ACADEMIC PRESS
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Algebra 256 (2002) 111–125
JOURNAL OF Algebra
www.academicpress.com

Semisimple strongly graded rings

E. Aljadeff,[a,*,1] Y. Ginosar,[b,2] and Á. del Río[c,3]

[a] Department of Mathematics, Technion—Israel Institute of Technology, 32000 Haifa, Israel
[b] Department of Mathematics, Ben Gurion University, 84105 Beer Sheva, Israel
[c] Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain

Received 7 May 2001

Communicated by Kent R. Fuller

1. Introduction

Let G be a finite group and R a strongly G-graded ring. The question of when R is semisimple (meaning in this paper semisimple artinian) has been studied by several authors. The most classical result is Maschke's Theorem for group rings. For crossed products over fields there is a satisfactory answer given by Aljadeff and Robinson [3]. Another partial answer for skew group rings was given by Alfaro et al. [1]. A reduction of the problem to crossed products over division rings was first given by Jespers and Okniński [10] and a more constructive version was given by Haefner and del Río [8]. So, in order to give a complete answer to the problem there is still a gap between crossed products over division rings and crossed products over fields. The first aim of the paper is to fill this gap, showing that the semisimplicity question for crossed products over division rings reduces to the same question for crossed products over fields. In Theorem 3.2 we make this reduction and then in Theorem 3.3 we put together all the pieces of the puzzle.

A strongly G-graded ring R with identity component A induces a group homomorphism $\sigma : G \to \mathrm{Pic}(A)$ (see Section 2 for the details). As a consequence of

* Corresponding author.
E-mail addresses: aljadeff@techunix.technion.ac.il (E. Aljadeff), uv@math.bgu.ac.il (Y. Ginosar), adelrio@fcu.um.es (Á. del Río).
[1] Supported by the Fund for the Promotion of Research at the Technion and the Technion VPR Fund.
[2] Supported by the TMR project "Algebraic Lie Representations".
[3] Partially supported by the DGI of Spain and Fundación Séneca of Murcia.

PII: S0021-8693(02)00113-8

Theorem 3.3, one deduces some necessary conditions for a group homomorphism $\sigma: G \to \mathrm{Pic}(A)$ to be induced by a semisimple strongly G-graded ring, namely the conditions (1)–(3) of Corollary 3.5. The *Twisting Problem* asks whether these necessary conditions are also sufficient, that is given a group homomorphism $\sigma: G \to \mathrm{Pic}(A)$ satisfying conditions (1)–(3) of Corollary 3.5, is there a semisimple strongly G-graded ring with coefficient ring A inducing σ? This problem has been investigated in [3] and in [4] for (outer) actions on fields. Our second result (Theorem 4.6) shows that the Twisting Problem for G a cyclic group and A finitely generated as a module over its centre has always a positive solution.

Our solution to the problem of semisimplicity of strongly graded rings has an application to actions of finite groups on division rings of prime characteristic. We include this in the last section of the paper. We show that if G is a finite group acting on a division ring D of characteristic p and H is the kernel of this action, then $\mathrm{tr}_G(D) \neq 0$ if and only if the elements of a p-Sylow subgroup of G are linearly independent over D if and only if the elements of a p-Sylow subgroup of H are linearly independent over D.

2. Preliminaries

Let S be a ring (we consider all rings unital and associative). We use the following notation:

$$Z(S) = \text{centre of } S,$$

$$S^* = \text{group of units of } S,$$

$$\mathrm{Aut}(S) = \text{group of automorphisms of } S,$$

$$\mathrm{Inn}(S) = \text{group of inner automorphisms of } S, \text{ and}$$

$$\mathrm{Out}(S) = \mathrm{Aut}(S)/\mathrm{Inn}(S) = \text{group of outer automorphisms of } S.$$

The action of $\alpha \in \mathrm{Aut}(S)$ on $x \in S$ is denoted by x^α, so that the product in $\mathrm{Aut}(S)$ is given by $\alpha\beta = \beta \circ \alpha$. If $u \in S^*$ then ι_u denotes the inner automorphism of S given by $x^{\iota_u} = x^u = u^{-1}xu$. If P is an invertible S-bimodule, then $[P]$ denotes the isomorphism class of P (as a bimodule) and $\mathrm{Pic}(S) = \{[P]\colon P \text{ is an invertible } S\text{-module}\}$ is the Picard group of S. We consider $\mathrm{Out}(S)$ canonically embedded in $\mathrm{Pic}(S)$. Recall that there is a canonical group homomorphism $\theta: \mathrm{Pic}(S) \to \mathrm{Aut}(Z(S))$ (see [5, II, 5.4]). More explicitly, for every invertible S-bimodule there are two ring isomorphisms $\lambda_P, \rho_P : Z(S) \to \mathrm{End}({}_S P_S)$ from $Z(S)$ to the ring of S-bimodule endomorphisms of P, given by $\lambda_P(a)(x) = ax$ and $\rho_P(a)(x) = xa$. Then $\theta_P = \rho_P \circ \lambda_P^{-1}$ is an automorphism of $Z(S)$ and it does not depend on the choice of the representative P in the class $[P]$. Then θ is given by $\theta([P]) = \theta_P$. If B is a subset of $Z(S)$, then $\mathrm{Pic}_B(S)$ denotes the subgroup of $\mathrm{Pic}(S)$ consisting of those elements that fix the elements of B, i.e. $[P] \in \mathrm{Pic}_B(S)$ if and only if $pb = bp$ for every $p \in P$ and $b \in B$.

