FREE UNIT GROUPS IN GROUP ALGEBRAS

J. Z. Gonçalves
D. S. Passman

University of São Paulo
University of Wisconsin-Madison

To our friend Sudarshan Sehgal on the occasion of his retirement

Abstract. Let $K[G]$ denote the group algebra of a finite group G over a field K. If either $\operatorname{char} K = 0$ and G is nonabelian, or K is a nonabsolute field of characteristic $\pi > 0$ and $G/\mathbb{O}_\pi(G)$ is nonabelian, then it is well known that the group of units $\mathrm{U}(K[G])$ contains a nonabelian free group. For the most part, this follows from the fact that $\mathrm{GL}_2(K)$ contains such a free subgroup. In this paper, we refine the above result by showing that there are two cyclic subgroups X and Y of G of prime power order, and two units $u_X \in \mathrm{U}(K[X])$ and $u_Y \in \mathrm{U}(K[Y])$, such that $\langle u_X, u_Y \rangle$ contains a nonabelian free group. Indeed, we obtain a rather precise description of these units by using an aspect of Tits' theorem on free subgroups in linear groups.

§1. Introduction

Let $K[G]$ denote the group algebra of a finite group G over a field K. In this paper, we are concerned with the existence of nonabelian free subgroups of the group of units $\mathrm{U}(K[G])$. For convenience and following [GP2], we say that an arbitrary group $\mathfrak{G}$ is 2-related if it contains no nonabelian free subgroup. Thus $\mathfrak{G}$ is 2-related if and only if every homomorphism from the 2-generator free group $\mathfrak{F}_2$ into $\mathfrak{G}$ has a nontrivial kernel and hence if and only if every two elements of $\mathfrak{G}$ are related, that is satisfy a nontrivial word in $\mathfrak{F}_2$. Obviously, the property of being 2-related is closed under taking subgroups and homomorphic images.

If G is abelian, then $\mathrm{U}(K[G])$ is commutative, and if $G/\mathbb{O}_\pi(G)$ is abelian, where $\operatorname{char} K = \pi > 0$ and $\mathbb{O}_\pi(G)$ is the largest normal π-subgroup of G, then $\mathrm{U}(K[G])$ is solvable since the kernel of the natural homomorphism $K[G] \to K[G/\mathbb{O}_\pi(G)]$ is a nilpotent ideal. Furthermore, if K is an absolute field, that is algebraic over a finite

2000 *Mathematics Subject Classification.* 16S34, 16U60.

Key words and phrases. Group algebra, unit group, free subgroup.

The first author's research was supported in part by CNPq and Fapesp - Brazil. The second author's research was supported in part by NSF Grant DMS-9820271.

field, then $\mathrm{U}(K[G])$ is a periodic group. Certainly, in all of these three situations, $\mathrm{U}(K[G])$ cannot contain a nonabelian free group and consequently it is 2-related. On the other hand, if $K[G]$ does not satisfy the above, then $\mathrm{U}(K[G])$ does contain a nonabelian free group. For the most part, this result of [G] follows from the fact that $\mathrm{GL}_2(K)$ contains such a free subgroup. See [HP] for the analogous problem in integral group rings.

If G has a nonnormal subgroup, then specific generators for a nonabelian free subgroup of the unit group of the integral group ring $\mathbf{Z}[G]$ were given in [MS]. A similar result for group algebras in positive characteristic can be found in [GP1]. In this paper, we consider units of a different nature, namely

Definition 1.1. *Let $K[G]$ be the group algebra of G over a nonabsolute field K, and let $X = \langle x \rangle$ be a cyclic subgroup of G of prime power order. Then we say that $u_X \in \mathrm{U}(K[X])$ is a special unit, depending upon the generator x, if one of the following three conditions is satisfied.*

i. $\mathrm{char}\, K = 0$ *and* $u_X = (x-r)/(x-s)$ *for suitable integers* $r, s \in \mathbf{Z} \subseteq K$ *with* $r, s \geq 2$.
ii. $\mathrm{char}\, K = \pi > 0$, $|X|$ *is prime to* π, *and* $u_X = (x-r)/(x-s)$ *for suitable* $r, s \in K$ *that are positive powers of a fixed element* $t \in K$ *transcendental over the prime subfield* $K_0 = \mathrm{GF}(\pi)$.
iii. $\mathrm{char}\, K = \pi > 0$, X *is a* π*-group, and* $u_X = 1 + t(1 + x + \cdots + x^{\pi-1})$ *where* $t \in K$ *is transcendental over* K_0.

In parts (ii) and (iii) above, we say more precisely that u_X is special, based on t. Using this notation, our main result is

Theorem 1.2. *Assume that either* $\mathrm{char}\, K = 0$ *and G is nonabelian, or that K is a nonabsolute field of characteristic $\pi > 0$ and $G/\mathbb{O}_\pi(G)$ is nonabelian. Then there are two cyclic subgroups X and Y of G of prime power order, and two special units $u_X \in \mathrm{U}(K[X])$ and $u_Y \in \mathrm{U}(K[Y])$ (based on the same preselected transcendental element if* $\mathrm{char}\, K > 0$*), such that $\langle u_X, u_Y \rangle$ is not 2-related.*

As a consequence, we obtain

Corollary 1.3. *Assume that either* $\mathrm{char}\, K = 0$ *and G is nonabelian, or that K is a nonabsolute field of characteristic $\pi > 0$ and $G/\mathbb{O}_\pi(G)$ is nonabelian. Then the subgroup of* $\mathrm{U}(K[G])$ *generated by units of the form $x - r$ with $x \in G$ and $r \in K$ has a nonabelian free subgroup.*

These results are proved, by induction on $|G|$, in Section 4. The key groups that must be considered are given by

Lemma 1.4. *Let G be a finite group and let π be a fixed prime. Suppose that $G/\mathbb{O}_\pi(G)$ is nonabelian, but that $H/\mathbb{O}_\pi(H)$ is abelian for every proper subgroup*

and every proper homomorphic image H of G. Then we have the following two possibilities.

i. (The p-group case) *G is a p-group with $p \neq \pi$, its center $\mathbb{Z}(G)$ is cyclic of index p^2, and $|G'| = p$. Furthermore, either $|G| = p^3$, or $G = X \rtimes Y$ where X is cyclic and $|Y| = p$.*
ii. (The Frobenius case) *$G = A \rtimes X$ where A is an elementary abelian q-group with the prime q different from π, X is cyclic of prime order $p \neq q$, and X acts faithfully and irreducibly on A.*

Proof. It is clear that $\mathbb{O}_\pi(G) = 1$. Suppose first that $\mathbb{Z}(G) \neq 1$ and choose Z to be a central subgroup of prime order p. Since $\mathbb{O}_\pi(G) = 1$, we have $p \neq \pi$ and it follows easily that $\mathbb{O}_\pi(G/Z) = 1$. Hence G/Z is an abelian π'-group by hypothesis. Thus G is nilpotent of class 2 and $Z = G'$. In particular, Z is unique, so $\mathbb{Z}(G)$ must be a cyclic p-group, and since G is nilpotent, we see that G is also a p-group. Using $p \neq \pi$, we conclude from the hypothesis that G is a minimal nonabelian p-group and hence, by [MM], either $|G| = p^3$ or $G = X \rtimes Y$ with X cyclic and $|Y| = p$.

We can now assume that $\mathbb{Z}(G) = 1$ and, in particular, that G is not nilpotent. Suppose next, by way of contradiction, that G is simple, and let $p \neq \pi$ be a prime divisor of $|G|$. If P is any nonidentity p-subgroup of G, then $\mathbb{N}_G(P)$ is proper and therefore has a normal p-complement by hypothesis. Frobenius' theorem (see [H, Satz IV.5.8(b)] now implies that G has a normal p-complement, and this contradicts the assumption that G is a simple group that is not nilpotent. Consequently, G is not simple, and we conclude from the hypothesis that G is solvable.

Finally, let A be a minimal normal subgroup of G. Then A is an elementary abelian q-group for some prime $q \neq \pi$, and A is not central. In particular, we can choose $x \in G$ to be an element of minimal order not centralizing A. Certainly x has prime power order, say $|x| = p^n$. Note that the group $\langle A, x\rangle$ has a nontrivial commutator subgroup contained in A, so $G = \langle A, x\rangle$ by hypothesis. The minimal nature of $|x|$ now implies that $x^p \in \mathbb{Z}(G) = 1$, and hence $X = \langle x\rangle$ is cyclic of prime order p. Clearly, $G = A \rtimes X$ and, since A is a minimal normal subgroup of G, we conclude that X acts faithfully and irreducibly on A. □

As we will see, the p-groups above are fairly easy to handle, but the Frobenius group work is much more difficult. The proof of our main theorem uses techniques from [GP2]. However, the objective of that paper was somewhat different from the problem here. In particular, since we were not concerned with a precise description of the unitary units in $K[G]$, we were able to finesse a serious study of the Frobenius group $G = A \rtimes X$ in [GP2]. Here, we have to come to grips with the representation theory of such groups. Surprisingly, there are interesting open questions concerning these representations, especially in positive characteristic. We start with a few simple properties. See [I1] for basic information on this subject. We do have to be a bit careful below to allow for the possibility that p is the characteristic of K.

Lemma 1.5. *Let $G = A \rtimes X$ where A is an elementary abelian q-group, X is cyclic of prime order p, and X acts faithfully and irreducibly on A. Let K be a field of characteristic $\neq q$, and assume that K contains a primitive qth root of unity.*

i. *If $\mu\colon K[A] \to K$ is a nonprincipal linear character of A, that is a nontrivial one-dimensional character, then the induced representation $\theta = \mu^G$ is an absolutely irreducible representation of $K[G]$.*
ii. *Conversely, if θ is a nonlinear irreducible representation of $K[G]$ and if $\mu\colon K[A] \to K$ is a constituent of the restriction θ_A, then $\mu \neq 1$ and $\theta = \mu^G$.*

In either situation, θ is faithful on the group G and $\deg\theta = p$. Furthermore, θ is injective on the group ring $K[X]$ and, by conjugating if necessary, we can assume that $\theta(\alpha) = \operatorname{diag}(\mu(\alpha), \mu(\alpha^x), \dots, \mu(\alpha^{x^{p-1}}))$ for all $\alpha \in K[A]$.

Proof. Since $G = A \rtimes X$ is a Frobenius group, X acts in a fixed-point-free manner on the dual group of A. Thus, each nonprincipal character of $K[A]$ has $p = |X|$ conjugates under the action of X.

(i) Let $\mu\colon K[A] \to K$ be a nonprincipal character and set $\theta = \mu^G$. Then $\deg\theta = p$ and $\theta_A = \mu_1 + \mu_2 + \cdots + \mu_p$ is the sum of the p distinct conjugates of μ. If ψ is an irreducible subrepresentation of θ, then ψ_A must contain some μ_i, and hence it contains the entire X-orbit of μ. In particular, we have $p = \deg\theta \geq \deg\psi \geq p$, so $\theta = \psi$ is irreducible.

(ii) Conversely, let θ be a nonlinear irreducible representation of $K[G]$ and let μ be an irreducible constituent of θ_A. If $\mu = 1$, then $G' = A \subseteq \ker\theta$ and θ is linear, a contradiction. Thus, $\mu \neq 1$ and hence, by (i) above, μ^G is irreducible. In particular, since θ is a quotient of $(\theta_A)^G$ and since the latter is a direct sum of copies of μ^G, we conclude that $\theta = \mu^G$, as required.

The remaining observations follow from the definition of induced representation and the fact that $A = G'$ is the unique nontrivial normal subgroup of G. □

§2. Frobenius Groups

As we indicated in the introduction, our proof relies on certain special case considerations. Indeed, the p-groups are easy to handle, while the Frobenius groups are much more of a challenge. The following result is well known. We include it here as motivation for later work.

