ON THE HOPF-SCHUR GROUP OF A FIELD

ELI ALJADEFF, JUAN CUADRA, SHLOMO GELAKI, AND EHUD MEIR

ABSTRACT. Let k be any field. We consider the Hopf-Schur group of k, defined as the subgroup of the Brauer group of k consisting of classes that may be represented by homomorphic images of Hopf algebras over k. We show here that twisted group algebras and abelian extensions of k are quotients of cocommutative and commutative Hopf algebras over k, respectively. As a consequence we prove that any tensor product of cyclic algebras over k is a quotient of a Hopf algebra over k, revealing so that the Hopf-Schur group can be much larger than the Schur group of k.

1. INTRODUCTION

Let k be any field and let H be a finite dimensional Hopf algebra over k. Let C be a simple algebra which is a homomorphic image of H. Clearly, C determines an element in $Br(L)$, the Brauer group of L, where L is the center of C. We say that an L-central simple algebra C is *Hopf-Schur* over L if it is a homomorphic image of a finite dimensional Hopf algebra over k, where k is a subfield of L. The Hopf-Schur group $HS(L)$ is the subgroup of $Br(L)$ generated by (and in fact consisting of) classes that may be represented by Hopf-Schur algebras over L. Since any Hopf-Schur algebra over L is a homomorphic image of a Hopf algebra over L (just by extension of scalars) we may restrict our discussion to Hopf-Schur algebras over k which are homomorphic images of finite dimensional Hopf algebras over k. Observe that a k-central simple algebra is a homomorphic image of a *semisimple* k-Hopf algebra H if and only if it is a simple component of the Wedderburn decomposition of H. The group $HS(k)$ clearly contains $S(k)$, the Schur group of k. Recall that a $k-$central simple algebra is said to be *Schur* over k if it is a homomorphic image of a group algebra kG for some finite group G. The group $S(k)$ is the subgroup of $Br(k)$ consisting of (Brauer) classes that may be represented by Schur algebras over k. In general $S(k)$ is "very small" compared to the full Brauer group. For instance if k contains no non-trivial cyclotomic extensions then $S(k) = 0$ whereas $Br(k)$ may be large (e.g., $k = \mathbb{C}(x_1, .., x_n)$, $n \geq 2$, see [FS]). Although the class of semisimple Hopf algebras over k is much richer than the class of group algebras over k, no example was known of an element in $HS(k)$ which is not in $S(k)$ (we refer the reader to [J] and [Y] for a comprehensive account on the Schur group). The main goal of this article is to show that such examples are abundant. In fact we will show that any cyclic algebra (and hence any tensor product of cyclic algebras) is a homomorphic image of a Hopf algebra. Recall that a *cyclic algebra C* over k is a crossed product algebra $(L/k, G, \alpha)$, $\alpha \in Z^2(G, L^*)$, where $G := Gal(L/k)$ is a cyclic group and L^* denotes the multiplicative group of L. The main result of the paper is the following:

Theorem 1.1. *Let C be a $k-$central simple algebra which is isomorphic to a tensor product of cyclic algebras over k. Then C is a homomorphic image of a semisimple Hopf algebra over k.*

Recall that it is a major open problem in Brauer group theory whether any element in $Br(k)$ is Brauer equivalent to a product of cyclic algebras. This is known to be true for number fields (Albert-Brauer-Hasse-Noether Theorem) and for fields containing all roots of unity (Merkurjev-Suslin Theorem). Thus, we naturally raise the question whether $HS(k) = Br(k)$ for arbitrary fields. Of course, this question may be solved (in the positive) independently of the above mentioned problem on cyclic algebras.

The first step in the proof of Theorem 1.1 is carried out in Section 2 where we prove the following result, which is of independent interest.

Theorem 1.2. *Let G be a finite group, and let $[\alpha] \in H^2(G, k^*)$ be an element of order m.*

(1) *The twisted group algebra $k^\alpha G$ is a homomorphic image of a finite dimensional cocommutative Hopf algebra A over k of dimension $m|G|$. When the characteristic of k does not divide $|G|$, A is semisimple.*

(2) *Suppose the characteristic of k does not divide m. Then the $k-$Hopf algebra A is a form of the group algebra $\bar{k}\widehat{G}$, i.e., $A \otimes_k \bar{k} \cong \bar{k}\widehat{G}$, where $\widehat{G}$ is the central extension (induced by $[\alpha]$) of G by $\mathbb{Z}/m\mathbb{Z}$.*

Remark 1.3. *We shall explain how $[\alpha]$ determines an extension of G by $\mathbb{Z}/m\mathbb{Z}$ in Section 2.*

Now let $C = (L/k, G, \alpha)$ be a cyclic algebra. It is well known that by passing to a cohomologous 2-cocycle we can assume that α has values in k^* (rather than in L^*). Hence C contains a k-subalgebra isomorphic to the twisted group algebra $k^\alpha G$. The next result, accomplished in Section 3, is the second step in the proof of Theorem 1.1.