Let G be a group with identity 1 and R a strongly G-graded ring, that is there is a decomposition $R = \bigoplus_{g\in G} R_g$, where each R_g is an additive subgroup and $R_g R_h = R_{gh}$ for every $g, h \in G$. We refer to $A = R_1$ as the coefficient ring of the graded ring R. If H is a subgroup of G, then $R_H = \bigoplus_{h\in H} R_h$ is a strongly H-graded ring. For every $g \in G$, R_g is an invertible A-bimodule and the map $g \mapsto [R_g]$ is a group homomorphism $\sigma : G \to \mathrm{Pic}(A)$. Composing with the group homomorphism $\mathrm{Pic}(A) \to \mathrm{Aut}(Z(A))$, one obtains an action of G on $Z(A)$ called the Miyashita action.

If R_g has a unit u_g for every $g \in G$, then R is said to be a crossed product. In this case $\{u_g\colon g \in G\}$ is a basis of R as a right A-module and there are maps

$$\beta : G \to \mathrm{Aut}(A), \qquad t : G \times G \to A^*$$

called the action and twisting, respectively. They are defined by

$$au_g = u_g a^{\beta(g)}, \qquad u_g u_h = u_{gh} t(g, h)$$

for every $g, h \in G$ and $a \in A$. Usually we simplify the notation and write a^g for $a^{\beta(g)}$. The action and twisting satisfy the following conditions:

$$\begin{aligned} &t(g_1g_2, g_3)t(g_1, g_2)^{\beta(g_3)} = t(g_1, g_2g_3)t(g_2, g_3),\\ &\beta(g_1g_2)\iota_{t(g_1,g_2)} = \beta(g_1)\beta(g_2) \end{aligned} \tag{2.1}$$

for every $g_1, g_2, g_3 \in G$ (see [15]). By (2.1), the map β induces a homomorphism $\alpha : G \to \mathrm{Out}(A) \subseteq \mathrm{Pic}(A)$ which is precisely the group homomorphism σ coming from the structure of strongly graded ring on R (we call this an outer action of G on A) and restricts to an action of G on $Z(A)$ which coincides with the Miyashita action.

Note that R is a crossed product if and only if the image of σ is embedded in $\mathrm{Out}(A)$. It is customary to denote a crossed product over G with coefficient ring A by $A * G$. When we want to emphasize the action and the twisting we will use the notation $A *_t^\beta G$.[4] The action and twisting depend on the selection of a unit in each homogeneous component; a change in this selection yields a change in the action and twisting; this is called a diagonal change of basis. A *twisted group ring* is a crossed product with trivial action; in this case the notation is $A *_t G$. Modulo a diagonal change of basis a twisted group ring is the same as a crossed product with trivial outer action. A *skew group ring* is a crossed product with trivial twisting and the notation is $A *^\beta G$. If H is a subgroup of G and B is a subring of A with $t(h, h') \in B^*$ for every $h, h' \in H$ and $\beta(h)$ restricts to an automorphism of B for every $h \in H$, then the corresponding subcrossed product is denoted by $B * H$ or $B *_t^\beta H$ (with the usual abuse of notation).

[4] This notation is slightly different from the one in [3].

3. Criterion for semisimplicity

Let R be a strongly G-graded ring with coefficient ring A. It is well known that if R is semisimple then R_H is semisimple for every subgroup H of G. This is a consequence of the fact that R_H is a direct summand of R as an R_H-bimodule (see, for example, [14, Propositions 1.2 and 1.3]). In particular if R is semisimple then A is semisimple.

If C is a Morita context between A and another ring A', then associated with C there is a strongly graded R' with coefficient ring A' so that the categories of graded modules R-gr and R'-gr are graded equivalent and hence R and R' are graded Morita equivalent. In particular, if A is semisimple, then R is graded Morita equivalent to a crossed product over a direct product of division rings. (Recall that every strongly graded ring over a direct product of division rings is a crossed product, see, e.g., the beginning of Section 6 in [8].) Since graded Morita equivalence implies Morita equivalence [11] and the coefficient ring of a semisimple strongly graded ring is semisimple, we conclude that in order to describe the semisimple strongly graded rings it is enough to describe the semisimple crossed products with a direct product of division rings as their coefficient rings. In fact, it is possible to reduce further, namely to crossed products over one division ring. This was first given in [10] and more constructively in [8]. That is, modulo the results of these two papers, it only remains to produce a criterion to decide when a crossed product over a division ring is semisimple. In this section we give one step ahead and reduce the problem to the case when the coefficient ring is a field and then use the characterization given by Aljadeff and Robinson [3] for this case.

Remark 3.1. Before going ahead we would like to mention that in the proof of Lemma 7.2 in [8] (which is a stage in the proof of [8, Proposition 7.4], and an essential step in the reduction of the semisimplicity problem from strongly graded rings with semisimple coefficient ring to crossed products over division rings) the authors make use of Skolem–Noether Theorem. This would suggest the implicit assumption that each division subring is finite dimensional over its centre. However, the use of Skolem–Noether Theorem in the mentioned lemma can be avoided by using [16, Corollary 2.9.19].

Let $D * G = D *_t^\beta G$ be a crossed product where D is a division ring with centre K of characteristic p (a divisor of $|G|$ to avoid the trivial case solved by Maschke's Theorem). Let $\alpha : G \to \mathrm{Out}(D)$ be the outer action induced by β. Let H be the kernel of α so that, after a diagonal change of basis $D * H = D *_{t'} H$ is a twisted group ring for some twisting $t' : G \times G \to D^*$. By (2.1), $t'(g, h) \in K^*$ for every $g, h \in H$ and hence one can consider the twisted group ring $K *_{t'} H$.