Lemma 2.1. *Let G be a nilpotent group of class ≤ 2 and let $\theta\colon K[G] \to \mathrm{M}_n(K)$ be a G-faithful absolutely irreducible representation. If T is a transversal for $\mathbb{Z}(G)$ in G, then $\theta(T)$ is a K-basis for $\mathrm{M}_n(K)$ and hence $n^2 = |T| = |G : \mathbb{Z}(G)|$.*

Proof. Since θ is absolutely irreducible, $\theta(K[G]) = \mathrm{M}_n(K)$. Now for each $g \in G$, let $\chi(g) \in K$ be the matrix trace of $\theta(g)$. Thus $\chi\colon G \to K$ is the character of G associated with θ. If $g \in \mathbb{Z}(G)$, then $\theta(g) = \lambda I$ is a scalar matrix, and hence $\chi(g) = \lambda n$. If $g \notin \mathbb{Z}(G)$, then since G has class ≤ 2, there exists $x \in G$ with

$x^{-1}gx = gz$ for some $1 \neq z \in \mathbb{Z}(G)$. Thus $\theta(x)^{-1}\theta(g)\theta(x) = \theta(g)\theta(z) = \mu\theta(g)$, where $\theta(z) = \mu I$, and $\mu \neq 1$ since $z \neq 1$ and θ is faithful. Taking matrix traces and using the fact that similar matrices have the same trace, we obtain $\chi(g) = \mu \cdot \chi(g)$ and hence $\chi(g) = 0$. In other words, χ vanishes off $\mathbb{Z}(G)$. Now all matrices in $\theta(\mathbb{Z}(G))$ are scalar, so it follows that $\theta(T)$ spans $\mathrm{M}_n(K)$. Furthermore, since there are matrices in $\mathrm{M}_n(K)$ with nonzero trace, we see that χ cannot vanish on G, and in particular we have $n \neq 0$ in K. Finally, suppose $\sum_{g \in T} k_g \theta(g) = 0$ is a linear dependence relation for $\theta(T)$. If $x \in T$, then multiplying this equation by $\theta(x^{-1})$ and taking traces yields $k_x n = 0$, since $gx^{-1} \in \mathbb{Z}(G)$ if and only if $g = x$. Thus $k_x = 0$ for all $x \in T$, and $\theta(T)$ is K-linearly independent, as required. $\square$

Next, we consider the necessary Frobenius groups. Specifically, let $G = A \rtimes X$, where A is an elementary abelian q-group, $X = \langle x \rangle$ is cyclic of prime order p, and X acts faithfully and irreducibly on A. Assume that K is a field of characteristic different from p and q, and that K contains a primitive (pq)th root of unity. We fix this notation throughout the remainder of the section.

If θ is a nonlinear irreducible representation of $K[G]$, then by Lemma 1.5, θ is faithful on G and $\theta(K[G]) = \mathrm{M}_p(K)$ has dimension p^2. In analogy with Lemma 2.1, it is appropriate to ask whether there is a natural basis for this matrix ring built from certain group elements. For example, if $1 \neq a \in A$, then $Y = aXa^{-1}$ is a cyclic subgroup of G of order p disjoint from X. Thus XY is a set of p^2 distinct elements of G and we ask whether $\theta(XY)$ is a basis for $\mathrm{M}_p(K)$. As it turns out, this is indeed the case if either $\operatorname{char} K = 0$ or $\operatorname{char} K$ is positive and sufficiently large as a function of p and q. On the other hand, we will show by example that there exists an appropriate $K[G]$ such that for all θ and all X, Y, the set $\theta(XY)$ is not a basis for the matrix ring.

Returning to the general group G, we know that $\theta(K[A])$ may be taken to be the set of diagonal matrices in $\mathrm{M}_p(K)$, and hence this image has dimension p. On the other hand, each nonidentity G-conjugacy class contained in A has size p, and we ask whether there exists such a class $\mathfrak{K}_a$ with $\theta(\mathfrak{K}_a)$ a basis for the diagonal matrices. This question turns out to be precisely equivalent to the preceding one, and hence has the same positive and negative answers. Fortunately, we are able to partially finesse the negative answers and prove a result just strong enough to enable us to construct the units we require.

We now start the formal considerations. Since X acts on A, it also acts on $K[A]$, and for each linear character $\lambda : K[X] \to K$, we define the λ-trace $\mathrm{tr}_\lambda \colon K[A] \to K[A]$ to be the K-linear map given by

$$\mathrm{tr}_\lambda \alpha = \sum_{i=0}^{p-1} \lambda(x^{-i}) \alpha^{x^i} = \sum_{i=0}^{p-1} \lambda(x^i) \alpha^{x^{-i}} \qquad \text{for all } \alpha \in K[A].$$

Basic properties are as follows.

Lemma 2.2. *With the above notation, we have* $(\mathrm{tr}_\lambda\,\alpha)^x = \lambda(x)\,\mathrm{tr}_\lambda\,\alpha$ *and*

$$(\mathrm{tr}_\lambda\,\alpha)(\mathrm{tr}_\mu\,\beta) = \sum_{k=0}^{p-1} \lambda(x^{-k})\,\mathrm{tr}_{\lambda\mu}(\alpha^{x^k}\beta) = \sum_{k=0}^{p-1} \mu(x^{-k})\,\mathrm{tr}_{\lambda\mu}(\alpha\beta^{x^k}).$$

Proof. For the first fact, note that

$$(\mathrm{tr}_\lambda\,\alpha)^x = \sum_i \lambda(x^{-i})\alpha^{x^{i+1}} = \lambda(x)\sum_i \lambda(x^{-(i+1)})\alpha^{x^{i+1}} = \lambda(x)\,\mathrm{tr}_\lambda\,\alpha.$$

For the second, write $i = j + k$ and observe that

$$\begin{aligned}(\mathrm{tr}_\lambda\,\alpha)(\mathrm{tr}_\mu\,\beta) &= \sum_{i,j} \lambda(x^{-i})\alpha^{x^i}\mu(x^{-j})\beta^{x^j} = \sum_{j,k} \lambda(x^{-(j+k)})\mu(x^{-j})\alpha^{x^{j+k}}\beta^{x^j} \\ &= \sum_k \lambda(x^{-k}) \sum_j \lambda\mu(x^{-j})(\alpha^{x^k}\beta)^{x^j} = \sum_k \lambda(x^{-k})\,\mathrm{tr}_{\lambda\mu}(\alpha^{x^k}\beta).\end{aligned}$$

The third formula follows from the above by interchanging the factors. □

Now suppose $\mu\colon K[X] \to K$ is a linear character. Then the idempotent $e_\mu \in K[X]$ associated with μ is given by

$$e_\mu = \frac{1}{p}\sum_{i=0}^{p-1} \mu(x^{-i})x^i = \frac{1}{p}\sum_{i=0}^{p-1} \mu(x^i)x^{-i}.$$

Indeed, we have

$$xe_\mu = \frac{1}{p}\sum_{i=0}^{p-1} \mu(x^{-i})x^{i+1} = \frac{\mu(x)}{p}\sum_{i=0}^{p-1} \mu(x^{-i-1})x^{i+1} = \mu(x)e_\mu.$$

The basic relation between these idempotents and the λ-traces is as follows.

Lemma 2.3. *Let* $\mu, \eta\colon K[X] \to K$ *be linear characters and let* $\alpha \in K[A]$. *Then*

$$e_\mu \alpha e_\eta = \frac{1}{p}(\mathrm{tr}_\lambda\,\alpha)e_\eta = \frac{1}{p}e_\mu(\mathrm{tr}_\lambda\,\alpha)$$

where $\lambda = \mu^{-1}\eta$.

Proof. To start with, we have

$$\begin{aligned}e_\mu \alpha e_\eta &= \frac{1}{p}\sum_{i=0}^{p-1} \mu(x^i)x^{-i}\alpha\cdot e_\eta = \frac{1}{p}\sum_{i=0}^{p-1} \mu(x^i)x^{-i}\alpha x^i\cdot x^{-i}e_\eta \\ &= \frac{1}{p}\sum_{i=0}^{p-1} \mu(x^i)\eta(x^{-i})x^{-i}\alpha x^i\cdot e_\eta\end{aligned}$$

since $x^{-i}e_\eta = \eta(x^{-i})e_\eta$. Thus, setting $\lambda = \eta\mu^{-1}$, we obtain

$$e_\mu \alpha e_\eta = \frac{1}{p}\sum_{i=0}^{p-1} \lambda(x^{-i})\alpha^{x^i}\cdot e_\eta = \frac{1}{p}(\mathrm{tr}_\lambda\, \alpha)\cdot e_\eta.$$

The second formula follows in a similar fashion. □

Recall, from Lemma 1.5, that every nonlinear irreducible representation θ of $K[G]$ has degree p. Furthermore, according to that lemma, we can always assume that $\theta(A)$ consists of diagonal matrices.

Lemma 2.4. *Let θ be a nonlinear irreducible representation of $K[G]$, and let $\mu\colon K[A] \to K$ be a constituent of the restriction θ_A. If $\alpha \in K[A]$, then $\theta(\mathrm{tr}_\lambda\, \alpha)$ is either zero or an invertible element in $\mathrm{M}_p(K) = \theta(K[G])$. It is invertible if and only if $\sum_{i=0}^{p-1} \lambda(x^{-i})\mu(\alpha^{x^i}) \neq 0$.*

Proof. Since $\mathrm{tr}_\lambda\, \alpha$ commutes with A and since $(\mathrm{tr}_\lambda\, \alpha)^x = \lambda(x)\,\mathrm{tr}_\lambda\, \alpha$, we see that $\theta(\mathrm{tr}_\lambda\, \alpha)\mathrm{M}_p(K)$ is a two-sided ideal of the matrix ring $\mathrm{M}_p(K) = \theta(K[G])$. With this, it is clear that $\theta(\mathrm{tr}_\lambda\, \alpha)$ is either zero or invertible. Furthermore, since $\theta(\mathrm{tr}_\lambda\, \alpha)$ is a diagonal matrix, it is invertible if and only its $(1,1)$-entry is not zero, and according to Lemma 1.5, this entry is equal to $\sum_{i=0}^{p-1} \lambda(x^{-i})\mu(\alpha^{x^i})$. □

We can now prove the equivalence of the various problems.

Lemma 2.5. *Let θ be a nonlinear irreducible representation of $K[G]$, and let μ be an irreducible constituent of θ_A. Fix $1 \neq a \in A$, and set $Y = aXa^{-1}$. The following are equivalent.*

i. *$\theta(XY) = \theta(X)\theta(Y)$ is a basis for $\mathrm{M}_p(K) = \theta(K[G])$.*
ii. *$\theta(\mathfrak{K}_a)$ is a basis for the diagonal matrices in $\mathrm{M}_p(K)$.*
iii. *$\theta(\mathrm{tr}_\lambda\, a) \neq 0$ for each $\lambda\colon K[X] \to K$.*
iv. *$\sum_{i=0}^{p-1} \lambda(x^{-i})\mu(a^{x^i}) \neq 0$ for each $\lambda\colon K[X] \to K$.*

Proof. We show that each of these conditions is equivalent to (iii), and note that (iv) $\Leftrightarrow$ (iii) follows from the previous lemma.

