

Uniform Distribution and the Schur Subgroup

RICHARD MOLLIN

Queen's University, Kingston, Ontario, Canada K7L 3N6

Communicated by I. N. Herstein

Received May 12, 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, undertaken in [9]. The notation is the same as in [9].

In the first section we investigate the index $|U(K)_q : S(K)_q|$ where q is an odd prime. We obtain [9, Theorem 2.7] as a special case of Theorem 1.2, wherein we obtain that the above index is infinite when $q \mid |K : Q(\epsilon_{q^a})|$, where ϵ_{q^a} is the highest q -power root of unity in K , $a > 0$ provided $q^{a+b} \nmid |L : K|$, where L is the smallest root of unity field containing K , and $\epsilon_{q^{a+b}}$ is the highest q -power root of unity in L .

In the case where $a^{a+b} \mid |L : K|$, the author's conjecture made in [9] is validated.

In Section 2, we show that $|U(K)_2 : S(K)_2|$ is infinite where K/Q is finite, imaginary, and abelian. As an illustration of this result we calculate generators of $U(Q(\epsilon_{p^n}))_2$ for primes $p \not\equiv 1 \pmod{4}$ explicitly.

1. THE INDEX QUESTION

We let K/Q be finite abelian and fix some additional notation from [6].

$L = Q(\epsilon_m)$ = the least root of unity field containing K .

$W = W(L)_q$ = group of roots of unity of q -power order in L .

q^a = order of $W(K)_q$.

q^{a+b} = order of $W(L)_q$.

p = prime not dividing m .

$G = \text{Gal}(L/K)$ identified with $\text{Gal}(L(\epsilon_p)/K(\epsilon_p))$.

$\langle \tau \rangle = \text{Gal}(L(\epsilon_p)/L)$.

$$Gx\langle\tau\rangle = \text{Gal}(L(\epsilon_p)/K).$$

$\sigma =$ element of G which satisfies $\sigma(w) = w^{1+p^a}$ for all w in W .

$C_1 =$ subgroup of G fixing W .

$C_1^{q^d} =$ subgroup of C_1 consisting of all q^d th powers of elements in C_1 .
 (By the phrase "the order of γ in $C_1/C_1^{q^d}$ ", we shall mean the order of the coset $\gamma C_1^{q^d}$ in the group $C_1/C_1^{q^d}$).

$r =$ prime dividing mp for which q divides $e(L(\epsilon_p)/K, r)$, ramification index.

$\rho = K$ -prime above r .

$\theta = \theta(r)$ a generator of the inertia group of ρ in $Gx\langle\tau\rangle$.

$\varnothing = \varnothing(r)$ Frobenius automorphism of ρ in $Gx\langle\tau\rangle$.

$\varnothing = \sigma^{k(r)}\xi_r\tau^{n(r)}$; $0 \leq k(r) < q^b$, $\xi_r \in C_1$, $0 \leq n(r) < p - 1$.

$f(r) = f(K/Q, r) =$ inertial degree of ρ over r .

$e(r) =$ order of θ .

$q^h =$ the power of q dividing $e(r)$.

$q^g =$ the power of q dividing $r^{f(r)} - 1$.

$v(r) = \max\{0, a + h - g\}$.

$V(t) = [(1 + p^a)^t - 1]/p^a$.

$Z(p) = [(p^{f(r)} - 1)/q^a] - V(k(p))$.

$X(p) =$ integer which satisfies $X(p) V(q^b) \equiv Z(p) \pmod{q^{a+b}}$.

$\mathcal{N}_0(p) = \sigma^{-a^b+v}\xi_p$.

$N(p) =$ order of $\mathcal{N}(p)$ in the group $C_1/C_1^{q^d}$ where $q^d = \text{gcd}(q^a, p - 1)$.

$S(L/K) =$ subgroup of $S(K)$ consisting of algebra classes split by L .

THEOREM 1.1 (J. Janusz [6]). *The maximum p -local index of an element in $S(K)_q$ is $\max\{q^{v(r)}, N(p)\}$, where p does not divide m .*

Now we use Theorem 1.1 to investigate $|U(K)_q : S(K)_q|$ when

$$q \mid \mid K : Q(\epsilon_{q^a}) \mid \quad \text{and} \quad q^{a+b} \nmid \mid L : K \mid.$$

We note that [9, Theorem 2.7, p. 17] is included as a case of the following theorem.

THEOREM 1.2. *If K/Q is finite abelian, q divides $|K : Q(\epsilon_{q^a})|$, $a > 0$ and $q^{a+b} \nmid \mid L : K \mid$, then $|U(K)_q : S(K)_q|$ is infinite.*

Proof. We begin by finding suitable primes p and using Theorem 1.1 to show there are no elements $[A]$ in $S(K)_q$ with $\text{ind}_p(A) = q^a$.

Case 1. $b > 0$. We first obtain the result for the case where G is of q -power order.

We choose a generator α of $\text{Gal}(L/Q(\epsilon_{m'}))$ where $m' = m/q^b$ satisfying $\alpha: \epsilon_{q^{a+b}} \rightarrow \epsilon_{q^{a+b}}^{1+q^a}$. We let α be the Frobenius automorphism in L/Q corresponding to some prime p . The order of α is q^b . Now we show that $\nu(p) < a$. First we need to show that $f(p) = q^b$.

For $0 \leq s \leq b$, the fixed field of α^{q^s} is $Q(\epsilon_{m''})$ where $m'' = m/q^{b-s}$. Thus if $\alpha^{q^s} \in \text{Gal}(L/K)$ then $K \subseteq Q(\epsilon_{m''})$ in which case, $s = b$. Therefore $f(p) = q^b$ as asserted. We have that $p \equiv 1 \pmod{q^a}$ and $p \not\equiv 1 \pmod{q^{a+1}}$, which implies that $h = a$. Also $p^{f(p)} \equiv 1 \pmod{q^{a+b}}$. Therefore $g = a + b$. Now: $a + h - g = a + a - a - b = a - b$. It follows that $\nu(p) < a$, since $b > 0$.

Now we proceed to show $N(p) < q^a$. Since α restricted to K has order q^b and the order of α is q^b then σ , the Frobenius automorphism of \mathcal{P} in G , is trivial. It follows that $\xi_p = 1 = \sigma^{k(p)}$. Hence $\mathcal{N}(p) = \sigma^{-q^b X(p)}$. However $q^{a+b} \nmid L : K$ by hypotheses, so that $\mathcal{N}(p)^{q^{a-1}} = 1$, since G is of q -power order. Clearly then $\mathcal{N}(p)^{q^{a-1}} \in C_1^{q^a}$, which implies that $N(p) < q^a$, as required.

Hence by Theorem 1.1, the maximum p -local index of an element in $S(K)_q$ is $\max\{q^{\nu(p)}, N(p)\} < q^a$. Therefore there are no elements $[A]$ in $S(K)_q$ with $\text{ind}_p(A) = q^a$.

