# A COUNTEREXAMPLE TO THE FIRST ZASSENHAUS CONJECTURE

FLORIAN EISELE AND LEO MARGOLIS

ABSTRACT. Hans J. Zassenhaus conjectured that for any unit $u$ of finite order in the integral group ring of a finite group $G$ there exists a unit $a$ in the rational group algebra of $G$ such that $a^{-1} \cdot u \cdot a = \pm g$ for some $g \in G$. We disprove this conjecture by first proving general results that help identify counterexamples and then providing an infinite number of examples where these results apply. Our smallest example is a metabelian group of order $2^7 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 19^2$ whose integral group ring contains a unit of order $7 \cdot 19$ which, in the rational group algebra, is not conjugate to any element of the form $\pm g$.

## 1. INTRODUCTION

Let $G$ be a finite group and denote by $RG$ the group ring of $G$ over a commutative ring $R$. Denote by $\mathcal{U}(RG)$ the unit group of $RG$. In the 1970's Zassenhaus made three strong conjectures about finite subgroups of $\mathcal{U}(\mathbb{Z}G)$ (cf. [Seh93, Section 37]). These conjectures, often called the first, second and third Zassenhaus conjecture and sometimes abbreviated as (ZC1), (ZC2) and (ZC3), had a lasting impact on research in the field. All three of these conjectures turned out to be true for nilpotent groups [Wei91], but metabelian counterexamples for the second and the third one were found by K. W. Roggenkamp and L. L. Scott [Sco92, Kli91]. Later M. Hertweck showed that there are counterexamples of order as small as $96$ [Her04, Section 11]. Unlike its siblings, the first Zassenhaus conjecture seemed to stand the test of time. Since it was the only one of the three to remain open, people in recent years started referring to it as *the* Zassenhaus conjecture, and we will do the same in this article.

**Zassenhaus Conjecture.** *If $u \in \mathcal{U}(\mathbb{Z}G)$ is a unit of finite order, then there is an $a \in \mathcal{U}(\mathbb{Q}G)$ such that $a^{-1} \cdot u \cdot a = \pm g$ for some $g \in G$.*

This conjecture first appeared in written form in [Zas74] and inspired a lot of research in the decades to follow. The first results on the conjecture were mostly concerned with special classes of metabelian groups, [HP72, PM73, AH80, LB83, RS83, PMS84, Mit86, PMRS86, SW86, MRSW87, LT90, LP92, LS98, JPM00, BHK04, RS06]. Almost all of these results were later generalised by Hertweck [Her06, Her08a]. Hertweck proved that the Zassenhaus conjecture holds for groups $G$ which have a normal Sylow $p$-subgroup with abelian complement or a cyclic normal subgroup $C$ such that $G = C \cdot A$ for some abelian subgroup $A$ of $G$. The latter result was further generalised in [CMR13], proving that the Zassenhaus conjecture holds for cyclic-by-abelian groups. In a different vein, A. Weiss' proof of the conjecture, or even a stronger version of it, for nilpotent groups [Wei88, Wei91], was certainly a highlight

*2010 Mathematics Subject Classification*. Primary 16S34. Secondary 16U60, 20C11, 20C05.

*Key words and phrases*. Unit Group, Group Ring, Zassenhaus Conjecture, Integral Representations.

The first author was supported by the EPSRC, grant EP/M02525X/1. The second author was supported by a Marie Curie Individual Fellowship from EU project 705112-ZC and the FWO (Research Foundation Flanders).

of the study. The conjecture is also known to hold for a few other classes of solvable groups [Fer87, DJ96, BKM16, MR17b, MR17c, MR17a], as well as for some small groups. In particular, the conjecture holds for groups of order smaller than $144$ [HK06, HS15, BHK+17].