We obtain the following criterion for semisimple crossed products over division rings.

Theorem 3.2. *With the above notation, the following are equivalent*:

(1) $D * G$ *is semisimple.*
(2) $D * H = D *_{t'} H$ *is semisimple.*
(3) $K *_{t'} H$ *is semisimple.*

Proof. (1) $\Rightarrow$ (2) is explained in the first paragraph of the section.

To prove the equivalence between (2) and (3) note that $D *_{t'} H = D \otimes_K (K *_{t'} H)$. Then (3) $\Rightarrow$ (2) is a consequence of [9, Lemma 4.1.1]. Furthermore, $D \otimes_K J(K *_{t'} H) \subseteq J(D * H)$, where J stands for the Jacobson radical, and (2) $\Rightarrow$ (3) follows.

(2) $\Rightarrow$ (1). Assume that $D * H$ is semisimple and let $\{u_g\}_{g\in G}$ be the set of homogeneous units that leads to the given action and twisting β and t. Consider $D * G = (D * H) *_\tau^\gamma (G/H)$ as a crossed product of $\overline{G} = G/H$ with coefficients in $D * H$. The action γ permutes the primitive central idempotents of the (semisimple) ring $D * H$. For every primitive central idempotent e of $D * H$ let $\overline{G}_e$ be the stabilizer of e under the action γ and $B_e = (D * H)e$. By [8, Theorem 7.5] there is an induced crossed product $B_e *_{\tau_e}^{\gamma_e} \overline{G}_e$, and $D * G$ is semisimple if and only if $B_e *_{\tau_e}^{\gamma_e} \overline{G}_e$ is semisimple for every primitive idempotent e. We claim that γ_e is outer, that is if $\gamma_e(g + H)$ is inner, then $g \in H$.

Assume that $\gamma_e(g + H) = \iota_u$ where $u = \sum_{h\in H} u_h x_h$ is a unit of B_e. That is $ux^{\gamma_e(g+H)} = xu$ for every $x \in B_e$. By the natural embedding of D in B_e we have $ua^{\gamma_e(g+H)} = au$ for every $a \in D$. However $a^g = a^{\gamma_e(g+H)}$ and so $x_h a^{h^{-1}g} = a x_h$ for every h in the support of u. Therefore $\beta_{h^{-1}g}$ is inner, so that $h^{-1}g \in H$ and hence $g \in H$. This proves the claim.

Now by a folklore argument (see, e.g., the proof of [12, Theorem 2.3]) one deduces that $B_e * \overline{G}_e$ is simple. $\square$

Now the characterization of semisimple strongly graded rings is complete by a combination of Theorem 3.2. [8] and [3]. We put together all the pieces. Let $R = \bigoplus_{g\in G} R_g$ be a strongly G-graded ring with coefficient ring $R_1 = A$. A necessary condition for R to be semisimple is that A is semisimple, so let us assume that for the rest of the section. Let B be the *basic ring* of A. That is B is a direct product of all division rings that appear in the decomposition of A. Then A and B are Morita equivalent and hence $\mathrm{Pic}(A) = \mathrm{Pic}(B) = \mathrm{Out}(B)$ so that $\sigma : G \to \mathrm{Pic}(R)$ induces an outer action of G on B. In fact, the structure of strongly G-graded ring of R induces a structure of crossed product $B * G$ with coefficients in B [8]. Moreover, σ induces an action on $Z(A) = Z(B)$. Let E be a set of representatives of the orbits of the primitive central idempotents under this action and for every $e \in E$ let G_e be the stabilizer of e. Then σ induces group homomorphisms $\sigma_e : G_e \to \mathrm{Out}(D_e)$, where $eA = M_{n_e}(D_e)$ for some $n_e \geqslant 1$ and a division ring D_e. In fact, σ_e also induces crossed product structures $D_e * G_e$ and $M_{n_e}(D_e) * G_e$ for every $e \in E$ [8]. Let H_e be the kernel of σ_e and let P_e

be a p-Sylow subgroup of H_e, where p is the characteristic of D_e. (If D_e has characteristic 0, then P_e is the trivial group.) Recall that if $P = \prod_{i=1}^m C_i$ is an abelian p-group where each C_i is cyclic of order p^{e_i} and K is a field of characteristic p then the second cohomology group $H^2(P, K^*)$ is isomorphic to $\bigoplus_{i=1}^m K^*/(K^*)^{p^{e_i}}$ [3], thus every element of $H^2(P, K^*)$ is represented by an m-tuple $(a_1(K^*)^{p^{e_i}}, \ldots, a_m(K^*)^{p^{e_m}})$.

