UNITARY UNITS IN GROUP ALGEBRAS

J. Z. Gonçalves
D. S. Passman

University of São Paulo
University of Wisconsin-Madison

Abstract. Let $K[G]$ denote the group algebra of the finite group G over the nonabsolute field K of characteristic $\neq 2$, and let $*\colon K[G] \to K[G]$ be the K-involution determined by $g^* = g^{-1}$ for all $g \in G$. In this paper, we study the group $\mathfrak{U} = \mathfrak{U}(K[G])$ of unitary units of $K[G]$ and we classify those groups G for which $\mathfrak{U}$ contains no nonabelian free group. If K is algebraically closed, then this problem can be effectively studied via the representation theory of $K[G]$. However, for general fields, it is preferable to take an approach which avoids having to consider the division rings involved. Thus, we use a result of Tits to construct fairly concrete free generators in numerous crucial special cases.

§1. Preliminaries

For convenience, 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.

Now let R be a ring with involution $*$. A unit $u \in R$ is said to be unitary if $uu^* = u^*u = 1$ and we denote by $\mathfrak{U}(R)$ the multiplicative group of all unitary units of R. If R is a K-algebra, we assume that $*$ is a K-involution, that is it acts trivially on K.

Lemma 1.1. *Let R be a ring with involution $*$.*

i. *If S is a $*$-stable subring or direct summand of R, then $\mathfrak{U}(S)$ embeds isomorphically into $\mathfrak{U}(R)$. In particular, if $\mathfrak{U}(R)$ is 2-related, then so is $\mathfrak{U}(S)$.*

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

Key words and phrases. Group algebra, involution, unitary unit, free subgroup.

The first author's research was supported in part by Capes and Fapesp - Brazil. The second author's research was supported in part by NSF Grant DMS-9224662.

ii. *Assume that R is a K-algebra with* $\operatorname{char} K \neq 2$ *and let $S = R/I$ where I is a $*$-stable nil ideal of R. Then every unitary unit of S lifts to one of R. In particular, $\mathfrak{U}(S)$ is a homomorphic image of $\mathfrak{U}(R)$.*

iii. *Let $S = R/I$ be as in* (ii). *If $\mathfrak{U}(R)$ is 2-related, then so is $\mathfrak{U}(S)$. Furthermore, the converse holds if* $\operatorname{char} K > 2$.

Proof. Part (i) is clear. For (ii), Let $\bar{u}$ be a unitary unit of $S = R/I$ and, since I is a nil ideal of R, let u be a unit of R which maps to $\bar{u}$. Then u^* maps to $\bar{u}^*$, so uu^* maps to $\bar{u}\bar{u}^* = 1$. In other words, $uu^* = 1 + x$ where x is a $*$-symmetric element of I, since uu^* is $*$-symmetric. By assumption, x is nilpotent. If $\operatorname{char} K = p > 0$, then $1 + x$ is a unit of order p^n for some n and hence it has finite odd order. It follows that $1 + x$ has a square root $1 + y = (1 + x)^t$ for some integer t. On the other hand, if $\operatorname{char} K = 0$, then $1 + x$ again has a square root $1 + y$ obtained by evaluating the Taylor series for $\sqrt{1 + \zeta}$ at the nilpotent element x. In both cases, y is a polynomial in x with zero constant term, so y is nilpotent and $*$-symmetric. Thus $uu^* = 1+x = (1+y)^2 = (1+y)(1+y)^*$, and $v = (1+y)^{-1}u$ is the required unitary unit of R which maps to $\bar{u}$.

Finally, since $\mathfrak{U}(R)$ maps onto $\mathfrak{U}(S)$, we know that if $\mathfrak{U}(R)$ is 2-related, then so is $\mathfrak{U}(S)$. Furthermore, the kernel of this map is contained in $1 + I$ and hence it is periodic if $\operatorname{char} K > 2$. In particular, any free subgroup of $\mathfrak{U}(R)$ is disjoint from the kernel and hence embeds isomorphically into $\mathfrak{U}(S)$. With this, we see that if $\operatorname{char} K > 2$ and if $\mathfrak{U}(S)$ is 2-related, then so is $\mathfrak{U}(R)$. This proves (iii). □

Part (ii) above is false in characteristic 2. As an example, let $\operatorname{char} K = 2$, let R be the commutative K-algebra $R = K + Kx + Ky$ where $x^2 = y^2 = xy = yx = 0$, and define $*$ to interchange x and y. Then $I = K(x + y)$ is a $*$-stable nil ideal of R and it is easy to see that $\mathfrak{U}(R) = 1 + I$, so the image of $\mathfrak{U}(R)$ in $\mathfrak{U}(R/I)$ is 1. On the other hand, $S = R/I = K + Ks$ where s is a $*$-symmetric element of square 0. Thus $\mathfrak{U}(S) = 1 + Ks$ is strictly larger than the image of $\mathfrak{U}(R)$.

The following is a standard Frattini argument.

Lemma 1.2. *Let G be a finite group and let* $\operatorname{char} K \neq 2$. *If $\mathfrak{U}(K[G])$ is 2-related, then so is $\mathfrak{U}(K[H])$ for every subgroup and homomorphic image H of G.*

Proof. If H is a subgroup of G, then $K[H]$ is a $*$-stable subalgebra of $K[G]$, so Lemma 1.1(i) yields the result.

Now let $H \cong G/N$. We proceed by induction on $|N|$, the result being trivial if $|N| = 1$. Suppose first that there exists a maximal subgroup M of G with $N \not\subseteq M$. Then $MN = G$, so $H \cong G/N = MN/N \cong M/(M \cap N)$. Now we know that $\mathfrak{U}(K[M])$ is 2-related and since $|M \cap N| < |N|$, we conclude by induction that $\mathfrak{U}(K[H])$ is 2-related.

Thus, we can assume that N is contained in all maximal subgroups of G, so N is contained in the Frattini subgroup of G. Hence N is nilpotent and if $P \neq 1$ is a Sylow p-subgroup of N, then P is characteristic in N and consequently normal in G. Furthermore, note that $G/N \cong (G/P)/(N/P)$ and that $|N/P| < |N|$. Thus, by induction, it suffices to show that $\mathfrak{U}(K[G/P])$ is 2-related, and there are two

cases here. If $p \neq \operatorname{char} K$, then $K[G/P]$ is isomorphic to a $*$-stable algebra direct summand of $K[G]$, so Lemma 1.1(i) again yields the result. On the other hand, if $p = \operatorname{char} K$, then the kernel of the natural map $K[G] \to K[G/P]$ is a $*$-stable nil ideal, and Lemma 1.1(iii) applies. $\square$

Now if K is an absolute field, that is algebraic over a finite field, then the unit group of $K[G]$ is locally finite and, in particular, $\mathfrak{U}(K[G])$ is 2-related. Thus, it is reasonable to assume for the remainder of this paper that K is nonabsolute. In other words, either $\operatorname{char} K = 0$ or $\operatorname{char} K > 0$ and K contains an element transcendental over its prime subfield. We can now state our main result.

Theorem 1.3. *Let G be a finite group and let K be a nonabsolute field of characteristic $\neq 2$. The unitary unit group $\mathfrak{U}(K[G])$ is 2-related if and only if*

i. *G has a normal Sylow p-subgroup P with $p = \operatorname{char} K$, and we set $\bar{G} = G/P$. By convention, $P = 1$ if $\operatorname{char} K = 0$.*
ii. *Either $\bar{G}$ is abelian or it has an abelian subgroup $\bar{A}$ of index 2. Furthermore, if the latter occurs, then either $\bar{G} = \bar{A} \rtimes \langle \bar{y} \rangle$ is dihedral, or $\bar{A}$ is an elementary abelian 2-group.*

Proof of the easy direction. We show here that if G satisfies (i) and (ii) above, then $\mathfrak{U}(K[G])$ is 2-related. Indeed, if F is the algebraic closure of K, then since $\mathfrak{U}(K[G]) \subseteq \mathfrak{U}(F[G])$, it clearly suffices to show that $\mathfrak{U}(F[G])$ is 2-related. Furthermore, if P is the normal Sylow p-subgroup of G with $p = \operatorname{char} K$, then the kernel of the natural epimorphism $F[G] \to F[G/P]$ is a nil $*$-stable ideal. Thus, by Lemma 1.1(iii), it suffices to prove the result for $\bar{G} = G/P$. In other words, we can assume that $G = \bar{G}$ has order prime to the characteristic of K. Since the result is clear if G is abelian, we can now assume that G has a normal abelian subgroup A of index 2 with appropriate properties.

Let χ be a nonlinear irreducible character of G. Since $|G : A| = 2$, it follows that $\deg \chi = 2$ and that χ vanishes off A. On the other hand, if $a \in A$, then under either assumption, we see that a is conjugate to a^{-1}. Thus $\chi(a) = \chi(a^{-1})$ and hence $\chi(g) = \chi(g^{-1})$ for all $g \in G$. Next, let $\mathfrak{X}$ be the irreducible representation associated with χ. Since $\mathfrak{X}(F[G]) = \mathrm{M}_2(F)$, it is clear that $\mathfrak{X}(A)$ cannot be central and also that $\mathfrak{X}(G \setminus A)$ cannot be central. Now, by assumption, either A consists of elements of square 1, or $G \setminus A$ consists of elements of square 1. Thus in either case, there exists an element $g \in G$ with $g^2 = 1$ and $\mathfrak{X}(g)$ not central. It follows that $\mathfrak{X}(g)$ has the two eigenvalues 1 and -1, so $\det \mathfrak{X}(g) = -1$ and hence $\det \chi \neq 1$.

