\mathscr{Q}^{-1}(y) \ker \phi_{L/K}^{(n)}$ where $\mathscr{Q}$ is a K-prime above q. The final step is to analyze $\phi_{L/K}^{(n)}(\mathscr{R}\mathscr{Q})$ and show that the required properties hold.

So, we begin now by showing that $\ker \phi_{L/K}^{(n)} \neq \ker \phi_{K^{(+)}/K}^{(n)}$. If we have that $\ker \phi_{L/K}^{(n)} = \ker \phi_{K^{(+)}/K}^{(n)}$, then

$$\mathrm{Gal}(K^{(+)}/K) \cong I_K^{(n)}/\ker \phi_{K^{(+)}/K}^{(n)} = I_K^{(n)}/\ker \phi_{L/K}^{(n)} \cong \mathrm{Gal}(L/K).$$

Therefore, $L = K^{(+)}$ which implies that $(\delta(p)\cdot p)^{1/2} \in K^{(+)}$. Hence p is ramified in $K^{(+)}/\mathbf{Q}$. However, $K^{(1)}$ is an unramified extension of K [5, Theorem 13.1, p. 191], and the only K-primes which ramify in $K^{(+)}$ are infinite primes [5, p. 203]. Hence p must ramify in $K/\mathbf{Q}$. But p does not divide d and $p \neq 2$ so that p does not divide the discriminant of $K = \mathbf{Q}(d^{1/2})$. Therefore p is unramified in $K/\mathbf{Q}$, a contradiction. Hence, we have that

$$\ker \phi_{L/K}^{(n)} \neq \ker \phi_{K^{(+)}/K}^{(n)}.$$

Now, we let $\langle\sigma\rangle = \mathrm{Gal}(L/K^{(+)})$ and choose $(y) \in \ker \phi_{K^{(+)}/K}^{(n)}$ such that $\phi_{L/K}^{(n)}(y) = \sigma$.

We have the chain of subgroups: $I_K^{(n)} \supseteq \ker \phi_{L/K}^{(n)} \supseteq i(K_{n,1})$. By [5, (4.6.2), p. 132; 5, Theorem 10.3, p. 182] we have that any coset of $\ker \phi_{L/K}^{(n)}$ in $I_K^{(n)}$ contains infinitely many primes which have relative degree one over $\mathbf{Q}$. If $\mathscr{Q}$ is a K-prime above q then $\mathscr{Q}^{-1}(y) \ker \phi_{L/K}^{(n)}$ is such a coset and we choose a prime $\mathscr{R}$ in this coset with relative degree one over $\mathbf{Q}$. Therefore, $\mathscr{R}\mathscr{Q} \in (y) \ker \phi_{L/K}^{(n)}$ and so $\phi_{L/K}^{(n)}(\mathscr{R}\mathscr{Q}) = \phi_{L/K}^{(n)}(y) = \sigma$.

Now, the final step is to analyze $\phi_{L/K}^{(n)}(\mathscr{R}\mathscr{Q})$. By hypothesis, $(q/p) = -1$ which implies that q is inert in $\mathbf{Q}((\delta(p)\cdot p)^{1/2})/\mathbf{Q}$ [5, Lemma 9.7, p. 46]. But q is ramified in K, so that q is inert in $K(\delta(p)\cdot p)^{1/2}/K$. If we let $E = K((\delta(p)\cdot p)^{1/2})$ then the last statement implies that $\phi_{E/K}^{(n)}(\mathscr{Q}) = \sigma$. From $\phi_{L/K}^{(n)}(\mathscr{R}\mathscr{Q}) = \sigma$ we get that $\phi_{E/K}^{(n)}(\mathscr{R}\mathscr{Q}) = \sigma$. But then $\phi_{E/K}^{(n)}(\mathscr{Q}) = \sigma$ implies $\phi_{E/K}^{(n)}(\mathscr{R}) = 1$, i.e., $\mathscr{R}$ splits completely in E/K. However, $\mathscr{R}$ was chosen to have relative degree one over $\mathbf{Q}$. Therefore, if $\mathscr{R}$ lies above r in $K/\mathbf{Q}$ we have that r splits in $\mathbf{Q}((\delta(p)\cdot p)^{1/2})/\mathbf{Q}$; i.e., $(r/p) = 1$ [5, Lemma 9.7, p. 46] (which is one of the required conditions).

It remains to show $a^2 - db^2 = rq$ where $a + b(d^{1/2})$ is an algebraic integer in K.