(ii) $\Leftrightarrow$ (iii). If $\theta(\mathfrak{K}_a) = \{\theta(a), \theta(a^x), \ldots, \theta(a^{x^{p-1}})\}$ is K-linearly independent, then certainly $\theta(\mathrm{tr}_\lambda\ a) \neq 0$ for each λ. Conversely, suppose that each $\theta(\mathrm{tr}_\lambda\ a) \neq 0$ and note that, by Lemma 2.2, each of these is an eigenvector for the conjugation action of $\theta(x)$ with distinct eigenvalue $\lambda(x)$. Thus, the various $\theta(\mathrm{tr}_\lambda\ a)$ are linearly independent and span a K-vector space of dimension p. Since this space is contained in the span of $\theta(\mathfrak{K}_a)$, we conclude that the latter span has dimension p and is equal to the set of diagonal matrices in $\mathrm{M}_p(K)$.

(i) $\Leftrightarrow$ (iii). Let $\mu, \eta\colon K[X] \to K$, let e_μ be the idempotent of $K[X]$ associated with μ, and let $f_\eta = ae_\eta a^{-1}$ be the idempotent of $K[Y]$ associated with η. Then,

by Lemma 2.3,

$$e_\mu f_\eta = (e_\mu a e_\eta)a^{-1} = \frac{1}{p}(\mathrm{tr}_\lambda\, a)e_\eta a^{-1},$$

where $\lambda = \mu^{-1}\eta$. Since θ is faithful on $K[X]$ and $K[Y]$, we know that $\theta(e_\mu)$ and $\theta(f_\eta)$ are not 0. If $\theta(X)\theta(Y)$ is linearly independent, then it follows immediately that $\theta(e_\mu)\theta(f_\eta) \neq 0$ for all μ, η, and hence that $\theta(\mathrm{tr}_\lambda\, a) \neq 0$ for all λ. Conversely, if $\theta(\mathrm{tr}_\lambda\, a) \neq 0$ for all λ, then since $\theta(\mathrm{tr}_\lambda\, a)$ and $\theta(a^{-1})$ are invertible, we see that $\theta(e_\mu)\theta(f_\eta) \neq 0$ for all μ, η. The orthogonality of the sets $\{e_\mu \mid \text{all } \mu\}$ and $\{f_\eta \mid \text{all } \eta\}$ now clearly implies that the set $\{\theta(e_\mu)\theta(f_\eta) \mid \text{all } \mu, \eta\}$ of size p^2 is linearly independent and hence spans $\mathrm{M}_p(K)$. Therefore, $\theta(X)\theta(Y)$ also spans $\mathrm{M}_p(K)$. □

It is now a simple matter to obtain the positive answers.

Proposition 2.6. *Let $G = A \rtimes X$, where A is an elementary abelian q-group, X is cyclic of prime order p, and X acts faithfully and irreducibly on A. Let K be a field with either* $\mathrm{char}\, K = 0$ *or with* $\mathrm{char}\, K > p^{(p-1)(q-1)}$*, and assume that K contains a primitive (pq)th root of unity. If θ is any nonlinear irreducible representation of $K[G]$ and if a is any nonidentity element of A, then $\theta(X)\theta(aXa^{-1})$ is a basis for $\mathrm{M}_p(K) = \theta(K[G])$ and $\theta(\mathfrak{K}_a)$ is a basis for the diagonal matrices in $\mathrm{M}_p(K)$.*

Proof. In view of Lemma 2.5, it suffices to show that $f(\lambda, \mu) = \sum_{i=0}^{p-1} \lambda(x^{-i})\mu(a^{x^i})$ is not zero for all nonprincipal $\mu\colon K[A] \to K$ and all $\lambda\colon K[X] \to K$. We begin with fields of characteristic 0.

Suppose first that $\lambda = 1$, and note that each $\mu(a^{x^i})$ is a qth root of unity. Let ε be a fixed primitive qth root of 1 and let c_j denote the number of $\mu(a^{x^i})$ equal to ε^j. Then $c_0 + c_1 + \cdots + c_{q-1} = p$ and $f(1, \mu) = c_0\varepsilon^0 + c_1\varepsilon^1 + \cdots + c_{q-1}\varepsilon^{q-1}$. If $f(1, \mu) = 0$, then the expression on the right must be a scalar multiple of the minimal polynomial $1 + \varepsilon + \cdots + \varepsilon^{q-1}$ for ε over the rationals $\mathbf{Q}$. Thus all c_j equal c_0 and, from $c_0 + c_1 + \cdots + c_{q-1} = p$, we obtain $qc_0 = p$, a contradiction.

Next, suppose that $\lambda \neq 1$ and let $\lambda(x) = \delta^{-1}$, where δ is a primitive pth root of unity. Then $f(\lambda, \mu) = \mu(a) + \mu(a^x)\delta + \cdots + \mu(a^{x^{p-1}})\delta^{p-1}$. Since the fields $\mathbf{Q}[\varepsilon]$ and $\mathbf{Q}[\delta]$ are linearly disjoint over $\mathbf{Q}$, the minimal polynomial of δ over $\mathbf{Q}[\varepsilon]$ is the same as over $\mathbf{Q}$, namely $1 + \delta + \cdots + \delta^{p-1}$. In particular, if $f(\lambda, \mu) = 0$, then all coefficents of the δ^i are equal, since $\mu(a^{x^i}) \in \mathbf{Q}[\varepsilon]$. In other words, μ is constant on the class $\mathfrak{K}_a$ and, by Lemma 1.5, $\theta(a)$ is central in $\mathrm{M}_p(K)$. But A is the unique nontrivial normal subgroup of G, so $\theta(A)$ is central in $\mathrm{M}_p(K)$, and hence so is $\theta(G)$, since G/A is cyclic. This contradicts the fact that θ is not linear, so we conclude that $f(\lambda, \mu) \neq 0$ for all appropriate λ and μ.

Finally, note that each $f(\lambda, \mu)$ is a nonzero algebraic integer, and that it and all its Galois conjugates are sums of p roots of unity. Hence each Galois conjugate of $f(\lambda, \mu)$ is nonzero and has absolute value $\leq p$. Since $f(\lambda, \mu) \in \mathbf{Q}[\varepsilon, \delta]$, we see that $\mathrm{N}(f(\lambda, \mu))$, the norm of the element under the Galois group $\mathrm{Gal}(\mathbf{Q}[\varepsilon, \delta]/\mathbf{Q})$ of order $(p-1)(q-1)$, is a nonzero integer of absolute value at most $p^{(p-1)(q-1)}$.

Thus, this norm remains nonzero when viewed in a field K of characteristic larger than $p^{(p-1)(q-1)}$. It then follows easily that $f(\lambda, \mu)$ is nonzero in all such fields of large positive characteristic, and the result is proved. $\square$

At this point, it is appropriate to offer an example. While the basic idea here is simple, the computations are tedious and require a computer algebra system. We use Maple V (see [BM]), but Maple 6 will also work. It is certainly possible that smaller counterexamples exist. We have not tried a systematic search.

Example 2.7. *There exists a group $G = A \rtimes X$ and an appropriate group algebra $K[G]$ with* $\operatorname{char} K$ *different from p and q such that, for all $1 \neq a \in A$,*

i. $(\operatorname{tr}_1 a)(\operatorname{tr}_1 a^{-1}) = e$, *where e is the principal idempotent of $K[A]$.*
ii. $(\operatorname{tr}_1 a)/p$ *is an idempotent.*
iii. $(\operatorname{tr}_\lambda a)(\operatorname{tr}_{\lambda^{-1}} a) = 0$ *for some $\lambda \neq 1$.*

In particular, if θ is a nonlinear irreducible representation of $K[G]$, then the product $\theta(X)\theta(aXa^{-1})$ is not a basis for $\mathrm{M}_p(K) = \theta(K[G])$ and $\theta(\mathfrak{K}_a)$ does not span the diagonal matrices in the matrix ring.

Proof. The computations in $K[G]$ simplify if we limit the number of G-conjugacy classes contained in A. Since there are no counterexamples with just two classes, we consider the case where there are precisely three. Furthermore, it is reasonable to assume that A is not cyclic. Thus, since each nonidentity class has size p, we want $|A| = q^n = 1 + 2p$ with $n > 1$, and it is easy to see that this equation requires q to equal 3 and n to be a prime. The smallest possibility here is $3^3 = 1 + 2{\cdot}13$, and the next is $3^7 = 1 + 2{\cdot}1093$. Presumably, one does not know if there are infinitely many solutions to this equation. The first few can be obtained from Maple V using the commands:

```
for i from 1 to 25 do
  n := ithprime(i) :
  p := (3^n - 1)/2 :
  isprime(p) :
od;
```

There are four solutions with $n < 100$, namely $n = 3, 7, 13$, and 71.

Suppose we take such a solution. Since p divides $3^n - 1$, there is a subgroup $X = \langle x \rangle$ of order p in the multiplicative group of $\mathrm{GF}(3^n)$. In particular, if A is the additive group of this field, then A is elementary abelian of order 3^n and X acts faithfully on A by field multiplication. Indeed, it acts irreducibly since $3^n - 1 = 2p$ implies that p cannot divide $3^m - 1$ for any $0 < m < n$. Form $G = A \rtimes X$ and note that no nonidentity element of A can be conjugate to its inverse since G has odd order. Thus, for any such $1 \neq a \in A$, the three G-conjugacy classes contained in A are $\mathfrak{K}_1 = \{1\}, \mathfrak{K}_a$, and $\mathfrak{K}_{a^{-1}}$.

(i) It is convenient to first work in the rational group ring $\mathbf{Q}[G]$. Here we have

$$(\operatorname{tr}_1 a)(\operatorname{tr}_1 a^{-1}) = u + v(\operatorname{tr}_1 a) + w(\operatorname{tr}_1 a^{-1})$$

for suitable integers u, v, and w. Clearly $u = p$ is the number of times the identity element occurs in the product. Next, note that the left-hand side is fixed under the usual antiautomorphism $*$ of $\mathbf{Q}[A]$ obtained by mapping each group element to its inverse. Thus the right-hand side is also $*$-stable and this implies that $v = w$. Finally, by applying the augmentation map $\mathbf{Q}[G] \to \mathbf{Q}$ to the above, or by just counting group elements, we obtain $p^2 = p + 2pv$. Hence $w = v = (p-1)/2$ and

$$(\mathrm{tr}_1\, a)(\mathrm{tr}_1\, a^{-1}) = \frac{p+1}{2} + \frac{p-1}{2}(1 + \mathrm{tr}_1\, a + \mathrm{tr}_1\, a^{-1}) = \frac{p+1}{2} + \frac{p-1}{2}|A|e,$$

where e is the principal idempotent in $\mathbf{Q}[A]$. In particular, if K is any field whose characteristic divides $(p+1)/2$, then, using the same notation in $K[G]$, we see that $(\mathrm{tr}_1\, a)(\mathrm{tr}_1\, a^{-1})$ is a scalar multiple of e. In fact, since $(p-1)/2 = (p+1)/2 - 1$ and $|A| = 3^n = 1 + 2p = 4((p+1)/2) - 1$, it follows that the scalar is equal to 1. When $n = 3$ and $p = 13$, we have $\mathrm{char}\, K = 7$, and when $n = 7$ and $p = 1093$, we have $\mathrm{char}\, K = 547$. The third example also yields only one characteristic, but the fourth with $n = 71$ yields five different possibilities. Note that, if θ is a nonlinear irreducible representation of $K[G]$, then $\theta(e) = 0$ and hence, by Lemma 2.4, either $\theta(\mathrm{tr}_1\, a) = 0$ or $\theta(\mathrm{tr}_1\, a^{-1}) = 0$.