Finally, let $\chi_1, \chi_2, \ldots, \chi_r$ be all the nonlinear irreducible characters of G with corresponding centrally primitive idempotents $e_1, e_2, \ldots, e_r$ in $F[G]$. From the formula for e_i and the fact that $\chi_i(g) = \chi_i(g^{-1})$ for all $g \in G$, it follows that $e_i^* = e_i$ for all i. In particular, if we set $e_0 = 1 - e_1 - e_2 - \cdots - e_r$, then $F[G] = \oplus \sum_{i=0}^{r} e_i F[G]$ is a $*$-decomposition of $F[G]$, and hence $\mathfrak{U} = \mathfrak{U}(F[G]) \cong \prod_{i=0}^{r} \mathfrak{U}_i$ where $\mathfrak{U}_i$ is the set of units u of the algebra $e_i F[G]$ with $u^* u = e_i$. Now $e_0 F[G]$ is commutative, so certainly $\mathfrak{U}_0$ is commutative. Furthermore, for

$i \geq 1$ we know that $e_iF[G] \cong \mathrm{M}_2(F)$ and that $*$ determines an involution on this matrix ring over the algebraically closed field F. If $*$ is simplectic, then it is the unique symplectic involution on $\mathrm{M}_2(F)$, namely the adjoint map. Hence, for all $g \in G$, we have $e_ig^{-1} = (e_ig)^* = \mathrm{adj}(e_ig) = (e_ig^{-1}) \det \chi_i(g)$, so $\det \chi_i = 1$, a contradiction. Thus $*$ must be orthogonal, so $\mathfrak{U}_i \cong \mathrm{O}_2(F)$, a suitable orthogonal group, and hence $\mathfrak{U}_i$ is solvable. Consequently, $\mathfrak{U}$ is solvable and contains no nonabelian free group. $\square$

The more difficult direction of this proof requires the work of the next two sections. To start with, in section 2, we use a result of Tits to construct fairly concrete (essentially) free generators in $\mathfrak{U}(K[G])$ in certain crucial special cases. We then use these special cases in section 3, along with a purely group theoretic argument, to complete the proof of Theorem 1.3.

§2. Concrete Examples

If R is a ring with involution $*$ and if $\alpha \in R$ commutes with α^*, then certainly $\alpha(\alpha^*)^{-1} \in \mathfrak{U}(R)$ provided, of course, that α, and hence α^*, is invertible. If R is a K-algebra, then it is convenient to introduce a second parameter here. Specifically if α commutes with α^* and if $k \in K$, then we write

$$u_k(\alpha) = (k - \alpha)(k - \alpha^*)^{-1} \in \mathfrak{U}(R),$$

again provided that $k - \alpha$, and hence $k - \alpha^*$, is invertible.

In this section, we construct concrete unitary units in $K[G]$ using the above formula, and then apply the result of Tits [T, Proposition 3.12] to show that these elements (essentially) generate a free group. 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. For example, if ν is a complete, discrete valuation and if the residue class field $\tilde{F}$ of F is finite, then it is easy to see that F is locally compact. For convenience, and to set notation, we state the above mentioned result in the form we require.

Proposition 2.1. [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.

We can now easily construct the locally compact fields we require.

Lemma 2.2. *Let $K[G]$ be given with $|G| = n$, and suppose that either $K = Q$ is the field of rationals, or $K = K_0(t)$ is the rational function field in one variable over some finite prime subfield K_0. Then there exists a field extension F of K, containing all nth roots of unity, such that F is locally compact with respect to the topology induced by a nonarchimedean valuation ν. Furthermore,*

i. *If $K = Q$ and if $\epsilon \in F$ is any nth root of 1, then there exist infinitely many integers $k \in Z \subseteq K$ 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 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 $F = Q_p$ 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 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 Z_p and that φ maps the roots in Z_p to those in $\tilde{F}$. In particular, since $n|(p-1)$, we see that 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 Z_p. Then $\varphi(\epsilon) \in \mathrm{GF}(p)$, so there exist infinitely many integers $k \in Z \subseteq K$ 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 powers of t.

Finally, if $0 \neq \epsilon \in F'$, then we know that there exist infinitely many distinct 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 $\nu(k - \delta) = 0$. □

Recall that if A is a subgroup of G, then there is a natural $F[A]$-bimodule projection $\pi_A \colon F[G] \to F[A] \subseteq F[G]$ given by $\pi_A(g) = g$ if $g \in A$ and $\pi_A(g) = 0$ for $g \in G \setminus A$. Part (i) of the following lemma allows us to easily verify the idempotent condition in most cases. See [I1] for basic properties of group representations.

Lemma 2.3. *Let $F[G]$ be given.*

i. *Let $A \triangleleft G$, let W be an $F[A]$-module, and let $V = W^G = W \otimes_{F[A]} F[G]$ be the induced $F[G]$-module. If $\alpha \in F[G]$ and $V\alpha = 0$, then $V\pi_A(\alpha) = 0$.*
ii. *Suppose $F[G]$ is semisimple, and let g and h be nonidentity elements of G. Then there exists an irreducible representation θ of $F[G]$ with $\theta(g) \neq 1$ and $\theta(h) \neq 1$.*

Proof. (i) Let T be a transversal for A in G with $1 \in T$, and write $\alpha = \sum_{t \in T} t\alpha_t$ with $\alpha_t \in F[A]$. If $w \in W$ and $x \in G$, then $w \otimes x \in V$, so $0 = (w \otimes x)\alpha = \sum_t (w \otimes xt)\alpha_t$. Note that $V = \oplus \sum_t W \otimes (xt)$ and that each $W \otimes (xt)$ is an $F[A]$-submodule of V. Thus we must have $(w \otimes xt)\alpha_t = 0$ for all $t \in T$. In particular, when $t = 1$, this yields $(w \otimes x)\alpha_1 = 0$. Consequently, $V\alpha_1 = \big(\sum_x W \otimes x\big)\alpha_1 = 0$ and $\pi_A(\alpha) = \alpha_1$ annihilates V.

(ii) If $h = g^{-1}$, let $\gamma = 1 - g$, and if $h \neq g^{-1}$, take $\gamma = (1 - g)(1 - h)$. In either case, we have $\gamma \neq 0$ and, since $F[G]$ is semisimple, there exists an irreducible representation θ with $\theta(\gamma) \neq 0$. Then certainly, $\theta(1-g) \neq 0$ and $\theta(1-h) \neq 0$. □

Now we list a few crucial special cases. Recall that if α commutes with α^*, then $u_k(\alpha) = (k - \alpha)(k - \alpha^*)^{-1}$ is a unitary unit. In the following, we use this formula to construct a pair of unitary units in $K[G]$. Then we apply Proposition 2.1 to verify that the two elements essentially generate a free group. With one exception, all the arguments are quite similar.

Proposition 2.4. *Let K be a nonabsolute field of characteristic $\neq 2$. If G is any of the groups listed below, then the unitary unit group $\mathfrak{U}(K[G])$ is not 2-related.*

i. *$G = \langle x \rangle \rtimes \langle y \rangle$, where $\langle x \rangle$ is cyclic of odd order prime to the characteristic of K, $\langle y \rangle$ is cyclic of odd prime order q, and $\langle y \rangle$ acts faithfully on $\langle x \rangle$.*
ii. *$G = \langle x, y \mid x^{2r} = 1,\ y^4 = 1,\ y^{-1}xy = x^{-1},\ x^r = y^2 \rangle$ is a quaternion group of order $4r$, with $r > 1$ prime to the characteristic of K.*
iii. *$G = (\langle x \rangle \times \langle w \rangle) \rtimes \langle y \rangle$ where $|x| = |y| = 4$, $|w| = 2$, $x^y = xw$, and $w^y = x^2 w$.*
iv. *$G = A \rtimes \langle y \rangle$, where A is abelian of odd order prime to* $\operatorname{char} K$*, and $\langle y \rangle$ is a cyclic group of order 4 acting in a fixed point free manner on A.*

v. *G is nonabelian, $|G|$ is prime to the characteristic of K, the center of G has an element z with $|z| > 2$, and all irreducible representations of G over the algebraic closure of K have degree at most 2.*

Proof. Without loss of generality, we can assume that either $K = Q$ is the field of rationals, or $K = K_0(t)$ 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 2.2. 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 to 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 in all cases expect possibly in part (i) when $q = \operatorname{char} K$. Thus, we split the part (i) argument in half, to deal separately with these two possibilities.

(i′) Here we assume that $q \neq \operatorname{char} K$. Write $x^y = x^r$ for some integer r and let $\lambda\colon \langle x\rangle \to F^\bullet$ be a faithful linear character. In particular, if $\lambda(x) = \epsilon$, then $|\epsilon| = |x|$ is odd. Furthermore, $\lambda^{y^i}(x) = \lambda(x^{y^i}) = \lambda(x^{r^i}) = \epsilon^{r^i} = \epsilon_i$, so $\epsilon_0, \epsilon_1, \dots, \epsilon_{q-1}$ are distinct, and consequently $\lambda, \lambda^y, \dots, \lambda^{y^{q-1}}$ are all distinct. Note also that ϵ has odd order and the automorphism of $\langle\epsilon\rangle$ given by $\epsilon \mapsto \epsilon^r$ has odd order q, so no ϵ_i^{-1} can equal an ϵ_j. Using Lemma 2.2, choose $k_0 \in K$ for ϵ_0 and $k_1 \in K$ for ϵ_1. Since there are infinitely many possible choices for these elements of K, we can assume that $k_0 - x$ and $k_1 - x^{-1}$ are invertible in $K[G]$. Furthermore, since x commutes with $x^* = x^{-1}$, we can set $a = u_{k_0}(x)u_{k_1}(x^{-1}) \in \mathfrak{U}(K[G])$.

Next, let δ be an element of order q in F and, by Lemma 2.2, choose $\ell \in K$ corresponding to δ. Since there are infinitely many such choices, we can assume that $\ell - y$ is invertible in $K[G]$, and we set $b = u_\ell(y)$.

We claim that $\langle a, b\rangle$ involves and hence contains a nonabelian free group. To this end, if $\theta\colon F[G] \to \mathrm{M}_q(F)$ is the induced representation $\theta = \lambda^G$, then we show that $\bar a = \theta(a)$ and $\bar b = \theta(b)$ satisfy the hypotheses of Proposition 2.1. First note that $\bar x = \theta(x) = \operatorname{diag}(\epsilon_0, \epsilon_1, \dots, \epsilon_{q-1})$, so $\bar a$ is diagonal with its ith entry given by

$$\bar a_i = \frac{k_0 - \epsilon_i}{k_0 - \epsilon_i^{-1}} \cdot \frac{k_1 - \epsilon_i^{-1}}{k_1 - \epsilon_i}.$$

By Lemma 2.2, the choice of k_0 and k_1, and the fact that $\epsilon_i^{-1} \neq \epsilon_j$, we see that $\nu(\bar a_0) > 0$, $\nu(\bar a_1) < 0$, and $\nu(\bar a_i) = 0$ 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 $q \neq \operatorname{char} K$, we see that $\bar{y}$ is similar to $\operatorname{diag}(1, \delta, \delta^2, \ldots, \delta^{q-1})$. Consequently, $\bar{b}$ is similar to $\operatorname{diag}(\bar{b}_0, \bar{b}_1, \ldots, \bar{b}_{q-1})$ where

$$\bar{b}_i = \frac{\ell - \delta^i}{\ell - \delta^{-i}}.$$

Since both δ and δ^{-1} occur as eigenvalues of $\bar{y}$, Lemma 2.2 implies that $\nu(\bar{b}_1) > 0$, $\nu(\bar{b}_{q-1}) < 0$, and $\nu(\bar{b}_i) = 0$ otherwise.