We have that

$$(y) \ker \phi_{L/K}^{(n)} \subseteq \ker \phi_{K^{(+)}/K}^{(n)} \subseteq \ker \phi_{K^{(+)}/K} = i(K_{m,1}),$$

where $\phi_{K^{(+)}/K}$ maps I_K onto $\mathrm{Gal}(K^{(+)}/K)$ and we recall that m = product of the real K-primes. But $\mathscr{R}\mathscr{Q} \in (y) \ker \phi_{L/K}^{(n)}$, which implies that $\mathscr{R}\mathscr{Q} \in i(K_{m,1})$ so that $\mathscr{Q}$ is principal with totally positive generator [5, p. 203]. We let $\mathscr{R}\mathscr{Q} = (a + b(d)^{1/2})$ where $a + b(d)^{1/2}$ is an algebraic integer in K with $(a + bd^{1/2}) > 0$ and $(a - bd^{1/2}) > 0$. Therefore, $N_{K/\mathbf{Q}}(\mathscr{R}\mathscr{Q}) = a^2 - b^2d = rq$ (where $N_{K/Q}$ denotes the norm in $K/\mathbf{Q}$). Q.E.D.

Now, before defining some algebras we need the concept of a crossed product and some notation.

If L is an extension field of K with Galois group $G = \mathrm{Gal}(L/K)$ and if α is a factor set from $G \times G$ to L then the crossed product made with L and α is denoted by $(L/K, \alpha)$ [4, Sect. 4, p. 107]. This is the central simple K-algebra having L-basis u_σ, $\sigma \in G$, subject to the rules

$$u_\sigma u_\tau = \alpha(\sigma, \tau)\, u_{\sigma\tau}, \qquad u_\sigma x = \sigma(x)\, u_\sigma \qquad \text{for} \quad x \in L.$$

In the case $G = \langle \sigma \rangle$ is cyclic then we write $(L/K, a)$ for the crossed product in which

$$\begin{aligned} (u_\sigma)^i &= u_{\sigma^i}, \qquad && 1 \leqslant i < |\sigma|, \\ &= a, && i = |\sigma|. \end{aligned}$$

Now we proceed to define algebras which will serve as generators of $U(\mathbf{Q}(d^{1/2}))$, $d > 0$ and square-free. By Dirichlet's density theorem [3, Corollary 9-2-7, p. 168] there are infinitely many primes p which are inert in K; i.e., for which the Legendre symbol $(d/p) = -1$ [5, Lemma 9.5, p. 45]. For each such p there exists at least one prime q_p dividing d such that $(q_p/p) = -1$. Now, we let p range over all odd primes such that $(d/p) = -1$. Then we let $L = \mathbf{Q}(d^{1/2}, (\delta(p) \cdot p)^{1/2})$, where $\delta(p) = (-1)^{(p-1)/2}$, and define for each such p the cyclic algebra:

$$A_{p,q_p} = (L/Q(d^{1/2}), a + b(d)^{1/2}), \tag{1.2}$$

where $a + b(d^{1/2})$ is an algebraic integer in K such that $a^2 - b^2d = rq_p$, and $(r/p) = 1$ where r is a suitably chosen prime. By Lemma 1.1, such a prime r exists.

If there exists more than one prime dividing d then for each such prime t, we define the cyclic algebra:

$$B_{t,s} = (\mathbf{Q}(d^{1/2}, s^{1/2})/\mathbf{Q}(d)^{1/2}, d^{1/2}), \tag{1.3}$$

where s is a prime chosen such that: (i) $(t/s) = -1$ (ii) $(u/s) = 1$ for all odd primes $u \neq t$ dividing d (iii) if $t = 2$ then $s \equiv 5 \pmod 8$ and if $t \neq 2$ then $s = 1 \pmod 8$.

Now we show that such a prime s exists. By Dirichlet's density theorem [3, Corollary 9-2-7, p. 168], there exist (infinitely many) primes w, y such

$(u/w) = 1$ for all primes $u \neq t$ dividing d. By the Chinese Remainder Theorem there is a solution to the equations: (1) $x \equiv w \pmod{u}$ for all odd primes $u \neq t$ dividing d, (2) $x \equiv 1 \pmod{8}$ for $u = 2 \neq t$, (3) (i) $x \equiv V \pmod{t}$ if $t \neq 2$; where $(V/t) = -1$ (ii) $x \equiv 5 \pmod{8}$ if $t = 2$. We let c be such a solution. Then by Dirichlet's theorem on primes in arithmetic progression [3, Corollary 9-2-8, p. 168] we have that there are infinitely many primes in the sequence $\{c + 8dn\}_{n \in Z}$. Any such prime s satisfies the required properties, and the assertion is proved.

We note that there are only finitely many algebras as in (1.3) since only finitely many ramified primes exist.

Furthermore, if 2 is inert in $\mathbf{Q}(d)^{1/2}$ then $d \equiv -3 \pmod{8}$, so that there is some prime u dividing d such that $u \equiv \pm 3 \pmod{8}$. For such a prime u we define the cyclic algebra:

$$C_{2,u} = (\mathbf{Q}(d^{1/2}, r^{1/2})/\mathbf{Q}(d^{1/2}), d^{1/2}), \tag{1.4}$$

where $r \equiv 3 \pmod{4}$ is a prime such that $(r/u) = -1$ and $(r/v) = 1$ for all $v \neq u$ dividing d.

To see that such a prime r exists, it is straightforward to carry out the same argument as given to show that s exists in (1.3) above.

Now we compute the invariants of the algebras given in (1.2) to (1.4) above.

