ISRAEL JOURNAL OF MATHEMATICS 91 (1995), 409–417

SOLUTION OF THE TWISTING PROBLEM FOR SKEW GROUP ALGEBRAS

BY

ELI ALJADEFF

Department of Mathematics
Technion—Israel Institute of Technology, 32000 Haifa, Israel

AND

DEREK J.S. ROBINSON*

Department of Mathematics
University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA

ABSTRACT

Let K be any field of characteristic $p > 0$ and let G be a finite group acting on K via a map τ. The skew group algebra $K_\tau G$ may be non-semisimple (precisely when $P|(H)$, $H = \mathrm{Ker}\, t$). In [1] necessary conditions were given for the existence of a class $\alpha \in H^2(G, K^*)$ which "twists" the skew group algebra $K_\tau G$ into a semisimple crossed product $K_\tau^\alpha G$. The "twisting problem" asks whether these conditions are sufficient. In [1] we showed that this is indeed so in many cases. In this paper we prove it in general.

1. Introduction

Let G be a group and K a field, and suppose that $\tau\colon G \to \mathrm{Aut}\ K$ is an action of G on K. Then we may form the skew group algebra $K_\tau G$; this is the K-space with basis $\{u_x |\ x \in G\}$ and ring product given by $(au_x)(bu_y) = ax(b)u_{xy}$ where $x(b)$ denotes $\tau(x)(b)$. Since K^* is a G-module, we can choose an α from $Z^2(G, K^*)$ and use it to "twist" $K_\tau G$ to form the **crossed product** $K_\tau^\alpha G$, where the product is

---

* During the period of this research the second author was an Associate at the Center for Advanced Study, Urbana, Illinois.

Received July 10, 1993 and in revised form April 28, 1994

given by the formula $(au_x)(bu_y) = ax(b)\alpha(x,y)u_{xy}$. It is well-known that up to isomorphism $K_\tau^\alpha G$ depends on α only through its cohomology class, so we may assume that $\alpha \in H^2(G,K^*)$.

In a previous paper [1] some necessary and sufficient conditions were found for $K_\tau^\alpha G$ to be a semisimple algebra when G is finite. In characteristic zero it is always semisimple. In characteristic $p > 0$ we have the

THEOREM ([1] Theorem B, Theorem 2): *Let $K_\tau^\alpha G$ be a crossed product algebra over a field K of characteristic $p > 0$. Denote the kernel of τ by H. Then $K_\tau^\alpha G$ is semisimple if and only if $K^{\overline{\alpha}}H$ is semisimple where $\overline{\alpha} = \mathrm{res}_H^G \alpha$. Furthermore, in this case,*

(*) *$H/O_{p'}(H)$ is an abelian group with rank not exceeding the p-degree of K over K^p.*

The theorem above gives only partial information about the "existence" of semisimple crossed products beyond, of course, trivial examples where $p = \mathrm{char}\, K \nmid |H|$.

The question of the existence of "non-trivial" semisimple crossed products, i.e., $p \mid |H|$, may be formulated in more than one way (see Theorem A and Theorem B below).

In [1] the following question was considered: when can a skew group algebra be twisted to a semisimple crossed product? More precisely, let $K_\tau G$ be a given skew group algebra, with G a finite group and K a field of characteristic $p > 0$. H denotes the kernel of τ. Is the necessary condition (*) above also sufficient for the existence of an $\alpha \in H^2(G,K^*)$ such that $K_\tau^\alpha G$ is semisimple? We call this question the twisting problem.

In [1] techniques were developed for attacking the twisting problem. Also the problem was solved in some special cases, notably when K is a local field or G is a p-group.

Our purpose here is to solve the problem in the general case by establishing

THEOREM A: *Let G be a finite group, K a field of prime characteristic p, and $\tau\colon G \to \mathrm{Aut}(K)$ an action of G on K with kernel H. Then there is an α in $H^2(G,K^*)$ such that $K_\tau^\alpha G$ is semisimple if and only if $H/O_{p'}(H)$ is an abelian group whose rank does not exceed the p-degree of K over K^p.*

As an easy consequence of this, we obtain necessary and sufficient conditions on a finite group G and a field K for the existence of a semisimple crossed product of G over K.