Now we prove the result for arbitrary G . We let G_q denote the Sylow q -subgroup of G and let F denote the fixed field of G_q . Then there is an element α in G_q such that $\alpha: \epsilon_{q^{a+b}} \rightarrow \epsilon_{q^{a+b}}^{1+q^a}$. We let α be the Frobenius automorphism corresponding to p , say. If there is $[A] \in S(K)$ with $\text{ind}_p(A) = q^a$ then $[A \otimes_K F] \in S(F)$. However, $|F : K|$ is relatively prime to q . Therefore, $\text{ind}_p(A \otimes_K F) = q^a$, a contradiction by the case previously covered.

We have shown that for $b > 0$ there are no elements of $S(K)$ with $\text{ind}_p(A) = q^a$.

Case 2. $b = 0$.

Choose any element \mathcal{B} of q -power order in $\text{Gal}(L/Q(\epsilon_{q^a}))$ such that \mathcal{B} restricts nontrivially to K . Such an element exists since $q \mid |K : Q(\epsilon_{q^a})|$.

By the Dirichlet density theorem [5, Corollary 9-2-7, p. 168], \mathcal{B} is the Frobenius automorphism in L/Q of infinitely many primes p .

J. Janusz [8] has shown that for $b = 0$, we have:

$$S(K)_q = \{S(Q(\epsilon_{q^a})) \otimes_{Q(\epsilon_{q^a})} K\} S(L/K)_q.$$

If there is an $[A]$ in $S(K)_q$ with $\text{ind}_p(A) = q^a$ then we have by Janusz' result that:

$$[A] = [B \otimes_{Q(\epsilon_{q^a})} K] \cdot [C],$$

where $[B] \in S(Q(\epsilon_{q^a}))_q$ and $[C] \in S(L/K)_q$. Thus, if \mathcal{P} is a K -prime above the $Q(\epsilon_{q^a})$ -prime \mathfrak{p} and if \mathfrak{p} lies above p in Q then:

$$\begin{aligned} \text{inv}_{\mathcal{P}}(A) &\equiv \text{inv}_{\mathcal{P}}(B \otimes_{Q(\epsilon_{q^a})} K) + \text{inv}_{\mathcal{P}}(C) \pmod{1} \\ &\equiv |K_{\mathcal{P}} : Q_{\mathfrak{p}}(\epsilon_{q^a})| \text{inv}_{\mathfrak{p}}(B) + \text{inv}_{\mathcal{P}}(C) \pmod{1} \end{aligned}$$

by [3, Chap. 7]. But $q \mid |K_{\mathcal{P}} : Q_{\mathfrak{p}}(\epsilon_{q^a})|$ by choice of p and $\text{ind}_{\mathfrak{p}}(B) \leq q^a$, by [9, Corollary 1.2, p. 5]. Thus $\text{ind}_{\mathfrak{p}}(B \otimes_{Q(\epsilon_{q^a})} K) < q^a$. Therefore; $\text{ind}_{\mathfrak{p}}(C) = q^a$ since $\text{ind}_{\mathfrak{p}}(A) = q^a$. However, L splits C . Therefore, if \mathcal{P}' is an L -prime above \mathcal{P} :

$$\text{inv}_{\mathcal{P}'}(C \otimes_K L) \equiv |L_{\mathcal{P}'} : K_{\mathcal{P}}| \text{inv}_{\mathcal{P}}(C) \pmod{1}.$$

It follows that $q^a \mid |L : K|$. This is a contradiction, since we assumed $q^{a+b} \nmid |L : K|$, and $b = 0$. Hence for $b = 0$ there are no elements $[A]$ in $S(K)$ with $\text{ind}_{\mathfrak{p}}(A) = q^a$. This completes Case 2.

We have shown that whenever $q \mid |K : Q(\epsilon_{q^a})|$ and $q^{a+b} \nmid |L : K|$, it is possible to find primes p such that there are no elements of $S(K)_q$ with $\text{ind}_{\mathfrak{p}}(A) = q^a$. We note that for each such p there is an $[A_p]$ in $U(K)$ with $\text{ind}_{\mathfrak{p}}(A_p) = q^a$ and $\text{ind}_{\mathfrak{r}}(A_p) = 1$ for $r \neq p$ by [9, Theorem 1.3, p. 5]. Moreover, by Dirichlet's density theorem [5, Corollary 9-2-7, p. 168] there are infinitely many such primes p . Thus there are infinitely many such $[A_p]$ in $U(K) - S(K)$. Moreover, $[A_p] \cdot [A_{p'}]^{-1} \notin S(K)$ for $p \neq p'$. Therefore the $[A_p]$'s provide an infinite number of coset representatives of $S(K)$ in $U(K)$.
Q.E.D.

Now we consider the case where $q^{a+b} \mid |L : K|$, $a > 0$ and $q \mid |K : Q(\epsilon_{q^a})|$. The following example validates the conjecture made by the author in [9, p. 19], to the effect that $q \mid |K : Q(\epsilon_{q^a})|$ is not a sufficient condition for $|U(K) : S(K)|_q$ to be infinite. In fact, the following is an example where $q \mid |K : Q(\epsilon_{q^a})|$ and $U(K)_q = S(K)_q$.

We let $L = Q(\epsilon_{3,19})$; $q = 3$. We let $\langle \sigma \rangle = \text{Gal}(L/Q(\epsilon_3))$ and let K be the fixed field of $\langle \sigma^a \rangle$. Thus, $a = 1$, $b = 0$, and $|L : K| = 3$ so that $q^{a+b} \mid |L : K|$, as required.

First we proceed to show that given any odd prime $p \equiv 1 \pmod{3}$, $p \neq 19$, then $\max\{3^{\nu(p)}, N(p)\} = 3$.

The list of notations given at the beginning of the section is in force.

Case 1. $f(p)$ is not divisible by 3.

It is easy to check that $\nu(p) = 1$ and $N(p) = 1$ or 3. Therefore, $\max\{3^{\nu(p)}, N(p)\} = 3$.

Case 2. $f(p)$ is divisible by 3.

Since $p \equiv 1 \pmod{3}$ then $X(p) \equiv Z(p) \equiv 0 \pmod{3}$. Hence $\mathcal{N}(p) = \xi_p$. However, since $\text{Gal}(L/Q(\epsilon_3))$ is cyclic and $f(p)$ is divisible by 3 then $\langle \phi(p) \rangle = \text{Gal}(L/K)$; so that $\langle \phi(p) \rangle = \langle \xi_p \rangle$. Now, $C_1 = \text{Gal}(L/K)$ and $C_1^3 = 1$ so that $N(p) = 3$.

It is easy to check that $\nu(p) = 0$ in this case. Hence, we have that $\max\{3^{\nu(p)}, N(p)\} = 3 \dots^*$.

Now the proof of Theorem 1.1 given in [6] shows the $\max\{3^{\nu(p)}, N(p)\}$ is attained by some element in $S(K)_3$. Thus there is an element $[A]$ of $S(K)$ with $\text{ind}_p(A) = 3$, for each $p \equiv 1 \pmod{3}$, $p \neq 19$.