LEMMA 1.5. (1) A_{p,q_p} (1.2) *have invariants* $\frac{1}{2}$ *at the K-prime above* p, *at the K-prime above* q_p, *and zero elsewhere.*

(2) $B_{t,u}$ (1.3) *have invariants* $\frac{1}{2}$ *at the K-prime above* t, *at the K-prime above* u *and zero elsewhere.*

(3) $C_{2,u}$ (1.4) *has invariants* $\frac{1}{2}$ *at the K-prime above* 2, *at the K-prime above* u *and zero elsewhere.*

(We note that the above algebras (1) to (3) are clearly in $U(K)$.)

Proof. (1) We let w be a rational prime. Thus $A_{p,q_p} \otimes_{\mathbf{Q}(d^{1/2})} \mathbf{Q}_w(d)^{1/2} \sim 1$ if and only if $a + b(d)^{1/2}$ is a norm in $\mathbf{Q}_w(d^{1/2}, (\delta(p) \cdot p)^{1/2})/\mathbf{Q}_w(d^{1/2})$ [1] and this holds if and only if $N(a + b(d^{1/2}))$ is a norm in $\mathbf{Q}_w((\delta(p) \cdot p)^{1/2})/\mathbf{Q}_w$, [3, Proposition 12.25, p. 221], where N denotes the norm in $\mathbf{Q}_w(d^{1/2})/\mathbf{Q}_w$.

We let w denote any finite prime of $\mathbf{Q}$ except p, r and q_p. Since $\delta(p) \cdot p \equiv 1 \pmod{4}$ the discriminant of $\mathbf{Q}((\delta(p) \cdot p)^{1/2})$ is p so $\mathbf{Q}_w((\delta(p) \cdot p)^{1/2})/\mathbf{Q}_w$ is unramified $(w \neq p)$. Since $(a + b(d^{1/2}))(a - b(d^{1/2})) = rq_p$ is a unit of $\mathbf{Q}_w$, ($w \neq r$ or q_p) then $N(a + b(d^{1/2}))$ is a unit of $\mathbf{Q}_w$ and hence a norm in the unramified extension $\mathbf{Q}_w((\delta(p) \cdot p)^{1/2})/\mathbf{Q}_w$ [5, Proposition 3.11, p. 153]. Consequently A_{p,q_p} splits at all finite primes $w \neq p, q_p, r$.

If w is the infinite prime then $\mathbf{Q}_w((\delta(p) \cdot p)^{1/2}) = \mathbf{R}$ or $\mathbf{C}$ depending on whether or not $\delta(p) = 1$. Now $\mathbf{Q}_w(d^{1/2}) = R = \mathbf{Q}_w$ so that $N(a + b(d)^{1/2}) = a + b(d)^{1/2}$, and by choice of $a + b(d)^{1/2}$ in Lemma 1.1, $a + b(d)^{1/2} > 0$ and $a - b(d)^{1/2} > 0$. Therefore, $N(a + b(d)^{1/2})$ is a norm in $\mathbf{Q}_w((\delta(p) \cdot p)^{1/2})/\mathbf{Q}_w$. Hence A_{p,q_p} is split at the infinite prime. It remains to check $w = p$, q_p and r.

For $w = r$ we have $(r/p) = 1$. Thus $(\delta(p) \cdot p/r) = 1$ by the quadratic reciprocity law. Therefore, $Q_r((\delta(p) \cdot p)^{1/2} = Q_r$ and so $N(a + b(d^{1/2}))$ is a norm in $Q_r((\delta(p) \cdot p)^{1/2})/Q_r$. Hence A_{p,q_p} is split at r.

If $w = p$ then $N(a + b(d)^{1/2}) = rq_p$ since p is inert in $\mathbf{Q}(d^{1/2})/\mathbf{Q}$. We have

$$(rq_p, \delta(p) \cdot p)_p = (r, \delta(p))_p (r, p)_p (q_p, \delta(p))_p (q_p, p)_p$$

by properties of the norm residue symbol [7, Proposition 2.5, p. 15]. Therefore

$$\begin{aligned}(rq_p, \delta(p) \cdot p)_p &= (r, p)_p (q_p, p)_p && \text{by [7, Proposition 2.5(5), p. 15],}\\ &= (r/p)(q_p/p) && \text{by [8, p. 251],}\\ &= (+1)(-1) = -1 && \text{by hypothesis.}\end{aligned}$$

Thus A_{p,q_p} is not split at p. It remains to check $w = q_p$.

But the index of A_{p,q_p} must divide $|\mathbf{Q}(d^{1/2}, (\delta(p) \cdot p)^{1/2}) : \mathbf{Q}(d^{1/2})| = 2$ [1]. Therefore A_{p,q_p} must have index equal to 2 at p. However, p is inert in $\mathbf{Q}(d^{1/2})$ since $(d/p) = -1$ by hypothesis [5, Lemma 9.5, p. 45]. Consequently by Hasse's Sum Theorem, A_{p,q_p} must be nonsplit at q_p as well. However, q_p, being ramified, has only one prime above it in K. Thus the index of A_{p,q_p} at q_p is 2 as required.