Theorem 3.3. *With the above notation, the following are equivalent*:

(1) *R is semisimple.*
(2) *$M_{n_e}(D_e) * G_e$ is semisimple for every $e \in E$.*
(3) *$D_e * G_e$ is semisimple for every $e \in E$.*
(4) *$D_e * H_e = D_e *_{t'_e} H_e$ is semisimple for every $e \in E$.*
(5) *$K_e *_{t'_e} H_e$ is semisimple for every $e \in E$, where $K_e = Z(D_e)$.*
(6) *$K_e *_{t'_e} P_e$ is semisimple for every $e \in E$.*
(7) *For every $e \in E$,*
   (a) *$|H'_e|$ is prime to p (so that P_e is abelian, say $P_e = \prod_{i=1}^m C_i$ with C_i cyclic of order p^{e_i}), and*
   (b) *if the restriction of t'_e to P_e is represented by an m-tuple $(a_1(K^*)^{p^{e_1}}, \ldots, a_m(K^*)^{p^{e_m}})$ then $X = \{a_1, \ldots, a_m\}$ is p-independent over K^p; that is, $K^p(Y) \neq K^p(X)$ for every proper subset Y of X.*
(8) *For every $e \in E$, $K_e *_{t'_e} P_e$ is a purely inseparable field extension of K_e.*

Proof. The equivalence between (1)–(3) was proved in [8], the equivalence between (3)–(5) is Theorem 3.2 and the equivalence between (5)–(8) was proved in [3]. See also [4, Theorem 1 and “Reductions” in pp. 411–412]. □

Corollary 3.4. *Let $R = \bigoplus_{g \in G} R_g$ be a strongly G-graded ring with coefficient ring $R_1 = A$. Assume that the action of G permutes transitively the primitive central idempotents of A (in particular all components have the same characteristic, say p), and let*

$$H = \left\{g \in G\colon\ [R_g] \in \operatorname{Pic}_{Z(eA)}(A) \text{ and } [eR_g] = [eA]\right\},$$

where e is a primitive central idempotent of A. Then the following are equivalent:

(1) *R is semisimple.*
(2) *R_H is semisimple.*
(3) *R_{H_p} is semisimple, where H_p is a p-Sylow subgroup of H if p is prime and $H_0 = \{1\}$.*

Proof. With the notation of Theorem 3.3, the assumptions imply that the set E has only one element, which we denote by e. Then, $G_e = \{g \in G\colon\ ex = xe$ for every $x \in R_g\}$ and $H = H_e$. By the equivalence of (1) and (6) in Theorem 3.3, the three conditions are equivalent to the semisimplicity of the twisted group ring $K * H_p$ where $K = Z(eA)$. □

In the next corollary p-$\deg(K)$ denotes the p-degree of a field K, that is, the minimal number of elements needed to generate K as a K^p-algebra, and $\mathrm{rank}(P)$ the rank of a group P, that is, minimal number of elements necessary to generate P.

Corollary 3.5. *If $R = \bigoplus_{g\in G} R_g$ is a semisimple strongly G-graded ring with coefficients in A, e is a primitive central idempotent of A, $K = Z(Ae)$,*

$$H = \bigl\{g \in G\colon\ [R_g] \in \mathrm{Pic}_{Z(eA)}(A) \text{ and } [eR_g] = [eA]\bigr\},$$

p is the characteristic of K and H_p a p-Sylow subgroup of H if p is prime and $H_0 = \{1\}$ then

(1) *A is semisimple,*
(2) *H_p is abelian, has a normal complement in H, and*
(3) $\mathrm{rank}(H_p) \leqslant p$-$\deg(K)$.

Proof. See the first paragraph of the section to obtain (1). For the proof of (2) and (3) we apply Theorem 3.3 and use its notation with $H_e = H$. By condition (7)(a) of Theorem 3.3, $|H'|$ is prime to p, so that H_p, is abelian and has a normal complement in H. Furthermore by condition (7)(b) of Theorem 3.3, $\mathrm{rank}(H_p) \leqslant p$-$\deg(K)$. □

Remarks 3.6. With the notation of Corollaries 3.4 and 3.5.

(1) By Noether–Skolem Theorem, if Ae is finite dimensional over its centre then $H = \{g \in G\colon\ [R_g] \in \mathrm{Pic}_{Z(eA)}(A)\}$, that is $g \in H$ if and only if $ax = xa$ for every $x \in R_g$ and $a \in Z(eA)$. In general, $g \in H$ if and only if there is $u \in eA^*$ such that $ax = xa^u$ for every $x \in R_g$ and $a \in eA$.
(2) If p does not divide $|H|$ then conditions (2) and (3) of Corollary 3.5 hold automatically.

4. The Twisting Problem for cyclic groups

Our objective in this section is to construct crossed products (and more generally strongly graded rings) with some prescribed data. The Twisting Problem for strongly graded rings asks whether a given group homomorphism $\sigma : G \to \mathrm{Pic}(A)$ can be realized by a semisimple strongly G-graded ring R assuming the necessary conditions (1)–(3) of Corollary 3.5 hold. This is a generalization of the Twisting Problem for crossed products considered in [2–4].

Of course to solve the Twisting Problem we first have to solve the problem of whether the homomorphism σ can be realized by a strongly graded ring. This is the *Realization Problem*. See [7] for a complete account of this classical question in case R is a crossed product and see [6] in case R is a general strongly graded ring.