Finally, note that the idempotents associated with the plus and minus spaces for $\bar{a}$ are the same as those for $\bar{x}$, so we can write them as $\bar{\alpha}_+ = \theta(\alpha_+)$ and $\bar{\alpha}_- = \theta(\alpha_-)$, where α_+ and α_- are primitive idempotents in $F[\langle x \rangle]$. Similarly, the idempotents associated with the plus and minus spaces of $\bar{b}$ can be written as $\bar{\beta}_+ = \theta(\beta_+)$ and $\bar{\beta}_- = \theta(\beta_-)$, where β_+ and β_- are primitive idempotents of $F[\langle y \rangle]$. In particular, the identity coefficients of β_+ and β_- are both equal to $1/q$. Hence if $\alpha \in F[\langle x \rangle]$ is either of the two idempotents for a and if $\beta \in F[\langle y \rangle]$ is either of the two idempotents for b, then $\pi_A(\alpha\beta) = \pi_A(\beta\alpha) = \alpha/q$, where we set $A = \langle x \rangle \triangleleft G$. It follows that $\bar{\alpha}\bar{\beta} \neq 0$ and $\bar{\beta}\bar{\alpha} \neq 0$. Indeed, if say $\bar{\alpha}\bar{\beta} = 0$, then $\alpha\beta$ annihilates the induced module associated with the representation $\theta = \lambda^G$, and then Lemma 2.3(i) implies that $\pi_A(\alpha\beta) = \alpha/q$ acts trivially, a contradiction. We can now conclude from Proposition 2.1 that $\langle \bar{a}, \bar{b} \rangle$ contains a free group of rank 2, and consequently so does $\mathfrak{U}(K[G]) \supseteq \langle a, b \rangle$.

(i″) Now let $q = \operatorname{char} K$. Since $\langle y \rangle$ acts nontrivially on $\langle x \rangle$, it acts nontrivially on some Sylow p-subgroup of $\langle x \rangle$. Thus, without loss of generality, we can assume that x is a p-element. But $p \neq q$, so this action is necessarily fixed point free, and each nonidentity $\langle y \rangle$-orbit on $\langle x \rangle$ has q elements. In particular, $\langle y \rangle$ acts nontrivially on the subgroup of $\langle x \rangle$ of order p, and again without loss of generality, we can assume that x has order p.

Note that the $\langle y \rangle$-orbits in $\langle x \rangle$ are the conjugacy classes of G contained in $\langle x \rangle$. Let $\kappa_x \in K[G]$ denote the class sum for the conjugates of x, and let $\kappa_{x^{-1}} \in K[G]$ denote the class sum for the conjugates of x^{-1}. Then $\kappa_x \kappa_{x^{-1}} = q1 + \sum_z c_z \kappa_z$ where z runs through a set of representatives for the nonidentity G-conjugacy classes $\langle x \rangle$. If we think of the c_z, for the moment, as nonnegative integers which count the multiplicity of the group element z in the product, then counting elements yields $q^2 = q + \sum_z c_z q$ and hence $q = 1 + \sum_z c_z$. Thus, there are nonzero c_zs, and each is less than q. Hence, $c_z \not\equiv 0 \mod q$ for some z, and $0 \neq \kappa_x \kappa_{x^{-1}} \in K[G]$. Indeed, $0 \neq \kappa_x \kappa_{x^{-1}} \in K[\langle x \rangle]$, so this element is not nilpotent, and there exists an irreducible representation θ of $F[G]$ with $\theta(\kappa_x \kappa_{x^{-1}}) \neq 0$. But, $\kappa_x \kappa_{x^{-1}}$ is central, so $\theta(\kappa_x \kappa_{x^{-1}}) = fI$ with $0 \neq f \in F$. Furthermore, since $\kappa_x \kappa_{x^{-1}}$ is a sum of commuting elements of order p, we see that $f \in F'$, the subfield of F given by Lemma 2.2(ii).

Let $\lambda\colon \langle x \rangle \to F^\bullet$ be an irreducible constituent of the restriction of θ to $F[\langle x \rangle]$. If $\lambda = 1$, then certainly $\lambda(\kappa_x \kappa_{x^{-1}}) = 0$, a contradiction. Thus $\lambda \neq 1$ and, since $\langle x \rangle$ is cyclic of prime order, we see that λ is faithful. The argument of (i′) now shows that $\lambda, \lambda^y, \ldots, \lambda^{y^{q-1}}$ are distinct, so $\theta = \lambda^G$. In addition, we can choose

appropriate elements $k_0, k_1 \in K$ so that if $a = u_{k_0}(x)u_{k_1}(x^{-1}) \in \mathfrak{U}(K[G])$, then $\bar{a} = \theta(a) = \mathrm{diag}(\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{q-1})$ with $\nu(\bar{a}_0) > 0$, $\nu(\bar{a}_1) < 0$, and with $\nu(\bar{a}_i) = 0$ otherwise. Next, let $Y = 1 + y + \cdots + y^{q-1} \in K[G]$. Then, as is well known, $y^iY = Yy^i = Y$ so $Y^2 = qY = 0$. Furthermore, if $1 \neq z \in \langle x \rangle$, then

$$YzY = \sum_{i=0}^{q-1} Yzy^i = \sum_{i=0}^{q-1} Yy^{-i}zy^i = Y\sum_{i=0}^{q-1} y^{-i}zy^i = Y\kappa_z,$$

and consequently, $YF[G]Y \subseteq YZ$, where Z is the center of $F[G]$. Now if $\gamma = xY$, then $\gamma^* = Y^*x^* = Yx^{-1}$, so $\gamma^*\gamma = Yx^{-1}xY = Y^2 = 0$ and $\gamma\gamma^* = xYYx^{-1} = 0$. In particular, if $\beta = \kappa_{x^{-1}}\gamma = \kappa_{x^{-1}}xY$, then $\beta^*\beta = \beta\beta^* = 0$ and, by Lemma 2.2, we can choose $k \in K$ for the element $f \in F'$ so that $k - \beta$ is invertible in $K[G]$. Then $b = u_k(\beta) \in \mathfrak{U}(K[G])$, and we claim that $\bar{a}$ and $\bar{b} = \theta(b)$ satisfy the hypotheses of Proposition 2.1.

To this end, first note that $\theta(\beta) \neq 0$, by Lemma 2.3(i), since $\pi_A(\beta) = \kappa_{x^{-1}}x$ acts nontrivially in this representation. Next, since $YxY = Y\kappa_x$, we have

$$\beta^2 = \kappa_{x^{-1}}xY\kappa_{x^{-1}}xY = \kappa_{x^{-1}}xY\kappa_{x^{-1}}\kappa_x = \kappa_{x^{-1}}\kappa_x\beta,$$

and hence $\theta(\beta)^2 = \theta(\kappa_{x^{-1}}\kappa_x)\theta(\beta) = f\theta(\beta)$. In other words, $\theta(\beta)/f$ is a nonzero idempotent in $\mathrm{M}_q(F)$. Furthermore, $YF[G]Y \subseteq YZ$ implies that $\beta F[G]\beta \subseteq \beta Z$. Hence $\theta(\beta)\mathrm{M}_q(F)\theta(\beta) \subseteq F\theta(\beta)$, and $\theta(\beta)/f$ is a rank 1 idempotent.

In a similar manner, since $\beta^* = \kappa_x Yx^{-1}$, we see that $\theta(\beta^*)/f$ is a rank 1 idempotent and, of course, $\beta\beta^* = \beta^*\beta = 0$ implies that the two idempotents are orthogonal. Now $b = (k - \beta)/(k - \beta^*)$, so it follows from the above that $\bar{b} = \theta(b)$ is similar to the diagonal matrix $\mathrm{diag}(\tilde{f}, \tilde{f}^{-1}, 1, 1, \ldots, 1)$ where $\tilde{f} = (k - f)/k$ and $\nu(\tilde{f}) > 0$ by the choice of k. Note that the idempotents corresponding to the positive and negative eigenspaces of $\bar{b}$ are precisely $\bar{\beta}_+ = \theta(\beta)/f$ and $\bar{\beta}_- = \theta(\beta^*)/f$.

Furthermore, there exist idempotents α_+ and α_- in $K[\langle x \rangle]$ such that $\bar{\alpha}_+ = \theta(\alpha_+)$ and $\bar{\alpha}_- = \theta(\alpha_-)$ are the idempotents corresponding to the positive and negative eigenspaces of $\bar{a}$. To show, for example, that $\bar{\alpha}_+\bar{\beta}_+ \neq 0$, it clearly suffices to prove that $\bar{\alpha}_+\theta(\beta) = \theta(\alpha_+)\theta(\beta) = \theta(\alpha_+\beta)$ is nonzero. But, recall that the representation θ is induced from $\langle x \rangle = A \triangleleft G$, and that $\pi_A(\beta) = \kappa_{x^{-1}}x$ acts as an invertible linear transformation. Thus $\theta(\pi_A(\alpha_+\beta)) = \theta(\alpha_+\pi_A(\beta)) = \bar{\alpha}_+\theta(\pi_A(\beta))$ is not zero, and hence by Lemma 2.3(i) neither is $\bar{\alpha}_+\bar{\beta}_+$. The remaining seven idempotent products can clearly be handled in a similar manner, so we conclude from Proposition 2.1 that $\langle \bar{a}, \bar{b} \rangle$ contains the nonabelian free group $\mathfrak{F}_2$.