(2) For a rational prime w, we have $B_{t,u} \otimes_{\mathbf{Q}(d^{1/2})} \mathbf{Q}_w(d)^{1/2} \sim 1$ if and only if $N(d^{1/2})$ is a norm in $\mathbf{Q}_w(s^{1/2})/\mathbf{Q}_w$ [3, Proposition 12.25, p. 221] where N denotes the norm in $\mathbf{Q}_w(d^{1/2})/\mathbf{Q}_w$.

We let w, $w \nmid sd$ be a finite prime. Then $\mathbf{Q}_w(s^{1/2})/\mathbf{Q}_w$ is unramified, and $-d = (d)^{1/2} - (d)^{1/2}$ is a unit of $\mathbf{Q}_w$, so $N(d^{1/2})$ is a unit of $\mathbf{Q}_w$, hence a norm from $\mathbf{Q}_w(s^{1/2})$. Consequently $B_{t,u}$ splits at all finite primes except possibly s or those primes dividing d.

If w is the infinite prime then $\mathbf{Q}_w(d^{1/2}, s^{1/2}) = R = \mathbf{Q}_w$, so that $B_{t,u}$ splits at w.

For odd primes $w \neq t$ dividing d we have $(-d, s)_w = (w, s)_w = (s/w)$ if $w \neq 2$ by [7, Proposition 2.5, p. 15; 8, p. 249]. Thus

$$(-d, s)_w = (s/w) = 1 \qquad \text{by hypothesis.}$$

If $w = 2$, then $t \neq 2$. Thus $s \equiv 1 \pmod 8$ by hypothesis, and so $(w, s)_w = 1$.

Hence $B_{t,u}$ splits at all odd primes $w \neq t, u$ dividing d.

For $w = s$ we have

$$(-d, s)_w = (d/w),$$

by [7, Proposition 2.5, p. 15; 8, p. 251]. But $(d/w) = -1$ by hypothesis. Hence $B_{t,u}$ is not split at s. It remains to check for $w = t$.

But the index of $B_{t,s}$ must divide $|\mathbf{Q}(d^{1/2}, s^{1/2}) : \mathbf{Q}(d^{1/2})| = 2$, so $B_{t,s}$ has index 2 at s. Since there is exactly one prime above t, $B_{t,s}$ has invariants $\frac{1}{2}$ at t. Consequently, by Hasse's Sum Theorem, $B_{t,s}$ cannot have nonzero invariant at the one prime above the ramified K-prime t. Hence, $B_{t,s}$ has invariants $\frac{1}{2}$ at t and s and zero elsewhere.

(3) For any rational prime w, we have $C_{2,u} \otimes_{\mathbf{Q}(d^{1/2})} \mathbf{Q}_w(d^{1/2}) \sim 1$ if and only if $N(d^{1/2})$ is a norm in $\mathbf{Q}_w(r^{1/2})/\mathbf{Q}_w$ [3, Proposition 12.25, p. 221], where N denotes the norm in $\mathbf{Q}_w(d^{1/2})/\mathbf{Q}_w$.

For w infinite $\mathbf{Q}_w(d^{1/2}, r^{1/2}) = \mathbf{Q}_w(d^{1/2}) = R$ so that $C_{2,u}$ is split at w.

We let $w \nmid 2rd$ be a finite prime. $\mathbf{Q}_w(r^{1/2})/\mathbf{Q}_w$ is unramified ($w \neq 2, r$), so that $-d = (d)^{1/2} - (d)^{1/2}$ is a unit of $\mathbf{Q}_w$ hence a norm from $\mathbf{Q}_w(r^{1/2})$. Consequently, $C_{2,u}$ splits for all finite primes $w \nmid 2rd$.

For any odd $w \neq u$ dividing d we have $(-d, r)_w = (w, r)_w = (r/w) = 1$ using properties of the norm residue symbol [7, Proposition 2.5, p. 15; 8, p. 251], and where the last equality follows by hypothesis. Consequently, $C_{2,u}$ splits for all $w \neq 2, u, r$.

For $w = u$ we have

$$(-d, r)_u = (u, r)_u = (r/u) = -1$$

by properties of the norm residue symbol, and where the last equality follows from the selection of r in (1.4). Therefore $C_{2,u}$ is not split at u.

For $w = r$ we have

$$\begin{aligned} (-d, r)_r &= (-d/r) && \text{by [8, p. 251]}, \\ &= -(d/r) && \text{since } r \equiv 3 \pmod 4. \end{aligned}$$

Now we show that $(d/r) = -1$. Since $d \equiv -3 \pmod 8$ by the hypothesis of (1.4) then there are an even number of primes dividing d which are congruent to 3 modulo 4. But $u \equiv \pm 3 \pmod 8$. By hypothesis of (1.4), $r \equiv 3 \pmod 4$ and $(r/u) = -1$. Therefore $(u/r) = 1$ if $u \equiv 3 \pmod 8$ (respectively, $(u/r) = -1$ if $u \equiv -3 \pmod 8$). The number of primes $v \neq u$ dividing d such that $v \equiv 3 \pmod 4$ is odd when $u \equiv 3 \pmod 8$ (respectively, even if $u \equiv -3 \pmod 8$). For these primes v we have $(v/r) = -1$, since $(r/v) = 1$ by hypothesis. For the remaining primes $v \neq u$ dividing d we have $(v/r) = 1$. Hence, $(d/r) = -1$, as required. Therefore $(-d, r)_r = -(d/r) = 1$, and so $C_{2,u}$ is split at r.