Theorem 1.4. *Let L/k be a finite abelian extension with $G := Gal(L/k)$ and let $Fun(\mathbb{Z}/2\mathbb{Z} \ltimes G, k)$ be the $k-$Hopf algebra of functions on $\mathbb{Z}/2\mathbb{Z} \ltimes G$ with values in k, where $\mathbb{Z}/2\mathbb{Z}$ acts on G by inversion. Then there exists a commutative semisimple Hopf algebra H over k of dimension $2[L : k]$ which satisfies the following:*

(1) *L is a homomorphic image of H.*

(2) *$H \otimes_k L \cong Fun(\mathbb{Z}/2\mathbb{Z} \ltimes G, k) \otimes_k L \cong Fun(\mathbb{Z}/2\mathbb{Z} \ltimes G, L)$. In particular, H is a $k-$form of $Fun(\mathbb{Z}/2\mathbb{Z} \ltimes G, k)$.*

Thus we have constructed two Hopf algebras A and H over k, such that $k^\alpha G$ and L are quotients of them, respectively. In order to complete the proof of Theorem 1.1 we "amalgamate" A and H to obtain a Hopf algebra X over k of which $C = (L/k, G, \alpha)$ is a quotient. This is done in Section 4.

In 1978 Lorenz and Opolka introduced the *projective Schur* subgroup, denoted by $PS(k)$, of $Br(k)$. It consists of Brauer classes that may be represented by homomorphic images of twisted group algebras, i.e., algebras of the form $k^\alpha G$ where α is a 2-cocycle of G with coefficients in k^*. Clearly $PS(k)$ contains $S(k)$. Moreover, it is easy to construct examples (e.g. symbol algebras $(a, b)_n$) which are in $PS(k)$ but not in $S(k)$. In general a twisted group algebra $k^\alpha G$ is not a Hopf algebra over k. In fact it is not difficult to show that $k^\alpha G$ is a Hopf algebra over k if

and only if α is cohomologically trivial. As an immediate consequence of Theorem 1.2 we have:

Corollary 1.5. $HS(k) \supseteq PS(k)$.

Remark 1.6. We point out that there are fields k for which $HS(k)$ properly contains $PS(k)$. This follows from Theorem 1.1 and the fact that there are cyclic algebras over suitable fields k (e.g. $k = \mathbb{Q}(x)$) which do not represent elements in $PS(k)$ (see [AS2]). On the other hand, there exist fields k for which $HS(k) = PS(k)$. For example, for number fields $PS(k) = Br(k)$, so $PS(k) = HS(k) = Br(k)$.

Remark 1.7. We do not know of any k-central simple algebra which is not a homomorphic image of a semisimple Hopf algebra. Also, from the above, it is not clear whether any element in $HS(k)$ is split by an abelian extension of k. The same question for $PS(k)$ was answered in the affirmative in [AS1].

2. THE PROOF OF THEOREM 1.2

Let k be any field, and let G be a finite group. Recall that the twisted group algebra $k^{\alpha}G$, with respect to a 2-cocycle $\alpha \in Z^2(G, k^*)$, is the k-algebra spanned as a k-vector space by the elements U_σ, $\sigma \in G$, with multiplication defined by the formula

$$U_\sigma U_\tau = \alpha(\sigma, \tau) U_{\sigma\tau}, \ \sigma, \tau \in G.$$

It is well known that up to isomorphism of k-algebras, $k^{\alpha}G$ does not depend on the cocycle α but only on the cohomology class $[\alpha] \in H^2(G, k^*)$ it represents. In this section we exhibit a Hopf algebra A over k such that $k^{\alpha}G$ is a quotient of A. We will first define the algebra structure on A and then we will define the counit, comultiplication and antipode.

Recall that every element in the group $H^2(G, k^*)$ is of finite order. Therefore there exist a natural number m and a 1-cochain f such that $\alpha^m = df$. This means that

(1) $$\alpha^m(\sigma, \tau) = f(\sigma)f(\tau)/f(\sigma\tau), \ \sigma, \tau \in G.$$

Without loss of generality we may assume that $\alpha(\sigma, 1) = \alpha(1, \sigma) = f(1) = 1$ for every $\sigma \in G$. From now on we shall denote by m the order of $[\alpha]$ For $n = 0, \ldots, m-1$, we shall denote the basis of $k^{\alpha^n}G$ by $\{U_\sigma^{(n)}\}_{\sigma \in G}$. Consider the algebra

$$A := \bigoplus_{n=0}^{m-1} k^{\alpha^n}G.$$

The algebra A has a counit ϵ given by $\epsilon(U_\sigma^{(n)}) = \delta_{n,0}$. It is easy to see that ϵ is an algebra morphism. Notice that the algebra A will not be semisimple if the characteristic of k divides the order of G (since kG is a direct summand of A). On the other hand, if $char(k)$ does not divide $|G|$, then $k^{\alpha^i}G$ is semisimple for all $i = 0, ..., m-1$. This shows that A is semisimple if and only if $char(k)$ does not divide $|G|$. We shall now make A into a Hopf algebra. For every $0 \le r, l < m$, $\sigma \in G$, define

$$\xi_{r,l}^\sigma = \begin{cases} 1 & \text{if } r + l < m \\ \frac{1}{f(\sigma)} & \text{if } r + l \ge m \end{cases}$$

Note that $\xi_{r,l}^\sigma = \xi_{l,r}^\sigma$ for all r, l and σ.

Now define a map $\Delta : A \to A \otimes A$ by

$$\Delta(U_\sigma^{(n)}) = \sum_{\substack{r+l \equiv n \\ mod.m}} \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(l)},$$

and a map $S : A \to A$ by

$$S(U_\sigma^{(n)}) = \begin{cases} U_{\sigma^{-1}}^{(0)} & \text{if } n = 0 \\ \frac{\alpha^n(\sigma, \sigma^{-1})}{f(\sigma^{-1})} U_{\sigma^{-1}}^{(m-n)} & \text{if } n > 0 \end{cases}$$

Note that Δ is invariant under the flip map $A \otimes A \to A \otimes A$. Therefore, after we will prove that A is a Hopf algebra, it will follow that A is cocommutative.