(ii) We continue with the above example. As we observed, $1 + \mathrm{tr}_1\, a + \mathrm{tr}_1\, a^{-1} = |A|e = -e$ and $(\mathrm{tr}_1\, a)(\mathrm{tr}_1\, a^{-1}) = e$. Furthermore, since $p = -1$ in the field K, we have $(\mathrm{tr}_1\, a)e = pe = -e$ and consequently

$$e = (\mathrm{tr}_1\, a)(-e) = (\mathrm{tr}_1\, a)(1 + \mathrm{tr}_1\, a + \mathrm{tr}_1\, a^{-1}) = \mathrm{tr}_1\, a + (\mathrm{tr}_1\, a)^2 + e.$$

Thus, $(\mathrm{tr}_1\, a)^2 = -(\mathrm{tr}_1\, a)$, and $(\mathrm{tr}_1\, a)/p = -(\mathrm{tr}_1\, a)$ is indeed an idempotent.

(iii) To proceed further, we need a more precise understanding of the action of $X = \langle x \rangle$ on A. Unfortunately, the smallest group with $p = 13$ does not yield an appropriate example, so it is necessary to work with $p = 1093$. To start with, the commands:

```
p := 1093;
cyclo := simplify( ( y^p - 1)/(y - 1) ) :
Factor(cyclo) mod 3;
```

yield a factorization modulo 3 of the cyclotomic polynomial for p. Choosing a nice factor, we let the action of x on $A = \mathrm{GF}(3^n)$ satisfy the trinomial $x^7 - x^5 - 1 = 0$. Thus, every element of A can be written uniquely as $a^{f(x)}$, where $f(x)$ is a polynomial in x over $\mathrm{GF}(3)$ of degree ≤ 6. We can list the exponents for the elements in the conjugacy class $\mathfrak{K}_a$ via:

```
trinom := x^7 - x^5 - 1;
class := array(0..(p-1),[]);
class[0] := 1;
for i from 1 to p-1 do
```

```
    class[i] := modp( rem(class[i-1]*x,trinom,x),3 ):
  od:
  test := modp( rem(class[p-1]*x,trinom,x),3 );
```

where the test should yield a value of 1 since $a^{x^p} = a^1$.

For convenience, we work in the group ring $F[G]$, where F is a field of characteristic 0 containing appropriate roots of unity. If λ is a nonprincipal character of X, then by Lemma 2.2,

$$(\mathrm{tr}_\lambda\, a)(\mathrm{tr}_{\lambda^{-1}}\, a) = u + v(\mathrm{tr}_1\, a) + w(\mathrm{tr}_1\, a^{-1}),$$

for some $u, v, w \in F$. Note that $u = 0$ since $a^{x^i} a^{x^j} = 1$ implies that a is conjugate to a^{-1}. Furthermore, since $\lambda \neq 1$, $\mathrm{tr}_\lambda\, a$ is contained in the augmentation ideal of $F[G]$, and this clearly implies that $w = -v$. Thus

$$(\mathrm{tr}_\lambda\, a)(\mathrm{tr}_{\lambda^{-1}}\, a) = v(\mathrm{tr}_1\, a - \mathrm{tr}_1\, a^{-1}),$$

and it remains to compute the coefficient v. If we set $y = \lambda(x^{-1})$, then Lemma 2.2 implies that $v = \sum' y^k$, where the sum is over all $0 \leq k \leq p-1$ with $a^{1+x^k} \in \mathfrak{K}_a$. We can compute this explicitly in Maple V using:

```
  classet := convert(class,set):
  coef := 0;
  for k from 0 to p-1 do
    if member( modp(1+class[k],3),classet ) then
    coef := coef + y^k
    fi:
  od:
```

Our goal now is to translate this information to fields of finite characteristic. In particular, we want a field K in which the coefficient polynomial vanishes, so that $(\mathrm{tr}_\lambda\, a)(\mathrm{tr}_{\lambda^{-1}}\, a) = 0$ in $K[G]$. But y must also be a primitive pth root of 1, so we need a common root of the coefficient polynomial and the cyclotomic polynomial. This leads us to obtain the resultant of the two; and then to factor the resultant. The commands:

```
  res := resultant(cyclo,coef,y);
  ifactor(res);
```

yield rather surprising numbers. Indeed, the resultant is an integer with 1167 digits, but it factors almost immediately since it is divisible by 3^{2114}. The remaining factor is $(37243)^{14}(5310037)^{14}$ and that yields two characteristics, different from 3 and p, where the resultant vanishes. Thus, if $\mathrm{char}\, K = 37243$ or 5310037, then there exists a nonprincipal character $\lambda\colon K[X] \to K$, independent of a, with $(\mathrm{tr}_\lambda\, a)(\mathrm{tr}_{\lambda^{-1}}\, a) = 0$. One can check this procedure by observing that:

```
  Gcd(cyclo,coef) mod 37243;
```

```
Gcd(cyclo,coef) mod 5310037;
```

both yield nontrivial polynomials. Hence if y is a root of either of these greatest common divisors, then $y = \lambda(x^{-1})$ will yield the required nonprincipal character.

Note that this computation with $p = 13$ and with any trinomial like $x^3 - x - 1 = 0$ yields a resultant equal to $729 = 3^6$. Thus, there are no factors prime to $|G|$ in this smaller case. The remaining comments for this example, concerning the nonlinear irreducible representations of $K[G]$, follow from Lemmas 2.4 and 2.5. □

We now return to the general Frobenius group situation to obtain results that hold in all characteristics other than p or q. To start with, we have

Lemma 2.8. *If* $\mathrm{Aut}_X(A)$ *denotes the group of automorphisms of* A *that commute with the action of* $X = \langle x \rangle$*, then* $\mathrm{Aut}_X(A)$ *is transitive on the nonidentity elements of* A*. In particular, for each* $\lambda\colon K[X] \to K$*, the group* $\mathrm{Aut}_X(A)$ *transitively permutes the* λ*-traces* $\mathrm{tr}_\lambda a$ *with* $1 \neq a \in A$*.*

Proof. Since X is cyclic and acts faithfully and irreducibly on the elementary abelian q-group A, the $\mathrm{GF}(q)$-subalgebra of $\mathrm{End}(A)$ generated by X is a finite field $F = \mathrm{GF}(q^n)$. It follows that $A \cong F^+$, the additive group of F, and that x acts on A like multiplication by an element of order p in the multiplicative group $F^\bullet$. In particular, multiplication by $F^\bullet$ is contained in $\mathrm{Aut}_X(A)$, and note that $F^\bullet$ is transitive on the nonzero elements of F^+. □

As a consequence, we obtain

Lemma 2.9. *If* b *and* c *are nonidentity elements of* A *with* $(\mathrm{tr}_1 b)(tr_1 c) = p(\mathrm{tr}_1 b)$*, then* $\mathrm{tr}_1 b = \mathrm{tr}_1 c$*, and* $(\mathrm{tr}_1 a)/p$ *is an idempotent for all* $1 \neq a \in A$*.*

Proof. We know that $K[A] = \oplus \sum_\mu K_\mu$ is the direct sum of copies of K, one for each linear character $\mu\colon K[A] \to K$. If $\gamma \in K[A]$, let $\mathrm{supp}\,\gamma = \{\mu \mid \mu(\gamma) \neq 0\}$. Thus the support of γ is the set of coordinates where γ has a nonzero entry. Now let $\mu \in \mathrm{supp}(\mathrm{tr}_1 b)$. Then $(\mathrm{tr}_1 b)(tr_1 c) = p(\mathrm{tr}_1 b)$ yields

$$\mu(\mathrm{tr}_1 b)\cdot\mu(tr_1 c) = p\cdot\mu(\mathrm{tr}_1 b) \neq 0,$$

so $\mu(\mathrm{tr}_1 c) = p \neq 0$ and $\mu \in \mathrm{supp}(\mathrm{tr}_1 c)$. In particular, $\mathrm{supp}(\mathrm{tr}_1 b) \subseteq \mathrm{supp}(\mathrm{tr}_1 c)$. But, by the previous lemma, all $\mathrm{tr}_1 a$ with $a \neq 1$ are conjugate under $\mathrm{Aut}_X(A)$, and hence they all have the same support size. Therefore, $\mathrm{supp}(\mathrm{tr}_1 b) = \mathrm{supp}(\mathrm{tr}_1 c)$ and, for all μ in this common support, we have $\mu(\mathrm{tr}_1 c) = p$. By Lemma 2.8 again, it follows that for any $1 \neq a \in A$, all nonzero coordinates of $\mathrm{tr}_1 a$ are equal to p. In particular, $\mathrm{tr}_1 a$ is uniquely determined by its support and, since $\mathrm{supp}(\mathrm{tr}_1 b) = \mathrm{supp}(\mathrm{tr}_1 c)$, we obtain $\mathrm{tr}_1 b = \mathrm{tr}_1 c$, as required. Finally, since all coordinates of $(\mathrm{tr}_1 a)/p$ are either 0 or 1, we conclude that $(\mathrm{tr}_1 a)/p$ is an idempotent. □

As we have seen in Example 2.7(ii), this situation can occur. Next, we need

Lemma 2.10. *Let $\beta_0, \beta_1, \dots, \beta_{p-1} \in K[A]$ and suppose that $\sum_{i=0}^{p-1} \beta_i \lambda(x^i) = 0$ for all nonprincipal linear characters $\lambda\colon K[X] \to K$. Then $\beta_0 = \beta_1 = \cdots = \beta_{p-1}$.*

Proof. Let $\lambda\colon K[X] \to K$ be a fixed nonprincipal linear character. Then λ^j is also nonprincipal for $j = 1, 2, \dots, p-1$, so the hypothesis implies that

$$\sum_{i=1}^{p-1} \beta_i \lambda^j(x^i) = -\beta_0 \qquad \text{for all } j = 1, 2, \dots, p-1.$$

We view the above display as a system of $p-1$ linear equations in the $p-1$ unknowns $\beta_1, \beta_2, \dots, \beta_{p-1}$. Since the matrix of coefficients $[\lambda^j(x^i)]$ here is Vandermonde with a nonzero determinant, this system has a unique solution. But observe that

$$\sum_{i=0}^{p-1} \beta_0 \lambda^j(x^i) = \beta_0 \sum_{i=0}^{p-1} \lambda^j(x^i) = 0$$

since $\lambda^j \neq 1$. Thus there is one solution with all β_i equal to β_0, and by uniqueness, this is the only possibility. $\square$

Finally, we are able to prove

Proposition 2.11. *Let $G = A \rtimes X$, where A is an elementary abelian q-group, X is cyclic of prime order p, and X acts faithfully and irreducibly on A. Suppose that $\operatorname{char} K \neq p$ or q, and that K contains a primitive (pq)th root of unity. Then there exists a nonprincipal character $\lambda\colon K[X] \to K$ with*

$$(\operatorname{tr}_1 a)(\operatorname{tr}_\lambda a)(\operatorname{tr}_{\lambda^{-1}} a^{-1}) \neq 0 \qquad \textit{for all } 1 \neq a \in A.$$

Proof. Fix $1 \neq a \in A$ and observe that, for any λ, we have

$$(\operatorname{tr}_\lambda a)(\operatorname{tr}_{\lambda^{-1}} a^{-1}) = \sum_{k=0}^{p-1} \lambda(x^{-k}) \cdot (\operatorname{tr}_1 a^{x^k - 1})$$

by Lemma 2.2. Thus,

$$(\operatorname{tr}_1 a)(\operatorname{tr}_\lambda a)(\operatorname{tr}_{\lambda^{-1}} a^{-1}) = \sum_{k=0}^{p-1} \lambda(x^{-k}) \cdot (\operatorname{tr}_1 a)(\operatorname{tr}_1 a^{x^k - 1}),$$

and our goal is to show that this expression cannot be zero for all $\lambda \neq 1$. Note that, when $k = 0$, we have $\operatorname{tr}_1 a^{x^0 - 1} = \operatorname{tr}_1 1 = p$. On the other hand, when $k \neq 0$, we have $a^{x^k - 1} \neq 1$. Indeed, if this were not the case, then x would act like an element of order $< p$ on a, so x would centralize a, contradicting the fact that $|\mathfrak{K}_a| = p$.