Progress on non-solvable groups was initially lagging. For many years the conjecture was only known to hold for the alternating and symmetric group of degree $5$ [LP89, LT91] and the special linear group $\mathrm{SL}(2,5)$ [DJPM97]. This state of affairs changed when Hertweck introduced a method to tackle the conjecture involving Brauer characters [Her07]. Nevertheless, results are still relatively far and between [Her07, Her08b, BH08, Gil13, BM16, KK17, BM17], and, for instance, the only non-abelian simple groups for which the conjecture has been verified are the groups $\mathrm{PSL}(2,q)$ where $q \leq 25$, $q = 32$ [BM16] or where $q$ is a Fermat or Mersenne prime [MRS16].

In the present article we show that the Zassenhaus conjecture is false by providing a series of metabelian groups $G$ such that $\mathbb{Z}G$ contains a unit of finite order not conjugate in $\mathbb{Q}G$ to any element of the form $\pm g$ for $g \in G$.

Let us describe these groups. To this end, let $p$ and $q$ be odd primes, $d$ an odd divisor of $p-1$ and $q-1$, $N$ the additive group $\mathbb{F}_{p^2} \oplus \mathbb{F}_{q^2}$, and let $\alpha$ and $\beta$ be primitive elements in the multiplicative groups $\mathbb{F}_{p^2}^\times$ and $\mathbb{F}_{q^2}^\times$, respectively. Consider the abelian group

$$A = \langle a, b, c \mid a^{\frac{p^2-1}{d}} = b^{\frac{q^2-1}{d}} = 1,\ c^d = a \cdot b \rangle$$

There is an action of $A$ on $N$ given by

$$(x,y)^a = (\alpha^d \cdot x, y),\ (x,y)^b = (x, \beta^d \cdot y), (x,y)^c = (\alpha \cdot x, \beta \cdot y)$$

and we may form the semidirect product $N \rtimes A$, which we denote by $G(p,q;d;\alpha,\beta)$. The following are our main results:

**Theorem A.** *Let $G = G(7,19;3;\alpha,\beta)$, where $\alpha$ is a root of the polynomial $X^2 - X + 3$ over $\mathbb{F}_7$ and $\beta$ is a root of $X^2 - X + 2$ over $\mathbb{F}_{19}$. There exists a unit $u \in \mathcal{U}(\mathbb{Z}G)$ of order $7 \cdot 19$ such that $u$ is not conjugate in $\mathbb{Q}G$ to any element of the form $\pm g$ for $g \in G$. In particular, the Zassenhaus conjecture does not hold for $G$.*

**Theorem B.** *Let $d$ be an odd positive integer, and let $N \in \mathbb{N}$ be arbitrary. There exist infinitely many pairs of primes $p$ and $q$ such that, for any admissible choice of $\alpha$ and $\beta$, for $G = G(p,q;d;\alpha,\beta)$ there are $u_1, \ldots, u_N \in \mathcal{U}(\mathbb{Z}G)$, each of order $p \cdot q$, such that neither one of the $u_i$ is conjugate in $\mathcal{U}(\mathbb{Q}G)$ to an element of the form $\pm g$ for $g \in G$, or to any other $u_j$ for $j \neq i$. In particular, the Zassenhaus conjecture does not hold for such a group $G$.*

A more precise version of Theorem B, specifying lower bounds for $p$ and $q$ as well as the rational conjugacy classes of the $u_i$, can be found in Corollary 7.3. The idea that groups like $G(p,q;d;\alpha,\beta)$ might be good candidates for a counterexample to the Zassenhaus conjecture was noted in [MR17a]. Looking at the various positive results mentioned above, it seems that metabelian groups would have been the next logical step, and people working in the field certainly attempted to prove the Zassenhaus conjecture for metabelian groups, to no avail. What is more, the class of metabelian groups provided E. Dade's counterexample to R. Brauer's question, which asked whether $KG \cong KH$ for all fields $K$ implies that $G$ and $H$ are isomorphic [Dad71]. The second Zassenhaus conjecture mentioned above, which asked if different (normalised) group bases of $\mathbb{Z}G$ are conjugate in $\mathbb{Q}G$, fails for metabelian groups as well [Kli91]. On the other hand, metabelian groups were one of the first classes of groups for which the isomorphism problem on integral group rings was known to have a positive answer [Whi68].