Let $\sigma : G \to \mathrm{Pic}(A)$ be a group homomorphism and set $\sigma(g) = [R_g]$, $g \in G$. Then for every $g_1, g_2 \in G$ there is a bimodule isomorphism

$$\mu_{g_1,g_2} : R_{g_1} \otimes_A R_{g_2} \to R_{g_1 g_2}$$

and for every $g_1, g_2, g_3 \in G$ there is a unique $c(g_1, g_2, g_3) \in Z(A)^*$ such that

$$\mu_{g_1 g_2, g_3} \circ (\mu_{g_1,g_2} \otimes 1_{R_{g_3}}) = c(g_1, g_2, g_3)\mu_{g_1, g_2 g_3} \circ (1_{R_{g_1}} \otimes \mu_{g_2,g_3}).$$

(See [6] for the details.) The map $c_\sigma = c : G^3 \to Z(A)^*$ (called the Teichmüller obstruction) is a 3-cocycle. It depends on the selection of the R's and the μ's up to a 3-coboundary, that is there is a well defined map

$$\begin{aligned} \mathrm{Hom}_{\mathrm{groups}}\bigl(G, \mathrm{Pic}(A)\bigr) &\to H^3\bigl(G, Z(A)^*\bigr), \\ \sigma &\to [c_\sigma]. \end{aligned}$$

The isomorphisms μ_{g_1,g_2} define a strongly G-graded ring structure on $\bigoplus_{g\in G} R_g$ if and only if c_σ is cohomologically trivial, so that σ can be realized by a strongly graded ring if and only if c_σ is a 3-coboundary. In that case all the solutions of the Realization Problem for σ are parameterized by $H^2(G, Z(A)^*)$ up to graded isomorphism. More concretely, let $R = \bigoplus_{g\in G} R_g$ be a strongly G-graded ring that realizes σ for every $g \in G$. For every $g_1, g_2 \in G$ let $\mu_{g_1,g_2} : R_{g_1} \otimes_A R_{g_2} \to R_{g_1 g_2}$ be the isomorphism induced by the product in R. If $q \in Z^2(G, Z(A)^*)$ then $\mu' = q\mu$ induces another structure of strongly G-graded ring over A (denoted by R^q) that realizes σ. All the structures of strongly G-graded rings that realize σ can be obtained in this form. Furthermore, R and R^q are graded isomorphic if and only if $q \in B^2(G, Z(A)^*)$ (see [13, Section A.1.3]).

We summarize the discussion above in the following proposition.

Proposition 4.1. *Given a group homomorphism $\sigma : G \to \mathrm{Pic}(A)$.*

(1) [6] *There exists a strongly graded ring inducing σ if and only if the* 3*-cocycle $c = c_\sigma$ is a coboundary. This is independently of the choices of the A-bimodules $R_g \in \sigma(g)$ and the isomorphisms $R_g \otimes_A R_h \simeq R_{gh}$.*
(2) [13, Section A.1.3] *Assume such a strongly graded ring does exist. Let B be the set of graded isomorphism classes of strongly G-graded rings that induce σ. Then the group $H^2(G, Z(A)^*)$ acts transitively and freely on B.*

If an outer action has a lifting to an action then the Realization Problem for crossed products always has a positive solution (the skew group ring). In particular this is the case for commutative rings. The following example shows that the Realization Problem may have a negative answer if the base ring is non-commutative.

Example 4.2. Let $D = \mathbb{C}^{q^2}(X, Y)$ be the skew field of fractions of the complex algebra generated by X and Y defined by the relation $XY = q^2 YX$, where $q \in \mathbb{C}$ is not a root of 1. Define an action of $C_2 = \langle\sigma\rangle$ on D as follows: $X^\sigma = -X$, $Y^\sigma = qY$. This action is outer since σ^2 acts as conjugation by X. Now, suppose this outer action admits a twisting f. We can assume that f is normalized, i.e., $f(1,1) = f(1,\sigma) = f(\sigma,1) = 1$. From (2.1) we conclude that conjugation by $f(\sigma,\sigma)$ is the same as conjugation by X (action of σ^2). This implies $f(\sigma,\sigma) = zX$ where $z \in Z(D)$. Now, by (2.1), putting $g_1 = g_2 = g_3 = \sigma$ we have $f(\sigma,\sigma)^\sigma = f(\sigma,\sigma)$, but $(zX)^\sigma = -zX \neq zX$, a contradiction. It is easy to see that if q is a root of 1, then there exists a twisting that realizes this outer action.

Since the trivial map $G \to \mathrm{Out}(A)$ can always be realized by a crossed product we obtain:

Lemma 4.3. *For every $\sigma \in \mathrm{Hom}(G, \mathrm{Pic}(A)$ the obstruction c_σ belongs to the kernel of the restriction map*

$$\mathrm{res}^G_{\mathrm{Ker}\,\sigma} : H^3\big(G, Z(A)^*\big) \to H^3\big(\mathrm{Ker}\,\sigma, Z(A)^*\big).$$

We now restrict our attention to a group homomorphism $\sigma : G \to \mathrm{Pic}(A)$ where G is cyclic and A is semisimple and finitely generated as a $Z(A)$ module. In order to show that the Realization Problem has a positive solution under these conditions, we address the following strengthening of Hilbert's 90th theorem for abelian groups.

Lemma 4.4. *Let K be a field and G an abelian group acting faithfully by automorphisms on $S = K^n$. If the restriction of the action of G on the primitive idempotents of S is transitive then $H^1(G, S^*) = 1$.*

Proof. Let $e_1, \dots, e_n$ be the primitive idempotents of S. Let $g_1, \dots, g_n$ be elements in G such that $g_i(e_1) = e_i$ for any $i = 1, \dots, n$, and let N be the stabilizer of e_i (it does not depend on i since G is abelian). Then N acts on the fields Se_i for every i and $g_1, \dots, g_n$ is a transversal set for N in G. We claim that the action of N on Se_1 (and hence on every Se_i) is faithful. Indeed, assume that $\tau \in N$ acts trivially on Se_1, then for every $r \in S$ and $1 \leqslant j \leqslant n$

$$\tau(re_j) = g_j \tau g_j^{-1}(re_j) = g_j \tau\big(r^{g_j^{-1}} e_1\big) = g_j\big(r^{g_j^{-1}} e_1\big) = re_j.$$

Thus, τ acts trivially on S and so $\tau = 1$.