It remains to check for $w = 2$. The index of $C_{2,u}$ must divide $|\mathbf{Q}(d^{1/2}, r^{1/2}) : \mathbf{Q}(d^{1/2})| = 2$ so that the index of $C_{2,u}$ at the one prime above the ramified prime u is 2. Since there is only one K-prime above 2, being inert by hypothesis, then Hasse's Sum Theorem yields that the index of $C_{2,u}$ at the K-prime above 2 must be 2. Q.E.D.

THEOREM 1.6. *Generators of* $U(K)$ *for the real quadratic field* $K = \mathbf{Q}(d^{1/2})$ *are*

(1) A_{p,q_p} *where* p *ranges over all primes such that* $(d/p) = -1$, *as given in* (1.2).

(2) $B_{t,u}$, *provided there is more than one odd prime dividing* d, *as given in* (1.3).

(3) $C_{2,u}$, *provided* 2 *is inert in* K, *as given in* (1.4).

(4) *Generators of* $S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$.

Proof. We let $[A]$ in $U(K)$ have nonzero invariants at primes in $S = \{p_1, \ldots, p_n\}$. By the definition of uniform distribution [6, p. 1] the maximum p_i-local index is 2.

For any odd $p_i \in S$ such that $(d/p_i) = 1$, i.e., p_i is completely split in K [5, Lemma 9.5, p. 45]; choose $[B_i]$ in $S(\mathbf{Q})$ with invariant $\frac{1}{2}$ at p_i and q, where q is any prime dividing d. $[B_i \otimes_{\mathbf{Q}} K]$ has nonzero invariants only at primes above p_i, and zero elsewhere (i.e., has invariant $\frac{1}{2}$ at each of the two K-primes above p_i, and zero elsewhere). Choose a similar B_i if p_i is the infinite prime. For the remaining primes of S which are either inert or ramified in K we may choose the proper combination of A_{p,q_p}, $B_{t,u}$, and $C_{2,u}$ required. Taking the product of the above algebras yields an algebra class equal to $[A]$ in $U(K)$. Q.E.D.

2. OTHER REAL FIELDS

If $K/\mathbf{Q}$ is finite abelian and K is a real field then $U(K)_2 = U(K)$ by the definition of uniform distribution [6, p. 1]. The question remains as to the relationship between $S(K) = S(K)_2$ and $U(K) = U(K)_2$ when K is a real field other than quadratic. Yamada [11] has shown that for real subfields K of $\mathbf{Q}(\epsilon_{p^n})$ where p is a prime we have $S(K) = U(K)$. Moreover, Yamada [14] has determined $S(K)$ where K is a real subfield of $\mathbf{Q}(\epsilon_n)$ and $\mathbf{Q}(\epsilon_n)/K$ is cyclic, for any integer n, where $\mathbf{Q}(\epsilon_n)$ is the smallest cyclotomic field containing K.

THEOREM 2.1. *If the real field K is contained in* $\mathbf{Q}(\epsilon_n)$, *where* $\mathbf{Q}(\epsilon_n)/K$ *is cyclic,* $n \not\equiv 2 \pmod 4$ *and n is divisible by at least two distinct primes then the index of $S(K)$ in $U(K)$ is infinite.*

Proof. We let $n = 2^a \prod_i p_i^{a_i}$, where a_i are integers and $a \neq 1$, p_i distinct odd primes. Choose $\sigma \in \mathrm{Gal}(\mathbf{Q}(\epsilon_n)/\mathbf{Q})$ such that $\sigma(\epsilon_{p_1^{a_1}}) = \epsilon_{p_1^{a_1}}^{-1}$ and $\sigma(\epsilon_{n/p_1^{a_1}}) = \epsilon_{n/p_1^{a_1}}$. σ restricts nontrivially to $\mathrm{Gal}(\mathbf{Q}(\epsilon_n + \epsilon_n^{-1})/\mathbf{Q})$ since otherwise $\sigma(\epsilon_n) = \epsilon_n^{-1}$, which is false.

By Dirichlet's density theorem there are infinitely many primes p with σ as Frobenius automorphism. Now, we show that there are not any elements in $S(K)$ with nonzero invariant at any such p. Yamada [14] has proved that if the following conditions are satisfied then the invariant of any element of $S(K)$ at p must be zero

(1) $p \nmid n$.

(2) $2 \mid f_p$, where f_p is the inertial degree of p in K/Q.