Proposition 2.1. *The above formulas define a cocommutative Hopf algebra structure on the algebra A.*

Proof. We shall show, by a direct calculation, that all the axioms of a Hopf algebra are valid in A.

1. Δ is coassociative. Since

$$(\Delta \otimes 1)\Delta(U_\sigma^{(n)}) = (\Delta \otimes 1)(\sum_{r+l \equiv n} \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(l)}) = \sum_{z+q+l \equiv n} \xi_{z,q}^\sigma \xi_{z+q,l}^\sigma U_\sigma^{(z)} \otimes U_\sigma^{(q)} \otimes U_\sigma^{(l)}$$

and

$$(1 \otimes \Delta)\Delta(U_\sigma^{(n)}) = (1 \otimes \Delta)(\sum_{r+l \equiv n} \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(l)}) = \sum_{r+s+t \equiv n} \xi_{r,s+t}^\sigma \xi_{s,t}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(s)} \otimes U_\sigma^{(t)},$$

we need to prove that for every $r, s, t < m$ we have

(2) $$\xi_{r,s+t}^\sigma \xi_{s,t}^\sigma = \xi_{r,s}^\sigma \xi_{r+s,t}^\sigma$$

where the sum of the indices is taken modulo m. We prove this by considering the following three possible cases:

a. $r + s + t < m$: In this case both sides of the equation equal 1.
b. $m \le r + s + t < 2m$: In this case in both sides of the equation one of the terms will equal $1/f(\sigma)$ and the other will equal 1.
c. $2m \le r + s + t$: In this case all the terms in the equation will be equal to $1/f(\sigma)$ and so both sides of the equation will equal $1/f(\sigma)^2$.

2. Δ is an algebra map. First,

$$\Delta(1_A) = \Delta(\sum_{n=0}^{m-1} U_1^{(n)}) = \sum_{r,l=0}^{m-1} \xi_{r,l}^1 U_1^{(r)} \otimes U_1^{(l)} = 1_{A \otimes A}.$$

So Δ sends the unit of A to the unit of $A \otimes A$. Next, if $n \neq p$, then

$$\begin{aligned} \Delta(U_\sigma^{(n)})\Delta(U_\tau^{(p)}) &= (\sum_{r+l \equiv n} \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(l)})(\sum_{a+b \equiv p} \xi_{a,b}^\tau U_\tau^{(a)} \otimes U_\tau^{(b)}) \\ &= 0 \\ &= \Delta(0) \\ &= \Delta(U_\sigma^{(n)} U_\tau^{(p)}), \end{aligned}$$

and

$$
\begin{aligned}
\Delta(U_\sigma^{(n)})\Delta(U_\tau^{(n)}) &= (\sum_{r+l\equiv n} \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(l)})(\sum_{r+l\equiv n} \xi_{r,l}^\tau U_\tau^{(r)} \otimes U_\tau^{(l)}) \\
&= \sum_{r+l\equiv n} \xi_{r,l}^\sigma \xi_{r,l}^\tau \alpha^r(\sigma,\tau) U_{\sigma\tau}^{(r)} \otimes \alpha^l(\sigma,\tau) U_{\sigma\tau}^{(l)} \\
&= \sum_{r+l\equiv n} \xi_{r,l}^\sigma \xi_{r,l}^\tau \alpha^{r+l}(\sigma,\tau) U_{\sigma\tau}^{(r)} \otimes U_{\sigma\tau}^{(l)}.
\end{aligned}
$$

On the other hand,

$$
\Delta(U_\sigma^{(n)} U_\tau^{(n)}) = \Delta(\alpha^n(\sigma,\tau) U_{\sigma\tau}^{(n)}) = \sum_{r+l\equiv n} \xi_{r,l}^{\sigma\tau} \alpha^n(\sigma,\tau) U_{\sigma\tau}^{(r)} \otimes U_{\sigma\tau}^{(l)}.
$$

So we need to prove that if $r + l \equiv n$ then

(3) $$\xi_{r,l}^\sigma \xi_{r,l}^\tau \alpha^{r+l}(\sigma,\tau) = \xi_{r,l}^{\sigma\tau} \alpha^n(\sigma,\tau).$$

There are two cases here:

  a. $r + l = n$: In this case both sides of the equation equal $\alpha^n(\sigma,\tau)$.
  b. $r + l = m + n$: In this case the equation becomes $1/(f(\sigma)f(\tau))\alpha^{n+m}(\sigma,\tau) = 1/f(\sigma,\tau)\alpha^n(\sigma,\tau)$ which is equivalent to $\alpha^m(\sigma,\tau) = f(\sigma)f(\tau)/f(\sigma\tau)$, which is exactly equation 1.

3. Δ and ϵ make A into a coalgebra. We compute

$$
(\epsilon \otimes 1)\Delta(U_\sigma^{(n)}) = (\epsilon \otimes 1)(\sum_{r+l\equiv n} \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(l)}) = \xi_{0,n}^\sigma U_\sigma^{(n)} = U_\sigma^{(n)}
$$

and the result follows. The fact that $(1 \otimes \epsilon)\Delta = id_A$ follows by a similar argument or by the above argument and the fact that A is cocommutative.