Now we show that for $p = 19$, $*$ holds. First we need some notation and a result taken from [6].

If r is a prime dividing m such that $e(r)$ is divisible by q then: $N_1(r) =$ maximum order of the elements $\psi(\theta, \sigma^{-p^b x(r)} \xi_r)$ as ψ ranges over all skew pairings of $C \times C_1$ into $W(K)_q$. (For the definition of skew pairings see [6]. For the purpose of this paper knowledge of the concept is not necessary). $N_2(r) =$ the order of θ' in C_1/C_1^q with $\theta = \theta(r)$ and $f = f(K/Q, r)$.

THEOREM 1.3 (J. Janusz [6]). *The maximum r -local index of any element in $S(K)_q$ is the number $\max\{q^{\nu(r)}, N_1(r), N_2(r)\}$.*

In [6] it is shown that each of $q^{\nu(r)}, N_1(r)$ is attained by some element of $S(K)_q$. We need only show then, for $r = 19$ that $\max\{3^{\nu(19)}, N_1(19), N_2(19)\} = 3$. However, the order of θ' in C_1/C_1^3 is 3 since $f = f(K/Q, 19) = 1$, $C_1 = G = \langle \theta \rangle$ and $C_1^3 = 1$. In other words, $N_2(19) = 3$, as required.

Hence we have shown that, given any prime $p \equiv 1 \pmod{3}$ there is an element $[A] \in S(K)_3$ such that $\text{ind}_p(A) = 3$. By [9, Theorem 1.1, p. 4] and [9, Corollary 1.2, p. 5] if $[A] \in U(K)_3$ with $\text{ind}_p(A) > 1$, then $p \equiv 1 \pmod{3}$, and $\text{ind}_p(A) \leq 3$. It follows that $S(K)_3 = U(K)_3$. This completes the example.

This example not only validates the aforementioned conjecture but also shows that $q \nmid |K : Q(\epsilon_{q^a})|$ is not a necessary condition for $U(K)_q = S(K)_q$. We showed in [9, Corollary 2.6, p. 16] that it is a sufficient condition.

We note that in the case where $q^{a+b} \mid |L : K|$ and $q \mid |K : Q(\epsilon_{q^a})|$ with $a > 0$ then it is also possible that $|U(K)_q : S(K)_q|$ is infinite. For example; we let $L = Q(\epsilon_{3 \cdot 13 \cdot 3})$, $\text{Gal}(L/Q(\epsilon_{3 \cdot 7})) = \langle \sigma_{13} \rangle$ and $\text{Gal}(L/Q(\epsilon_{3 \cdot 13})) = \langle \sigma_7 \rangle$. Then if K is the fixed field of $\langle \sigma_7^3 \cdot \sigma_{13}^4 \rangle$ we get $|L : K| = 6$, $a = 1$, $b = 0$ and $|K : Q(\epsilon_3)| = 12$. Thus for $q^a = 3$ we get $q^{a+b} \mid |L : K|$ and $q \mid |K : Q(\epsilon_{q^a})|$. It is straightforward to check that $|U(K) : S(K)|$ is infinite using the result of J. Janusz [8] that:

$$S(K)_q = \{S(Q(\epsilon_{q^a}))_q \otimes_{Q(\epsilon_{q^a})} K\} S(L/K)_q.$$

2. $U(K)$ FOR AN IMAGINARY FIELD, K

Let K/Q be finite abelian. Throughout this section K is assumed to be imaginary. We shall mean *finite* prime when referring to the primes in this section, since for any $[A]$ in the Brauer group of an imaginary Galois extension of Q , A necessarily splits at the infinite primes.

In this section we investigate the relationship between the 2-primary part $S(K)_2$ of $S(K)$, and the 2-primary part $U(K)_2$ of $U(K)$. The relationship between $S(K)_p$ and $U(K)_p$ was investigated for certain fields in Section 1 and in [9].

From the first theorem we get that $S(K)_2$ is of infinite index in $U(K)_2$. We illustrate this result by calculating the generators of $U(Q(\epsilon_{p^n}))_2$ for primes $p \not\equiv 1 \pmod{4}$ explicitly. These generators are the generators of $S(Q(\epsilon_{p^n}))_2$ as given by Benard and Schacher [2, Theorem 3, p. 384] combined with elements $[B \otimes_{O(-p^{1/2})} Q(\epsilon_{p^n})]$, where $p \equiv 3 \pmod{4}$, (respectively, $[B \otimes_{O(i)} Q(\epsilon_{2^n})]$ where $p = 2$), such that $[B]$ ranges over suitably chosen generators of $U(Q(-p^{1/2}))_2$ where $p \equiv 3 \pmod{4}$, (respectively, $U(Q(i))_2$, where $p = 2$).

We note that for $U(Q(\epsilon_{p^n}))_2$ where $p \equiv 1 \pmod{4}$, no generators are of this form. In fact, the most that can be said is that

$$U(Q(\epsilon_{p^n}))_2 = U(Q(\epsilon_p))_2 \otimes_{O(\epsilon_p)} Q(\epsilon_{p^n}),$$

and this holds for any odd prime.

We do not calculate the generators of $U(Q(\epsilon_{p^n}))_2$ where $p \equiv 1 \pmod{4}$ as a result of the difficulty which arises in resolving norm questions in this case.

Now we let $B(K)^{(n)}$ be the subgroup of $B(K)$ generated by elements of order n , and let $S(K)^{(n)} = S(K) \cap B(K)^{(n)}$, where n is a positive integer. M. Schacher [10, Theorem 1, p. 15], proved that for K/Q finite abelian then $S(K)^{(n)}$ is of infinite index in $B(K)^{(n)}$, for $n \geq 2$ except when $n = 2$ and $K = Q$. We generalize this result for the case $n = 2$ and K/Q finite imaginary and abelian.

THEOREM 2.1. *If K/Q is finite, imaginady, and abeliad then $S(K)^{(2)}$ is of infinite index in $U(K)^{(2)}$.*

Proof. If E is the maximal real subfield of K then we have $|K : E| = 2$. We let $\langle \sigma \rangle$ be the subgroup of $G(K/Q)$ with E as fixed field. Then by applying the Dirichlet density theorem [5, Corollary 9.2.7, p. 168] to σ we get that there exist infinitely many rational primes, denoted by the set S , which split completely in E/Q and are inert in K/E . We arrange S in disjoint pairs λ , arbitrarily. Hasse's sum theorem yields that we have an element $[A_\lambda]$ in

$U(K)$ with invariants $\frac{1}{2}$ at all K -primes lying over the two primes in λ and zero elsewhere. Thus the $[A_\lambda]$'s are in $U(K)^{(2)}$.

Now, we show $[A_\lambda]$ is not in $S(K)^{(2)}$ for any λ . We use Field's and Herstein's result [4, Theorem 2, p. 71], which yields that an element $[A]$ of order 2 in $S(K)$ has the form $[A] = [B \otimes_E K]$, where $[B]$ in $S(E)$ has index 2.