Now, let $f=(f_1,\dots,f_n)\in Z^1(G,S^*)$ be a 1-cocycle. The elements of N are linearly independent over Se_1 and therefore there exists an element $ae_1\in Se_1$ satisfying

$$be_1=\sum_{h\in N} f(h)h(ae_1)\in (Se_1)^*.$$

Hence

$$\begin{aligned} s &= \sum_{g\in G} f(g)g(ae_1)=\sum_{i=1}^{n}\sum_{h\in N} f(g_ih)g_ih(ae_1)\\ &= \sum_{i=1}^{n} f(g_i)g_i\sum_{h\in N} f(h)h(ae_1)=\sum_{i=1}^{n} f(g_i)g_i(be_1)\\ &= \sum_{i=1}^{n} f(g_i)g_i(be_1)e_i\\ &= \bigl(f_1(g_1)g_1(be_1), f_2(g_2)g_2(be_1),\dots, f_n(g_n)g_n(be_1)\bigr)\in S^*. \end{aligned}$$

Now it is easily seen that for every $\sigma\in G$, $f(\sigma)=s\sigma(s)^{-1}$ (see, e.g., the proof of [19, Theorem 1-5-4]) which says that the cocycle $f\in Z^1(G,S^*)$ is actually a coboundary. □

Proposition 4.5. *Let G be a cyclic group and $\sigma: G\to \mathrm{Pic}(A)$ a group homomorphism where A is semisimple and finitely generated as a module over $Z(A)$. Then σ can be realized by a strongly G-graded ring.*

Proof. By the first paragraph of Section 3 we may assume that $A=\prod_{i=1}^n D_i$ where each D_i is a division algebra finite dimensional over its centre and $\sigma: G\to \mathrm{Out}(A)$ is an outer action of G on A. The outer action σ permutes the D_i's. Let $A_1,\dots,A_k$ be the direct products of the orbits of this action giving rise to outer actions σ_i on each A_i. We need to show that the obstruction of each σ_i vanishes in $H^3(G,Z(A_i))$ (Proposition 4.1), so, without loss of generality, we may assume that $A=A_1$, that is the action is transitive on the primitive idempotents of A. Observe that for the cohomology groups of degree 3 we have an exact sequence

$$H^3\bigl(G/H,Z(A)^*\bigr)\xrightarrow{\text{inf}} H^3\bigl(G,Z(A)^*\bigr)\xrightarrow{\text{res}} H^3\bigl(H,Z(A)^*\bigr)$$

where $H=\mathrm{Ker}\,\sigma$. Indeed, since G is cyclic, the sequence above is naturally isomorphic to the sequence

$$H^1\bigl(G/H,Z(A)^*\bigr)\xrightarrow{\text{inf}} H^1\bigl(G,Z(A)^*\bigr)\xrightarrow{\text{res}} H^1\bigl(H,Z(A)^*\bigr)$$

which is exact (see [17, Chapter VII, Section 6, Proposition 4]).

By Skolem–Noether Theorem G/H acts faithfully on $Z(A)$, and hence $H^1(G/H,Z(A)^*)=1$ by Lemma 4.4. Thus, the restriction map res is injective and by Lemma 4.3 c_σ is cohomologically trivial. It follows by Proposition 4.1 that the Realization Problem has a positive solution for σ. $\square$

Note that the condition of A being finitely generated as a $Z(A)$ module in Proposition 4.5 cannot be omitted as Example 4.2 shows.

We now show that the Twisting Problem has a positive solution if G and A satisfy the conditions of Proposition 4.5.

Theorem 4.6. *The Twisting Problem has a positive solution for finite cyclic groups and rings finitely generated as modules over their centre. That is, if $G = C_m = \langle g\rangle$ is a cyclic group and $\sigma : G \to \mathrm{Pic}(A)$ is a group homomorphism with A finitely generated as module over $Z(A)$, then the following conditions are equivalent*:

(1) *There is a semisimple strongly G-graded ring that realizes σ.*
(2) (a) *A is semisimple and*
  (b) *for every primitive central idempotent e of A such that $K_e = Z(Ae)$ has characteristic $p \neq 0$, either no element of order p of G fixes the elements of K_e or K_e is not perfect.*

Proof. Assume that (1) holds. Let e be an idempotent of A such that $K = K_e$ has characteristic $p > 0$, and let P be the p-Sylow subgroup of the stabilizer of e. By Corollary 3.5, $\mathrm{rank}(P) \leqslant p\text{-}\deg(K)$. It follows that either $P = 1$, that is no element of order p of G fixes the elements of K_e, or else $p\text{-}\deg(K) \geqslant 1$, which means that K_e is not perfect.