Here is an outline of our strategy to prove Theorems A and B:

(1) If $U$ is a cyclic group of order $n$, then a unit $u \in \mathcal{U}(RG)$ of order $n$ corresponds to a certain $R(G \times U)$-module ${}_u(RG)_G$, called a "double action module". This is the well-known double action formalism explained in Section 2, and the defining property of double action modules is that their restriction to $G$ is a free $RG$-module of rank one. This principle works for any commutative ring $R$.
(2) Once we fix a conjugacy class of units of order $n$ in $\mathcal{U}(\mathbb{Q}G)$, or equivalently a $\mathbb{Q}(G \times U)$-double action module $V = {}_u(\mathbb{Q}G)_G$ corresponding to it, we need to find a $\mathbb{Z}(G \times U)$-lattice in $V$ whose restriction to $G$ is free.
(3) Let $\mathbb{Z}_{(p)}$ denote the localisation of $\mathbb{Z}$ at the prime ideal $(p)$. We provide a fairly general construction of double action modules over $\mathbb{Z}_{(p)}(G \times U)$ for groups of the form $N \rtimes A$, where $N$ is abelian. This is done in Section 5, and, of course, subject to a whole list of conditions. The double action modules we construct are direct sums of direct summands of permutation modules (see Definition 5.4), and as a consequence the local version of the counterexample is fairly explicit (see Proposition 7.11 at the end).
(4) The problem of turning a family of "compatible" $\mathbb{Z}_{(p)}(G \times U)$-lattices in $V$ with free restriction to $G$ into a $\mathbb{Z}(G \times U)$-lattice in $V$ with the same property can be solved using a rather general local-global principle, provided the centraliser $C_{\mathcal{U}(\mathbb{Q}G)}(u)$ of the unit is big enough (think of $u$ as already being fixed up to conjugacy in $\mathcal{U}(\mathbb{Q}G)$). This is done in Section 6.
(5) In the last section we study groups of the form $G(p, q; d; \alpha, \beta)$ as defined above. All of the more general results of the preceding sections become explicit and elementarily verifiable in this situation. We use the general result of that section, Theorem 7.2, to prove Theorems A and B.

In regard to future research, it seems worth pointing out that many variations and weaker versions of the Zassenhaus conjecture remain open. An overview of the weaker forms of the conjecture can be found in [MR17c]. In particular, the question if the orders of torsion units of augmentation one in $\mathcal{U}(\mathbb{Z}G)$ coincide with the orders of elements in $G$ remains open. It also might still be true that if $u \in \mathcal{U}(\mathbb{Z}G)$ is a torsion unit then $u$ is conjugate in $\mathcal{U}(\mathbb{Q}H)$ to $\pm g$ for some $g \in G$, where $H \supseteq G$ is some larger group containing $G$.

Going in a different direction, the $p$-version of even the strongest of the three Zassenhaus conjectures remains open. This variation asks if it is true that any $p$-subgroup of $\mathcal{U}(\mathbb{Z}G)$ consisting of elements of augmentation one is conjugate in $\mathcal{U}(\mathbb{Q}G)$ to a subgroup of $G$. This is sometimes called "(p-ZC3)" or the "Strong Sylow Theorem" for $\mathbb{Z}G$. An overview of results relating to this problem can be found in [BKM16]. For the counterexample to the Zassenhaus conjecture presented in the present article it is of fundamental importance that the order of the unit is divisible by at least two different primes.

Throughout the paper we are going to use the following notation, most of which is quite standard.

**Notation and basic definitions.**
(1) Let $G$ be a finite group and let $U$ be a subgroup of $G$. For a character $\chi$ of $U$ we write $\chi \uparrow_U^G$ for the induced character, and for a character $\psi$ of $G$ we write $\psi|_U$ for the restriction to $U$. The trivial character of $G$ is denoted by $1_G$.
(2) For a prime number $p$ we denote by $G_p$ a Sylow $p$-subgroup of $G$ and by $g_p$ the $p$-part of an element $g \in G$. The conjugacy class of $g \in G$ is denoted by $g^G$. We also use $G_{p'}$ to

denote a $p'$-Hall subgroup of $G$ (this is used only for nilpotent $G$) and $g_{p'}$ for the $p'$-part of $g$.