Suppose, by way of contradiction, that the above displayed expression vanishes for all $\lambda \neq 1$. Then Lemma 2.10 implies that the coefficients $(\mathrm{tr}_1 a)(\mathrm{tr}_1 a^{x^k-1})$ are equal for all $k = 0, 1, \ldots, p-1$. In other words,

$$(\mathrm{tr}_1 a)(\mathrm{tr}_1 a^{x^k-1}) = (\mathrm{tr}_1 a)(\mathrm{tr}_1 1) = p(\mathrm{tr}_1 a)$$

for all $k = 1, 2, \ldots, p-1$, so Lemma 2.9 implies that $\mathrm{tr}_1 a = \mathrm{tr}_1 a^{x^k-1}$ and that $(\mathrm{tr}_1 a)^2 = p(\mathrm{tr}_1 a)$. By Lemma 2.2, we now have

$$(\mathrm{tr}_1 a)(\mathrm{tr}_1 a^{-1}) = \sum_{k=0}^{p-1} \mathrm{tr}_1 a^{x^k-1} = p + (p-1)(\mathrm{tr}_1 a)$$

and, multiplying the above by $\mathrm{tr}_1 a$ and using the fact that $(\mathrm{tr}_1 a)^2 = p(\mathrm{tr}_1 a)$, we obtain $p(\mathrm{tr}_1 a)(\mathrm{tr}_1 a^{-1}) = p^2(\mathrm{tr}_1 a)$. It follows that

$$p(\mathrm{tr}_1 a) = (\mathrm{tr}_1 a)(\mathrm{tr}_1 a^{-1}) = p + (p-1)(\mathrm{tr}_1 a),$$

so $\mathrm{tr}_1 a = p$, and again this contradicts the fact that $|\mathfrak{K}_a| = p$.

We have therefore shown that there exists $\lambda \neq 1$, depending on the fixed element $1 \neq a \in A$, with $(\mathrm{tr}_1 a)(\mathrm{tr}_\lambda a)(\mathrm{tr}_{\lambda^{-1}} a^{-1}) \neq 0$. By Lemma 2.8, this product is nonzero for the given λ and for all $1 \neq a \in A$. $\square$

In view of Example 2.7(i) and the fact that $\mathrm{tr}_\lambda a$ is contained in the augmentation ideal of $K[A]$, we cannot adjoin the extra factor $(\mathrm{tr}_1 a^{-1})$ to the product $(\mathrm{tr}_1 a)(\mathrm{tr}_\lambda a)(\mathrm{tr}_{\lambda^{-1}} a^{-1})$ and guarantee that the new product is nonzero. Furthermore, in view of Example 2.7(iii), it is at least problematic that we could adjoin a factor like $(\mathrm{tr}_{\lambda^{-1}} a)$ or $(\mathrm{tr}_\lambda a^{-1})$ and get a result analogous to the above proposition.

§3. Construction of Units

In this section, we construct concrete units in $K[G]$, and use a result of Tits [T, Proposition 3.12] to show that these elements generate a group which is not 2-related. To start with, let F be a field with a nonarchimedean valuation ν. Then we say that F is locally compact, with respect to the topology induced by ν, if every element of F has a neighborhood with compact closure. It is known that F is locally compact if and only if ν is a complete, discrete valuation with residue class field $\tilde{F}$ finite. For convenience, and to set notation, we state the above mentioned result in the form we require.

Proposition 3.1. [T]. *Let a and b be semisimple elements in $\mathrm{GL}_m(F)$, where F is a locally compact field with nonarchimedean valuation ν. Let $\mathrm{GL}_m(F)$ act on the m-dimensional vector space V and write $V = A_+ \oplus A_0 \oplus A_-$. Here A_+, A_0, and A_- are a-stable subspaces of V with $\dim A_+ = \dim A_- = 1$. Furthermore, assume that the*

eigenvalues of a on these three spaces are contained in F and have valuations which are positive, zero, and negative, respectively. Similarly, write $V = B_+ \oplus B_0 \oplus B_-$ with corresponding properties for the element b. If $A_i \not\subseteq B_j \oplus B_0$ and $B_i \not\subseteq A_j \oplus A_0$ for all $i, j \in \{+, -\}$, then the nonabelian free group $\mathfrak{F}_2$ is involved in $\langle a, b\rangle$.

The conclusion of [T, Proposition 3.12] is actually somewhat stronger than stated here. Namely, it asserts that there exists an integer s_0 such that for all $s \geq s_0$, the image of $\langle a^s, b^s\rangle$ in $\mathrm{PGL}_m(F)$ is free of rank 2. The eight subspace noninclusions listed above are usually trivially satisfied when $m = 2$. In general, if we let α_+ denote the projection of $V = A_+ \oplus A_0 \oplus A_-$ onto A_+ and if α_-, β_+, and β_- are defined similarly, then these assumptions are equivalent to $\alpha_i\beta_j \neq 0$ and $\beta_i\alpha_j \neq 0$ for all $i, j \in \{+, -\}$. For obvious reasons, we call these the idempotent conditions, and the work of the previous section will enable us to verify them.

The locally compact fields we require are obtained as follows.

Lemma 3.2. *Suppose that either $K = \mathbf{Q}$ is the field of rationals, or $K = K_0(t)$ is the rational function field in one variable over some finite prime field K_0. If n is any fixed positive integer, then there exists a field extension F of K, containing a splitting field of $x^n - 1$, such that F is locally compact with respect to the topology induced by a nonarchimedean valuation ν. Furthermore,*

i. *If $K = \mathbf{Q}$ and if $\epsilon \in F$ is any nth root of 1, then there exist infinitely many integers $k \in \mathbf{Z} \subseteq K$ larger than 1 such that $\nu(k - \epsilon) > 0$ and $\nu(k - \delta) = 0$ for all other $\delta \in F$ with $\delta^n = 1$.*
ii. *If $K = K_0(t)$ and if $0 \neq \epsilon \in F'$, where F' is the finite subfield of F generated by all nth roots of 1, then there exist infinitely many elements $k \in K$, which are positive powers of t, such that $\nu(k - \epsilon) > 0$ and $\nu(k - \delta) = 0$ for all other $\delta \in F'$.*

Proof. (i) By an elementary special case of Dirichlet's theorem [I2, Theorem 20.14], we can choose a prime p with $p \equiv 1 \mod n$, and let $F = \mathbf{Q}_p$ denote the p-adic field. Then F is endowed with a complete, discrete valuation ν, and it has finite residue field $\tilde{F} = \mathrm{GF}(p)$. Thus, we know that F is locally compact. Let $\varphi\colon F \to \tilde{F} \cup \{\infty\}$ denote the place map corresponding to ν. Then φ yields a homomorphism from the p-adic integers $\mathbf{Z}_p$ to $\tilde{F}$. Since the polynomial $x^p - x$ splits completely and has distinct roots in $\tilde{F}$, Hensel's lemma implies that it splits completely in $\mathbf{Z}_p$ and that φ maps the roots in $\mathbf{Z}_p$ to those in $\tilde{F}$. In particular, since $n|(p-1)$, we see that $\mathbf{Z}_p$ contains all nth roots of unity and that they are mapped by φ in a one-to-one manner to the nth roots of unity in $\mathrm{GF}(p)$.

Finally, let ϵ be any nth root of unity in $\mathbf{Z}_p$. Then $\varphi(\epsilon) \in \mathrm{GF}(p)$, so there exist infinitely many positive integers $k \in \mathbf{Z} \subseteq K$ with $\varphi(k) = \varphi(\epsilon)$. Thus $\varphi(k - \epsilon) = 0$ and $\nu(k - \epsilon) > 0$. On the other hand, if δ is an nth root different from ϵ, then $\varphi(\delta) \neq \varphi(\epsilon)$ so $\varphi(k - \delta) = \varphi(\epsilon) - \varphi(\delta) \neq 0$ and consequently $\nu(k - \delta) = 0$.

(ii) Here $K = K_0(t)$ and we let F' denote the splitting field over K_0 of the polynomial $x^n - 1$, so that F' is a finite field generated by all nth roots of unity. Choose $\gamma \in F'$ to generate the cyclic multiplicative group of this field, and let $F = F'((t-\gamma)) \supseteq K$ be the field consisting of all Laurent series over F' in the variable $t - \gamma$. Certainly, F has a complete, discrete valuation ν with finite residue field F'. In particular, F is locally compact. Let $\varphi\colon F \to F' \cup \{\infty\}$ denote the place map corresponding to ν. Then $\varphi(t-\gamma) = 0$ so $\varphi(t) = \gamma$. Since γ is a cyclic generator for the multiplicative group of F', it follows that each nonzero element of F' is an image of infinitely many distinct positive powers of t.

Finally, if $0 \neq \epsilon \in F'$, then we know that there exist infinitely many distinct positive powers $k = t^j \in K$ with $\varphi(k) = \varphi(t^j) = \gamma^j = \epsilon = \varphi(\epsilon)$. Thus $\varphi(k - \epsilon) = 0$ and $\nu(k - \epsilon) > 0$. On the other hand, if $\delta \in F'$ is different from ϵ, then $\varphi(\delta) = \delta \neq \epsilon = \varphi(\epsilon)$ so $\varphi(k - \delta) = \varphi(\epsilon) - \varphi(\delta) \neq 0$ and consequently $\nu(k - \delta) = 0$. □

If K is a nonabsolute field of positive characteristic then, by definition, K is not algebraic over its prime subfield K_0. Thus this field contains numerous transcendental elements, and for all the constructions given below, we select a fixed such element t. We begin with the p-group case. Recall that a minimal nonabelian p-group is a group that satisfies the conditions of Lemma 1.4(i).

Lemma 3.3. *Let K be a nonabsolute field of characteristic $\neq p$, and let G be a minimal nonabelian p-group. Then there exist subgroups $X = \langle x \rangle$ and $Y = \langle y \rangle$ of G and special units u_X and u_Y (based on the same transcendental element $t \in K$ if $\operatorname{char} K > 0$), such that $\langle u_X, u_Y \rangle$ is not 2-related.*

Proof. Without loss of generality, we can assume that either $K = \mathbf{Q}$ is the field of rationals, or that $K = K_0(t)$ is the rational function field in one variable over some finite prime subfield K_0. Write $n = |G|$ and let F and ν be given by Lemma 3.2. Then F contains all nth roots of unity, so it follows from [I1, Corollary 9.15 and Theorem 10.3] that F is a splitting field for $K[G]$. In other words, all irreducible representations $\mathfrak{X}$ of $F[G]$ are maps onto full matrix rings over F. Furthermore, if $g \in G$, then all eigenvalues of $\mathfrak{X}(g)$ are contained in F. Observe that, by assumption, n is prime to the characteristic of K. Since G has the structure given by Lemma 1.4(i), there are a number of cases to be considered.

Case 1. *$G = X \rtimes Y$, where $X = \langle x \rangle$ is cyclic and $Y = \langle y \rangle$ has order p.*

Proof. Let $\lambda\colon F[X] \to F$ be a linear character faithful on X. Then conjugation by Y does not fix λ, so λ has p distinct conjugates under this action. In particular, since x generates X, it follows that the values $\lambda^{y^i}(x) = \varepsilon_i$, for $i = 0, 1, \ldots, p-1$, are distinct. Using Lemma 3.2, choose $r \in K$ (either an integer larger than 1 or a positive power of t) for ε_0 and choose $s \in K$ for ε_1. Since r and s are not roots of unity, $x - r$ and $x - s$ are invertible in $K[G]$, and we set $u = u_X = (x-r)/(x-s) \in \mathrm{U}(K[G])$. Similarly, let $\delta_0, \delta_1, \ldots, \delta_{p-1}$ be the distinct pth roots of unity in F and,

using Lemma 3.2, choose $r' \in K$ for δ_0 and $s' \in K$ for δ_1. Since r' and s' are not roots of unity, we can define $v = u_Y = (y - r')/(y - s') \in \mathrm{U}(K[G])$.