4. S is an antipode for A. If $0 < n < m$ then

$$
\begin{aligned}
m(S \otimes 1)\Delta(U_\sigma^{(n)}) &= m(S \otimes 1)(\sum_{r+l\equiv n} \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(l)}) \\
&= \sum_{r+l\equiv n} \xi_{r,l}^\sigma \alpha^r(\sigma,\sigma^{-1})/f(\sigma^{-1}) U_{\sigma^{-1}}^{(m-r)} U_\sigma^{(l)} \\
&= 0 \\
&= \epsilon(U_\sigma^{(n)}).
\end{aligned}
$$

The third equality follows from the fact that if $m - r = l$, then $m = r + l$, contradicting the assumption that $r + l \equiv n$. If $n = 0$ then

$$
\begin{aligned}
m(S \otimes 1)\Delta(U_\sigma^{(0)}) &= m(S \otimes 1)\big(U_\sigma^{(0)} \otimes U_\sigma^{(0)} + \sum_{r=1}^{m-1} \xi_{r,m-r}^\sigma U_\sigma^{(r)} \otimes U_\sigma^{(m-r)}\big) \\
&= U_\sigma^{(0)} U_{\sigma^{-1}}^{(0)} + \sum_{r=1}^{m-1} \xi_{r,m-r}^\sigma \alpha^r(\sigma, \sigma^{-1})/f(\sigma^{-1}) U_{\sigma^{-1}}^{(m-r)} U_\sigma^{(m-r)}\big) \\
&= U_1^{(0)} + \sum_{r=1}^{m-1} (1/f(\sigma))(\alpha^r(\sigma, \sigma^{-1})/f(\sigma^{-1}))\alpha^{m-r}(\sigma^{-1}, \sigma) U_1^{(m-r)} \\
&= U_1^{(0)} + \alpha^m(\sigma, \sigma^{-1})/(f(\sigma)f(\sigma^{-1})) \sum_{r=1}^{m-1} U_1^{(m-r)} \\
&= \sum_{r=0}^{m-1} U_1^{(r)} \\
&= 1_A \\
&= \epsilon(U_\sigma^{(0)}),
\end{aligned}
$$

and therefore S is an antipode. During the computation we have used in the third equality the fact that $\alpha(\sigma, \sigma^{-1}) = \alpha(\sigma^{-1}, \sigma)$, and in the fourth one that

$$
\alpha^m(\sigma, \sigma^{-1}) = f(\sigma)f(\sigma^{-1})/f(1) = f(\sigma)f(\sigma^{-1}).
$$

This completes the proof that A is a Hopf algebra. $\qquad\square$

Remark 2.2. It is well known that for representations V and W of $k^{\alpha^i}G$ and $k^{\alpha^j}G$, respectively, $V \otimes W$ is a representation of the twisted group algebra $k^{\alpha^{i+j}}G$. This defines a tensor structure on $\mathrm{Rep}(A)$, which explains the comultiplication on A. It is also known that V^* is a representation of $k^{\alpha^{-i}}G \cong k^{\alpha^{m-i}}G$. This means that the category $\mathrm{Rep}(A)$ is rigid, which explains the antipode on A. The trivial one dimensional representation of A, k, on which $U_\sigma^{(n)}$ acts as the scalar $\delta_{n,0}$, explains the counit of A. Thus the maps which make the algebra A into a Hopf algebra can be reconstructed from the rigid tensor structure of the category $\mathrm{Rep}(A)$. (See e.g., [G] for more details on reconstruction.)

The twisted group algebra $k^\alpha G$ and every quotient of it is clearly a quotient of A. Thus, we have showed that every twisted group algebra, and hence every projective Schur algebra, is a quotient of a Hopf algebra.

We shall now prove the second part of Theorem 1.2. Consider the cocycle α as a cocycle with values in $\bar{k}^*$ rather than in k^*. Since α^m is cohomologically trivial, there is a 1-cochain $f : G \to \bar{k}^*$ such that

$$
\alpha^m(\sigma, \tau) = f(\sigma)f(\tau)/f(\sigma\tau).
$$

Define a 1-cochain $g : G \to \bar{k}^*$ by $g(\sigma) = f(\sigma)^{1/m}$, where $f(\sigma)^{1/m}$ is any element of $\bar{k}^*$ whose mth power equals $f(\sigma)$. It is easy to see that all the values of the cocycle $\bar{\alpha} = \alpha/dg$ are mth roots of unity, and that $\bar{\alpha}$ is cohomologous to α. Suppose that the characteristic of k does not divide m. In this case the group of mth roots of unity in $\bar{k}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$, and we can consider $\bar{\alpha}$ as a central extension

$$
\bar{\alpha} : 1 \to \mathbb{Z}/m\mathbb{Z} \to \widehat{G} \to G \to 1.
$$

Let $\zeta \in \bar{k}$ be a primitive mth root of unity. We have seen that there is a cocycle $\bar{\alpha}$ cohomologous to α such that $\bar{\alpha}(\sigma, \tau) \in \langle \zeta \rangle \cong \mathbb{Z}/m\mathbb{Z}$ for every $\sigma, \tau \in G$. So we shall assume henceforth that α has all its values in $\langle \zeta \rangle$. In that case α^m is the cocycle which is identically 1. The map f is then taken as that one being identically 1. The group $\widehat{G}$ is the set of all ordered pairs of the form (σ, i), where $\sigma \in G$ and $i \in \mathbb{Z}/m\mathbb{Z}$, with multiplication given by the formula

$$(\sigma, i)(\tau, j) = (\sigma\tau, i + j + \alpha(\sigma, \tau)).$$

We consider α as a cocycle with values in the group $\mathbb{Z}/m\mathbb{Z}$, and define the following $\bar{k}$-linear map

$$\phi : \bar{k}\widehat{G} \to \bar{k} \otimes_k A, \ \ (\sigma, i) \mapsto \sum_{j=0}^{m-1} \zeta^{ij} \otimes U_\sigma^{(j)}.$$