(3) $|f_p{}^1|_2 < |\mathbf{Q}(\epsilon_n) : K|$, where $f_p{}^1$ is the inertial degree of p in $\mathbf{Q}(\epsilon_n)/K$ and $|m|_2$ denotes the 2-part of the integer m.

(4) If $a > 0$ then $p^{f^*/2} \equiv \pm 1 \pmod{2^a}$, where f^* is the smallest positive integer with $p^{f^*} \equiv 1 \pmod n$, i.e., the inertial degree of p in $\mathbf{Q}(\epsilon_n)/\mathbf{Q}$ [3, Theorem 6.2.15, p. 103].

We now show that these conditions are satisfied by p. (1) is clearly satisfied. To show that (2) holds we recall that σ restricts nontrivially to $\mathbf{Q}(\epsilon_n + \epsilon_n^{-1})$. Therefore, since $\mathrm{Gal}(\mathbf{Q}(\epsilon_n)/K)$ is cyclic then $\sigma \notin \mathrm{Gal}(\mathbf{Q}(\epsilon_n)/K)$; i.e., σ restricts nontrivially to K, so that (2) holds. Now $f_p{}^1 = 1$ since $\sigma \notin G(\mathbf{Q}(\epsilon_n)/K)$ so that (3) holds. Also σ fixes $\mathbf{Q}(\epsilon_{2^a})$ so that if $a > 0$ then $p \equiv 1 \pmod{2^a}$ [3, Theorem 6.2.15, p. 103]. Therefore (4) is satisfied.

We have shown that there is no element in $S(K)$ with nonzero invariant at any such p above.

Now we arrange these infinitely many primes in distinct pairs $\{\lambda\}$. We define $[A_\lambda]$ in $U(K)$ by requiring that A_λ have invariants at the pair of distinct primes p in λ, and zero elsewhere. We have by Hasse's Sum Theorem that such algebras A_λ exist and they are clearly in $U(K)$. Moreover, $[A_\lambda] \cdot [A_{\lambda^1}]^{-1}$ is not in $S(K)$ for all such $[A_\lambda] \neq [A_{\lambda^1}]$ defined above. Thus, such algebras form an infinite number of coset representatives of $S(K)$ in $U(K)$. Q.E.D.

We note that a special case of the above theorem is for $K = \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})$. Now, in order to determine the index of $S(K)$ in $U(K)$ for a real field of even degree not covered by the above theorem we prove a result which will lead to a partial answer. The following theorem is interesting in its own right in that it is the exact analog of Yamada's result on real quadratic fields [13].

THEOREM 2.2. *Let* $K = \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})$, *where n is odd and divisible by at least two distinct primes. Then*

$$S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$$

if and only if there is a prime q dividing n such that $q \equiv 3 \pmod 4$.

Proof. First we assume that n is divisible by a prime $q \equiv 3 \pmod 4$. We let $[A]$ in $S(K)$ have nonzero invariants at the primes in $S = \{p_1, \ldots, p_s\}$. There are no ramified primes in S by [14] so $p_i \nmid n$ for each i.

We let $p_i = p$ be arbitrary in S. We define $[B]$ in $S(\mathbf{Q})$ to have nonzero invariants $\frac{1}{2}$ at p and at some other prime r with even inertial degree in $K/\mathbf{Q}$, and zero invariant elsewhere. Such an r exists, since by hypothesis, at least two distinct odd primes divide n so that $|K : \mathbf{Q}|$ is even.

Now we show $[B \otimes_{\mathbf{Q}} K]$ in $S(K)$ has invariant $\frac{1}{2}$ exactly at the K-primes above p.

If $\mathscr{R}$ lies over r in $K/\mathbf{Q}$ then

$$\mathrm{inv}_{\mathscr{R}}(B \otimes_{\mathbf{Q}} K) \equiv |K_{\mathscr{R}} : \mathbf{Q}_r| \, \mathrm{inv}_q(B) \pmod 1,$$

by formulas in [2, Chap. 7]. But $|K_{\mathscr{R}} : \mathbf{Q}_r|$ is even, so that

$$\mathrm{inv}_{\mathscr{R}}(B \otimes_{\mathbf{Q}} K) \equiv 0 \pmod 1.$$

It remains to show that $B \otimes_{\mathbf{Q}} K$ is not split at the K-primes above p.

Case 1. p is infinite.

Since $K/\mathbf{Q}$ is real then p splits completely in K. Thus; $B \otimes_{\mathbf{Q}} K$ has invariant $\frac{1}{2}$ exactly at the infinite K-primes.

In the following cases we assume p is finite unramified. We let f be the least integer such that $p^f \equiv 1 \pmod n$, i.e., the inertial degree of p in $\mathbf{Q}(\epsilon_n)/\mathbf{Q}$ [3, Theorem 6.2.15, p. 103].

Case 2. f is odd.