THEOREM B: *Let G be a finite group and K a field of prime characteristic p. Then there is a semisimple crossed product of G over K if and only if G has a normal subgroup H such that the following hold:*

(i) *G/H is isomorphic with a subgroup of* $\mathrm{Aut}(K)$*;*

(ii) *$H/O_{p'}(H)$ is an abelian group whose rank does not exceed the p-degree of K over K^p.*

This result is most interesting when the finite subgroups of $\mathrm{Aut}(K)$ are restricted.

Example: Let K be the field of rational functions in t over the field $\mathbb{F}_q$ of $q = p^m$ elements where p is any prime. If $\sigma \in \mathrm{Aut}\,(K)$, then σ must normalize $\mathbb{F}_q$ since this is the subfield of algebraic elements. If σ acts as the identity on $\mathbb{F}_q$, then it must be of the form

$$t \longmapsto \frac{at+b}{ct+d}$$

where $a, b, c, d, \in \mathbb{F}_q$ and $ad - bc \neq 0$ ([4], p. 496, 9.1). Thus each automorphism of K has the form

$$u \mapsto \sigma(u), \quad t \mapsto \frac{at+b}{ct+d} \quad \text{where} \;\; u \in \mathbb{F}_q, \quad \sigma \in \mathrm{Aut}\,(\mathbb{F}_q).$$

Hence $\mathrm{Aut}\,(K) \simeq \mathrm{P\Gamma L}_2(q)$, the group of semilinear fractional transformations of $\mathbb{F}_q$. The subgroups of $\mathrm{PSL}_2(q)$ are known ([3], II, 8.27), so in principle it is possible to determine the subgroups of $\mathrm{P\Gamma L}_2(q)$.

Since K has p-degree 1 over K^p, the conditions in Theorem B require the existence of a normal subgroup H such that G/H is isomorphic with a subgroup of $\mathrm{P\Gamma L}_2(q)$ and $H/O_{p'}(H)$ is cyclic.

2. Reductions

We shall now summarize the reductions in the twisting problem which were obtained in [1].

Let $\tau\colon G \to \mathrm{Aut}\ K$ be an action of a finite group G on a field K of characteristic $p > 0$, and put $Q = \mathrm{Im}\ \tau$. Further assume that $H = \mathrm{Ker}\ \tau$ satisfies the condition: $H/O_{p'}(H)$ is abelian with rank r not greater than the p-degree of K over K^p. Denote by P a Sylow p-subgroup of H, and observe that P is an abelian group of rank r. According to [1], Proposition 1, there is an α in $H^2(P, K^*)$ for which the twisted group algebra $K^\alpha P$ is semisimple and, in fact, it is a purely inseparable field extension of K. Now if α can be extended to $\beta \in H^2(G, K^*)$, then $K^\beta_\tau G$ will be semisimple, by [2], Theorem 3.2 and [5], p. 184. So the challenge is to find an α in $\operatorname{Im}(\operatorname{res}^G_P)$ for which $K^\alpha P$ is semisimple.

By [1], Proposition 7, it can be assumed that $H = P$. Then an easy spectral sequence argument ([1], Lemma 8) shows that

$$\operatorname{Im}(\operatorname{res}^G_P) = \operatorname{Ker} d$$

where d: $H^2(P, K^*)^Q \to H^3(Q, K^*)$ is the differential in the Lyndon–Hochschild –Serre spectral sequence for $P \hookrightarrow G \twoheadrightarrow Q$.

Next, a result of great importance [1], Proposition 9, asserts that

$$H^2(P, K^*)^Q \simeq \operatorname{Hom}_{\mathbb{Z}_{p^e}Q}\left(P, K^*/(K^*)^{p^e}\right) \tag{1}$$

where p^e is the exponent of P. This effectively transfers the problem to the realm of module homomorphisms.