(ii) Let $\lambda\colon \langle x \rangle \to F^\bullet$ be a faithful linear character and let $\theta = \lambda^G$ be the induced representation $\theta\colon F[G] \to \mathrm{M}_2(F)$. Since $|x| \geq 4$, we see that $\lambda^y = \lambda^{-1} \neq \lambda$, and hence θ is irreducible. Furthermore, $\theta(x) = \mathrm{diag}(\epsilon, \epsilon^{-1})$, for some $\epsilon \in F$ of order $|x| = 2r$ and, since $\theta(y^2) = \theta(x^r) = \mathrm{diag}(-1, -1)$, it follows that $\theta(y)$ is similar to $\mathrm{diag}(i, -i)$, where $i^2 = -1$. By Lemma 2.2, we can choose $k \in K$ corresponding to ϵ with $k - x$ invertible in $K[G]$, and we can choose $\ell \in K$ corresponding to i

with $\ell - y$ invertible in $K[G]$. We claim that the subgroup of $\mathfrak{U}(K[G])$ generated by $a = u_k(x)$ and $b = u_\ell(y)$ contains a free group of rank 2. Indeed, note that $\theta(a) = \mathrm{diag}(f_1, f_1^{-1})$, where $f_1 = (k-\epsilon)/(k-\epsilon^{-1})$ satisfies $\nu(f_1) > 0$, and $\theta(b)$ is similar to $\mathrm{diag}(f_2, f_2^{-1})$, where $f_2 = (\ell - i)/(\ell + i)$ satisfies $\nu(f_2) > 0$. Finally, if the idempotent condition does not hold, then since $m = 2$, $\theta(x)$ and $\theta(y)$ would have a common eigenvector, contradicting the fact that θ is an irreducible representation. Thus the idempotent condition is satisfied, and Proposition 2.1 yields the result.

(iii) First note that $(xy)^2 = y^2(y^{-2}xy^2)(y^{-1}xy) = y^2x^{-1}xw = y^2w \neq 1$ and that $(xy)^4 = (y^2w)^2 = y^4w^2 = 1$. Again let $i \in F$ with $i^2 = -1$ and choose $k \in K$ corresponding to i, and with $k - y$ and $k - xy$ both invertible in $K[G]$. We claim that the subgroup of $\mathfrak{U}(K[G])$ generated by the units $a = u_k(y)$ and $b = u_k(xy)$ contains a free group of rank 2. To this end, let λ be the linear character of $A = \langle x \rangle \times \langle w \rangle$ given by $\lambda(x) = i$ and $\lambda(w) = 1$. Then $\lambda^y(x) = \lambda(x^y) = \lambda(xw) = i$, $\lambda^{y^2}(x) = \lambda(x^{y^2}) = \lambda(x^{-1}) = -i$ and $\lambda^{y^3}(x) = \lambda(x^{y^3}) = \lambda(x^{-1}w) = -i$. In particular, if $\theta\colon F[G] \to \mathrm{M}_4(F)$ is the induced representation $\theta = \lambda^G$, then $\theta(x) = \mathrm{diag}(i, i, -i, -i)$, so

$$\theta(y) = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ 1 & & & \end{bmatrix} \qquad \text{and} \qquad \theta(xy) = \begin{bmatrix} & i & & \\ & & i & \\ & & & -i \\ -i & & & \end{bmatrix}.$$

Since G can also be written as $A \rtimes \langle xy \rangle$, we see that both $\theta(y)$ and $\theta(xy)$ are similar to $\mathrm{diag}(1, i, -1, -i)$, and therefore both a and b are similar to $\mathrm{diag}(1, f, 1, f^{-1})$ where $f = (k-i)/(k+i)$. By Lemma 2.2, $\nu(f) > 0$ and $\nu(f^{-1}) < 0$.

It remains to check the idempotent condition. Here

$$\begin{aligned}
\bar{\alpha}_+ &= \frac{1}{4}[1 + i^{-1}\theta(y) + i^{-2}\theta(y)^2 + i^{-3}\theta(y)^3] \\
\bar{\alpha}_- &= \frac{1}{4}[1 + i\theta(y) + i^2\theta(y)^2 + i^3\theta(y)^3] \\
\bar{\beta}_+ &= \frac{1}{4}[1 + i^{-1}\theta(xy) + i^{-2}\theta(xy)^2 + i^{-3}\theta(xy)^3] \\
\bar{\beta}_- &= \frac{1}{4}[1 + i\theta(xy) + i^2\theta(xy)^2 + i^3\theta(xy)^3],
\end{aligned}$$

so it is a simple matter (using computer algebra software) to determine these matrices and to verify that all appropriate eight products are nonzero. Indeed, each entry in each product is nonzero, so it suffices to check only the $(1,1)$-entry. With this, Proposition 2.1 yields the result.

(iv) By assumption, $\langle y^2 \rangle$ acts fixed point free on the abelian group A of odd order. Hence y^2 must act in a dihedral manner on A. In particular, if $\mu\colon A \to F^\bullet$ is any linear character, then $\mu^{y^2} = \mu^{-1}$ and $\ker \mu^{y^2} = \ker \mu^{-1} = \ker \mu$. Note also that $\langle y \rangle$ acts fixed point freely on the nonprincipal linear characters of A.

Now let λ be a fixed nonprincipal linear character of A, so that $\lambda, \lambda^y, \lambda^{y^2}, \lambda^{y^3}$ are all distinct. If $\ker\lambda = \ker\lambda^y$, then all four characters have the same kernel. In particular, if we choose $x \in A$ to generate the cyclic quotient $A/(\ker\lambda)$, then the four values $\lambda^{y^i}(x)$ must be distinct. Thus, setting $\theta = \lambda^G$, we see that $\theta(x) = \mathrm{diag}(\epsilon, \epsilon^{-1}, \delta, \delta^{-1})$ with all eigenvalues distinct. On the other hand, if $\ker\lambda \neq \ker\lambda^y$, then we can take $x \in \ker\lambda^y \setminus \ker\lambda$. In this case, $\theta(x) = \mathrm{diag}(\epsilon, \epsilon^{-1}, 1, 1)$ with $\epsilon \neq \epsilon^{-1}$. Thus in either case, we have an element $x \in A$ satisfying $\theta(x) = \mathrm{diag}(\epsilon, \epsilon^{-1}, \delta, \delta^{-1})$ with $\epsilon \neq \epsilon^{-1}, \delta, \delta^{-1}$. Now, by Lemma 2.2, let $k \in K$ correspond to ϵ with $k - x$ invertible in $K[G]$, and set $a = u_k(x) \in \mathfrak{U}(K[G])$. Then $\theta(a) = \mathrm{diag}(\bar{a}_1, \bar{a}_1^{-1}, \bar{a}_2, \bar{a}_2^{-1})$ with $\nu(\bar{a}_1) > 0$ and $\nu(\bar{a}_2) = 0$.

Of course, $\theta(y)$ is similar to $\mathrm{diag}(i, -i, 1, -1)$ where $i^2 = -1$. So if $\ell \in K$ corresponds to i, then $b = u_\ell(y) \in \mathfrak{U}(K[G])$, and we see that $\theta(b)$ is similar to $\mathrm{diag}(\bar{b}, \bar{b}^{-1}, 1, 1)$ with $\nu(\bar{b}) > 0$. Since θ is induced from A and since $a \in K[A]$, Lemma 2.3(i) implies, as usual, that the idempotent condition is satisfied. We therefore conclude from Proposition 2.1 that $\langle \theta(a), \theta(b) \rangle$ contains a nonabelian free group, and hence the same is true of $\mathfrak{U}(K[G])$.

(v) Choose $x, y \in G$ with commutator $w = [x, y] \neq 1$. It clearly suffices to assume that $G = \langle x, y, z \rangle$. Since $w, z^2 \neq 1$, it follows from Lemma 2.3(ii) that there exists an irreducible representation θ of $F[G]$ with $\theta(w) \neq 1$ and $\theta(z^2) \neq 1$. Note that $[\theta(x), \theta(y)] = \theta(w) \neq 1$, so $\theta(x)$ and $\theta(y)$ are not central. In particular, $\deg\theta > 1$ and consequently, by assumption and the fact that F is a splitting field for $K[G]$, we have $\deg\theta = 2$ and $\theta\colon F[G] \to \mathrm{M}_2(F)$. Write $\theta(z) = \mathrm{diag}(\delta, \delta)$. Since $\theta(z^2) \neq 1$, we know that $\delta^2 \neq 1$, so the three elements 1, δ, and δ^{-1} are distinct.

For convenience, let us assume that $\theta(x)$ is diagonal. Say $\theta(x) = \mathrm{diag}(\epsilon_1', \epsilon_2')$ with $\epsilon_1' \neq \epsilon_2'$ since $\theta(x)$ is not central. Now $1, \delta, \delta^{-1}$ are distinct, so we can choose $i = 0, \pm 1$ so that if $x_1 = xz^i$, then $\theta(x_1) = \mathrm{diag}(\epsilon_1, \tilde{\epsilon}_1)$ with $\epsilon_1 \neq \pm 1$. Similarly, there exists $x_2 = xz^j$ so that $\theta(x_2) = \mathrm{diag}(\tilde{\epsilon}_2, \epsilon_2)$ with $\epsilon_2 \neq \pm 1$. If $\tilde{\epsilon}_1 = \epsilon_1^{-1}$, let $a = u_{k_1}(x_1)$ where $k_1 \in K$ corresponds to ϵ_1. If $\tilde{\epsilon}_1 \neq \epsilon_1^{-1}$ but $\tilde{\epsilon}_2 = \epsilon_2^{-1}$, let $a = u_{k_2}(x_2)$ where $k_2 \in K$ corresponds to ϵ_2. Finally, if $\tilde{\epsilon}_1 \neq \epsilon_1^{-1}$ and $\tilde{\epsilon}_2 \neq \epsilon_2^{-1}$, take $a = u_{k_1}(x_1)u_{k_2}(x_2)^{-1}$ where $k_1 \in K$ corresponds to ϵ_1 and $k_2 \in K$ corresponds to ϵ_2. In all cases, we see that $a \in \mathfrak{U}(K[G])$, and $\theta(a) = \mathrm{diag}(\alpha_1, \alpha_2)$ with $\nu(\alpha_1) > 0$ and $\nu(\alpha_2) < 0$.