Thus, if $\mathscr{P}$ is a K-prime lying over p we have $|K_{\mathscr{P}} : \mathbf{Q}_p|$ is odd so that

$$\begin{aligned}\mathrm{inv}_{\mathscr{P}}(B \otimes_{\mathbf{Q}} K) &\equiv |K_{\mathscr{P}} : \mathbf{Q}_p| \, \mathrm{inv}_p(B) \pmod 1\\ &\equiv \mathrm{inv}_p(B) \equiv \tfrac{1}{2} \pmod 1.\end{aligned}$$

Thus $B \otimes_{\mathbf{Q}} K$ has invariants $\frac{1}{2}$ exactly at the K-primes above p.

Case 3. f is even.

Therefore, by Yamada [14] $p^{f/2} \equiv -1 \pmod{n}$. Therefore $p^{f/2} \equiv -1 \pmod{q}$ where $q \equiv 3 \pmod{4}$. So that $f/2$ is odd since -1 is not a square mod q. Now we note that by Yamada [14] p is inert in $\mathbf{Q}(\epsilon_n)/K$. Thus $| K_{\mathscr{P}} : \mathbf{Q}_p | = f/2$ is odd. We have

$$\mathrm{inv}_{\mathscr{P}}(B \otimes_{\mathbf{Q}} K) \equiv | K_{\mathscr{P}} : \mathbf{Q}_p | \, \mathrm{inv}_p(B) \equiv \mathrm{inv}_p(B) \equiv \tfrac{1}{2} \pmod{1}.$$

Therefore $B \otimes_{\mathbf{Q}} K$ has invariants $\frac{1}{2}$ exactly at the K-primes above p.

Hence, by taking $[B \otimes_{\mathbf{Q}} K]$ for each p in S we get $[A] = \prod [B \otimes_{\mathbf{Q}} K]$, which yields $S(K) \subseteq S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$. But $S(K) \supseteq S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$ so that $S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$.

Conversely, we assume $S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$. We assume there does not exist a prime $q \equiv 3 \pmod{4}$ such that q divides n. Thus $-1 \equiv a_i^2 \pmod{q_i^{\alpha_i}}$, for some integer a_i, where $n = \prod_i q_i^{\alpha_i}$. We let p be a rational prime such that $p \equiv a_i \pmod{q_i^{\alpha_i}}$ for each i. Such a prime p is obtained by using the Chinese Remainder Theorem to solve the equations $c \equiv a_i \pmod{q_i^{\alpha_i}}$ for c. Then choose a prime p in the sequence $c + m \prod_i q_i^{\alpha_i}$, $m = 1, 2, \ldots$ by using Dirichlet's theorem on primes in arithmetic progression [3, Corollary 9.2.8, p. 168]. So $p^2 \equiv -1 \pmod{n}$. Therefore, by Yamada [14], there is an $[A] \in S(K)$ such that $\mathrm{inv}_{\mathscr{P}}(A) \neq 0$ for a K-prime $\mathscr{P}$ above p. But $S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$. Thus

$$\begin{aligned} \mathrm{inv}_{\mathscr{P}}(A) &= \mathrm{inv}_{\mathscr{P}}(B \otimes_{\mathbf{Q}} K), \qquad \text{for} \quad [B] \in S(\mathbf{Q}) \\ &\equiv | K_{\mathscr{P}} : \mathbf{Q}_p | \, \mathrm{inv}_p(B) \pmod{1}. \end{aligned}$$

But by Yamada [14], $p^2 \equiv -1 \pmod{n}$ implies p is inert in $\mathbf{Q}(\epsilon_n)/K$. Thus $| K_{\mathscr{P}} : \mathbf{Q}_p | = 2$, so $\mathrm{inv}_p(A) = 0$, a contradiction. Hence n is divisible by a prime $q \equiv 3 \pmod{4}$. Q.E.D.

Yamada [11] has shown that for any real subfield K of $\mathbf{Q}(\epsilon_{p^n})$, p a prime, we have $U(K) = S(K)$. Therefore the condition in Theorem 2.2 does not apply to all maximal real subfields. In fact, it is easy to check using Yamada [11] that $S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$ where $K = \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})$ and $n = 4n_1$, where n_1 is odd. If n_1 is even it is easy to check that $S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$ is properly contained in $S(K)$.

COROLLARY 2.3. *If $K/\mathbf{Q}$ is real of even degree and K is in $\mathbf{Q}(\epsilon_n)$ where n is odd and divisible by at least two distinct primes, and no prime congruent to* 1 *modulo* 4 *divides n then*

$$S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K.$$

Proof. If $[A]$ is in $S(K)$ then A has zero invariant at any prime divisor q of n since $\mathrm{ind}_q(A)$ divides the odd integer $(q - 1)/2$ by Yamada [9, Theorem 4.4, p. 43; 10].