(3) Let $G$ be a finite group and let $H_1$ and $H_2$ be subgroups of $G$ such that $G = H_1 \times H_2$. If $\chi_1$ and $\chi_2$ are characters of $H_1$ and $H_2$, respectively, then $\chi_1 \otimes \chi_2$ denotes the corresponding character of $G$. Similarly, if $L_1$ and $L_2$ are $RG$-modules for some commutative ring $R$, $L_1 \otimes L_2$ denotes $L_1 \otimes_R L_2$ with the natural $RG$-module structure.

(4) We write "$\sum_{g^G}$" to denote a sum ranging over a set of representatives of the conjugacy classes of $G$. If $G$ acts on a set $H$ we write "$\sum_{h^G, h \in H}$" for the sum ranging over representatives of the $G$-orbits in $H$.

(5) If $G$ and $H$ are groups, and $H$ acts on $G$ by automorphisms, we denote by $\mathrm{Irr}_{\mathbb{Q}}(G)/H$ the set of $H$-orbits of irreducible rational characters of $G$. We write "$\sum_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(G)/H}$" for a sum ranging over representatives of these orbits.

(6) For a cyclic group $U = \langle c \rangle$ and an element $g \in G$ we define

$$[g] = \langle (g, c) \rangle \leq G \times U$$

We will often use the fact that $[g]_p = \langle (g_p, c_p) \rangle$ and $[g]_{p'} = \langle (g_{p'}, c_{p'}) \rangle$ for all primes $p$.

(7) If $R$ is a ring and $M$ is an $R$-module we write $M^{\oplus n}$ for the direct sum of $n$ copies of $M$.

(8) If $R$ is a ring, $M$ is an $R$-module and $X \subseteq M$ is an arbitrary subset, we write $R \cdot X$ for the $R$-module generated by $X$.

(9) Let $R$ be a commutative ring and let $u = \sum_{g \in G} r_g \cdot g$ be an arbitrary element of $RG$. Then

$$\varepsilon_{g^G}(u) = \sum_{h \in g^G} r_h$$

is called the *partial augmentation* of $u$ at $g$.

## 2. Double action formalism

The "double action formalism" (see, for instance, [Seh93, Section 38.6]) is a commonly used way of studying the Zassenhaus conjecture and other questions relating to units in group algebras via certain bimodules, the so-called "double action modules". In this section we give a short (but complete, at least for our purposes) overview of this formalism. For the rest of this section let $G$ be a finite group and let $U = \langle c \rangle$ be a cyclic group of order $n \in \mathbb{N}$. By $R$ we denote an arbitrary commutative ring.

**Definition 2.1.** *(1) Given a unit $u \in \mathcal{U}(RG)$ satisfying $u^n = 1$ we define an $R(G \times U)$-module ${}_u(RG)_G$ as follows: as an $R$-module, ${}_u(RG)_G$ is equal to $RG$, and the (right) action of $G \times U$ is given by*

$${}_u(RG)_G \times (G \times U) \longrightarrow {}_u(RG)_G : \ (x, (g, c^i)) \mapsto (u^\circ)^i \cdot x \cdot g$$

*where the product on the right hand side of the assignment is taken within the ring $RG$, and $-^\circ : \ RG \longrightarrow RG : g \mapsto g^{-1}$ denotes the standard involution on $RG$. We call this $R(G \times U)$-module the* double action module *associated with the unit $u$.*

*(2) An $R(G \times U)$-module $M$ is called $G$-*regular *if $M|_G$ is free of rank one as an $RG$-module (that is, it is isomorphic to $RG$ considered as a right module over itself).*

A double action module is clearly $G$-regular, but it turns out that the converse is true as well:

**Proposition 2.2.** *(1) If $M$ is a $G$-regular $R(G \times U)$-module, then $M \cong {}_u(RG)_G$ for some unit $u \in \mathcal{U}(RG)$ with $u^n = 1$.*