Conversely, assume that (2) holds. As in the proof of Proposition 4.5 we may assume that A is a direct product of division rings. Furthermore, we may assume that the action on the primitive central idempotents is transitive hence $A = D^n$, where D is a division ring finite dimensional over its centre. Let $K = Z(D)$ (hence $Z(A) = K^n$), and let p be the characteristic of K. By Proposition 4.5, σ can be realized by a strongly graded ring, and under the assumption $A = D^n$, there is even a crossed product $R = A *_t^\alpha G$ that realizes σ. Assume that R is not semisimple (otherwise we are done). By Maschke's theorem $p > 0$. Fix a primitive central idempotent e of A and identify K with $Z(Ae)$. Let $H = H_e$ be the subgroup of elements of G that fix K element-wise and $P = P_e$ a p-Sylow subgroup of H. By Theorem 3.2, $P \neq 1$ and the cocycle of the subcrossed product $K * P$ is represented by an element $a \in K^{*p}$. By our assumption K is not perfect. Let $k = K^G$ be the fixed subfield of K under the action of G. Since K is a finite extension of k, k is not perfect as well and hence there exists $b \in k \setminus k^p$. Now, if we define the cocycle $f \in Z^2(G, K^*)$ by

$$f\left(g^i, g^j\right) = \begin{cases} b, & i + j \geqslant m, \\ 1, & i + j < m, \end{cases}$$

then the crossed product $S = A *^{\alpha}_{tf} G$ realizes σ and is semisimple as it is semisimple when restricted to P. $\square$

5. An application to division algebras

For an action of a finite group G on a ring R, let $\mathrm{tr}_G : R \to R^G$ denote the trace map, i.e., $\mathrm{tr}_G(x) = \sum_{g\in G} x^g$. In this section we prove the following theorem.

Theorem 5.1. *Let G be a finite group and D a division ring with centre K of characteristic $p > 0$. Suppose G acts on D via a homomorphism $\beta : G \to \mathrm{Aut}(D)$. Let $H = \beta^{-1}(\mathrm{Inn}(D))$ and let G_p and H_p be Sylow p-subgroups of G and H, respectively. Then the following are equivalent*:

(1) $\mathrm{tr}_G(D) \neq 0$.
(2) *The skew group ring $D *^{\beta} G$ is semisimple.*
(3) $\mathrm{tr}_H(D) \neq 0$.
(4) *The skew group ring $D *^{\beta} H$ is semisimple.*
(5) $\mathrm{tr}_{H_p}(D) \neq 0$ (*in particular $H_p \cap \ker(\beta) = \{1\}$ and hence $H_p \leqslant \mathrm{Aut}(D)$*).
(6) *The skew group ring $D *^{\beta} H_p$ is semisimple.*
(7) *The elements of H_p (viewed in $\mathrm{End}(D)$) are linearly independent over D.*
(8) *The elements of G_p (in $\mathrm{End}(D)$) are linearly independent over D.*

Remark 5.2. By Corollary 3.5, the conditions above yield that H_p is abelian with normal complement in H or equivalently H' is a p'-group. By [18] $\beta(H)'$ is a cyclic p'-group.

Proof. For the equivalence of (1)–(6) recall that the trace map tr_G is non-trivial if and only if D is projective over the skew group ring $D *^{\beta} G$ and these are equivalent to the semisimplicity of $D *^{\beta} G$ (see [8, Theorem 7.6]). In our case we have already shown that semisimplicity of one of the skew group rings $D *^{\beta} G$, $D *^{\beta} H$, $D *^{\beta} H_p$ is equivalent to the semisimplicity of each one of the others. Clearly (8) $\Rightarrow$ (7) $\Rightarrow$ (5). Furthermore (7) implies (8) follows from Lemma 5.4 below.

Let us prove that (5) implies (7). Assume that (5) holds. Since H_p acts by inner automorphisms on D we have $H_p \leqslant D^*/K^*$. The group extension

$$1 \to K^* \to D^* \to D^*/K^* \to 1$$

gives an extension

$$1 \to K^* \to \widehat{H}_p \to H_p \to 1.$$

For every $h \in H_p$ choose a representative $u_h \in \widehat{H}_p$, that is $x^h = u_h^{-1} x u_h$ for every $x \in D$. Since the p-group H_p is abelian (see Corollary 3.5) and K^* has no non-trivial pth roots of 1, it follows from the universal coefficients theorem that $\widehat{H}_p$ is also an abelian group. Now. if

$$1 = A_0 < A_1 < \cdots < A_t = H_p$$

is a sequence of subgroups of H_p such that $A_{i+1}/A_i \simeq C_p$ is cyclic of order p, then the corresponding extensions $\widehat{A}_i$ form a sequence of subgroups of $\widehat{H}_p$, where $\widehat{A}_{i+1}/\widehat{A}_i \simeq C_p$. For every $i = 0, \ldots, t$ let K_i be the subalgebra of D generated by $\widehat{A}_i$. Each extension K_{i+1}/K_i is either purely inseparable of degree p or trivial. We claim that K_t is p^t-dimensional over K and consequently the elements $\{u_h\}_{h\in H_p}$ are linearly independent over K. Indeed, if $\dim_K K_t < p^t = |H_p|$ then $K_{i+1} = K_i$ for some i and then $C_D(\widehat{A}_i) = C_D(K_i) = C_D(K_{i+1}) = C_D(\widehat{A}_{i+1})$ where $C_D(T)$ denotes the centralizer of T in D. This implies that the generator of $\widehat{A}_{i+1}$ modulo $\widehat{A}_i$ commutes with the image of tr_{A_i} in D. It follows that $\mathrm{tr}_{A_{i+1}} = 0$ and so $\mathrm{tr}_{H_p} = 0$, a contradiction.