Thus, if $[A_\lambda]$ is in $S(K)^{(2)}$ for any λ then $[A_\lambda] = [B \otimes_E K]$ where B in $S(E)^{(2)}$ is of index 2.

Now, if \mathcal{P} is a K -prime lying above the E -prime \mathfrak{p} which is above the rational prime $p \in \lambda$; then $\text{inv}_{\mathcal{P}}(A_\lambda) = \text{inv}_{\mathcal{P}}(B \otimes_E K)$ implies:

$$\text{inv}_{\mathcal{P}}(A_\lambda) \equiv |K_{\mathcal{P}} : E_{\mathfrak{p}}| \text{inv}_{\mathfrak{p}}(B) \pmod{1}.$$

But $|K_{\mathcal{P}} : E_{\mathfrak{p}}| = 2$ since $\mathcal{P}|\mathfrak{p}$ is inert in K/E by choice. Therefore, $\text{inv}_{\mathcal{P}}(A_\lambda) \equiv 0 \pmod{1}$, a contradiction. Hence, for each λ we have $[A_\lambda]$ is in $U(K)^{(2)} - S(K)^{(2)}$.

Now we show $[A_\lambda] \cdot [A_{\lambda'}]^{-1}$ is not in $S(K)^{(2)}$ for any $\lambda \neq \lambda'$. If $\lambda \neq \lambda'$ then we have:

$$\text{inv}_{\mathcal{P}}(A_\lambda \otimes_K A_{\lambda'}^{\text{op}}) \equiv \text{inv}_{\mathcal{P}}(A_\lambda) - \text{inv}_{\mathcal{P}}(A_{\lambda'}) \pmod{1}$$

by a formula which can be found in [3, Chap. 7]; where $A_{\lambda'}^{\text{op}}$ is in $[A_{\lambda'}]^{-1}$. But $p \notin \lambda'$ so that $\text{inv}_{\mathcal{P}}(A_{\lambda'}) = 0$. Therefore:

$$\text{inv}_{\mathcal{P}}(A_\lambda \otimes_K A_{\lambda'}^{\text{op}}) \equiv \text{inv}_{\mathcal{P}}(A_\lambda) \pmod{1}.$$

Thus, it suffices to show $[A_\lambda] \notin S(K)^{(2)}$, which we have already accomplished. Therefore, $[A_\lambda] \cdot [A_{\lambda'}]^{-1}$ is not $S(K)^{(2)}$ for any $\lambda \neq \lambda'$.

Hence, the A_λ 's form an infinite number of coset representatives of $S(K)^{(2)}$ in $U(K)^{(2)}$, and the proof is completed. Q.E.D.

COROLLARY 2.2. *If K/Q is finite, imaginary and abelian then $S(K)_2$ is of infinite index in $U(K)_2$.*

Proof. This is clear from the theorem. Q.E.D.

Now we investigate generators of $U(Q(\epsilon_{2^n}))$. First we calculate generators of $U(Q(i))$ and show that for $n > 2$ the generators of $U(Q(\epsilon_{2^n}))$ are the generators of $S(Q(\epsilon_{2^n}))$ combined with elements $[B \otimes_{Q(i)} Q(\epsilon_{2^n})]$, where $[B]$ ranges over certain generators of $U(Q(i))$.

Now we introduce some algebras which, together with generators for $S(Q(i))$ will serve as generators for $U(Q(i))$. First, we let $K = Q(i)$, and let p range over all primes congruent to 3 modulo 4; i.e., over all primes which are

inert in K/Q . We define the cyclic algebra (2.3), as the crossed product given by:

$$A_p = (K(2p)^{1/2}/K, a + bi) = K(2p)^{1/2} u_\alpha \oplus K(2p)^{1/2} \quad (\text{direct sum}),$$

where $\langle \sigma \rangle = \text{Gal}(K(2p)^{1/2}/K)$, and

- (1) $u_\sigma x = x^\sigma u_\sigma; x \in K(2p)^{1/2};$
- (2) $u_\sigma^2 = a + bi;$

with a and b integers such that $a^2 + b^2 = q_p$, a prime such that $q_p \equiv 5 \pmod{8}$ and $q_p \equiv -1 \pmod{p}$.

First, we show that such a prime q_p exists. By the Chinese remainder theorem there is a solution to the equations $s \equiv 5 \pmod{8}$ and $s \equiv -1 \pmod{p}$. Then by Dirichlet's theorem on primes in arithmetic progression [5, Corollary 9.2.8, p. 168], there are infinitely many primes in the sequence $\{s + 8pn\}_{n \in \mathbb{Z}}$. Any prime q_p in this sequence has the required property, i.e., that $q_p \equiv 5 \pmod{8}$, $q_p \equiv -1 \pmod{p}$ and $q_p = a^2 + b^2$; $a, b \in \mathbb{Z}$, since any integer congruent to 1 modulo 4 can be expressed as the sum of the squares of two integers.

We note in passing that A_p is independent of which q_p is chosen in the above sequence. Now we determine the invariants of A_p .

In the following, we have occasion to use the norm residue symbol and the Legendre symbol extensively. Therefore, before proceeding we state some fundamental results.

DEFINITION 2.4. For every prime p of Q finite or infinite, we have the norm residue symbol:

$$(a, b)_p = \begin{cases} +1 & \text{if } a \text{ is a norm of an element of } Q_p(b)^{1/2}, \\ -1 & \text{otherwise.} \end{cases}$$

Some easily verified properties are:

PROPOSITION 2.5 [11, Proposition 6.6.1, p. 249]. *If a, b, c are in Q_p^* , p any prime, then:*

- (1) $(a^2, b)_p = (a, b^2)_p = 1;$
- (2) $(a, b)_p = (b, a)_p;$
- (3) $(a, -a)_p = 1;$
- (4) $(a, b)_p = -1$ if and only if $a < 0$ and $b < 0$.
- (5) for $p \neq \infty; (a \cdot b, c)_p = (a, c)_p (b, c)_p.$

Further properties, when $p = 2$, which will be especially useful later are:

PROPOSITION 2.6 [11, Proposition 6.6.3, p. 251]. *Let p, q be odd primes, $p \neq q$, then:*

$$\begin{aligned} (-1, p)_2 &= \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}, \end{cases} \\ (2, p)_2 &= \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}, \end{cases} \\ (q, p)_2 &= \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod{4}, \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

PROPOSITION 2.7. $[A_p]$ in $U(K)$ has q -local invariant equal to $\frac{1}{2}$ at $q = 2, p$ and 0 elsewhere. (2 and p have just one prime above them in K .)