A straightforward verification shows that this is a Hopf algebra isomorphism, and thus A is a $\bar{k}$−form of $\bar{k}\widehat{G}$, as desired. This completes the proof of Theorem 1.2. □

3. The proof of Theorem 1.4

Let L be an abelian Galois extension of k with (abelian) Galois group G of order n. Recall the definition of $\mathrm{Fun}(G, k)$, the algebra of functions on G with values in k. It is the dual of the group algebra kG. It has a k-basis consisting of the mutually orthogonal idempotents $\{e_\sigma\}_{\sigma \in G}$ given by $e_\sigma(\tau) = \delta_{\sigma,\tau}$. We define H, as an algebra, to be

$$H := L \oplus \mathrm{Fun}(G, k).$$

We shall denote the unit of L in H by 1_L, to avoid confusion with the unit of H. Let us write the unit of $Fun(G, k)$ as $e = \sum_{\sigma \in G} e_\sigma$. The unit of H will then be $1_L + e$. There is also a natural counit ϵ, given by $\epsilon(e_\sigma) = \delta_{\sigma,1}$, and $\epsilon(L) = 0$. It is easy to see that ϵ is an algebra map. H also has an anti-algebra morphism, $S : H \to H$, defined by $S(x) = x$ for $x \in L$, and $S(e_\sigma) = e_{\sigma^{-1}}$. This will be the antipode of H. Notice that H is a semisimple commutative algebra, and that L is a quotient of H. We will now define the comultiplication on H.

Since L is a direct summand of H, $L \otimes_k L$ will be a direct summand of $H \otimes_k H$, so we begin with some analysis of $L \otimes_k L$. From Galois theory we know that $L \otimes_k L$ decomposes as the direct sum of n copies of L. Explicitly, for every $\sigma \in G$ consider the algebra map $\Psi_\sigma : L \otimes_k L \to L$ defined by $\Psi_\sigma(x \otimes y) = \sigma(x)y$. Then we can write

$$L \otimes_k L = \oplus_{\sigma \in G} L\mathcal{E}_\sigma$$

where $\mathcal{E}_\sigma$ is the idempotent lying in the kernels of all the maps $\Psi_\tau, \tau \neq \sigma$. For every $\sigma \in G$, let ω_σ be the automorphism of $L \otimes L$ given by $\omega_\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y)$. Then for $\mu \in G$ we have $\omega_\sigma(\mathcal{E}_\mu) = \mathcal{E}_{\sigma\mu\sigma^{-1}} = \mathcal{E}_\mu$(because G is abelian). If we write $\mathcal{E}_\mu = \sum_i x_i \otimes y_i$ then this means that $\sum_i x_i \otimes y_i = \sum_i \sigma(x_i) \otimes \sigma(y_i)$.

Now define a map $\Delta : H \to H \otimes H$ by

$$\Delta(x) = \sum_{\mu \in G} \left(\mu^{-1}(x) \otimes e_\mu + e_\mu \otimes \mu(x) \right), \ x \in L,$$

and

$$\Delta(e_\xi) = \sum_{\sigma\mu=\xi} e_\sigma \otimes e_\mu + \mathcal{E}_\xi.$$

Proposition 3.1. *The maps Δ, ϵ and S defined above equip H with the structure of a semisimple commutative Hopf algebra.*

Proof. One can verify easily that Δ is an algebra map. The fact that Δ is coassociative can be proved directly or by the following argument. Consider the set $D := Hom_{k-alg}(H, L)$; it contains the following elements: for every $\sigma \in G$ we have the map $\phi_\sigma : H \to L$ given by $\phi_\sigma(x) = 0$ for $x \in L$ and $\phi_\sigma(e_\tau) = \delta_{\sigma,\tau}$, and the map $\zeta_\sigma : H \to L$ given by $\zeta_\sigma(x) = \sigma(x)$ for $x \in L$, and $\zeta_\sigma(e_\tau) = 0$. It is easy to check that these $2n$ maps are all the k-algebra morphisms from H to L. Since L is commutative and Δ is multiplicative, the map Δ defines a convolution product $*$ on D. It is easy to check that the following holds by using the formulas for Δ given above:

$$\phi_\sigma * \phi_\tau = \phi_{\sigma\tau}$$
$$\phi_\sigma * \zeta_\tau = \zeta_{\sigma\tau}$$
$$\zeta_\tau * \phi_\sigma = \zeta_{\tau\sigma^{-1}}$$
$$\zeta_\sigma * \zeta_\tau = \phi_{\tau^{-1}\sigma}.$$

We have used in the last equality that

$$m_L(\zeta_\sigma \otimes \zeta_\tau)(\mathcal{E}_\mu) = \Psi_{\sigma\tau^{-1}}(\tau \otimes \tau)(\mathcal{E}_\mu) = \Psi_{\sigma\tau^{-1}}(\mathcal{E}_\mu).$$

By a direct verification, $(D, *)$ is isomorphic as a set with a binary operation to the group $\mathbb{Z}_2 \ltimes G$, where $\mathbb{Z}_2$ acts on G by inversion. The correspondence between these two sets is given by $\phi_\sigma \leftrightarrow (0, \sigma)$, $\zeta_\sigma \leftrightarrow (1, \sigma)$, where we write $\mathbb{Z}_2 = \{0, 1\}$. In particular, this means that $*$ is *associative* on D, and therefore, for every 3 elements $x, y, z \in D$ we have