Now, consider the K-algebra maps

$$\eta_1 : D \to \mathrm{End}\big(D_{D^{H_p}}\big) \qquad \text{(left multiplication)} \quad \text{and}$$
$$\eta_2 : K_t \to \mathrm{End}\big(D_{D^{H_p}}\big) \qquad \text{(right multiplication)}.$$

Clearly, the images of η_1 and η_2 commute and so we obtain a map

$$\eta = \eta_1 \otimes \eta_2 : D \otimes_K K_t \to \mathrm{End}\big(D_{D^{H_p}}\big)$$

which is injective since $D \otimes_K K_t$ is simple. In order to show that the elements of H_p are linearly independent over D let $\sum_{h\in H_p} d_h h = 0$. Then for every $x \in D$, $\sum_{h\in H_p} d_h u_h x u_h^{-1} = 0$. This says that $\eta(\sum_{h\in H_p} d_h u_h \otimes u_h^{-1}) = 0$ and by the injectivity of η, one has that $\sum_{h\in H_p} d_h u_h \otimes u_h^{-1} = 0$. Finally, by the linear independence of $\{u_h\}_{h\in H_p}$ (and hence of $\{u_h^{-1}\}_{h\in H_p}$) over K, $d_h = 0$ for all $h \in H_p$ as desired. □

Remark 5.3. By the proof of [12, Lemma 2.18], $[D : D^{H_p}] = \dim_K K_t$ and by the preceding paragraph they are equal to $\mathrm{ord}(H_p)$. It follows that $D \otimes_K K_t$ and $\mathrm{End}_{D^{H_p}}(D)$ have the same dimension over D^{H_p} and hence η is an isomorphism.

We still owe the reader

Lemma 5.4. *Let D be a division ring, G a group of automorphisms of D and $H = G \cap \mathrm{Inn}(D)$. Then the automorphisms of G (viewed in $\mathrm{End}(D)$) are linearly independent over D if and only if the elements of H are linearly independent over D.*

Proof. Assume that the elements of H are linearly independent. If the theorem is false there is a non-empty subset $\{\sigma_1, \ldots, \sigma_n\}$, $n \geqslant 2$, of G and elements $\{\alpha_i\}_{i=1}^n$ in D (not all zeroes) such that

$$\phi = \alpha_1\sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_n\sigma_n = 0.$$

Without loss of generality we can assume n is minimal, $\alpha_1 = 1 \in D$, $\sigma_1 = 1 \in G$ and $\sigma_2 \notin H$. It follows that there is $s \in D$ such that $\sigma_2(s) \neq \alpha_2^{-1} s \alpha_2$. Then

$$\begin{aligned} 0 &= s^{-1}\phi s - \phi \\ &= 1 + s^{-1}\alpha_2\sigma_2(s)\sigma_2 + s^{-1}\alpha_3\sigma_3(s)\sigma_3 + \cdots + s^{-1}\alpha_n\sigma_n(s)\sigma_n \\ &\quad - (1 + \alpha_2\sigma_2 + \alpha_3\sigma_3 + \cdots + \alpha_n\sigma_n) \\ &= \big(s^{-1}\alpha_2\sigma_2(s) - \alpha_2\big)\sigma_2 + \big(s^{-1}\alpha_3\sigma_3(s) - \alpha_3\big)\sigma_3 + \cdots \\ &\quad + \big(s^{-1}\alpha_n\sigma_n(s) - \alpha_n\big)\sigma_n. \end{aligned}$$

This linear combination is non-trivial since $s^{-1}\alpha_2\sigma_2(s) - \alpha_2 \neq 0$ and its length is $\leqslant n - 1$, a contradiction. □

References

[1] R. Alfaro, P. Ara, Á. del Río, Regular skew group rings, J. Austral. Math. Soc. Ser. A 58 (1995) 167–182.

[2] E. Aljadeff, Y. Ginosar, U. Onn, Projective representations and relative semisimplicity, J. Algebra 217 (1) (1999) 249–274.

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

[4] E. Aljadeff, D.J.S. Robinson, Solution of the twisting problem for skew group algebras, Israel J. Math. 91 (1995) 409–417.

[5] H. Bass, Algebraic K-Theory, Benjamin, 1968.

[6] A.M. Cegarra, A.R. Garzón, Obstructions to Clifford system extensions of algebras, Proc. Indian Acad. Sci., in print.

[7] M. Hacque, Produits croisés mixtes: Extensions des groupes et extensions d'anneaux, Comm. Algebra 19 (1991) 1993–2049.

[8] J. Haefner, Á. del Río, Actions of Picard groups on graded rings, J. Algebra 218 (1999) 573–607.

[9] I.N. Herstein, Noncommutative Rings, Math. Assoc. of America, 1973.

[10] E. Jespers, J. Okniński, Descending chain conditions for graded rings, J. Algebra 178 (1995) 458–479.

[11] C. Menini, C. Năstăsescu, When is R-gr equivalent to the category of modules?, J. Pure Appl. Algebra 51 (1988) 277–291.

[12] S. Montgomery, Fixed rings of finite automorphism groups of associative rings, LNM 818 (1980).

[13] C. Năstăsescu, F. Van Oystaeyen, Graded Ring Theory, in: North-Holland Math. Library, Vol. 28, North-Holland, Amsterdam, 1982.

[14] C. Năstăsescu, M. Van der Bergh, F. Van Oystaeyen, Separable functors applied to graded rings, J. Algebra 123 (1989) 397–413.

[15] D.S. Passman, Infinite Crossed Products, Academic Press, 1989.

[16] L. Rowen, Ring Theory, Vol. I, Academic Press, 1988.

[17] J.P. Serre, Local Fields, Springer-Verlag, 1979.
[18] M. Shirvani, The finite inner automorphism groups of division rings, Math. Proc. Cambridge Philos. Soc. 118 (2) (1995) 207–213.
[19] E. Weiss, Cohomology of Groups, Academic Press, 1969.