Proof. We first show that for $q \neq 2, p$ the q -local invariant is zero. We note that if \mathfrak{q} lies over q in $Q(i)/Q$ then $(Q(i))_{\mathfrak{q}} = Q_{\mathfrak{q}}(i)$. We let N denote the norm in $Q_{\mathfrak{q}}(i)/Q_{\mathfrak{q}}$. Now, we let $(A_p)_{\mathfrak{q}} = A_p \otimes_{Q(i)} Q_{\mathfrak{q}}(i)$, and note that: $(A_p)_{\mathfrak{q}} \sim 1$ if and only if $a + bi$ is a norm in $Q_{\mathfrak{q}}(i, (2p)^{1/2})/Q_{\mathfrak{q}}(i)[1]$, and this holds if and only if $N(a + bi)$ is a norm in $Q_{\mathfrak{q}}(2p)^{1/2}/Q_{\mathfrak{q}}$, [5, Proposition 12.2.5, 0. 221]. We shall use this fact throughout.

Now $N(a + bi) = a + bi$ or q_p depending on whether or not $Q_{\mathfrak{q}}(i) = Q_{\mathfrak{q}}$. For $q \neq 2, p$ or q_p , then $Q_{\mathfrak{q}}(2p)^{1/2}/Q_{\mathfrak{q}}$ is unramified since the discriminant of $Q(2p)^{1/2}/Q$ is $8p$ and q_p is a unit in $Q_{\mathfrak{q}}$. Moreover $a + bi$, being an algebraic integer, dividing $q_p = (a + bi)(a - bi)$, is also a unit in $Q_{\mathfrak{q}}$. Thus, $N(a + bi)$ being a unit, is a norm in the unramified extension $Q_{\mathfrak{q}}(2p)^{1/2}/Q_{\mathfrak{q}}$, so that $\text{inv}_{\mathfrak{q}}(A_p) = 0$ for all K -primes above $q \neq 2, p, q_p$.

Now we investigate the case $q = q_p$.

First we have $(2/q) = -1$ since $q \equiv 5 \pmod{8}$. By the quadratic reciprocity law $(p/q_p) = (q_p/p)$, and by hypothesis $q \equiv -1 \pmod{p}$ so $(q/p) = (-1/p)$. But $p \equiv 3 \pmod{4}$ so that $(-1/p) = -1$. Hence $(p/q) = -1$. Thus:

$$(2p/q) = (2/q)(p/q) = (-1)(-1) = 1.$$

Therefore, q is completely split in $Q(2p)^{1/2}/Q$ so that $Q_{\mathfrak{q}}((2p)^{1/2}, i) = Q_{\mathfrak{q}}(i)$. We let N' denote the norm in $Q_{\mathfrak{q}}((2p)^{1/2}, i)/Q_{\mathfrak{q}}(i)$. This implies $N'(a + bi) = a + bi$; and so $(A_p)_{\mathfrak{q}} \sim 1$ for K -primes \mathfrak{q} above $q = q_p$.

We have shown that $(A_p)_{\mathfrak{q}} \sim 1$ for all K -primes above $q \neq 2, p$.

For $q = 2$ we have $N(a + bi) = q_p$ since 2 is ramified in $Q(i)/Q$. By properties of the norm residue symbol; (2.6); $(q_p, 2p)_2 = (q_p, 2)_2(q_p, p)_2 = (-1)(+1) = -1$. Therefore, q_p is *not* a norm in $Q_2(2p)^{1/2}/Q_2$.

Thus A_p has a nonzero 2-local invariant. But the index of A_p must divide $|Q((2p)^{1/2}, i) : Q(i)| = 2$ [1]. Since there is only one K -prime above 2 and above p then, by Hasse's sum theorem, the 2 and p local invariants of A_p are equal to $\frac{1}{2}$. Q.E.D.

We note that an alternative proof for the case $p \equiv 3 \pmod{8}$ is possible wherein we choose $A_p = (K(2p)^{1/2}/K, 1 + i)$. However, no single factor set $a + bi$ suffices for the case $p \equiv -1 \pmod{8}$.

PROPOSITION 2.8. *Let $K = Q(i)$. Then $U(K)$ is generated by:*

- (1) A_p , defined above, as p ranges over all primes $p \equiv 3 \pmod{4}$;
- (2) C_p , as p ranges over primes $p \equiv 1 \pmod{4}$, where $[C_p]$ generate $S(K)$ as given in [2, Theorem 3, p. 384].

Proof. We let $[B] \in U(K)$ and let S denote the set of primes at which B has nonzero invariants. S is finite by Hasse's sum theorem.

We let S' be the subset of S containing primes p such that $\text{ind}_p(B) = \frac{1}{2}$. If $S - S'$ is nonempty then [9, Lemma 2.3, p. 8] yields that the sum of the invariants at K -primes above a given prime in $S - S'$ is zero modulo 1. For primes $p \equiv 3 \pmod{4}$ in S we note that by [9, Theorem 1.1, p. 4] $\text{ind}_p(B) = 2$ so that in fact $p \in S'$. Since primes $p \equiv 3 \pmod{4}$ are inert in K then $2 \in S'$ if and only if there are an odd number of primes $p \in S'$ with $p \equiv 3 \pmod{4}$ by Hasse's sum theorem.

Then for each $p \equiv 3 \pmod{4}$ in S' we pick A_p . The product of such A_p as p ranges over primes $p \equiv 3 \pmod{4}$ in S' has invariant $\frac{1}{2}$ at all such p in S' , at 2 if $2 \in S'$, and zero elsewhere.

If $q \equiv 1 \pmod{4}$ then there is an element $\mathcal{C}_q \in S(K)$ with $\text{ind}_q(C_q) = 4$ and $\text{ind}_p(C_q) = 1$ for all primes $p \neq q$ [2, Theorem 3, p. 384]. From [9, Corollary 1.2, p. 5] we have $\text{ind}_q(B) \leq 4$, so that if $q \in S$ then C_q raised to the appropriate power has the same q -local invariants as B .

Hence, we can find algebras C_q, A_p for each p, q in S such that the product of these $[A_p], [C_q]$ is $[B]$ in $U(K)$. Q.E.D.

Now we find generators for $U(Q(\epsilon_{2^n}))$, $n > 2$.

THEOREM 2.9. *Let $L = Q(\epsilon_{2^n})$, $n > 2$. $U(L)$ is generated by:*

- (1) generators of $S(L)$, [2], and
- (2) $[A_p \otimes_{Q(i)} Q(\epsilon_{2^n})]$ for all $p \equiv -1 \pmod{2^n}$ where A_p is defined in (2.3).

Proof. We let $[B] \in U(L)$ and let S be the set of primes at which B has nonzero invariants.

First we show $2 \notin S$. If $2 \in S$ then by [9, Theorem 1.1, p. 4] $\text{ind}_2(B) = 2$. We have by [9, Lemma 2.3, p. 8] that, if $q \in S$ with $\text{ind}_q(B) > 2$ then the sum of the invariants at the L -primes above q is zero modulo 1. But the sum of all invariants of B must sum to zero modulo 1, by the Hasse sum theorem. Since 2 is totally ramified in L/Q there is only one prime above it. Therefore, among those primes $p \in S$ with $\text{ind}_p(B) = 2$, there must be at least one with an odd

number of L -primes above it. If g is the number of primes into which such a prime p splits in L/Q then g divides $|L : Q| = 2^{n-1}$. Therefore $g = 1$; i.e., p is inert in L/Q . But the Dirichlet density theorem [5, Corollary 9.2.7, p. 168] yields that p is inert in L/Q if and only if $G(L/Q)$ is cyclic. However, for $n > 2$, $G(L/Q)$ is not cyclic, a contradiction. Hence, $2 \notin S$.