In a similar manner, by temporarily diagonalizing $\theta(y)$, we construct a unit $b \in \mathfrak{U}(K[G])$ determined by y and z. Note that the eigenspaces of $\theta(a)$ are those of $\theta(x)$, and the eigenspaces of $\theta(b)$ are those of $\theta(y)$. Thus, if $\theta(a)$ and $\theta(b)$ have a common eigenspace, then this would yield a subspace stable under the action of $G = \langle x, y, z \rangle$, contradicting the fact that θ is irreducible. Therefore, since $m = 2$, the idempotent condition for $\theta(a)$ and $\theta(b)$ is satisfied, and we conclude from Proposition 2.1 that the free group $\mathfrak{F}_2$ is involved in $\langle a, b \rangle$. $\square$

We need two more concrete examples. For these, we must first briefly discuss $\mathrm{GL}_2(K)$ and $\mathrm{O}_3(K)$, where $\mathrm{O}_3(K)$ is the set of 3×3 matrices X with $X^T X = I$. In other words, $\mathrm{O}_3(K)$ is the unitary group (really the orthogonal group)

corresponding to the transpose involution. The following is well known.

Lemma 2.5. *Let K be a nonabsolute field of characteristic $\neq 2$. Then $GL_2(K)$ and $O_3(K)$ contain nonabelian free groups.*

Proof. Let G be the quaternion group of order 8. Then

$$K[G] = K \oplus K \oplus K \oplus K \oplus \mathcal{Q}(K)$$

where $\mathcal{Q}(K)$ is the usual quaternion algebra with K-basis $\{1, i, j, k\}$ and relations $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$ and $ki = j$. Since $\mathfrak{U}(K[G])$ is not 2-related, by Proposition 2.4(ii), it follows that the unit group $\mathcal{U}(K)$ of $\mathcal{Q}(K)$ has a nonabelian free subgroup.

Let $\mathcal{P}(K) = \{\alpha i + \beta j + \gamma k |\ \alpha, \beta, \gamma \in K\}$ be the 3-dimensional space of pure quaternions. Then $\mathcal{U}(K)$ acts on $\mathcal{P}(K)$ by conjugation, and this gives rise to a homomorphism $\theta{:}\mathcal{U}(K) \to \mathrm{GL}_3(K)$. It is easy to check that the image is contained in $\mathrm{O}_3(K)$. Indeed, let $u \in \mathcal{U}(K)$, let $a, b \in \{i, j, k\}$ and let $\mathrm{tr}\colon \mathcal{Q}(K) \to K$ denote the usual trace map. Since $a^2 = b^2 = -1$, the matrix entries satisfy

$$\theta(u)_{a,b} = -\mathrm{tr}(u^{-1}aub) = -\mathrm{tr}(ubu^{-1}a) = \theta(u^{-1})_{b,a}.$$

Thus $\theta(u)^{-1} = \theta(u^{-1}) = \theta(u)^T$, and $\theta{:}\mathcal{U}(K) \to \mathrm{O}_3(K)$. Since the kernel of θ is clearly equal to $\mathcal{U}(K) \cap K^\bullet$, it follows from the remarks of the previous paragraph that $\mathrm{O}_3(K)$ contains a nonabelian free group.

Finally, if $\mathrm{char}\, K > 0$, then $\mathcal{Q}(K) \cong \mathrm{M}_2(K)$, so $\mathcal{U}(K) \cong \mathrm{GL}_2(K)$ and $\mathrm{GL}_2(K)$ contains a copy of $\mathfrak{F}_2$. On the other hand, if $\mathrm{char}\, K = 0$, then [S] supplies concrete generators for a rank 2 free subgroup of $\mathrm{SL}_2(Z)$. $\square$

With this in hand, we can now prove

Lemma 2.6. *Let K be a nonabsolute field of characteristic $\neq 2$ and let $G = A \rtimes \langle x \rangle$, where A is abelian of order prime to the characteristic of K and $\langle x \rangle$ is cyclic of prime order $q > 2$. If $\langle x \rangle$ does not normalize all subgroups of A, then $\mathfrak{U}(K[G])$ is not 2-related.*

Proof. Since A is abelian, both $\langle x \rangle$ and $*$ permute the finitely many primitive idempotents of $K[A]$. Indeed, if e is such an idempotent, then $(e^x)^* = (x^{-1}ex)^* = x^*e^*(x^{-1})^* = x^{-1}e^*x = (e^*)^x$, so the actions commute. Furthermore, each idempotent of $K[A]$ is uniquely a sum of primitives. Now, by assumption, $\langle x \rangle$ does not normalize some subgroup B of A. Hence $\langle x \rangle$ does not fix the principal idempotent e_B of $K[B]$, and consequently $\langle x \rangle$ does not fix at least one of the primitive idempotent summands of e_B.

Now let e be any primitive idempotent of $K[A]$ that is moved by x. Then the element $f = e + e^x + \cdots + e^{x^{q-1}}$ is a sum of q orthogonal idempotents, and hence it is an idempotent in $K[A]$ which is clearly central in $K[G]$. Note that $*$ permutes the $\langle x \rangle$-orbits of primitive idempotents, so there are two cases to consider according to whether $*$ fixes $\{e, e^x, \ldots, e^{x^{q-1}}\}$ or not.

Suppose first that $*$ fixes the orbit. Then $fK[G]$ is a $*$-stable direct summand of $K[G]$, and it suffices to show that the group $\mathfrak{U}(fK[G])$ is not 2-related. Note that $*$ has order 2 and permutes the set $\{e, e^x, \dots, e^{x^{q-1}}\}$ containing an odd number of elements. Thus $*$ must fix at least one member of this set, say e. Next, observe that $\langle fx\rangle$ is a group of units of order q in $fK[G]$ that transitively permutes the set $\{e, e^x, \dots, e^{x^{q-1}}\}$. Furthermore, the latter idempotents are the summands of an orthogonal decomposition of f, the identity of $fK[G]$. Thus, if we define $e_{i,j} = x^{-j}ex^i$ for $i, j = 0, 1, \dots, q-1$ then, by the proof of [P, Lemma 6.1.6], $\{e_{i,j}\}$ is a set of matrix units for $\mathrm{M}_q(K)$, a K-subalgebra of $fK[G]$. Indeed, since $e_{i,j}^* = (x^{-j}ex^i)^* = x^{-i}ex^j = e_{j,i}$, we see that $\mathrm{M}_q(K)$ is $*$-stable with $*$ acting as the transpose. Thus $\mathfrak{U}(fK[G]) \supseteq \mathfrak{U}(\mathrm{M}_q(K)) = \mathrm{O}_q(K) \supseteq \mathrm{O}_3(K)$. But $\mathrm{O}_3(K)$ contains a free group of rank 2, by the previous lemma, so this case follows.

On the other hand, suppose that $*$ moves the orbit $\{e, e^x, \dots, e^{x^{q-1}}\}$. Then it is clear that f^* is orthogonal to f, and hence that $S = fK[G] \oplus f^*K[G]$ is a $*$-stable direct summand of $K[G]$. Again, it suffices to show that $\mathfrak{U}(S)$ is not 2-related. Now, as above, we know that $fK[G]$ contains a subalgebra isomorphic to $\mathrm{M}_q(K)$. With this, we get an embedding of $\mathrm{GL}_q(K)$ into $\mathfrak{U}(S)$ given by $u \mapsto u \oplus (u^*)^{-1}$. Thus $\mathfrak{U}(S)$ contains an isomorphic copy of $\mathrm{GL}_q(K) \supseteq \mathrm{GL}_2(K)$, and hence Lemma 2.5 implies that it contains a free group of rank 2. This completes the proof. □

The next argument is similar, and even quicker. Note that, if $|G|$ is prime to the characteristic of the algebraically closed field F, then the representation theory of $F[G]$ mirrors that of the complex group algebra $C[G]$.

Lemma 2.7. *Let K be a nonabsolute field of characteristic $\neq 2$ and let F denote its algebraic closure. Suppose G is a 2-group with a normal elementary abelian subgroup A of index 4. If $F[G]$ has an irreducible representation of degree > 2, then $\mathfrak{U}(K[G])$ is not 2-related.*

Proof. By assumption, G has an irreducible character χ with $\deg \chi \geq 4$. If λ is an irreducible constituent of χ_A, the restriction of χ to A, then λ is linear and Frobenius reciprocity [I1, Lemma 5.2] implies that χ is a constituent of the induced character λ^G of degree 4. Thus $\chi = \lambda^G$ has degree 4. Furthermore, we know that G/A transitively permutes the irreducible constituents of χ_A, and it is now clear that G/A must act regularly. Indeed, if this were not the case, then there would exist a subgroup $B \supseteq A$ fixing λ, with $|B : A| = 2$. But then the image of A is central in the representation associated with λ^B, so λ^B would split into two linear constituents, and then $\chi = \lambda^G = (\lambda^B)^G$ would also split, a contradiction.

Let e be the primitive idempotent of $F[A]$ corresponding to λ. Since A is an elementary abelian 2-group, $\lambda\colon A \to \{\pm 1\}$ and hence $e \in K[A]$. Furthermore, $*$ acts trivially on $K[A]$, so $e^* = e$. Now let x_1, x_2, x_3, x_4 be coset representatives for A in G. Then $f = e^{x_1} + e^{x_2} + e^{x_3} + e^{x_4}$ is a sum of four orthogonal idempotents, and hence f is a $*$-stable central idempotent of $K[G]$. In addition, if we set $e_{i,j} = x_j^{-1}ex_i$, then the proof of [P, Lemma 6.1.6] implies that $\{e_{i,j} |\ i, j =$

$1, 2, 3, 4\}$ is a set of matrix units in $fK[G]$. Thus $fK[G] \supseteq \mathrm{M}_4(K)$ and, since $e_{i,j}^* = (x_j^{-1} e x_i)^* = x_i^{-1} e x_j = e_{j,i}$, we see that $\mathfrak{U}(fK[G]) \supseteq \mathrm{O}_4(K) \supseteq \mathrm{O}_3(K)$. Thus, by Lemma 2.5, $\mathfrak{U}(fK[G])$ contains the free group $\mathfrak{F}_2$, and hence the same is true for $\mathfrak{U}(K[G])$. $\square$

§3. Group-Theoretic Reductions

In this final section, we complete the proof of Theorem 1.3 by showing that if $\mathfrak{U}(K[G])$ is 2-related, then G has the appropriate structure. We proceed in a series of steps, each step being proved by induction. Specifically, we know by Lemma 1.2 that if $\mathfrak{U}(K[G])$ is 2-related, then so is $\mathfrak{U}(K[H])$ for every subgroup and every homomorphic image H of G. Thus, we are able to assume at each step that all proper subgroups and homomorphic images of G satisfy the conclusion of the step. In particular, if G is a minimal counterexample, then we are able to show that G is one of the handful of special cases considered in Proposition 2.4, Lemma 2.6 and Lemma 2.7. We start with

Lemma 3.1. *Assume that $\mathfrak{U}(K[G])$ is 2-related. If G is a q-group for some odd prime q different from the characteristic of K, then G is abelian.*

Proof. Let G be a minimal counterexample to the conclusion. Then G is a nonabelian q-group having all proper subgroups and homomorphic images abelian. The structure of such minimal nonabelian groups is well known, and a quick derivation of this result is included in the argument below. First, G is not cyclic, so it has two distinct maximal subgroups A and B, each normal of index q. By assumption, A and B are abelian and, since $A \cap B$ is centralized by $G = AB$, we see that $Z = \mathbb{Z}(G) = A \cap B$ has index q^2 in G with G/Z abelian of period q. Next, let J be a central subgroup of G of order q. Then G/J is abelian, so $G' \subseteq J$, and hence $G' = J$. Thus J is unique and Z is cyclic of order, say, q^n.