Write $P = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle$ where $|x_i| = p^{e_i}$ and $0 < e_i \leq e$. Let

$$k = K^Q$$

be the fixed field of Q. By [1], Lemma 13, there is a subset $\{a_1, \ldots, a_r\}$ of k^* which is p-independent over K^p. Since K is Galois over k, there is a z in K such that $\sigma(z) \neq z$ if $1 \neq \sigma \in Q$. It was shown in [1], Theorem 11 that the a_i can be chosen so that the $(1 + a_i z^p)\,(K^*)^{p^e}$ generate a free $\mathbb{Z}_{p^e}Q$ submodule of $K^*/(K^*)^{p^e}$. By a simple technique for embedding a module in a free module, one can then construct an embedding φ of P in $K^*/(K^*)^{p^e}$. This is given by

$$\varphi(x) = \prod_{i=1}^{r} \prod_{x \in Q} (1 + a_i \sigma(z)^p)^{(\sigma^{-1}(x))_i} (K^*)^{p^e}$$

where $(y)_i$ is the exponent of x_i in $y \in P$. We can write $\varphi(x_j) = b_j^{p^{e-e_j}} (K^*)^{p^e}$ where

$$b_j = \prod_{i=1}^{r} \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{(\sigma^{-1}(x_j))_i}.$$

Next, by (1), φ determines an α in $H^2(P, K^*)^Q$, and, according to [1], Lemma 10, $K^\alpha P$ will be semisimple if and only if $\{b_1, \ldots, b_r\}$ is p-independent over K^p. Thus our aim is to show that z and the a_i can be chosen so that the b_j's are p-independent.

3. The main step in the proof

Let K be a field of characteristic $p > 0$, Q a finite subgroup of Aut K, and M a finite $\mathbb{Z}_{p^e}Q$-module with positive rank r which does not exceed the p-degree of K over K^p. Write $M = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$ where $|x_i| = p^{e_i}$ and $0 < e_i \leq e$. Finally, let $k = K^Q$ be the fixed field.

The result that is needed to prove Theorem A is

PROPOSITION 1: *There is an element z of K satisfying $\sigma(z) \neq z$ for $1 \neq \sigma \in Q$, and a subset $\{a_1, \ldots, a_r\}$ of k which is p-independent over K^p such that the following hold:*

(a) *the elements $(1 + a_i z^p)(K^*)^{p^e}$ freely generate a free $\mathbb{Z}_{p^e}Q$-submodule of $K^*/(K^*)^{p^e}$;*

(b) *the elements $b_j = \prod_{i=1}^{r} \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{(\sigma^{-1}(x_j))_i}$, $j = 1, \ldots, r$, are p-independent over K^p.*

The first step in the proof of Proposition 1 is to show that there are many subsets of k which have the free generation property.

PROPOSITION 2: *Let K be a field of characteristic $p > 0$, Q a finite subgroup of* Aut K *and r a positive integer. Assume that $\{c_1, \ldots, c_r\}$ is a subset of the fixed field $k = K^Q$ which is p-independent over K^p. Then there are elements $u_1, \ldots, u_r$ of $(k^*)^p$ such that for all positive e the elements $(1 + a_i z^p)(K^*)^{p^e}$ freely generate a free $\mathbb{Z}_{p^e}Q$-submodule of $K^*/(K^*)^{p^e}$ where $a_i = c_i u_i$. Moreover, once $u_1, \ldots, u_{i-1}$ have been chosen, all but a finite number of the elements of $(k^*)^p$ qualify as u_i.*

Proof: Note that K, and hence k, is infinite. Observe also that it is sufficient to prove the result for $e = 1$ since extraction of roots in K^* is unique.

Assume that the elements $1 + a_1 z^p, \ldots, 1 + a_{i-i} z^p$ have the free generation property where $a_j = c_j u_j$. Let $u \in (k^*)^p$ and put $a_i = c_i u$. We shall argue that $1 + a_1 z^p, \ldots, 1 + a_i z^p$ have the free generation property for almost all u.