Now we consider primes $p \equiv -1 \pmod{2^n}$, $p \in S$, separately, since by [12, Corollary 8.7, p. 138] there are no elements in $S(L)$ with nonzero invariant at such a prime p . For such a p we have $p \equiv 1 \pmod{8}$, since $n > 2$. So choose A_p as in (2.3). We let $A_p \otimes_{Q(i)} Q(\epsilon_{2^n}) = B_p$, and show B_p has $\text{ind}_p(B_p) = 2$ and $\text{ind}_q(B_p) = 1$ for all primes $q \neq p$. We note that by [9, Theorem 1.1, p. 4] $\text{ind}_p(B) = 2$ for such $p \in S$, so that we are essentially going to show that B_p and B have equal p -local invariants.

If \mathcal{P} lies over p in L/Q then:

$$\text{inv}_{\mathcal{P}}(B_p) \equiv |Q_p(\epsilon_{2^n}) : Q_p(i)| \text{inv}_{\mathcal{P}}(A_p) \pmod{1},$$

where $\mathcal{P} = \mathcal{P} \cap Q(i)$, by formulas in [3, Chap. 7]. However, p is inert in $Q(i)/Q$. Also $p^2 \equiv 1 \pmod{2^n}$ implies the inertial degree of p in L/Q is 2. Therefore the inertial degree of p in $L/Q(i)$ is 1; i.e., $|Q_p(\epsilon_{2^n}) : Q_p(i)| = 1$. Thus:

$$\text{inv}_{\mathcal{P}}(B_p) \equiv \frac{1}{2} \pmod{1}.$$

Now the only other possibility for $\text{ind}_q(B_p) > 1$ is for $q = 2$ since A_p has $\text{ind}_q(A_p) > 1$ exactly at $q = 2, p$. But if \mathcal{R} lies over 2 in L/Q , then:

$$\text{inv}_{\mathcal{R}}(B_p) \equiv |Q_2(\epsilon_{2^n}) : Q_2(i)| \text{inv}_{\mathcal{R}}(A_p) \pmod{1},$$

where $\mathcal{U} = \mathcal{R} \cap Q(i)$. Since 2 is totally ramified in K/Q we have

$$|Q_2(\epsilon_{2^n}) : Q_2(i)| = 2^{n-2},$$

$n > 2$, and this implies:

$$\text{inv}_{\mathcal{R}}(B_p) \equiv 0 \pmod{1}.$$

Hence we have shown $\text{ind}_q(B_p) = 1$ for all $q \neq p$ and $\text{ind}_p(B_p) = 2$; i.e., that B_p and B have equal p -local invariants.

Now, we obtain for each $p \in S$ with $p \not\equiv -1 \pmod{2^n}$ an element $[C_p]$ in $S(K)$ with the same p -local invariants as $[B]$. If $p = 1 + 2_\alpha d$, with $(2, d) = 1$, then by [2, Theorem 3, p. 384] there is an element $[C_p]$ in $S(K)$ with $\text{ind}_p(C_p) = \min\{c, n\}$, and $\text{ind}_q(C_p) = 1$ for $q \neq p$. By [9, Corollary 1.2, p. 5] $\text{ind}_p(B) \leq \min\{c, n\}$. So we can see that by raising C_p to an appropriate power we get that C_p and B have equal p -local invariants.

If we take the product of the $[B_p]$'s and $[C_q]$'s found above we get $[B]$ in $U(K)$. Q.E.D.

Now we investigate the generators of $U(Q(\epsilon_{p^n}))_2, p \neq 2$. We want to determine whether or not a similar result to the above holds in the odd prime case. First we consider the case $p \equiv 3 \pmod{4}$, and give generators for $U(Q(-p)^{1/2})_2$. We show that $U(Q(\epsilon_{p^n}))_2$ is generated by elements: $[B \otimes_{Q(-p)^{1/2}} Q(\epsilon_{p^n})]$, where $[B]$ ranges over generators of $U(Q(-p)^{1/2})_2$ and by generators of $S(Q(\epsilon_{p^n}))_2$.

Before we define the algebras which serve as generators for $U(Q(-p)^{1/2})_2$, we need a lemma:

LEMMA 2.10. *Let p be an odd prime such that $p \equiv 3 \pmod{4}$ and let $q \neq p$ be a prime then there is a prime r with*

- (1) $(q/r) = 1$;
- (2) $r \equiv 3 \pmod{4}$, and
- (3) $a^2 + pb^2 = r$, where $2a, 2b \in \mathbb{Z}$.

Proof. We let $K = Q(-p)^{1/2}$ and let $K^{(1)}$ be the Hilbert class field for K . The main step of the lemma is to obtain a generator of

$$G(K^{(1)}(q^{1/2}, i)/K^{(1)}(q)^{1/2})$$

as the Frobenius automorphism of some prime r . First we must ensure that $i \notin K^{(1)}(q)^{1/2}$.

We note that if $q^{1/2}$ or $(-q)^{1/2} \in K^{(1)}$ then q is ramified in $K^{(1)}/Q$. But $K^{(1)}/K$ is unramified, [7, Theorem 13.1, p. 191] so that q is ramified in K/Q . However, the discriminant of K/Q is $-p$ since $p \equiv 3 \pmod{4}$ and $q \neq p$. Thus, q does not ramify in K/Q , a contradiction. Similarly, since $p \equiv 3 \pmod{4}$, $i \notin K^{(1)}$. Therefore, $|K^{(1)}(q^{1/2}, i) : K^{(1)}| = 4$ and so $i \notin K^{(1)}(q)^{1/2}$ as required.

Now, choose a generator of $G(K^{(1)}(q^{1/2}, i)/K^{(1)}(q)^{1/2})$ as the Frobenius automorphism corresponding to some prime r . Therefore, r is completely split in $K^{(1)}(q)^{1/2}/Q$ and inert in $K^{(1)}(q^{1/2}, i)/K^{(1)}(q)^{1/2}$.

Since r is completely split in $K^{(1)}(q)^{1/2}/Q$ then r is completely split in $Q(q)^{1/2}/Q$, i.e., $(q/r) = 1$. Hence we have condition (1).

Since r is inert in $K^{(1)}(q^{1/2}, i)/K^{(1)}(q)^{1/2}$, then r is inert $Q(i)/Q$ because $G(K^{(1)}(q^{1/2}, i)/K^{(1)}(q)^{1/2}) \cong G(Q(i)/Q)$. Therefore $r \equiv 3 \pmod{4}$, and we have condition (2).