We claim that $\langle u_X, u_Y \rangle = \langle u, v \rangle$ involves and hence contains a nonabelian free group. To this end, let $\theta\colon F[G] \to \mathrm{M}_p(F)$ be the induced representation $\theta = \lambda^G$. We show that $\bar{u} = \theta(u)$ and $\bar{v} = \theta(v)$ satisfy the hypotheses of Proposition 3.1. First note that $\bar{x} = \theta(x) = \mathrm{diag}(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{p-1})$, so $\bar{u}$ is diagonal with its ith entry given by $\bar{u}_i = (\varepsilon_i - r)/(\varepsilon_i - s)$. By Lemma 3.2 and the choice of r and s, we see that $\nu(\bar{u}_0) > 0$, $\nu(\bar{u}_1) < 0$, and $\nu(\bar{u}_i) = 0$ otherwise.

Next, since $\theta = \lambda^G$, it follows that

$$\bar{y} = \theta(y) = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}$$

and hence, since $p \neq \mathrm{char}\, F$, we see that $\bar{y}$ is similar to $\mathrm{diag}(\delta_0, \delta_1, \dots, \delta_{p-1})$. Consequently, $\bar{v}$ is similar to $\mathrm{diag}(\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{p-1})$ where $\bar{v}_i = (\delta_i - r')/(\delta_i - s')$. Again, Lemma 3.2 implies that $\nu(\bar{v}_0) > 0$, $\nu(\bar{v}_1) < 0$, and $\nu(\bar{v}_i) = 0$ otherwise.

Finally, note that the idempotents associated with the plus and minus spaces for $\bar{u}$ are the same as those for $\bar{x}$, so we can write them as $\bar{e}_+ = \theta(e_+)$ and $\bar{e}_- = \theta(e_-)$, where e_+ and e_- are primitive idempotents in $F[X]$. Similarly, the idempotents associated with the plus and minus spaces of $\bar{v}$ can be written as $\bar{f}_+ = \theta(f_+)$ and $\bar{f}_- = \theta(f_-)$, where f_+ and f_- are primitive idempotents of $F[Y]$. In particular, the identity coefficients of f_+ and f_- are both equal to $1/p$. Furthermore, note that $\bar{e}_+$ and $\bar{e}_-$ are diagonal and that $\bar{y}^i$ has no diagonal entries for $i = 1, 2, \dots, p-1$. Hence if $e \in F[X]$ is either of the two idempotents for u and if $f \in F[Y]$ is either of the two idempotents for v, then the diagonal entries of $\bar{e}\bar{f}$ or $\bar{f}\bar{e}$ are the same as the diagonal entries for $\bar{e}/p$, and hence at least one such entry is nonzero (see also [GP2, Lemma 2.3(i)]). We can now conclude from Proposition 3.1 that $\langle \bar{u}, \bar{v} \rangle$ contains a free group of rank 2, and consequently so does $\langle u, v \rangle$. $\square$

If G is a nonabelian p-group of order p^3 and if G is not of the form $X \rtimes Y$, then either p is odd and G has period p, or $p = 2$ and G is quaternion of order 8.

Case 2. *p is odd and G is a nonabelian p-group of period p and order p^3.*

Proof. Let $X = \langle x \rangle$ and $Y = \langle y \rangle$ be subgroups of order p that generate G, and let θ be a nonlinear irreducible representation of $F[G]$. Then $\deg \theta = p$ and each of $\bar{x} = \theta(x)$ and $\bar{y} = \theta(y)$ is similar to $\mathrm{diag}(\delta_0, \delta_1, \dots, \delta_{p-1})$, where $\delta_0, \delta_1, \dots, \delta_{p-1}$ are the p distinct pth roots of unity in F. Using Lemma 3.2, let $r, s \in K$ correspond to δ_0 and δ_1, respectively, and set $u = u_X = (x-r)/(x-s)$ and $v = u_Y = (y-r)/(y-s)$. Then u and v are units in $K[G]$ and, as in the preceding case, we see that $\bar{u} = \theta(u)$ and $\bar{v} = \theta(v)$ satisfy the eigenvalue hypothesis of Proposition 3.1.

Finally, note that the idempotents associated with the plus and minus spaces for $\bar{u}$ are the same as those for $\bar{x}$, so we can write them as $\bar{e}_+ = \theta(e_+)$ and $\bar{e}_- = \theta(e_-)$, where e_+ and e_- are primitive idempotents in $F[X]$. Similarly, the idempotents associated with the plus and minus spaces of $\bar{v}$ can be written as $\bar{f}_+ = \theta(f_+)$ and $\bar{f}_- = \theta(f_-)$, where f_+ and f_- are primitive idempotents of $F[Y]$. Furthermore, if $Z = \mathbb{Z}(G)$, then $G = ZXY = ZYX$, so XY and YX are both sets of p^2 coset representatives for Z in G. Thus, by Lemma 2.1, the sets $\theta(XY) = \theta(X)\theta(Y)$ and $\theta(YX) = \theta(Y)\theta(X)$ are bases for $\theta(F[G]) = \mathrm{M}_p(F)$. It now follows immediately from the linear independence of these sets that if $\bar{e}$ is one of $\bar{e}_+$ or $\bar{e}_-$, and if $\bar{f}$ is one of $\bar{f}_+$ or $\bar{f}_-$, then $\bar{e}\bar{f} \neq 0$ and $\bar{f}\bar{e} \neq 0$. This proves the idempotent condition, and we conclude from Proposition 3.1 that $\langle \bar{u}, \bar{v} \rangle$ contains a nonabelian free subgroup. Hence the same is true for $\langle u, v \rangle = \langle u_X, u_Y \rangle$. □

Case 3. *$p = 2$ and G is the quaternion group of order 8.*

Proof. Here we let x and y be elements of order 4 that generate G, and we let θ be the nonlinear irreducible representation of $F[G]$. Then $\deg\theta = 2$ and each of $\bar{x} = \theta(x)$ and $\bar{y} = \theta(y)$ is similar to $\mathrm{diag}(i, -i)$, where $i = \sqrt{-1}$. Using Lemma 3.2, let $r, s \in K$ correspond to i and $-i$, respectively, and set $u = u_X = (x - r)/(x - s)$ and $v = u_Y = (y - r)/(y - s)$. Then u and v are units in $K[G]$, and $\bar{u} = \theta(u)$ and $\bar{v} = \theta(v)$ satisfy the eigenvalue hypothesis of Proposition 3.1. Furthermore, since $\deg\theta = 2$, the idempotent condition is automatically satisfied. Indeed, if this were not the case, then $\bar{x}$ and $\bar{y}$ would have a common eigenvector, contradicting the irreducibility of θ. As above, Proposition 3.1 yields the result. □

Now we move on to the Frobenius case. Thus, for the remainder of this section, we let $G = A \rtimes X$, where A is an elementary abelian q-group, $X = \langle x \rangle$ is cyclic of prime order p, and X acts faithfully and irreducibly on A. Furthermore, we let K be a nonabsolute field of characteristic different from p and q, and we use the notation of the preceding section.

In the following lemma we assume that either $K = \mathbf{Q}$ is the field of rational numbers or that $K = K_0(t)$ is the rational function field in one variable over some finite prime subfield K_0. Furthermore, we write $n = |G|$, and we let F and ν be given by Lemma 3.2. Since F contains a primitive (pq)th root of unity, basic properties of the representation theory of $F[G]$ are contained in Lemma 1.5.

Lemma 3.4. *Let $\alpha \in U(K[A])$ and let K and F be as above. Suppose there exists a nonlinear irreducible representation $\theta\colon F[G] \to \mathrm{M}_p(F)$ and a nonprincipal linear character $\lambda\colon F[X] \to F$ such that $\theta(\mathrm{tr}_\sigma\, \alpha) \neq 0$ and $\theta(\mathrm{tr}_\sigma\, \alpha^{-1}) \neq 0$ for $\sigma = 1, \lambda, \lambda^{-1}$. Then there exist elements $r, s \in K$ so that the special unit $u = (x - r)/(x - s)$ and its conjugate $\alpha^{-1}u\alpha$ generate a subgroup of $\mathrm{U}(K[G])$ that is not 2-related.*

Proof. Define $\delta = \lambda(x)$ so that δ is a primitive pth root of unity. Since θ is induced from a linear representation of $F[A]$, it follows that $\bar{x} = \theta(x)$ is similar to $\mathrm{diag}(1, \delta, \ldots, \delta^{p-1})$, a matrix with distinct eigenvalues, and hence, using

Lemma 3.2, we can choose $r, s \in K$ corresponding to 1 and δ, respectively. Then $u = (x-r)/(x-s)$ and $v = \alpha^{-1}u\alpha$ are units of $K[G]$ with $\bar{u} = \theta(u)$ and $\bar{v} = \theta(v) = \bar{u}^{\theta(\alpha)}$ both satisfying the eigenvalue hypothesis of Proposition 3.1.

Note that the idempotents associated with the positive and negative spaces for $\bar{u}$ are the same as those for $\bar{x}$, namely $\theta(e_1)$ and $\theta(e_\lambda)$, in the notation of the preceding section. This follows since r corresponds to the eigenvalue 1 and s corresponds to $\delta = \lambda(x)$. Furthermore, the positive and negative idempotents for $\bar{v}$ are $\theta(\alpha^{-1}e_1\alpha)$ and $\theta(\alpha^{-1}e_\lambda\alpha)$. In particular, since $\theta(\alpha)$ and $\theta(\alpha^{-1})$ are units in $\mathrm{M}_p(F)$, the idempotent condition is equivalent to

$$\theta(e_\mu \alpha e_\eta) \neq 0, \quad \theta(e_\mu \alpha^{-1} e_\eta) \neq 0 \qquad \text{for all } \mu, \eta \in \{1, \lambda\}.$$

But, by Lemma 2.3,

$$e_\mu \alpha e_\eta = \frac{1}{p}(\mathrm{tr}_\sigma\, \alpha)e_\mu, \quad e_\mu \alpha^{-1} e_\eta = \frac{1}{p}(\mathrm{tr}_\sigma\, \alpha^{-1})e_\mu,$$

where $\sigma = \mu^{-1}\eta$ is contained in $\{1, \lambda.\lambda^{-1}\}$. Thus, the hypothesis implies that $\theta(\mathrm{tr}_\sigma\, \alpha) \neq 0$ and $\theta(\mathrm{tr}_\sigma\, \alpha^{-1}) \neq 0$ for all appropriate μ, η, and therefore, by Lemma 2.4, these six elements are all invertible in the matrix ring. In particular, since $\theta(e_\mu) \neq 0$ by Lemma 1.5, the idempotent condition is satisfied, and we conclude from Proposition 3.1 that $\langle \bar{u}, \bar{v} \rangle$, and hence $\langle u, v \rangle$, is not 2-related. □

As an immediate consequence, we have

Proposition 3.5. *Let $G = A \rtimes X$, where A is an elementary abelian q-group, X is cyclic of prime order p, and X acts faithfully and irreducibly on A. Let K be a nonabsolute field with either* $\mathrm{char}\, K = 0$ *or with* $\mathrm{char}\, K > p^{(p-1)(q-1)}$. *If $1 \neq x \in X$ and $1 \neq a \in A$, then there exist elements $r, s \in K$ so that the special units $u = (x-r)/(x-s)$ and $a^{-1}ua$ generate a subgroup of* $\mathrm{U}(K[G])$ *that is not* 2*-related.*

Proof. It suffices to assume that K and F are as in the preceding lemma. Then, F contains a primitive (pq)th root of unity, so Lemma 2.5 and Proposition 2.6 apply to the group algebra $F[G]$. In particular, if θ is any nonlinear irreducible representation of $F[G]$, then $\theta(\mathrm{tr}_\lambda\, a) \neq 0$ and $\theta(\mathrm{tr}_\lambda\, a^{-1}) \neq 0$ for all linear characters $\lambda\colon F[X] \to F$. Lemma 3.4 now yields the result. □

Note that if $y = x^a$, then $u_X = u = (x-r)/(x-s)$ and $u_Y = u^a = (y-r)/(y-s)$ are the units given in the above proposition, and they are both special (based on the same transcendental element $t \in K$ if $\mathrm{char}\, K > 0$). On the other hand, a result of this nature does not hold in the p-group case. Indeed, if H is a minimal nonabelian p-group, then $H' \subseteq \mathbb{Z}(H)$. Thus, for any $x, a \in H$, the elements x and $y = x^a$ commute, and hence the corresponding units u_X and u_Y generate an abelian group.