*(2) If $u, v \in \mathcal{U}(RG)$ are two units satisfying $u^n = v^n = 1$, then*

$$ {}_u(RG)_G \cong {}_v(RG)_G $$

*if and only if $u$ and $v$ are conjugate inside $\mathcal{U}(RG)$.*

*Proof.* Assume that $M$ is $G$-regular. Then we may choose an isomorphism of $RG$-modules $\varphi : M \longrightarrow RG$, where we view $RG$ as a right module over itself. As before, let $-^\circ : RG \longrightarrow RG : g \mapsto g^{-1}$ denote the standard involution of the group algebra, and define $u = \varphi(\varphi^{-1}(1)\cdot c)^\circ$. Then we have, for all $m \in M$,

$$ \varphi(m \cdot c) = \varphi(\varphi^{-1}(1) \cdot \varphi(m) \cdot c) = \varphi(\varphi^{-1}(1) \cdot c) \cdot \varphi(m) = u^\circ \cdot \varphi(m) $$

where we made use of the fact that $m = \varphi^{-1}(1) \cdot \varphi(m)$. It now follows immediately from the above that $u^n = 1$, and the map $M \longrightarrow {}_u(RG)_G : x \mapsto \varphi(x)$ is easily seen to be an isomorphism of $R(G \times U)$-modules.

Let us now prove the second part of the proposition. To this end, fix an isomorphism $\varphi : {}_u(RG)_G \longrightarrow {}_v(RG)_G$. Then $\varphi(1) \cdot u^\circ = \varphi(1 \cdot u^\circ) = \varphi(u^\circ) = \varphi(1 \cdot c) = \varphi(1) \cdot c = v^\circ \cdot \varphi(1)$. As an equation purely in the ring $RG$ this yields $u \cdot \varphi(1)^\circ = \varphi(1)^\circ \cdot v$. So it only remains to show that $\varphi(1)^\circ$ is an invertible element of $RG$, which follows from the fact that $\varphi(1)$ generates ${}_v(RG)_G$ as an $RG$-module. □

As we have seen so far, double action modules are in one-to-one correspondence with conjugacy classes of elements of $\mathcal{U}(RG)$ whose order divides $n$. Evidently this means that each property of torsion units should have a counterpart in the language of double action modules. An important tool in the study of the Zassenhaus conjecture is the criterion given in [MRSW87, Theorem 2.5]. It states that a unit $u \in \mathcal{U}(\mathbb{Z}G)$ of finite order and augmentation one is conjugate in $\mathcal{U}(\mathbb{Q}G)$ to an element of $G$ if and only if $\varepsilon_{g^G}(u^i) \geq 0$ for all $g \in G$ and all $i \geq 0$. In particular, finding a counterexample to the Zassenhaus conjecture is equivalent to finding a unit $u$ of finite order and augmentation one which has a negative partial augmentation. Hence it is important for us to have a way of recovering the partial augmentations of a unit from the corresponding double action module.

**Proposition 2.3.** *Let $u \in \mathcal{U}(RG)$ be a unit satisfying $u^n = 1$. Let*

$$ \theta_u : G \times U \longrightarrow R $$

*denote the character of the $R(G \times U)$-module ${}_u(RG)_G$. Then*

$$ \theta_u((g, c^i)) = |C_G(g)| \cdot \varepsilon_{g^G}(u^i) $$

*Proof.* Let us first calculate the trace of the linear map $\mu(g, h) : RG \longrightarrow RG : x \mapsto g^{-1} \cdot x \cdot h$ for arbitrary $g, h \in G$. This trace is equal to the number of $y \in G$ such that $g^{-1} \cdot y \cdot h = y$, or, equivalently, $h = y^{-1} \cdot g \cdot y$. If $g^G = h^G$ then this number is equal to $|C_G(g)|$, otherwise it is zero. Now, if