(4) $$m_L(1 \otimes m_L)(x \otimes y \otimes z)(1 \otimes \Delta)\Delta = m_L(m_L \otimes 1)(x \otimes y \otimes z)(\Delta \otimes 1)\Delta.$$

It follows that Equation 4 will hold if we replace x, y, z by L-linear combinations of elements of D. From Galois theory we know that the elements of G are L-linear independent. It follows that the elements of D are L-linear independent when we consider them as elements of the L-vector space $V = Hom_k(H, L)$, where L acts by $(xf)(h) = xf(h)$, $x \in L$, $f \in V$, and $h \in H$. Since $dim_L V = 2n$, D is a basis of V, and therefore for every $x, y, z \in V$, Equation 4 holds. But this implies that Δ is coassociative. The fact that ϵ is a counit follows from the following computations $(x \in L)$:

$$(\epsilon \otimes 1)\Delta(x) = (\epsilon \otimes 1)(\sum_{\mu \in G} (\mu^{-1}(x) \otimes e_\mu + e_\mu \otimes \mu(x))) = x$$

and

$$(\epsilon \otimes 1)\Delta(e_\xi) = (\epsilon \otimes 1)(\sum_{\sigma\mu=\xi} e_\sigma \otimes e_\mu + \mathcal{E}_\xi) = \sum_{\sigma\mu=\xi} \delta_{1,\sigma} e_\mu = e_\xi.$$

A symmetric calculation shows that $(1 \otimes \epsilon)\Delta(x) = x$ and $(1 \otimes \epsilon)\Delta(e_\xi) = e_\xi$.

The fact that S is an antipode follows from the following computations $(x \in L)$:

$$\begin{aligned} m(S \otimes 1)\Delta(x) &= m(S \otimes 1)(\sum_{\mu \in G}(\mu^{-1}(x) \otimes e_\mu + e_\mu \otimes \mu(x))) \\ &= \sum_{\mu \in G} (\mu^{-1}(x)e_\mu + e_{\mu^{-1}}\mu(x)) \\ &= 0 \\ &= \epsilon(x) \end{aligned}$$

and

$$m(S \otimes 1)\Delta(e_\xi) \quad = m(S \otimes 1)(\sum_{\sigma\mu=\xi} e_\sigma \otimes e_\mu + \mathcal{E}_\xi)$$

$$= \sum_{\sigma\mu=\xi} e_{\sigma^{-1}}e_\mu + m(\mathcal{E}_\xi)$$

$$= \delta_{1,\xi}(\sum_{\sigma\in G} e_\sigma + 1_L)$$

$$= \epsilon(e_\xi).$$

The computations for $1 \otimes S$ are exactly the same. This completes the proof that H is a Hopf algebra and the first part of Theorem 1.4.

We now prove that $H \otimes_k L \cong \mathrm{Fun}(\mathbb{Z}/2\mathbb{Z} \ltimes G, L)$. Since $L \otimes_k L = \oplus_{\sigma\in G} L\mathcal{E}_\sigma$ and $\mathrm{Fun}(G,k) \otimes_k L \cong \mathrm{Fun}(G,L)$, we know that as an $L-$algebra $H \otimes_k L$ has a basis consisting of $2n$ mutually orthogonal idempotents. The group $Hom_{L-alg}(H\otimes_k L, L)$ thus contains $2n$ elements. There is a natural monomorphism $Hom_{k-alg}(H, L) \rightarrow Hom_{L-alg}(H \otimes_k L, L)$ given by extension of scalars. We know that the group $Hom_{k-alg}(H, L)$ contains $2n$ elements and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \ltimes G$. The monomorphism above is thus an isomorphism and therefore the set of group-like elements of $(H \otimes_k L)^*$ is $Hom_{L-alg}(H \otimes_k L, L)$, which is isomorphic to $\mathbb{Z}_2 \ltimes G$. Since $dim_L((H \otimes_k L)^*) = dim_L(L[\mathbb{Z}/2\mathbb{Z} \ltimes G])$, it follows that the Hopf algebras $H \otimes_k L$ and $\mathrm{Fun}(\mathbb{Z}_2 \ltimes G, L)$ are isomorphic, as claimed. $\square$

4. THE PROOF OF THEOREM 1.1

Let L be a cyclic extension of k with a cyclic Galois group G, and let $\alpha \in Z^2(G, L^*)$. The crossed product algebra $L_t^\alpha G$ has an L-basis given by $\{U_\sigma\}_{\sigma\in G}$, and the multiplication is given by the rule

$$(xU_\sigma)(yU_\tau) = x\sigma(y)\alpha(\sigma,\tau)U_{\sigma\tau}, \text{ where } x, y \in L, \ \sigma, \tau \in G.$$

As mentioned in the introduction, since the Galois group G is cyclic, we assume (as we may) that α gets values in $k = L^G$ (in fact α is cohomologous to a 2-cocycle β of the form

$$\beta(\sigma^i, \sigma^j) = \left\{ \begin{array}{ll} 1 & \text{if } i+j < |G| \\ b & \text{if } i+j \geq |G| \end{array} \right. , \text{ where } 0 \leq i, j \leq |G|.$$

where b is in $k = L^G$). In that case consider the k-subalgebra of $L_t^\alpha G$ generated by the elements U_σ. It is easy to see that this is the twisted group algebra $k^\alpha G$ and by Theorem 1.2, it is the quotient of a semisimple Hopf algebra A over k. By Theorem 1.4, we know that the field extension L is a quotient of a semisimple Hopf algebra H over k. We now show how to "amalgamate" these two constructions to obtain a Hopf algebra X which projects onto the cyclic algebra $L_t^\alpha G$.