If this is not true, free generation must fail for infinitely many u. Since there are only finitely many $\mathbb{Z}_p Q$-linear relations that can hold between the $(1 + a_j z^p)(K^*)^p$, there exist integers $\lambda_{j\sigma}$, not all zero, such that $0 \leq \lambda_{j\sigma} < p$ and

$$\prod_{j=1}^{i} \prod_{\sigma \in Q} (1 + a_j \sigma(z)^p)^{\lambda_{j\sigma}} \in (K^*)^p. \tag{2}$$

Expand the product in (2) and write it as a linear combination of the monomials $a_1^{\ell_1} \cdot \ldots \cdot a_i^{\ell_i}$, $0 \le \ell_j < p$. Then

$$\sum_{\underline{\ell}} f_{\underline{\ell}}(a_1, \ldots, a_i)^p a_1^{\ell_1} \cdots a_i^{\ell_i} \in (K^*)^p \tag{3}$$

where $\underline{\ell} = (\ell_1, \ldots, \ell_i)$, $0 \le \ell_j < p$ and $f_{\underline{\ell}}$ is a polynomial in i indeterminates over $\mathbb{F}_p(\sigma(z)|\sigma \in Q)$. Now the monomials $a_1^{\ell_1} \cdots a_i^{\ell_i}$ are linearly independent over K^p since $a_1, \ldots, a_i$ are p-independent over K^p ([1], Lemma 12). Therefore $f_{\underline{\ell}}(a_1, \ldots, a_i) = 0$ for $\underline{\ell} \neq (0, \ldots, 0)$. Since there are infinitely many choices for u, it follows that $f_{\underline{\ell}}(a_1, \ldots, a_{i-1}, t) = 0$ where t is an indeterminate.

Replacing a_i by t in (2) and expanding the product as in (3), we obtain

$$\begin{aligned} b \cdot \prod_{\sigma \in Q} (1 + t\sigma(z)^p)^{\lambda_{i\sigma}} &= \sum_{\underline{\ell}} f_{\underline{\ell}}(a_1, \ldots, a_{i-1}, t)^p a_1^{\ell_1} \cdots a_{i-1}^{\ell_{i-1}} t^{\ell_i} \\ &= f_0(a_1, \ldots, a_{i-1}, t)^p = g(t^p) \end{aligned} \tag{4}$$

where

$$g \in K^p[t] \quad \text{and} \quad b = \prod_{j=1}^{i-1} \prod_{\sigma \in Q} (1 + a_j \sigma(z)^p)^{\lambda_{j\sigma}} \neq 0.$$

Suppose that $\lambda_{i\sigma_0} \neq 0$. Then, by raising both sides of (4) to a suitable power, we may assume that $\lambda_{i\sigma_0} = 1$. Now differentiate (4) with respect to t and put $t = -\sigma_0(z)^{-p}$. Since $\sigma(z) \neq \sigma_0(z)$ if $\sigma_0 \neq \sigma \in Q$, we obtain a contradiction. Therefore all the $\lambda_{i\sigma}$ vanish, which means that $1 + a_1\sigma(z)^p, \ldots, 1 + a_{i-1}\sigma(z)^p$ do not have the free generation property.

COROLLARY 3: *Let S be the Q-submodule of K^* generated by the elements $1 + a_i z^p$, and let e be a positive integer. Then $S \cap (K^*)^{p^e} = S^{p^e}$ and S/S^{p^e} is freely generated as a $\mathbb{Z}_{p^e} Q$-module by the $(1 + a_i z^p) S^{p^e}$.*

One further preparatory result is required before the proof of Proposition 1.

LEMMA 4: *Let K be a finite Galois extension of an infinite field k, with $(K\colon k) = n$. If $0 \neq f \in K[t_1, \ldots, t_n]$, then $f(z_1, \ldots, z_n) \neq 0$ for some normal basis $\{z_1, \ldots, z_n\}$ of K over k.*

Proof: Let $\{e_1, \ldots, e_n\}$ be any k-basis of K, and let $\mathrm{Gal}(K/k) = \{\sigma_1, \ldots, \sigma_n\}$. If $z \in K$, we can write $z = \sum_{i=1}^n a_i e_i$ with $a_i \in k$; then

$$f(\sigma_1(z), \ldots, \sigma_n(z)) = \sum_{i=1}^{n} g_i(a_1, \ldots, a_n) e_i$$

where $g_i \in k[t_1, \ldots, t_n]$. By [7], 3.5.3 there is a z in K such that $f(\sigma_1(z), \ldots, \sigma_n(z)) \neq 0$; thus some g_j is not 0.