Since $q \neq 2$ and G' is central of period q, the q-power map $\sigma\colon x \mapsto x^q$ is a homomorphism into Z. In particular, if H is the kernel of σ, then H is normal in G and consists of all elements of G of order 1 or q. If σ is onto Z, then G has a cyclic subgroup C of order q^{n+1} and hence of index q. Furthermore, $|H| = q^2$ and $|H \cap C| = q$, so $G = C \rtimes \langle y \rangle$ for some element y of order q. But this group cannot occur, by Proposition 2.4(i), and thus σ is not onto. It follows that $\sigma(G) = \sigma(Z) = Z^q$, so $G = ZH$ and H is nonabelian. By the minimal nature of G, we see that $G = H$ is a nonabelian q group of order q^3 and period q. But this group has the structure described in Lemma 2.6, so again we obtain a contradiction. $\square$

More to the point, we now prove

Lemma 3.2. *If $\mathfrak{U}(K[G])$ is 2-related, then G has subgroups $P \subseteq T \subseteq G$ with*

i. *P is a normal Sylow p-subgroup of G with p equal to the characteristic of K. By convention, $P = 1$ if* $\operatorname{char} K = 0$.

ii. *T is a normal 2-complement of G, so that T has odd order and G/T is a 2-group.*
iii. *T/P is abelian.*

Proof. Note that a normal Sylow subgroup and a normal Sylow complement are necessarily characteristic subgroups. Assume by way of contradiction that the result is false, and let G be a counterexample of minimal order. Then every proper subgroup and homomorphic image of G satisfies the conclusion of this lemma. We proceed in a series of steps.

Step 1. *G has no proper normal subgroup of order divisible by $p = \operatorname{char} K$. Furthermore, G has no proper homomorphic image of even order.*

Proof. Suppose N is a proper normal subgroup of order divisible by p. Then N has a nonidentity characteristic p-subgroup $\tilde{P}$, so $\tilde{P} \triangleleft G$. Since $G/\tilde{P}$ satisfies the conclusion of this lemma, it is clear that G does also, a contradiction.

On the other hand, suppose that G has a proper homomorphic image $\bar{G}$ of even order. Then $\bar{G}$ has a nonidentity 2-group as a homomorphic image, and hence so does G. In other words, there exists $M \triangleleft G$ with G/M a nonidentity 2-group. Since M satisfies the conclusion of this lemma, it is now clear that G does also, again a contradiction. □

Step 2. *G has odd order.*

Proof. If G has even order, then it follows from Step 1 that G does not have a normal 2-complement. On the other hand, every proper subgroup of G does have a normal 2-complement. Thus, by Frobenius' theorem [H, Satz IV.5.8(b)], G must have a nonidentity normal 2-subgroup, and we choose A to be such a subgroup of minimal order. By Step 1, G/A has odd order, so A is a Sylow 2-subgroup of G. Furthermore, G/A is solvable, so there exists a normal subgroup H of G with $A \subseteq H \subseteq G$ and G/H cyclic of odd prime order q.

By the minimal nature of G, H has a normal 2-complement T and $T \triangleleft G$. But G/T has even order, since $T \cap A = 1$, so Step 1 implies that $T = 1$ and $H = A$. In other words, $G = A \rtimes \langle y \rangle$ where A is a 2-group and $\langle y \rangle$ is cyclic of odd prime order q. Furthermore, the minimal nature of A guarantees that A has no proper characteristic subgroup. Thus A is an elementary abelian 2-group and $\langle y \rangle$ acts irreducibly on A. If $|A| = 2$, then $\langle y \rangle$ acts trivially, so $\langle y \rangle \triangleleft G$ and $G/\langle y \rangle \cong A$, contradicting Step 1. Thus $|A| > 2$ and A has nonidentity subgroups not normalized by $\langle y \rangle$. Thus G satisfies the assumptions of Lemma 2.6, contradicting the fact that $\mathfrak{U}(K[G])$ is 2-related. □

Step 3. *Final contradiction.*

Proof. A repetition of the above argument will yield the result. We now know that G has odd order. Furthermore, any group of odd order satisfying the conclusion of this lemma has a normal q-complement for every prime q different from $p = \operatorname{char} K$. Conversely, suppose that G has a normal q-complement C_q

for each prime divisor q of $|G|$ different from p. Then $\bigcap_q C_q$ is a normal Sylow p-subgroup of G and hence, by Step 1, $\bigcap_q C_q = 1$. It then follows that G is nilpotent of odd order prime to p, and consequently Lemma 3.1 implies that G is abelian, a contradiction.

Thus, for some prime t dividing $|G|$ and different from $\operatorname{char} K$, G does not have a normal t-complement. Indeed, G has no proper homomorphic image of order divisible by t. To see this, suppose $\bar{G}$ is such a homomorphic image with t dividing $|\bar{G}|$. Then $\bar{G}$ has a normal t-complement, so it has a nonidentity t-group as a homomorphic image. It follows that there exists $M \lhd G$ with G/M a nonidentity t-group. But M has a normal t-complement N, and N is surely a normal t-complement in G, contradiction.

Since every proper subgroup of G has a normal t-complement, Frobenius' theorem [H, Satz IV.5.8(b)] implies that G has a nonidentity normal t-subgroup, and we choose A to be such a subgroup of minimal order. By the above observation, G/A has order prime to t, so A is a Sylow t-subgroup of G. Furthermore, G/A is solvable, so there exists a normal subgroup H of G with $A \subseteq H \subseteq G$ and G/H cyclic of odd prime order $q \neq t$.

By the minimal nature of G, H has a normal t-complement T and $T \lhd G$. But G/T has order divisible by t, since $T \cap A = 1$, so the above observation implies that $T = 1$ and $H = A$. In other words, $G = A \rtimes \langle y \rangle$ where A is a t-group and $\langle y \rangle$ is cyclic of odd prime order $q \neq t$. Furthermore, the minimal nature of A guarantees that A has no proper characteristic subgroup. Thus A is an elementary abelian t-group and $\langle y \rangle$ acts irreducibly on A. If $\langle y \rangle$ acts trivially, then $\langle y \rangle \lhd G$ and $G/\langle y \rangle \cong A$, contradicting our comments about the possible homomorphic images of G. Thus $\langle y \rangle$ must act faithfully on A.

Finally, if A is not cyclic, then A has nonidentity subgroups not normalized by $\langle y \rangle$. Thus G satisfies the assumptions of Lemma 2.6, contradicting the fact that $\mathfrak{U}(K[G])$ is 2-related. On the other hand, if A is cyclic, then G is the type of group considered in Proposition 2.4(i), and again we obtain the necessary contradiction. □

For the next step, it is convenient to first isolate the following fact.

Lemma 3.3. *Let G be a 2-group with center Z of index 8, and assume that every nonabelian homomorphic image of G has a center which is an elementary abelian 2-group. Then G has an abelian subgroup of index 2.*

Proof. Assume, by way of contradiction, that G has no abelian subgroup of index 2. Then certainly G/Z has no elements of order 4. It follows that G/Z is an elementary abelian 2-group, and hence that G has class 2. By assumption, Z is an elementary abelian 2-group. Suppose $g \in G \setminus Z$. If $|G : \mathbb{C}_G(g)| = 2$, then $\mathbb{C}(g)$ is clearly an abelian subgroup of G of index 2, a contradiction. Thus $|G : \mathbb{C}(g)| = 4$ and hence the commutator group $[g, G]$ has order 4. In particular, we have $|G'| \geq 4$.

Let x, y, z generate G/Z and let u, v and w be the three commutators $u =$

$[x,y],\ v=[y,z],\ w=[z,x]$. Then u,v,w generate G', so $|G'|\le 8$. If $|G'|=4$, we note that the result of the previous paragraph yields $[g,G]=G'$ for all $g\in G\setminus Z$. In this case, if T is any subgroup of G' of order 2, then G/T is a group with commutator G'/T of order 2 and with center Z/T of index 8. As is well known, this cannot occur. For example, let $\bar g$ and $\bar h$ to be elements of $\bar G=G/T$ which do not commute. Then $\mathbb{C}_{\bar G}(\bar g)$ and $\mathbb{C}_{\bar G}(\bar h)$ are distinct abelian subgroups of $\bar G$ of index 2, and hence $\mathbb{C}_{\bar G}(\bar g)\cap\mathbb{C}_{\bar G}(\bar h)$ is a central subgroup of $\bar G$ of index 4, contradiction. Thus u,v,w generate an elementary abelian 2-group of order 8.