As a coalgebra, we let $X := H \otimes A$. This means that the comultiplication is given by the formula

$$(5) \qquad \Delta(h \otimes a) = \sum h_{(1)} \otimes a_{(1)} \otimes h_{(2)} \otimes a_{(2)}.$$

The counit will be naturally given by

$$(6) \qquad \epsilon(h \otimes a) = \epsilon(h)\epsilon(a).$$

Consider the algebra $L \otimes k^{\alpha^n} G$ with multiplication

$$(7) \qquad (x \otimes U_\sigma^{(n)})(y \otimes U_\tau^{(n)}) = x\sigma(y)\alpha^n(\sigma,\tau) \otimes U_{\sigma\tau}^{(n)}.$$

Notice that this is exactly the same as $L_t^{\alpha^n}G$. Consider also the tensor algebra $Fun(G,k) \otimes k^{\alpha^n}G$, whose multiplication is

$$(8) \qquad (e_\mu \otimes U_\sigma^{(n)})(e_\nu \otimes U_\tau^{(n)}) = \delta_{\mu,\nu} e_\mu \otimes \alpha^n(\sigma,\tau) U_{\sigma\tau}^{(n)}.$$

Then, as an algebra,

$$X = \left(\bigoplus_{n=0}^{m-1} L \otimes k^{\alpha^n}G \right) \bigoplus \left(\bigoplus_{n=0}^{m-1} Fun(G,k) \otimes k^{\alpha^n}G \right),$$

where m is the order of $[\alpha]$.

The antipode S on X is given by

$$(9) \qquad S(x \otimes U_\sigma^{(n)}) = \sigma^{-1}(x) \otimes \alpha^n(\sigma,\sigma^{-1})/f(\sigma^{-1}) U_{\sigma^{-1}}^{(m-n)},$$

and

$$(10) \qquad S(e_\tau \otimes U_\sigma^{(n)}) = e_{\tau^{-1}} \otimes \alpha^n(\sigma,\sigma^{-1})/f(\sigma^{-1}) U_{\sigma^{-1}}^{(m-n)}.$$

Proposition 4.1. *The above multiplication and antipode equip X with a Hopf algebra structure. The dimension of X equals $2m|G|[L : k]$. Furthermore, the crossed product $L_t^\alpha G$ is a quotient of X.*

Proof. Since the tensor product of two coalgebras is again a coalgebra, we know that X is a coalgebra. It is also easy to see that the multiplication defined above makes X into an algebra. So we only need to check that the two structures are compatible. The fact that ϵ is an algebra map is easy, and can be proved directly, using Equations (7) and (8). The fact that Δ is an algebra map can also be proved directly by the above equations. We give here a brief description of the computations. By the way Δ was defined it is easy to see that $\Delta(1_X) = \Delta(1 \otimes 1) = 1 \otimes 1 \otimes 1 \otimes 1 = 1_{X \otimes X}$. Also, we have

$$\begin{aligned} \Delta(h \otimes a) \;&= \sum h_{(1)} \otimes a_{(1)} \otimes h_{(2)} \otimes a_{(2)} \\ &= (\sum h_{(1)} \otimes 1 \otimes h_{(2)} \otimes 1)(\sum 1 \otimes a_{(1)} \otimes 1 \otimes a_{(2)}) \\ &= \Delta(h \otimes 1)\Delta(1 \otimes a). \end{aligned}$$

Since we already know that Δ is multiplicative on H and on A, it is easy to see that we only need to prove that for every $h \in H$ and $a \in A$, $\Delta(1 \otimes a)\Delta(h \otimes 1) = \Delta((1 \otimes a)(h \otimes 1))$. In order to show this we need to recall the property about the idempotents of $L \otimes L$ previously used, that is, $\omega_\sigma(\mathcal{E}_\mu) = (\sigma \otimes \sigma)(\mathcal{E}_\mu) = \mathcal{E}_\mu$ for all $\sigma, \mu \in G$. Writing $\mathcal{E}_\mu = \sum_i x_i \otimes y_i$ this means that $\sum_i x_i \otimes y_i = \sum_i \sigma(x_i) \otimes \sigma(y_i)$.

For $x \in L$ we compute:

$$\begin{aligned} &\Delta(1 \otimes U_\sigma^{(n)})\Delta(x \otimes 1) \\ &= (\sum_{r+l\equiv n} 1 \otimes \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes 1 \otimes U_\sigma^{(l)})(\sum_{\mu \in G} \mu^{-1}(x) \otimes 1 \otimes e_\mu \otimes 1 + e_\mu \otimes 1 \otimes \mu(x) \otimes 1) \\ &= \sum_{r+l\equiv n}\sum_{\mu\in G} \xi_{r,l}^\sigma \sigma\mu^{-1}(x) \otimes U_\sigma^{(r)} \otimes e_\mu \otimes U_\sigma^{(l)} + \xi_{r,l}^\sigma e_\mu \otimes U_\sigma^{(r)} \otimes \sigma\mu(x) \otimes U_\sigma^{(l)} \\ &= \sum_{r+l\equiv n}\sum_{\mu\in G} \xi_{r,l}^\sigma \mu^{-1}\sigma(x) \otimes U_\sigma^{(r)} \otimes e_\mu \otimes U_\sigma^{(l)} + \xi_{r,l}^\sigma e_\mu \otimes U_\sigma^{(r)} \otimes \mu\sigma(x) \otimes U_\sigma^{(l)} \\ &= \Delta(\sigma(x) \otimes U_\sigma^{(n)}) \\ &= \Delta((1 \otimes U_\sigma^{(n)})(x \otimes 1)). \end{aligned}$$