Now we consider $q \nmid n$; i.e., q is unramified. If q has even inertial degree in $K/\mathbf{Q}$ then q must have odd inertial degree in $\mathbf{Q}(\epsilon_n)/K$ since $\operatorname{Gal}(\mathbf{Q}(\epsilon_n)/\mathbf{Q})$ has no element of order 4. Therefore, if some $[A]$ in $S(K)$ has $\operatorname{ind}_q(A) = 2$ for some prime q, then $| \mathbf{Q}_q(\epsilon_n + \epsilon_n^{-1}) : K_{\mathscr{Q}^1} |$ is odd where $\mathscr{Q}^1$ is a K-prime above q. But we have $S(\mathbf{Q}(\epsilon_n + \epsilon_n^{-1})) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})$ by the theorem. Therefore

$$\operatorname{inv}_{\mathscr{Q}}(A \otimes_K \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})) = \operatorname{inv}_{\mathscr{Q}}(B \otimes_{\mathbf{Q}} \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})),$$

where $[B]$ is in $S(\mathbf{Q})$. Thus $A \otimes_K \mathbf{Q}(\epsilon_n + \epsilon_n^{-1})$ in $S(\mathbf{Q}(\epsilon_n + \epsilon_n^{-1}))$ has nonzero invariant at q which has even inertial degree in $K/\mathbf{Q}$. But $S(\mathbf{Q}(\epsilon_n + \epsilon_n^{-1})) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$ yields a contradiction. Therefore there does not exist any element in $S(K)$ with nonzero invariant at any prime with even inertial degree in $K/\mathbf{Q}$.

Hence for any $[A] \in S(K)$ with nonzero invariants at primes in $T = \{p_1, \ldots, p_t\}$ we choose $[B] \in S(\mathbf{Q})$ with nonzero invariants at the primes in T, and if the number of primes in T is odd, then also at some prime with even inertial degree in $K/\mathbf{Q}$. $[B \otimes_{\mathbf{Q}} K]$ then has nonzero invariants $\frac{1}{2}$ only at the primes in S. Hence $[A] = [B \otimes_{\mathbf{Q}} K]$. Therefore $S(K) \subseteq S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$, and clearly $S(\mathbf{Q}) \otimes_{\mathbf{Q}} K \subseteq S(K)$ so that $S(K) = S(\mathbf{Q}) \otimes_{\mathbf{Q}} K$. Q.E.D.

We note that a special case of the above corollary is Yamada's result for real quadratic fields subjected to the restriction on n as in the corollary.

COROLLARY 2.4. *For K as in Corollary 2.3, $| U(K) : S(K)|$ is infinite.*

Proof. Choose a prime p_i with even inertial degree in $K/\mathbf{Q}$; then define $[A_i]$ in $U(K)$ with invariant $\frac{1}{2}$ at the primes of K above two of the chosen primes p_i. By Hasse's Sum Theorem $[A_i]$'s exist and are clearly in $U(K)$. By Dirichlet's density theorem [3, Corollary 9.2.7, p. 168] there are infinitely many such primes p_i, hence infinitely many algebras $[A_i]$. Clearly $[A_i]$ is not in $S(\mathbf{Q}) \otimes_{\mathbf{Q}} K = S(K)$ since A_i is defined at a prime with even inertial degree in $K/\mathbf{Q}$. Moreover, $[A_i] \cdot [A_j]^{-1}$ is not in $S(K)$ by the same argument. Thus the $[A_i]$ provide infinitely many coset representatives of $S(K)$ in $U(K)$. Q.E.D.

REFERENCES

1. A. A. ALBERT, "Structure of Algebras," Amer. Math. Soc., Providence, R.I., 1961.
2. M. DEURING, "Algebren," Springer, Berlin, 1935.
3. L. J. GOLDSTEIN, "Analytic Number Theory," Prentice-Hall, Englewood Cliffs, N.J., 1971.
4. I. N. HERSTEIN, "Noncommutative Rings," Carus Monograph 15, Math. Amer. Assoc., Washington, D.C., 1968.

5. G. J. JANUSZ, "Algebraic Number Fields," Academic Press, New York, 1973.
6. R. MOLLIN, "Algebras with Uniformly Distributed Invariants," Queen's Mathematical Preprints, No. 1975-9; *J. Algebra* (to appear).
7. R. MOLLIN, "Uniform Distribution and the Schur Subgroup," Queen's Mathematical Preprints, No. 1975-16; *J. Algebra* (to appear).
8. E. WEISS, "Algebraic Number Theory," McGraw–Hill, New York, 1963.
9. T. YAMADA, "The Schur subgroup of the Brauer Group," Lecture Notes in Mathematics, No. 397, Springer–Verlag, Berlin/New York, 1974.
10. T. YAMADA, Characterization of the simple components of the group algebras over the p-adic number field, *J. Math. Soc. Japan* **23** (1971), 295–310.
11. T. YAMADA, The Schur subgroup of the Brauer group, I, *J. Algebra* **27** (1973), 579–589.
12. T. YAMADA, The Schur subgroup of a real quadratic field, I, "Symposia Mathematica" (Proceedings of the Conference on Structure of Algebraic Fields, INDAM, Rome, April 5–10, 1973), Academic Press, London, to appear.
13. T. YAMADA, The Schur subgroup of a real quadratic field, II, *J. Algebra* (to appear.
14. T. YAMADA, The Shur subgroup of a real cyclotomic field, *Math. Z.* **139** (1974), 35–44.