Again, let $g\in G\setminus Z$. Since $[g,G]$ has order 4, this group is properly smaller than G'. Hence $G/[g,G]$ is nonabelian, so its center is an elementary abelian 2-group by hypothesis. But the image of g is contained in this center, so we conclude that $g^2\in[g,G]$ for all such g. In particular, we must have $x^2=u^\alpha w^\beta$, $y^2=u^\gamma v^\delta$ and $z^2=v^\sigma w^\tau$ for suitable exponents $\alpha,\beta,\gamma,\delta,\sigma,\tau\in\{0,1\}$. Now, let $g=x^ay^bz^c\in G\setminus Z$. Then $[g,x]=u^{-b}w^c$, $[g,y]=u^av^{-c}$ and $[g,z]=w^{-a}v^b$ generate $[g,G]$, so we see that $[g,G]=\{u^rv^sw^t\mid rc+sa+tb\equiv 0 \mod 2\}$. Next, observe that

$$\begin{aligned}
g^2 &= x^ay^bz^c\cdot x^ay^bz^c = x^ay^b\cdot x^az^c\cdot y^bz^c\cdot[z^c,x^a]\\
&= x^{2a}y^b\cdot y^bz^{2c}\cdot[y^b,x^a][z^c,y^b][z^c,x^a]\\
&= x^{2a}y^{2b}z^{2c}\cdot u^{-ab}v^{-bc}w^{ac}\\
&= u^{(a\alpha+b\gamma-ab)}v^{(b\delta+c\sigma-bc)}w^{(a\beta+c\tau+ac)}.
\end{aligned}$$

In particular, since $g^2\in[g,G]$, we have

$$\begin{aligned}
0 &\equiv c(a\alpha+b\gamma-ab)+a(b\delta+c\sigma-bc)+b(a\beta+c\tau+ac)\\
&\equiv ab(\delta+\beta)+ac(\alpha+\sigma)+bc(\gamma+\tau)-abc \mod 2
\end{aligned}$$

and this holds for all choices of a,b,c not all 0. Now, with $a=b=1$ and $c=0$, we deduce that $\beta+\delta=0$. Similarly, $a=c=1,\ b=0$ yields $\alpha+\sigma=0$, and $b=c=1,\ a=0$ implies that $\gamma+\tau=0$. Thus the above displayed equation simplifies to $0\equiv -abc \mod 2$, a contradiction when $a=b=c=1$. It follows that G has an abelian subgroup of index 2, as required. □

Now if $\mathfrak{U}(K[G])$ is 2-related then Lemma 3.2 implies that G has a normal Sylow p-subgroup P for $p=\operatorname{char}K$. Furthermore, by Lemma 1.2, $\mathfrak{U}(K[G/P])$ is also 2-related. Thus, for most of the remainder of this paper, it suffices study G/P, or equivalently we can assume that $|G|$ is prime to the characteristic of K. The next major step in the proof of Theorem 1.3 is

Lemma 3.4. *If $\mathfrak{U}(K[G])$ is 2-related and if $|G|$ is prime to the characteristic of K, then either G is abelian or it has an abelian subgroup of index 2.*

Proof. Assume by way of contradiction that the result is false, and let G be a counterexample of minimal order. Then every proper subgroup and homomorphic image of G satisfies the conclusion of this lemma. Let F denote the algebraic closure of K. We proceed in a series of steps.

Step 1. *G has the following properties.*

i. *If H is a proper subgroup or homomorphic image of G, then either H is abelian or $\mathbb{Z}(H)$ is an elementary abelian 2-group.*
ii. *$F[G]$ has an irreducible representation of degree > 2, and $\mathbb{Z}(G)$ is cyclic.*
iii. *G has no normal cyclic subgroup of order 4.*

Proof. (i) If H is a proper subgroup or homomorphic image of G, then H is either abelian or has an abelian subgroup of index 2. Thus, all irreducible representations of $F[H]$ have degree ≤ 2, and Proposition 2.4(v) yields the result.

(ii) If all irreducible representations of $F[G]$ have degree ≤ 2, then a theorem of Amitsur (see [I1, Theorem 12.11] or [P, pages 263–264]) implies that either G has an abelian subgroup of index ≤ 2 or $|G : \mathbb{Z}(G)| = 8$. By assumption, the former case does not occur. If the latter case occurs, then $\mathbb{Z}(G)$ is an elementary abelian 2-group by Proposition 2.4(v). Thus, by (i) above, G satisfies the hypotheses of Lemma 3.3, and G has an abelian subgroup of index 2, contradiction.

It follows that $F[G]$ has an irreducible representation of degree > 2, and any such representation must be faithful on G. Otherwise, it corresponds to a representation of $F[H]$ for some proper homomorphic image H of G, and we know that $F[H]$ has all representations of degree ≤ 2. In particular, $\mathbb{Z}(G)$ is cyclic.

(iii) Suppose that L is a normal cyclic subgroup of G of order 4. Then $|\mathrm{Aut}(L)| = 2$, so $|G : \mathbb{C}_G(L)| \leq 2$. If $\mathbb{C}_G(L)$ has index 2, then $\mathbb{C}_G(L)$ is abelian by (i) above, a contradiction. Thus, L must be central. Now if 8 divides $|G|$, then Lemma 3.2 implies that G has a normal subgroup H of index 2 containing L, and again H is abelian. On the other hand, if 8 does not divide $|G|$, then Lemma 3.2 implies that $G = L \times A$ is abelian, where A is the normal abelian 2-complement of G. □

Step 2. *G is a 2-group.*

Proof. Let A be the normal abelian 2-complement of G given by Lemma 3.2, and assume that $A \neq 1$. Note that $|G/A| \geq 4$ since G does not have an abelian subgroup of index ≤ 2. Let $C = \mathbb{C}_G(A) \lhd G$. We know that G has a normal subgroup H of index 2, and that H has an abelian subgroup H_0 of index ≤ 2. Since $A \subseteq H_0$, it follows that $H_0 \subseteq \mathbb{C}_G(A) = C$, and hence that $|G : C| = 1,\ 2$, or 4. If $|G : C| = 2$, then C is abelian by Step 1(i), and if $|G : C| = 1$, then H is abelian by the same result. Thus we must have $|G : C| = 4$.

Let L be any subgroup of G with $L \supseteq C$ and $|L : C| = 2$. Then $A \cap \mathbb{Z}(L) = 1$ by Step 1(i), so L/C acts fixed point freely on the abelian group A of odd order, and hence L/C acts in a dihedral manner. Thus, L must be the unique such group, and consequently G/C is cyclic of order 4. Finally, let y be a 2-element of G generating the quotient G/C, and consider the subgroup of G given by $\langle A, y\rangle = A \rtimes \langle y\rangle$. Then y^4 is central in this group, so $\tilde{G} = \langle A, y\rangle/\langle y^4\rangle \cong A \rtimes \langle \tilde{y}\rangle$ is involved in G. But $\mathfrak{U}(K[\tilde{G}])$ is not 2-related, by Proposition 2.4(iv), and hence we have the required contradiction. □

Step 3. *Final contradiction.*

Proof. We now know that G is a 2-group and, by Step 1(ii)(iii), $J = \mathbb{Z}(G)$ has order 2. It follows from the minimal nature of G that G/J has an abelian subgroup H/J of index 2, and since H is nonabelian, we have $H' = J$. Furthermore, H has an abelian subgroup B of index 2, and hence $H = \langle B, t\rangle$ for some $t \in H$. Note that the commutator map $b \mapsto [b, t]$ is a homomorphism from B onto H' with kernel $Z = \mathbb{Z}(H)$. Thus, since $|H'| = 2$, we see that $|B : Z| = 2$ and $|H : Z| = 4$. By Step 1(i), Z is an elementary abelian 2-group, and the group $G/H = \{1, \bar{g}\}$ of order 2 acts on Z with $\mathbb{C}_Z(\bar{g}) = \mathbb{Z}(G)$. Since each Jordan block for the matrix representation of $\bar{g}$ yields a fixed point and since $|\mathbb{Z}(G)| = 2$, there can be only one such block and $|Z| \leq 4$. If $|Z| = 2$, then $|H| = 8$ and H must be the dihedral group by Proposition 2.4(ii). But then H has a characteristic cyclic subgroup of order 4 and this yields a normal cyclic subgroup of G of order 4, contradicting Step 1(iii). It follows that $|Z| = 4$, $|H| = 16$ and $|G| = 32$.

Now $Z \subseteq H \subseteq G$ is a normal series for G, so there exists $A \lhd G$ with $Z \subseteq A \subseteq H$ and $|A : Z| = 2$. Clearly A is abelian and, since Z is abelian of type $(2, 2)$, we see that A is abelian of type $(2, 2, 2)$ or $(4, 2)$. In the first case, since $|G/A| = 4$, we obtain a contradiction from Step 1(ii) and Lemma 2.7. Thus, we can assume that A is type (4,2), and we can now completely describe the group G. To start with, let $A = \langle x, w\rangle = \langle x\rangle \times \langle w\rangle$ with $|x| = 4$ and $|w| = 2$. Since $A^2 = \langle x^2\rangle \lhd G$, it follows that $A^2 = \mathbb{Z}(G) = H'$. Furthermore, we know that $Z = \mathbb{Z}(H) = \langle x^2, w\rangle$ since Z is elementary abelian. In particular, if we set $H = \langle A, h\rangle$, then $x^h = x{\cdot}x^2 = x^{-1}$ and $w^h = w$. Also, $h^2 \in Z = \langle x^2, w\rangle$, so there are four possibilities. If $h^2 = x^2$, then $\langle x, h\rangle$ is isomorphic to the quaternion group of order 8, contradicting Proposition 2.4(ii). On the other hand, if $h^2 = w$ or x^2w, and if $\tilde{Z} = \langle x^2w\rangle$ or $\langle w\rangle$, respectively, then $H/\tilde{Z}$ is isomorphic to the quaternion group of order 8, again a contradiction. Thus $h^2 = 1$ and $H = A \rtimes \langle h\rangle$ is a dihedral group and, in particular, every element of $H \setminus A$ has order 2.