$$ u^i = \sum_{g \in G} \alpha_g \cdot g $$

then the linear endomorphism of $RG$ induced by $(g, c^i)$ is equal to $\sum_{h \in G} \alpha_h \cdot \mu(h, g)$. The character value $\theta_u((g, c^i))$ is the trace of this map, which is equal to

$$ \sum_{h \in G} \alpha_h \cdot \mathrm{Tr}(\mu(h, g)) = \sum_{h \in g^G} \alpha_h \cdot |C_G(g)| = |C_G(g)| \cdot \varepsilon_{g^G}(u^i) $$

as claimed. □

We now turn our attention to the case of rational coefficients, i.e. $R = \mathbb{Q}$. In that situation $G$-regularity of $G \times U$-modules can readily be checked on the level of characters, and Proposition 2.3 can be used to ascertain whether the corresponding torsion unit in $\mathcal{U}(\mathbb{Q}G)$ is indeed not conjugate to an element of $G$.

**Proposition 2.4.** *Let $g_1, \dots, g_k$ be pair-wise non-conjugate elements of $G$ whose order divides $n$, and let $a_1, \dots, a_k \in \mathbb{Z}$ such that $a_1 + \ldots + a_k = 1$. Assume that*

$$\theta = \sum_{i=1}^{k} a_i \cdot 1 \uparrow_{[g_i]}^{G \times U} \tag{1}$$

*is in fact a character of $G \times U$, rather than just a virtual character. Then $\theta$ is the character of ${}_u(\mathbb{Q}G)_G$ for some $u \in \mathcal{U}(\mathbb{Q}G)$ satisfying $u^n = 1$. Moreover $\varepsilon_{g_i^G}(u) = a_i$ for all $i \in \{1, \dots, k\}$ and $\varepsilon_{g^G}(u) = 0$ whenever $g$ is not conjugate to any of the $g_i$.*

*Proof.* Let us first prove that $\theta$ can be realised as the character of a $\mathbb{Q}(G \times U)$-module, rather than just a $\mathbb{C}(G \times U)$-module. By definition $\theta$ can be written as the difference of the characters of two $\mathbb{Q}(G \times U)$-modules, say $V$ and $W$. Without loss of generality we may assume that $V$ and $W$ share no isomorphic simple direct summands. But then $\mathrm{Hom}_{\mathbb{Q}(G\times U)}(V, W) = 0$, which implies $\mathrm{Hom}_{\mathbb{C}(G\times U)}(\mathbb{C} \otimes_{\mathbb{Q}} V, \mathbb{C} \otimes_{\mathbb{Q}} W) = 0$. That is, $\mathbb{C} \otimes_{\mathbb{Q}} V$ and $\mathbb{C} \otimes_{\mathbb{Q}} W$ share no isomorphic simple direct summands, which means that $\theta$ can only be a proper character if $W = \{0\}$, which means that $V$ is a $\mathbb{Q}(G \times U)$-module affording $\theta$.

To verify that $\theta$ is the character of ${}_u(\mathbb{Q}G)_G$ for some $u \in \mathcal{U}(\mathbb{Q}G)$ satisfying $u^n = 1$, it suffices to show that $\theta|_G$ is equal to the regular character of $G$, which is equal to $1 \uparrow_{\{1\}}^G$. Note that by Mackey's theorem we have

$$1 \uparrow_{[g_i]}^{G\times U} |_G = \sum_x 1 \uparrow_{[g_i]^x \cap G}^G$$

where $x$ ranges over a transversal for the double cosets $[g_i] \setminus G \times U/G$. Since $[g_i] \cdot G = G \times U$, there is just one such double coset, and therefore

$$1 \uparrow_{[g_i]}^{G\times U} |_G = 1 \uparrow_{[g_i]\cap G}^G = 1 \uparrow_{\{1\}}^G$$

independent of $i$. Combining this fact with (1) we get

$$\theta|_G = \sum_{i=1}^{k} a_i \cdot 1 \uparrow_{\{1\}}^G = 1 \uparrow_{\{1\}}^G$$