The condition for $\sigma_1(z), \ldots, \sigma_n(z)$ to form a normal basis of K over k is that these elements be linearly independent over k, i.e. that a certain polynomial h in $k[t_1, \ldots, t_n]$ should not vanish at $(a_1, \ldots, a_n)$. Since k is infinite, we may choose $a_1, \ldots, a_n$ in k so that $g_j h$ does not vanish at $(a_1, \ldots, a_n)$. Writing $z = \sum_{i=1}^{n} a_i e_i$, we conclude that f does not vanish at the ordered normal basis $(\sigma_1(z), \ldots, \sigma_n(z))$.

Proof of Proposition 1: Since $r > 0$, the field k is infinite. Let z be an element of a normal basis of K over k, and choose a subset $\{c_1, \ldots, c_r\}$ of k which is p-independent over K^p; this exists by [1], Lemma 13. By Proposition 2 there are elements $u_1, \ldots, u_r$ of $(k^*)^p$ such that the $(1 + a_i z^p)(K^*)^{p^e}$ freely generate a free $\mathbb{Z}_{p^e}Q$-submodule of $K^*/(K^*)^{p^e}$ where $a_i = c_i u_i$. Also there are infinitely many choices for u_i once $u_1, \ldots, u_{i-1}$ have been chosen.

If the proposition is false, the elements

$$b_j = \prod_{i=1}^{r} \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{(\sigma^{-1}(x_j))_i}, \qquad j = 1, 2, \ldots, r,$$

are p-dependent over K^p for all choices of z and the u_i. Thus the monomials $b_1^{\ell_1} \ldots b_r^{\ell_r}$, $0 \leq \ell_i < p$, are linearly dependent over K^p, and there is a relation

$$\sum_{\underline{\ell}} d_{\underline{\ell}} b_1^{\ell_1} \cdots b_r^{\ell_r} = 0$$

where $\underline{\ell} = (\ell_1, \ldots, \ell_r)$, $d_{\underline{\ell}} \in K^p$, and not all the $d_{\underline{\ell}}$ are 0. Substituting for the b_j, we obtain

$$\sum_{\underline{\ell}} d_{\underline{\ell}} \prod_{i=1}^{r} \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{\lambda_{i\sigma}^{(\underline{\ell})}} = 0 \tag{5}$$

where $\lambda_{i\sigma}^{(\underline{\ell})} = \left(\sigma^{-1}(\ell_1 x_1 + \cdots + \ell_r x_r)\right)_i$. Since non-zero pth powers can be absorbed in $d_{\underline{\ell}}$, we may assume that $0 \leq \lambda_{i\sigma}^{(\underline{\ell})} < p$ and that

$$\lambda_{i\sigma}^{(\underline{\ell})} \equiv \left(\sigma^{-1}(\ell_1 x_1 + \cdots + \ell_r x_r)\right)_i (\operatorname{mod} p).$$

Expand the products in (5) and express the left hand side as a linear combination of the monomials $a_1^{\ell_1} \cdots a_r^{\ell_r}$, $0 \leq \ell_i < p$. Each coefficient of a monomial is itself a linear combination of the $d_{\underline{\ell}}$ over the field $\mathbb{F}_p(a_1, \ldots, a_r, \sigma_1(z), \ldots, \sigma_n(z))^p$, where $Q = \{\sigma_1, \dots, \sigma_n\}$. Since the monomials are linearly independent over K^p, we obtain a system of p^r linear equations in the p^r coefficients $d_{\underline{\ell}}$. Let A be the coefficient matrix of the linear system. Then det(A) has the form $f(a_1, \dots, a_r, \sigma_1(z), \dots, \sigma_n(z))^p$ where $f \in \mathbb{F}_p[t_1, \dots, t_r, y_1, \dots, y_n]$. Of course A is singular, so

$$f(a_1, \dots, a_r, \sigma_1(z), \dots, \sigma_n(z)) = 0.$$

Now fix z, $a_1, \dots, a_{r-1}$ and vary the u_r in $a_r = c_r u_r$ infinitely. It follows that $f(a_1, \dots, a_{r-1}, t_r, \sigma_1(z), \dots, \sigma_n(z)) = 0$ where t_r is an indeterminate. By the same argument each a_i can be replaced by an indeterminate t_i, so that