Since r is completely split in $K^{(1)}/K$, then the K -primes above r are principal. Therefore there is an algebraic integer $a + b(-p)^{1/2}$ in K , namely, a generator of any one of the aforementioned principal ideals, such that

$N_{K/Q}(a + b(-p)^{1/2}) = a^2 + pb^2 = r$, where $2a, 2b \in Z$, which is condition (3), and the lemma is proved. Q.E.D.

Now we define some algebras. We let $K = Q((-p)^{1/2})$ where $p \equiv 3 \pmod{4}$. For each prime q such that $(q/p) = -1$, i.e., such that q is inert in K . We let $A_{p,q}$ be the cycle algebra (2.11):

$$(K(q)^{1/2}/K, a + b(-p)^{1/2})$$

where $a + b(-p)^{1/2}$ is an algebraic integer in $Q(-p)^{1/2}$; (i.e., $2a, 2b \in Z$) and $a^2 + pb^2 = rp$, where r is a prime such that $(q/r) = 1$ and $r \equiv 3 \pmod{4}$.

We note that by the above lemma, we have a prime r as given in the definition of $A_{p,q}$.

Now we calculate the invariants of $A_{p,q}$.

PROPOSITION 2.12. *As q ranges over all primes such that $(q/p) = -1$ then $[A_{p,q}]$ in $U(K)_2$ has s -local invariant equal to $1/2$ at $s = p, q$ and 0 elsewhere, except when*

- (1) $p \equiv -1 \pmod{8}$ and $q \equiv 3(4)$, and
- (2) $(a + b(-p)^{1/2}, q)_2 = -1$,

in which case $[A_{p,q}]$ has s -local invariant equal to $\frac{1}{2}$ at $s = p, q, 2$, and zero elsewhere.

Proof. Let \mathcal{S} be a prime of K above some rational prime s . Then: $A_{p,q} \otimes_K K_{\mathcal{S}} \sim 1$ if and only if $a + b(-p)^{1/2}$ is a norm in $Q_s((-p)^{1/2}, q^{1/2})/Q_s(-p)^{1/2}$ [1], and this holds if and only if $N(a + b(-p)^{1/2})$ is a norm in $Q_s(q)^{1/2}/Q_s$, [5, Proposition 12.7.5, p. 221], where N denotes the norm in $Q_s(-p)^{1/2}/Q_s$.

Now $N(a + b(-p)^{1/2}) = rp$ or $a + b(-p)^{1/2}$ depending on whether or not $Q_s(-p)^{1/2} = Q_s$.

We consider the case $s \neq r, p, q, 2$. $Q_s(q)^{1/2}/Q_s$ is unramified for all $s \neq 2, q$ and rp is a unit in Q_s for all $s \neq p, r$. But $(a + b(-p)^{1/2})$ is an algebraic integer dividing $rp = (a + b(-p)^{1/2})(a - b(-p)^{1/2})$. Therefore, $a + b(-p)^{1/2}$ is a unit in Q_s for all $s \neq p, r$. Hence $N(a + b(-p)^{1/2})$, being a unit, is a norm in the unramified extension $Q_s(q)^{1/2}/Q_s$ for all $s \neq r, p, q, 2$.

We have shown that $A_{p,q}$ is split at all primes $s \neq r, p, q, 2$.

Case 1. $s = r$.

By choice $(q/r) = 1$, which means r is completely split in $Q(q)^{1/2}/Q$, i.e., $Q_r(q)^{1/2} = Q_r$. Therefore $N'(a + b(-p)^{1/2}) = a + b(-p)^{1/2}$ where N' denote the norm in $Q_r((-p)^{1/2}, q^{1/2})/Q_r(-p)^{1/2}$. Hence $A_{p,q}$ is split at r .

Case 2. $s = p$.

By properties of the norm residue symbol (2.5),

$$(rp, q)_p = (r, q)_p (p, q)_p = (q, p)_p = (q/p)$$

and

$$(q/p) = -1$$

by hypothesis. Therefore rp is not a norm in $Q_p(q)^{1/2}/Q_p$. But $N(a + b(-p)^{1/2}) = rp$, since p is ramified in $Q(-p)^{1/2}/Q$, and so $A_{p,q}$ is *not* split at p .

Case 3. $s = q$.

(a) If $q \neq 2$ then by properties of the norm residue symbol (2.5) we have

$$\begin{aligned} (rp, q)_q &= (r, q)_q = (r/q)(p/q) \\ &= (-1)(+1) = -1, & \text{if } q \equiv 3 \pmod{4} \\ &= (+1)(-1) = -1, & \text{if } q \equiv 1 \pmod{4}. \end{aligned}$$

(b) If $q = 2$ then by properties of the norm residue symbol (2.5) and (2.6):

$$(rp, 2)_2 = (r, 2)_2 (p, 2)_2.$$

But, by (2.11), $(2/r) = 1$ so that $r \equiv \pm 1 \pmod{8}$. Also $r \equiv 3 \pmod{4}$ by (2.11), so that $r \equiv -1 \pmod{8}$. Therefore $(r, 2)_2 = 1$. But $(2/p) = -1$ by hypothesis, so that $p \equiv +3 \pmod{8}$. Also $p \equiv 3 \pmod{4}$ by hypothesis, so that $p \equiv 3 \pmod{8}$. Therefore $(p, 2)_2 = -1$. Hence:

$$(rp, 2)_2 = (r, 2)_2 (p, 2)_2 = (+1)(-1) = -1.$$

Therefore in Case 3(a) or 3(b), rp is not a norm in $Q_q(q)^{1/2}/Q_q$. But $N(a + b(-p)^{1/2}) = rp$, since $(q/p) = -1$ and so $A_{p,q}$ is *not* split at q .

Case 4. $s = 2 \neq q$.

By properties of the norm residue symbol (2.5) and (2.6):

$$\begin{aligned} (rp)_2 &= (r, q)_2 (p, q)_2 = (-1)(-1) = 1 & \text{if } q \equiv 3 \pmod{4} \\ &= (+1)(+1) = 1 & \text{if } q \equiv 1 \pmod{4}. \end{aligned}$$

Therefore rp is a norm in $Q_2(q)^{1/2}/Q_2$. Now, if $p \not\equiv -1 \pmod{8}$ or $q \not\equiv 3 \pmod{4}$ then $A_{p,q}$ is split at 2 because:

(a) If $q \not\equiv 3 \pmod{4}$ then 2 is unramified in $Q(q)^{1/2}/Q$. Thus, rp being a unit in Q_2 , is a norm in the unramified extension $Q_2(q)^{1/2}/Q_2$. Thus $a + b(-p)^{1/2}$ is a unit, hence a norm, in $Q_2(q)^{1/2}/Q_2$. Therefore $N(a + b(-p)^{1/2})$ is a norm in $Q_2(q)^{1/2}/Q_2$. Hence, $A_{p,q}$ is split at 2.