Let $\mu \in G$. Then

$$\Delta(1 \otimes U_\sigma^{(n)})\Delta(e_\mu \otimes 1)$$

$$= (\sum_{r+l \equiv n} 1 \otimes \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes 1 \otimes U_\sigma^{(l)})(\sum_{\rho\eta=\mu} e_\rho \otimes 1 \otimes e_\eta \otimes 1 + \sum_i x_i \otimes 1 \otimes y_i \otimes 1)$$

$$= \sum_{r+l \equiv n} \sum_{\rho\eta=\mu} e_\rho \otimes \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes e_\eta \otimes U_\sigma^{(l)} + \sum_{r+l \equiv n} \sum_i \sigma(x_i) \otimes \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes \sigma(y_i) \otimes U_\sigma^{(l)}$$

$$= \sum_{r+l \equiv n} \sum_{\rho\eta=\mu} e_\rho \otimes \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes e_\eta \otimes U_\sigma^{(l)} + \sum_{r+l \equiv n} \sum_i x_i \otimes \xi_{r,l}^\sigma U_\sigma^{(r)} \otimes y_i \otimes U_\sigma^{(l)}$$

$$= \Delta(e_\mu \otimes U_\sigma^{(n)})$$

$$= \Delta((1 \otimes U_\sigma^{(n)})(e_\mu \otimes 1)).$$

This finishes the proof that Δ is multiplicative.

Finally we show that S is an antipode. Notice that by the way S was defined, we have $S(h \otimes a) = (1 \otimes S_A(a))(S_H(h) \otimes 1)$. This can be easily checked using equations (7) – (10). We now compute

$$\begin{aligned} m(S \otimes 1)\Delta(h \otimes a) &= m(S \otimes 1)(\sum h_{(1)} \otimes a_{(1)} \otimes h_{(2)} \otimes a_{(2)}) \\ &= \sum(1 \otimes S_A(a_{(1)}))(S_H(h_{(1)}) \otimes 1)h_{(2)} \otimes a_{(2)} \\ &= \epsilon(h)\sum(1 \otimes S_A(a_{(1)}))(1 \otimes a_{(2)}) \\ &= \epsilon(h)\epsilon(a)1 \otimes 1 \otimes 1 \otimes 1 \\ &= \epsilon(h \otimes a)1_X. \end{aligned}$$

Similarly, $m(1 \otimes S)\Delta(h \otimes a) = \epsilon(h \otimes a)1_X$. Thus S is an antipode for X, and X is indeed a Hopf algebra. Since $L_t^\alpha G$ is a direct summand of X, it is a quotient of X. The proof is complete. □

Remark 4.2. One can also view X as a bicrossed product of the Hopf algebras A and H. By Theorems 1.2 and 1.4, X is a $\bar{k}-$form of the bicrossed product of the Hopf algebras $\bar{k}\widehat{G}$ and $\mathrm{Fun}(\mathbb{Z}/2\mathbb{Z} \ltimes G, \bar{k})$. (See e.g. [K, IX.2] for details about bicrossed products.)

Remark 4.3. In order to construct X the field extension L need not by cyclic. All we really need is that L will be an abelian extension, and that the cocycle α will be in the image of $H^2(G, k^*) \to H^2(G, L^*)$.

ACKNOWLEDGMENTS

REFERENCES

[AS1]   E. Aljadeff and J. Sonn, Projective Schur algebras have abelian splitting fields. J. Algebra 175 (1995), no. 1, 179–187.

[AS2]   E. Aljadeff and J. Sonn, On the projective Schur group of a field. J. Algebra 178 (1995), no. 2, 530–540.

[FS]   B. Fein and M. Schacher, Brauer groups of rational function fields, in "Groupe de Brauer", Lecture Notes in Mathematics, vol 844, Springer-Verlag, New York/Berlin, 1981.

[G]   S. Gelaki, Semisimple triangular Hopf algebras and Tannakian categories, *Proceedings of Symposia in Pure Mathematics* **70** (2002), 497–516 (editors M. Fried and Y. Ihara, 1999 Von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16-27, 1999 MSRI).

[J]   G. Janusz, The Schur group of an algebraic number field, *Ann. of Math.* (2) **103** (1976), no. 2, 253–281.

[K]   C. Kassel, Quantum Groups, Graduate Texts in Mathematics **155**, Springer-Verlag, 1995.

[Y]   T. Yamada, The Schur Subgroup of the Brauer Group, Lecture Notes in Mathematics **397**, Springer-Verlag, 1970.

Department of Mathematics, Technion-Israel Institute of Technology, Haifa 32000, Israel
    E-mail address: aljadeff@tx.technion.ac.il

Departamento de Álgebra y Análisis Matemático, Universidad de Almería, E04120 Almería, Spain
    E-mail address: jcdiaz@ual.es

Department of Mathematics, Technion-Israel Institute of Technology, Haifa 32000, Israel
    E-mail address: gelaki@math.technion.ac.il

Department of Mathematics, Technion-Israel Institute of Technology, Haifa 32000, Israel
    E-mail address: ehudm@techunix.technion.ac.il