$$f(t_1, \dots, t_r, \sigma_1(z), \dots, \sigma_n(z)) = 0.$$

We argue next that each $\sigma_j(z)$ may be replaced by an indeterminate s_j. To this end, choose and fix $v_1, \dots, v_r$ in k; then $f(v_1, \dots, v_r, s_1, \dots, s_n) \in k[s_1, \dots, s_n]$ vanishes at every normal basis $(\sigma_1(z), \dots, \sigma_n(z))$ of K over k. Lemma 4 now shows that $f(v_1, \dots, v_r, s_1, \dots, s_n) = 0$, so that

$$f(t_1, \dots, t_r, s_1, \dots, s_n) = 0.$$

Putting $s_1 = 1$ and $s_2 = \cdots = s_n = 0$, we obtain

$$f(t_1, \dots, t_r, 1, 0, \dots, 0) = 0,$$

which, on reversing the procedure that led to (5), shows that the linear system

$$\sum_{\underline{\ell}} d_{\underline{\ell}} \prod_{i=1}^{r} (1 + t_i)^{\ell_i} = 0 \tag{6}$$

has a nontrivial solution for the $d_{\underline{\ell}}$ in $\mathbb{F}_p(t_1, \dots, t_r)$: notice here that $\lambda_{i1}^{(\underline{\ell})} = \ell_i < p$. It follows from (6) that the coefficient matrix A of the linear system has its $(\underline{m}, \underline{\ell})$ entry equal to $\binom{\ell_1}{m_1} \cdots \binom{\ell_r}{m_r}$ where $\underline{m} = (m_1, \dots, m_r)$, $\underline{\ell} = (\ell_1, \dots, \ell_r)$. Hence A is just the rth tensor power of the $p \times p$ matrix T with (i,j) entry equal to $\binom{j}{i}$. Since T is unitriangular, so is A and det $(A) = 1$, a final contradiction.

4. Conclusion of the proof of Theorem A

The deduction of Theorem A from Proposition 1 and the reductions described in §2 proceeds as in [1], §6. It must be verified that if $\alpha \in H^2(Q, K^*)$ corresponds to the $\mathbb{Z}_{p^e}Q$-homomorphism $\varphi\colon H \to K^*/(K^*)^{p^e}$ which is determined by the b_j's in Proposition 1, then $\alpha \in \operatorname{Ker} d$ where $d\colon H^2(H, K^*)^Q \to H^3(Q, K^*)$ is the differential in the spectral sequence. A simple restriction-corestriction argument shows that it suffices to verify that $\alpha \in \operatorname{Ker} \overline{d}$ where $\overline{d}$ is the corresponding differential for R, a Sylow p-subgroup of Q. Let S be the Q-submodule of K^* generated by the $1 + a_i z^p$. Then φ maps H onto $S(K^*)^{p^e}/(K^*)^{p^e}$, which is isomorphic with S/S^{p^e}; also the latter is freely generated by the $(1 + a_i z^p)\, S^{p^e}$ (see Corollary 3). Therefore S/S^{p^e} is a free R-module, and $H^3(R, S) = 0$ by [6] (Theorem 6, p. 143). From this it follows that $\alpha \in \operatorname{Ker} \overline{d}$.

ACKNOWLEDGEMENT: We would like to thank Roy Meshulam for very useful conversations he had with the first author of this paper.

References

[1] E. Aljadeff and D.J.S. Robinson, *Semisimple algebras, Galois actions and group cohomology*, Journal of Pure and Applied Algebra **94** (1994), 1–15.

[2] E. Aljadeff and S. Rosset, *Global dimensions of crossed products*, Journal of Pure and Applied Algebra **40** (1986), 103–113.

[3] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[4] G. Karpilovsky, *Field Theory*, Marcel Dekker, New York, 1988.

[5] D.S. Passman, *Infinite Crossed Products*, Academic Press, San Diego, 1989.

[6] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[7] D. Winter, *Structure of Fields*, Springer, New York, 1978.