(b) If $p \not\equiv -1 \pmod{8}$, then since $p \equiv 3 \pmod{4}$, we have $p \equiv 3 \pmod{8}$. Therefore $(2/p) = -1$. Thus, 2 is insert in $Q(-p)^{1/2}/Q$. We recall that there is only one prime above p in $Q(-p)^{1/2}$ and only one prime above q in $Q(-p)^{1/2}$ with $A_{p,q}$ having invariant $\frac{1}{2}$ at each. Therefore the invariant of $A_{p,q}$ at 2 must be zero, by Hasse's to sum theorem; i.e., $A_{p,q}$ is split at 2.

Now we consider the case $p \equiv -1 \pmod{8}$ and $q \equiv 3 \pmod{4}$. Now, $p \equiv -1 \pmod{8}$ implies $(2/p) = -1$, which yields that 2 splits in $Q(-p)^{1/2}/Q$. If $(a + b(-p)^{1/2}, q)_2 = -1$ then, since $N(a + b(-p)^{1/2}) = a + b(-p)^{1/2}$, we have $A_{p,q}$ is not split at 2, i.e., $A_{p,q}$ has invariant equal to $\frac{1}{2}$ at each of the two K -primes above 2.

Also if $(a + b(-p)^{1/2}, q)_2 = 1$ then $A_{p,q}$ is split at the K -primes above 2.

In summary, we have shown that $A_{p,q}$ has invariant equal to $\frac{1}{2}$ at the prime above p and at the prime above q , and zero elsewhere except in the special case outlined above when $A_{p,q}$ also has invariant $\frac{1}{2}$ at each of the two K -primes above 2. Hence, it is clear that $[A_{p,q}] \in U(K)$, and the proposition is completed.

Q.E.D.

THEOREM 2.13. *If $K = Q(-p)^{1/2}$ where $p \equiv 3 \pmod{4}$, then $U(K)_2$ is generated by:*

- (1) $A_{p,q}$ as given in (2.8),
- (2) generators of $S(K)_2$.

Proof. Let $[A] \in U(K)$ and let S be the set of rational primes at which A has nonzero invariants. For any $q \in S$ with $(q/p) = 1$, i.e., q completely split in K , choose an element $(C_q) \in S(Q) = U(Q)$, with invariant $\frac{1}{2}$ at q and at the infinite prime of Q , and zero elsewhere. Such an algebra $[C_q] \in S(Q)$ exists by Hasse's sum theorem. If \mathcal{Q} is a K -prime above q then

$$\text{inv}_{\mathcal{Q}}(C_q \otimes_Q K) \equiv |K_{\mathcal{Q}} : Q_q| \text{inv}_q(C_q) \pmod{1}$$

by formulas in [3, Chap. 7]. But $|K_{\mathcal{Q}} : Q_q| = 1$ since q is completely split in $K | Q$; and $\text{inv}_{\mathcal{Q}}(C_q) = \frac{1}{2}$. Therefore we have:

$$\text{inv}_{\mathcal{Q}}(C_q \otimes_Q K) \equiv \frac{1}{2} \pmod{1}.$$

$C_q \otimes_Q K$ is split at the infinite prime of K since K has no real primes. Therefore $C_q \otimes_Q K$ has invariant $\frac{1}{2}$ at the two K -primes above q and zero elsewhere. If we let $C_q \otimes_Q K = B_q$ then B_q and A have equal q -local invariants.

For the primes $q' \in S$ with $(q'/p) = -1$ choose $A_{p,q'}$. Then the product of the $A_{p,q'}$ has invariant $\frac{1}{2}$ at each $q' \in S$, and at p if the number of $q' \in S$ with $(q'/p) = -1$ is odd. We note that $p \in S$ if and only if the number of $q' \in S$

with $(q'/p) = -1$ is odd. This follows from Hasse's sum theorem since there is only one prime above p , and above each such q' , and since the invariant must be $\frac{1}{2}$ for A at any prime.

Hence we have shown that:

$$[A] = \prod_q [B_q] \prod_{q'} [A_{p,q'}],$$

where q ranges over primes of S with $(q/p) = 1$ and q' ranges over primes of S with $(q'/p) = -1$. Q.E.D.

Now we want to find the generators of $U(Q(\epsilon_{p^n}))$, $p \equiv 3 \pmod{4}$. We note that $U(Q(\epsilon_{p^n})_p = S(Q(\epsilon_p t))_p$, [9, Corollary 2.6, p. 16]. We consider therefore only $U(Q(\epsilon_{p^n}))_2$.

THEOREM 2.14. *For $p \equiv 3 \pmod{4}$, $L = Q(\epsilon_{p^n})$ and $K = Q(-p)^{1/2}$ then:*

$$U(L)_2 = U(K)_2 \otimes_K L$$

(i.e., $U(L)_2$ is generated by $[A_{p,q} \otimes_K L]$ and $[B_{q'} \otimes_K L]$ where $[A_{p,q}]$ are generators of $U(K)_2$ given in (2.8) and $[B_{q'}]$ are generators of $S(K)_2$.)

Proof. Since there is no higher 2 power root of unity in L than in K and $|L : K| = p^{n-1}(p - 1)/2$, which is odd since $p \equiv 3 \pmod{4}$, then by [9, Theorem 2.4, p. 9],

$$U(L)_2 = U(K)_2 \otimes_K L.$$

Q.E.D.

In the case $p \equiv 1 \pmod{4}$ the above result is false. The most that can be said is that for $K = Q(\epsilon_{p^n})$ where $p \equiv 1 \pmod{4}$ we have:

$$U(K)_2 = U(Q(\epsilon_p))_2 \otimes_{Q(\epsilon_p)} K,$$

which follows from [9, Theorem 2.4, p. 9], and this, in fact, holds for any odd prime.

REFERENCES

1. A. A. ALBERT, "Structure of Algebras," Amer. Math. Soc., Providence, R.I., 1961.
2. M. BENARD AND M. M. SCHACHER, "The Schur subgroup II, *J. Algebra* **22** (1972), 378-385.
3. M. DEURING, "Algebren," Springer, Berlin, 1935.
4. K. L. FIELDS AND I. N. HERSTEIN, On the Schur subgroup of the Brauer group, *J. Algebra* **20** (1972), 70-71.

5. L. J. GOLDSTEIN, "Analytic Number Theory," Prentice-Hall, Englewood Cliffs, New Jersey, 1971.
6. G. J. JANUSZ, The Schur group of an algebraic number field, to appear.
7. G. J. JANUSZ, "Algebraic Number Fields," Academic Press, New York, 1973.
8. G. J. JANUSZ, The Schur group of cyclotomic fields, *J. Number Theory*, to appear.
9. R. MOLLIN, "Algebras with Uniformly Distributed Invariants," Queen's Mathematical Preprints, No. 1975-9.
10. M. M. SCHACHER, More on the Schur subgroup, *Proc. Amer. Math. Soc.* **31** (1972), 15-17.
11. E. WEISS, "Algebraic Number Theory," McGraw-Hill, New York, 1963.
12. T. YAMADA, "The Schur Subgroup of the Brauer Group," Lecture notes in Mathematics, No. 397, Springer-Verlag, Berlin, 1974.