To proced further in the Frobenius case, we need the following observation in positive characteristic. Here $K = K_0(t)$ with K_0 a finite field, and F is given by Lemma 3.2 based on $n = |G|$.

Lemma 3.6. *Let $1 \neq a \in A$, let t be a transcendental element of K, and set*

$$\alpha = \frac{a - t^q}{a - t} \in \mathrm{U}(K[A]).$$

Suppose θ is a nonlinear irreducible representation of $F[G]$ and let $\lambda\colon F[X] \to F$ be a linear character. If either $\theta(\mathrm{tr}_\lambda\, \alpha) = 0$ or $\theta(\mathrm{tr}_\lambda\, \alpha^{-1}) = 0$, then $\theta(\mathrm{tr}_\lambda\, a^i) = 0$ for all $i = 0, 1, \ldots, q-1$.

Proof. Let F' be the finite subfield of F generated by all nth roots of unity. Then, by Lemma 1.5, $\theta(F[G]) = \mathrm{M}_p(F)$ and we can assume that $\theta(A)$ is contained in the subring $\mathrm{D}(F')$ of diagonal matrices with entries in F'. In particular, since $\lambda(X) \subseteq F'$, we see that each $\theta(\mathrm{tr}_\lambda\, a^i)$ is contained in $\mathrm{D}(F')$.

Next, note that if $k \in K$ with $k^q \neq 1$, then

$$\frac{1}{1 - a^{-1}k} = \frac{1}{1 - k^q} \sum_{i=0}^{q-1} a^{-i}k^i$$

since $a^q = 1$. Hence, since

$$\alpha = \frac{1 - a^{-1}t^q}{1 - a^{-1}t},$$

we see that α is a nonzero scalar multiple of

$$(1 - a^{-1}t^q) \sum_{i=0}^{q-1} a^{-i}t^i = \sum_{i=0}^{q-1} a^{-i}t^i - \sum_{i=0}^{q-1} a^{-i-1}t^{i+q}.$$

In particular, if $\theta(\mathrm{tr}_\lambda\, \alpha) = 0$, then linearity implies that

$$0 = \sum_{i=0}^{q-1} \theta(\mathrm{tr}_\lambda\, a^{-i})t^i - \sum_{i=0}^{q-1} \theta(\mathrm{tr}_\lambda\, a^{-i-1})t^{i+q}.$$

But $\theta(\mathrm{tr}_\lambda\, a^{-i}) \in \mathrm{D}(F')$ and $1, t, \ldots, t^{2q-1}$ are linearly independent over F', so we conclude that each $\theta(\mathrm{tr}_\lambda\, a^{-i})$ is zero, as required.

Similarly, α^{-1} is a nonzero scalar multiple of

$$(1 - a^{-1}t) \sum_{i=0}^{q-1} a^{-i}t^{qi} = \sum_{i=0}^{q-1} a^{-i}t^{qi} - \sum_{i=0}^{q-1} a^{-i-1}t^{qi+1}.$$

Thus, since $1, t^q, t^{2q}, \ldots, t^{(q-1)q}, t, t^{q+1}, t^{2q+1}, \ldots, t^{(q-1)q+1}$ are linearly independent over F', we again conclude that if $\theta(\mathrm{tr}_\lambda\, \alpha^{-1}) = 0$, then $\theta(\mathrm{tr}_\lambda\, a^{-i}) = 0$ for all $i = 0, 1, \ldots, q-1$. $\square$

Obviously t^q could be replaced by t^m, in the above, for any $m \geq q$. Finally, we prove

Proposition 3.7. *Let $G = A \rtimes X$, where A is an elementary abelian q-group, X is cyclic of prime order p, and X acts faithfully and irreducibly on A. Let K be a nonabsolute field of positive characteristic and let $t \in K$ be a fixed transcendental element. If $1 \neq x \in X$ and $1 \neq a \in A$, then there exist elements $r, s \in K$ that are positive powers of t, such that the special units $u_X = (x - r)/(x - s)$ and $u_A = (a - t^q)/(a - t)$ generate a subgroup of $\mathrm{U}(K[G])$ that is not 2-related.*

Proof. As usual, we can assume that $K = K_0(t)$ and that F is given by Lemma 3.2 based on $n = |G|$. Thus, F contains a primitive (pq)th root of unity, and we can conclude from Proposition 2.11, applied to the group algebra $F[G]$, that there exists a nonprincipal linear character $\lambda\colon F[X] \to F$ with

$$\tau = (\mathrm{tr}_1\, a)(\mathrm{tr}_\lambda\, a)(\mathrm{tr}_{\lambda^{-1}}\, a^{-1}) \neq 0$$

in $F[A]$. The semisimplicity of $F[A]$ now implies that there exists an irreducible representation $\mu\colon F[A] \to F$ with $\mu(\tau) \neq 0$ and hence with $\mu(\mathrm{tr}_1\, a) \neq 0$, $\mu(\mathrm{tr}_\lambda\, a) \neq 0$, and $\mu(\mathrm{tr}_{\lambda^{-1}}\, a^{-1}) \neq 0$. Note that $\mu \neq 1$ since $\mathrm{tr}_\lambda\, a$ is contained in the augmentation ideal of $F[A]$. In particular, if we set $\theta = \mu^G$, then Lemma 1.5 implies that θ is an irreducible representation of $F[G]$ with $\theta(\mathrm{tr}_1\, a) \neq 0$, $\theta(\mathrm{tr}_\lambda\, a) \neq 0$, and $\theta(\mathrm{tr}_{\lambda^{-1}}\, a^{-1}) \neq 0$.

Set $\alpha = u_A = (a - t^q)/(a - t) \in \mathrm{U}(K[A])$. Then, by applying the preceding lemma to the linear characters $1, \lambda, \lambda^{-1}$ in turn, we see that $\theta(\mathrm{tr}_\sigma\, \alpha) \neq 0$ and $\theta(\mathrm{tr}_\sigma\, \alpha^{-1}) \neq 0$ for all $\sigma \in \{1, \lambda, \lambda^{-1}\}$. With this, Lemma 3.4 now yields a special unit $u = u_X = (x - r)/(x - s)$ with the property that $\langle u, \alpha^{-1}u\alpha\rangle$ contains a nonabelian free group. Since $\langle u, \alpha\rangle \supseteq \langle u, \alpha^{-1}u\alpha\rangle$, the result follows. □

§ 4. The Modular Case

It remains to handle the p-groups and the Frobenius groups in the modular case, namely where $\mathrm{char}\, K = \pi > 0$ divides $|G|$. Since any such group G must have $G/\mathbb{O}_\pi(G)$ nonabelian, the only possibility occurs when $G = A \rtimes X$ is Frobenius with $|X| = p = \pi$. For the most part, we handle this situation using techniques reminiscent of [MS] and [GP1]. Indeed, only the $p = 2$ case requires that we revert to an application of Proposition 3.1. To start with, we note

Lemma 4.1. *Let R be an algebra in characteristic $p > 0$, and let $R[t]$ denote the polynomial ring over R in the variable t. Suppose $\alpha, \beta \in R$ with $\alpha^2 = 0 = \beta^2$ but with $\alpha\beta$ not nilpotent. If we set $u = 1 + t\alpha$ and $v = 1 + t\beta$, then u and v are units of order p in $R[t]$ with $\langle u, v\rangle = \langle u\rangle * \langle v\rangle$, the free product of the two cyclic groups.*

Proof. Observe that $u^i = (1 + t\alpha)^i = 1 + it\alpha$, so $|u| = p$, and similarly $v^j = 1 + jt\beta$, so $|v| = p$. Furthermore, if $\tau = u^{i_1}v^{j_1}u^{i_2}v^{j_2}\cdots u^{i_n}v^{j_n}$ is a nontrivial product with $i_s, j_s \in \{1, 2, \ldots, p-1\}$, then τ is a polynomial in t with constant term 1 and with leading coefficient $c_{2n} = (i_1j_1i_2j_2\cdots i_nj_n)(\alpha\beta)^n \neq 0$, since $\alpha\beta$ is not nilpotent.

Thus $\tau \neq 1$, and the same argument handles products which start with v or end with u. Obviously, $\langle u, v\rangle = \langle u\rangle * \langle v\rangle$, as required. $\square$

If C_p denotes the cyclic group of order p, then the free product $C_p * C_p$ contains a nonabelian free group when $p > 2$. On the other hand, $C_2 * C_2$ is the infinite dihedral group and hence it is solvable. Because of this, the groups with $p = 2$ have to be dealt with in a different manner.

Lemma 4.2. *Let $G = A \rtimes X$, where A is an elementary abelian q-group, $|X| = p$, and $X = \langle x\rangle$ acts faithfully and irreducibly on A. Suppose K is a nonabsolute field of characteristic p with transcendental element t, and set*

$$u = 1 + t(1 + x + \cdots + x^{p-1}) \in \mathrm{U}(K[X]).$$

If $1 \neq a \in A$, then $\langle u, a^{-1}ua\rangle = \langle u\rangle * \langle a^{-1}ua\rangle \cong C_p * C_p$.

Proof. Let K_0 be the prime subfield of K and set $R = K_0[G]$. Since t is transcendental over K_0, we see that $K[G] \supseteq R[t]$, where the latter is isomorphic to the polynomial ring in the variable t over R. If $\alpha = 1 + x + \cdots + x^{p-1}$ and $\beta = \alpha^a$, then by the preceding lemma, it suffices to show that $\alpha^2 = 0 = \beta^2$, but that $\alpha\beta$ is not nilpotent. To start with, since $x\alpha = \alpha$, we see that $\alpha^2 = p\alpha = 0$, and hence the same is true of β. Indeed, if $y = x^a$ and $Y = \langle y\rangle = X^a$, then $\beta = 1 + y + \cdots + y^{p-1}$. Furthermore, since G is a Frobenius group and $1 \neq a \in A$, we have $X \cap Y = 1$. Thus, every element in the set product XY occurs precisely once, and consequently $\alpha\beta$ is a sum of p^2 distinct group elements each with coefficient 1. In fact, since $xA = yA$, we see that $x^i y^j \in A$ if and only if $j \equiv -i \mod p$. Thus there are precisely p elements in $XY \cap A$ and precisely one such product is the identity element. By combining all of this information, we see that $\alpha\beta$ is a sum of p^2 distinct elements, one is the identity, $p - 1$ are nonidentity elements of A, and the remaining $p^2 - p$ belong to $G \setminus A$. Again, using the structure of Frobenius groups, we know that all elements of $G \setminus A$ have order p. In other words, the sum of the coefficients of those group elements in $\alpha\beta$ having order 1 or p is precisely equal to $1 + (p^2 - p) = 1$, using $\mathrm{char}\, K = p$. We therefore conclude from [P, Lemma 2.3.3(i)] that $\alpha\beta$ is not nilpotent, and Lemma 4.1 yields the result. $\square$

As we observed above, if $y = x^a$, then the two units are given by

$$u_X = 1 + t(1 + x + \cdots + x^{p-1}) \quad \text{and} \quad u_Y = 1 + t(1 + y + \cdots + y^{p-1}).$$

Of course, they are both special, based on t. At this point, we factor a variant of these units obtained by replacing t by the transcendental element $-t^{p-1}$.