Finally, let $G = \langle H, y\rangle$. Since $\langle x\rangle \lhd H$ and $\langle x\rangle \not\lhd G$, by Step 1(iii), we must have $x^y = xw$ or $x(x^2w)$. But $A = \langle x\rangle \times \langle w\rangle = \langle x\rangle \times \langle x^2w\rangle$, so without loss of generality, we can assume that $x^y = xw$. Furthermore, w is not central in G, but it is central in G/J since $|Z/J| = 2$, so $w^y = x^2w$. Next, observe that $y^2 \in H$ and that $x^{y^2} = x^y w^y = xwx^2w = x^{-1}$, so $y^2 \in H \setminus A$. Hence y^2 has order 2 and y has order 4. It follows that $G = A \rtimes \langle y\rangle$ with $A = \langle x\rangle \times \langle w\rangle$, $|x| = |y| = 4$, $|w| = 2$, $x^y = x^{-1}$, and $w^y = x^2w$. In other words, G is the group of Proposition 2.4(iv) and we conclude that $\mathfrak{U}(K[G])$ is not 2-related. □

We can now complete the proof of the main result. Specifically, we offer the

Proof of the hard direction of Theorem 1.3. Here we assume that $\mathfrak{U}(K[G])$ is 2-related. The goal is to show that G has the structure given in parts (i) and (ii) of the statement of the theorem. To start with, by Lemma 3.2(i), G has a normal Sylow p-subgroup with $p = \operatorname{char} K$. Thus, since $\mathfrak{U}(K[G/P])$ is 2-related, it suffices to study G/P. Equivalently, we can now assume that $P = 1$ so that $|G|$

is prime to the characteristic of K. If G is abelian, the result is proved. Therefore, by Lemma 3.4, we can assume that G has a noncentral abelian subgroup A of index 2. We must show that either A has period 2, that is $A^2 = \{a^2 |\ a \in A\} = 1$, or that $G = A \rtimes \langle x \rangle$ is dihedral. Note that, if $G = \langle A, g \rangle$, then $g^2 \in \mathbb{Z}(G)$ and, for any $a \in A$, we have $(ag)^2 = ag^2g^{-1}ag = aa^g g^2$. In other words, G is dihedral if and only if $(G \setminus A)^2 = \{b^2 |\ b \in G \setminus A\} = 1$. Note also that if F is the algebraic closure of K, then all irreducible representations of $F[G]$ have degree ≤ 2. Thus, by Proposition 2.4(v), $\mathbb{Z}(G)$ is an elementary abelian 2-group. For convenience, we split the argument into three cases.

Case 1. *If G has at least two distinct abelian subgroups of index 2, then G has precisely three abelian subgroups of index 2, $|G : \mathbb{Z}(G)| = 4$, and G' has order 2. Furthermore, G has an elementary abelian subgroup of index 2.*

Proof. If A and B are distinct abelian subgroups of G of index 2, then $Z = A \cap B$ is central in $G = AB$. Hence $Z = \mathbb{Z}(G)$ has index 4 in G, and in fact G/Z is abelian of type (2,2). Furthermore, all abelian subgroups of G of index 2 contain Z, so there are precisely three such, say A_1, A_2, A_3. Note that $G = \langle Z, x, y \rangle$ for some x, y, and that $[x, y] \in Z$ has order 2. Thus, since G is abelian modulo $\langle [x, y] \rangle$, it follows that $G' = \langle [x, y] \rangle$ has order 2.

We prove by induction that at least one of A_1, A_2, A_3 has period 2. Suppose first that $|Z| \geq 8$, and choose four distinct central subgroups J_1, J_2, J_3, J_4 different from G'. Then G/J_i is nonabelian and has three abelian subgroups of index 2, namely A_1/J_i, A_2/J_i and A_3/J_i. Thus, by induction on $|G|$, there exists a subscript $f(i) \in \{1, 2, 3\}$ such that $(A_{f(i)}/J_i)^2 = 1$ or equivalently $(A_{f(i)})^2 \subseteq J_i$. Since there are four J_is and only three A_ks, there must exist $i \neq i'$ and k with $A_k^2 \subseteq J_i \cap J_{i'} = 1$, as required.

Thus we can assume that $|Z| \leq 4$. If $|Z| = 2$, then G is nonabelian of order 8 and, since G is not quaternion by Proposition 2.4(ii), we see that G is dihedral and hence has an elementary abelian subgroup of index 2. Finally, suppose $|Z| = 4$ and let C and D be the subgroups of Z of order 2 different from G'. Then G/C is dihedral of order 8 and hence has two elementary abelian subgroups of index 2. Thus there exist distinct k, k' with $A_k^2, A_{k'}^2 \subseteq C$. Similarly, there exist distinct ℓ, ℓ' with $A_\ell^2, A_{\ell'}^2 \subseteq D$. But there are only three subscripts, so $\{k, k'\} \cap \{\ell, \ell'\} \neq \emptyset$ and if say $k = \ell$, then $A_k^2 \subseteq C \cap D = 1$. $\square$

Case 2. *The result holds if G is a 2-group.*

Proof. For convenience, let σ denote the automorphism of A determined by the action of the nonidentity element of G/A. As we have observed above, $Z = \mathbb{Z}(G)$ is elementary abelian, and the quaternion group of order 8 is not involved in G. Since A is abelian, it is clear that $(G \setminus A)^2 \subseteq Z$. As usual, we proceed by induction on the order of G.

Let $B = \{a \in A |\ a^\sigma = a^{-1}\}$. Then B is a subgroup of A containing Z, and indeed Z is precisely the set of elements of B of order ≤ 2. In particular, if B is properly larger than Z, then there exists an element $b \in B$ with $|b| = 4$. We

show in this case that $(G \setminus A)^2 = 1$. Suppose, by way of contradiction that there exists $x \in G \setminus A$ with $x^2 \neq 1$. Then we have $1 \neq x^2 \in Z$ and $b^x = b^\sigma = b^{-1}$ with $1 \neq b^2 \in Z$. Furthermore, there is a homomorphic image $\bar{Z}$ of Z in which x^2 and b^2 are identified. Thus, there exists a homomorphic image $\langle \bar{b}, \bar{x} \rangle$ of $\langle b, x \rangle$ such that $\bar{b}^{\bar{x}} = \bar{b}^{-1}$ and $\bar{b}^2 = \bar{x}^2 \neq 1$. But this shows that the quaternion group of order 8 is involved in G, a contradiction. Thus $(G \setminus A)^2 = 1$ and G is dihedral.

We can now assume that $B = Z$. Next observe that $G' = \{a^\sigma a^{-1} |\ a \in A\}$ so clearly $G' \subseteq B = Z$. Furthermore, the map $A \to G'$ given by $a \mapsto a^\sigma a^{-1}$ is a homomorphism onto G' with kernel Z. Thus $A/Z \cong G' \subseteq Z$ and, since Z is elementary abelian, we conclude that $A^2 \subseteq Z$ and $|A| = |Z|\,|G'| \leq |Z|^2$.

Suppose that $|A| = |Z|^2$, and consider the endomorphism of A given by $a \mapsto a^\sigma a$ with image I. Clearly $I \subseteq Z$ and, since the kernel of this map is $B = Z$, we have $|Z|^2 = |A| = |B|\,|I| = |Z|\,|I|$, so $I = Z$. Now if $w \in G \setminus A$ and if $a \in A$, then $(aw)^2 = aa^\sigma w^2$ and it follows that $(G \setminus A)^2 = Iw^2 = Zw^2 = Z$. In this situation, we claim that $A^2 = 1$. Indeed, if this is not the case, let $a \in A$ with $|a| = 4$. Since $(G \setminus A)^2 = Z$ and $a^2 \in Z$, we can choose $y \in G \setminus A$ with $y^2 = a^2$. Furthermore, $a \notin Z$, so the commutator $u = [y, a]$ is a nonidentity element of $G' \subseteq Z$. As above, Z has a homomorphic image identifying y^2 with u, and hence $\langle a, y \rangle$ has a homomorphic image $\langle \tilde{a}, \tilde{y} \rangle$ satisfying $\tilde{a}^4 = 1$ and $\tilde{a}^2 = \tilde{y}^2 = [\tilde{y}, \tilde{a}] \neq 1$. In other words, $\langle \tilde{a}, \tilde{y} \rangle$ is isomorphic to the quaternion group of order 8, a contradiction. Thus $A^2 = 1$, and we are done in this case.

It now suffices to assume that $|A| > |Z|^2$ and, since $|A| = |G'|\,|Z|$, we see that Z properly contains G'. Furthermore, if $|G'| = 2$, then $|A : Z| = 2$ and G/Z is abelian of type (2,2). Thus G has at least three abelian subgroups of index 2, and Case 1 yields the result. Finally, if $|G'| \geq 4$, then since Z is properly larger, there exist three different subgroups J_1, J_2, J_3 of Z of order 2 that are disjoint from G'. Note that $(G/J_i)' = G'J_i/J_i \cong G'$ has order ≥ 4 so, by Case 1, G/J_i has a unique abelian subgroup of index 2, namely A/J_i. By induction, either A/J_i has period 2 so $A^2 \subseteq J_i$ or G/J_i is dihedral in which case $(G \setminus A)^2 \subseteq J_i$. Since there are three different subscripts and only two possible outcomes, we see that there exist $i \neq j$ with either $A^2 \subseteq J_i \cap J_j = 1$ or $(G \setminus A)^2 \subseteq J_i \cap J_j = 1$. Thus, either A has period 2 or G is dihedral. $\square$

Case 3. *The result holds in general.*

Proof. In view of Case 2, we can now assume that G is not a 2-group. In particular, G has a nonidentity normal abelian 2-complement $B \subseteq A$, and $B \cap \mathbb{Z}(G) = 1$ since $\mathbb{Z}(G)$ is an elementary abelian 2-group. It follows that G/A acts fixed point freely on B, and hence G/A must act in a dihedral manner. The goal here is to show that G is a dihedral group or equivalently that $(G \setminus A)^2 = 1$. If this does not occur, then we can choose $x \in G \setminus A$ with $x^2 \neq 1$. As we observed before, $x^2 \in (G \setminus A)^2 \subseteq \mathbb{Z}(G)$, so $(x^2)^2 = 1$ and $|x| = 4$. Finally, let $1 \neq b \in B$ be any element and let $|b| = r$. Then r is odd and $b^x = b^{-1}$, so $\langle b, x \rangle$ has a cyclic subgroup $\langle bx^2 \rangle$ of order $2r$ and index 2. Furthermore, $(bx^2)^x = b^{-1}x^2 = (bx^2)^{-1}$ and $(bx^2)^r = x^2 \neq 1$. In other words, $\langle b, x \rangle$ is a quaternion group of order $4r$,

contradicting Proposition 2.4(ii), and this completes the proof. □

References

[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.
[P] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977.
[S] I. N. Sanov, *A property of a representation of a free group*, Doklady Akad. Nauk SSSR **57** (1947), 657–659. (Russian)
[T] J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.

Department of Mathematics, University of São Paulo, São Paulo 05389-970, Brazil
E-mail address: jzg@ime.usp.br

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