Lemma 4.3. *Let x and t be commuting elements of a characteristic p algebra R. If t is a unit of R, then*

$$1 - t^{p-1}(1 + x + \cdots + x^{p-1}) = -t^{p-1} \prod_{i=1}^{p-1} (x - 1 - it^{-1}).$$

Proof. If ζ belongs to a characteristic p algebra, then $1+\zeta+\cdots+\zeta^{p-1} = (\zeta-1)^{p-1}$ and $\zeta^{p-1}-1 = \prod_{i=1}^{p-1}(\zeta - i)$. Thus, since x and t commute, we have

$$\begin{aligned} 1 - t^{p-1}(1+x+\cdots+x^{p-1}) = 1 - [t(x-1)]^{p-1} &= -\prod_{i=1}^{p-1}[t(x-1)-i] \\ &= -t^{p-1}\prod_{i=1}^{p-1}(x-1-it^{-1}), \end{aligned}$$

as required. □

Finally, we quickly handle the $p = 2$ case.

Lemma 4.4. *Let $G = A \rtimes X$, where A is an elementary abelian q-group, $|X| = 2$, and $X = \langle x \rangle$ acts faithfully and irreducibly on A. Suppose K is a nonabsolute field of characteristic 2, and let $t \in K$ be a fixed transcendental element. If $1 \neq a \in A$, then there exist $r, s \in K$ that are positive powers of t, such that the special units $u_{\langle a \rangle} = (a-r)/(a-s)$ and $u_X = 1 + t(1+x)$ generate a group that is not 2-related.*

Proof. As usual, we can assume that $K = K_0(t)$, and we let $F \supseteq K$ be given by Lemma 3.2 with $n = |G|$. Since x has order 2 and acts faithfully and irreducibly on A, it follows that $A = \langle a \rangle$ is cyclic of order q and that $a^x = a^{-1}$. Let $\mu\colon F[A] \to F$ be a nonprincipal linear character and set $\theta = \mu^G$. Then $\theta(F[G]) = \mathrm{M}_2(F)$, $\theta(a) = \mathrm{diag}(\varepsilon, \varepsilon^{-1})$, where $\varepsilon = \mu(a)$ is a primitive qth root of unity, and $\theta(x) = \left[\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right]$. Using Lemma 3.2, choose $r \in K$ for ε and $s \in K$ for ε^{-1}, with r and s both positive powers of t. Since q is odd, $\varepsilon \neq \varepsilon^{-1}$, and hence $u = (a-r)/(a-s)$ is a unit in $K[A]$ with $\theta(u)$ a diagonal matrix satisfying the eigenvalue assumption of Proposition 3.1. As in the preceding lemmas, $v = 1 + t(1+x)$ is a unit in $K[X]$. Thus, $u^v = v^{-1}uv \in \mathrm{U}(K[G])$, and $\theta(u^v)$ also satisfies the eigenvalue assumption of Proposition 3.1.

Finally, note that the matrix units $e_{1,1}$ and $e_{2,2}$ are the idempotents associated with the positive and negative subspaces for $\theta(u)$. Hence $f_+ = \theta(v)^{-1}e_{1,1}\theta(v)$ and $f_- = \theta(v)^{-1}e_{2,2}\theta(v)$ are the idempotents associated with the positive and negative subspaces for $\theta(v^{-1}uv)$. Since $\theta(x) = \left[\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right]$, we have $\theta(v) = \left[\begin{smallmatrix} 1+t & t \\ t & 1+t \end{smallmatrix}\right]$, and thus

$$f_+ = \begin{bmatrix} 1+t^2 & t+t^2 \\ t+t^2 & t^2 \end{bmatrix} \quad \text{and} \quad f_- = \begin{bmatrix} t^2 & t+t^2 \\ t+t^2 & 1+t^2 \end{bmatrix}.$$

Note that these matrices have all nonzero entries, so they do not annihilate $e_{1,1}$ or $e_{2,2}$ on either side. In other words, the idempotent condition is satisfied, and we conclude from Proposition 3.1 that $\theta(u)$ and $\theta(u^v)$ generate a group that is not 2-related. It follows that $\langle u, u^v \rangle$ contains a nonabelian free group, and hence so does $\langle u, v \rangle \supseteq \langle u, u^v \rangle$. □

It is now a simple matter to prove our main results. To start with, we offer the

Proof of Theorem 1.2. If $\operatorname{char} K > 0$, fix a transcendental element $t \in K$. We procede by induction on $|G|$, and we divide the argument into two parts.

Case 1. *$K[G]$ is nonmodular.*

Proof. By assumption, the order of G is prime to the characteristic of K. Thus, the hypothesis on G is equivalent to the group being nonabelian. If G has a proper nonabelian subgroup H, then by induction, $K[H]$ contains special units u_X and u_Y with $\langle u_X, u_Y\rangle$ not 2-related, so the result is proved in this situation. Thus, it suffices to assume that all proper subgroups of G are abelian.

Similarly, suppose that G has a proper nonabelian homomorphic image $\bar{G}$. By induction, there exist prime power elements $\bar{x}, \bar{y} \in \bar{G}$ and scalars $r, s, r', s' \in K$ with the special units $\bar{u} = (\bar{x} - r)/(\bar{x} - s)$ and $\bar{v} = (\bar{y} - r')/(\bar{y} - s')$ generating a group that is not 2-related. Choose prime power elements $x, y \in G$ which map to $\bar{x}$ and $\bar{y}$, respectively. Then $u_X = (x - r)/(x - s)$ and $u_Y = (y - r')/(y - s')$ are special units of $K[G]$, since r, s, r', s' are not roots of unity. Furthermore, $u_X \mapsto \bar{u}$ and $u_Y \mapsto \bar{v}$ under the homomorphism $K[G] \to K[\bar{G}]$. Thus, $\langle u_X, u_Y\rangle$ is not 2-related, and we can now assume that all proper homomorphic images of G are abelian.

In other words, G satisfies the hypothesis of Lemma 1.4, with π any prime not dividing $|G|$, and we conclude that G is either a minimal nonabelian p-group or a Frobenius group of the form $G = A \rtimes X$. Fortunately, these groups have already been considered. Indeed, Lemma 3.3 yields the special units in the p-group case, while Propositions 3.5 and 3.7 handle the Frobenius groups. With this, the nonmodular case is proved. □

Case 2. *$K[G]$ is modular.*

Proof. Here $\operatorname{char} K = \pi > 0$ divides $|G|$, and $G/\mathbb{O}_\pi(G)$ is nonabelian. As in the preceding argument, it suffices to assume that, for all proper subgroups H of G, we have $H/\mathbb{O}_\pi(H)$ abelian.

Next, suppose that G has a proper homomorphic image $\bar{G}$ with $\bar{G}/\mathbb{O}_\pi(\bar{G})$ nonabelian. By induction, $K[\bar{G}]$ has two special units $\bar{u}$ and $\bar{v}$ with appropriate properties. As we observed in the preceding case, units of the form $(\bar{x} - r)/(\bar{x} - s)$ can be lifted to units of a similar type in $K[G]$. Furthermore, special units of the form $\bar{u} = 1 + t(1 + \bar{x} + \cdots + \bar{x}^{\pi-1})$, with $\bar{x}$ a π-element, can also be lifted. Indeed, there exists a π-element $x \in G$ that maps to $\bar{x}$, and then $u = 1 + t(1 + x + \cdots + x^{\pi-1}) \mapsto \bar{u}$. Furthermore, u is a unit since $1 + x + \cdots + x^{\pi-1} \in K_0[G]$ is algebraic over $K_0 = \mathrm{GF}(\pi)$ (it is in fact nilpotent), and hence it has only algebraic eigenvalues. With this, it is clear that the result holds for G.

Thus, it suffices to assume that all proper homomorphic images $\bar{G}$ of G have $\bar{G}/\mathbb{O}_\pi(\bar{G})$ abelian. Lemma 1.4 now implies that G is either a minimal nonabelian p-group or a Frobenius group having a particular structure. But $G/\mathbb{O}_\pi(G)$ is nonabelian and π divides $|G|$, so the only possibility here is that $G = A \rtimes X$ with

$|X| = p = \pi$. Fortunately, such groups have already been considered. Indeed, Lemmas 4.2 and 4.4 yield the result since $C_p * C_p$ is not 2-related when $p > 2$. □

Finally, we have the

Proof of Corollary 1.3. Let $\mathfrak{U}$ be the subgroup of $\mathrm{U}(K[G])$ generated by units of the form $g - k$ with $g \in G$ and $k \in K$. If $\operatorname{char} K = 0$ then, since all units of the form $(x - r)/(x - s)$ are contained in $\mathfrak{U}$, we conclude from Theorem 1.2 that $\mathfrak{U}$ is not 2-related. Thus, it suffices to assume that $\operatorname{char} K = \pi > 0$. Again, any special unit of the form $(x - r)/(x - s)$ is contained in $\mathfrak{U}$ and hence in $\mathfrak{U}K^\bullet$, where $K^\bullet$ is the multiplicative group of K. Furthermore, so are units of the form $1 - t^{\pi-1}(1 + x + \cdots + x^{\pi-1})$, by Lemma 4.3. Thus, by Theorem 1.2, with t replaced by $-t^{\pi-1}$, we see that $\mathfrak{U}K^\bullet$ contains a rank 2 free group $\mathfrak{F}_2$. But $K^\bullet$ is central, so $K^\bullet \cap \mathfrak{F}_2 = 1$, and hence $\mathfrak{U}/(\mathfrak{U} \cap K^\bullet) \cong \mathfrak{U}K^\bullet/K^\bullet$ contains a copy of $\mathfrak{F}_2$. Since this is a homomorphic image of $\mathfrak{U}$, we conclude that $\mathfrak{U}$ is not 2-related, and the corollary is proved. □

References

[BM] N. R. Blachman and M. J. Mossinghoff, *Maple V Quick Reference*, Brooks/Cole, Pacific Grove, 1994.

[G] J. Z. Gonçalves, *Free subgroups of units in group rings*, Canad. Math. Bull. **27** (1984), 309–312.

[GP1] J. Z. Gonçalves and D. S. Passman, *Construction of free subgroups in the group of units of modular group algebras*, Commun. Algebra **24** (1996), 4211–4215.

[GP2] ———, *Unitary units in group algebras* (to appear).

[HP] B. Hartley and P. F. Pickel, *Free subgroups in the unit group of integral group rings*, Canad. J. Math. **32** (1980), 1342–1352.

[H] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[I1] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[I2] ———, *Algebra: A Graduate Course*, Brooks/Cole, Pacific Grove, 1994.

[MS] Z. Marciniak and S. K. Sehgal, *Constructing free subgroups of integral group ring units*, Proc. A.M.S. **125** (1997), 1005–1009.

[MM] G. Miller and H. Moreno, *Non-abelian groups in which every subgroup is abelian*, Trans. A.M.S. **4** (1903), 398–404.

[P] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977.

[T] J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.

Department of Mathematics, University of São Paulo, São Paulo 05389, Brazil
E-mail address: jzg@ime.usp.br

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: passman@math.wisc.edu