All that is left to prove now is our claim on the partial augmentations. We know by now that $\theta = \theta_u$ for some $u$, with $\theta_u$ as defined in Proposition 2.3. Thus, Proposition 2.3 yields

$$\varepsilon_{g^G}(u) = \frac{\theta((g,c))}{|C_G(g)|} = \frac{1}{|C_G(g)|} \sum_{i=1}^{k} a_i \cdot 1 \uparrow_{[g_i]}^{G\times U} ((g,c)) \tag{2}$$

The character $1 \uparrow_{[g_i]}^{G\times U}$ evaluated on $(g,c)$ is equal to the number of $h \in G$ such that $(g,c) \in [g_i^h] = \langle (g_i^h, c) \rangle$. Since the order of $g_i$ divides $n$, which is the order of $c$, it follows that the projection from $[g_i^h]$ to $U$ is an isomorphism, and hence $(g_i^h, c)$ is the only element of $[g_i^h]$ whose projection to $U$ is $c$. This implies that $(g,c) \in [g_i^h]$ if and only if $g = g_i^h$. It follows that $1 \uparrow_{[g_i]}^{G\times U} ((g,c))$ is equal to zero if $g^G \neq g_i^G$, and equal to $|C_G(g)|$ if $g^G = g_i^G$. Plugging this back into (2) yields the desired result for the partial augmentations of $u$. □

## 3. Local and semi-local rings of coefficients

Let $R$ be the ring of integers in an algebraic number field $K$. For a maximal ideal $p$ of $R$ we let $R_{(p)}$ denote the localisation of $R$ at the prime $p$. If $\pi = \{p_1, \ldots, p_k\}$ is a finite collection of maximal ideals of $R$, we define

$$R_\pi = \bigcap_{p \in \pi} R_{(p)},$$

which is a semi-local ring whose maximal ideals are precisely $p_i \cdot R_\pi$ for $i = 1, \ldots, k$. Testing whether a particular module is a double action module of a unit is particularly easy over $R_{(p)}$, as the following proposition shows:

**Proposition 3.1.** *Let $M$ be an $R_{(p)}(G \times U)$-module such that $M|_G$ is projective and $K \otimes_{R_{(p)}} M$ is $G$-regular. Then $M$ is $G$-regular.*

*Proof.* By assumption $M|_G$ is projective and its character is equal to the character of the regular $R_{(p)}G$-module. We need to show that this implies that $M|_G$ is isomorphic to the regular $R_{(p)}G$-module. This follows from the fact that two projective $R_{(p)}G$-modules are isomorphic if and only if their characters are the same, a consequence of the fact that the decomposition matrix of a finite group has full row rank (see [CR81, Corollary 18.16] for the precise statement we are using). □

Constructing a $G$-regular $R_\pi(G \times U)$-module is actually equivalent to constructing a $G$-regular $R_{(p)}(G \times U)$-module for each $p \in \pi$ in such a way that all of these modules have the same character.

**Proposition 3.2.** *Let $\Lambda$ be an $R$-order in a finite-dimensional semisimple $K$-algebra $A$ and let $V$ be a finite-dimensional $A$-module.*

*(1) Assume that we are given full $R_{(p)}\Lambda$-lattices $L(p) \leq V$ for each $p \in \pi$. Then*

$$L = \bigcap_{p \in \pi} L(p)$$

*is an $R_\pi\Lambda$-lattice in $V$ with the property that $R_{(p)}L = L(p)$ for each $p \in \pi$.*

*(2) Given two $R_\pi\Lambda$-lattices $L$ and $L'$ in $V$, we have $L \cong L'$ if and only if $R_{(p)}L \cong R_{(p)}L'$ for each $p \in \pi$.*

*Proof.* $L$ is clearly a $R_\pi\Lambda$-module, and in order to show that it is a lattice it suffices to show that it is contained in some $R_\pi$-lattice. If $L'$ is an arbitrary full $R$-lattice in $V$, then for each $p \in \pi$ there is a number $e(p) \in \mathbb{Z}_{\geq 0}$ such that $L(p) \subseteq p^{-e(p)} \cdot R_{(p)}L'$. Let $0 \neq N \in \mathbb{Z}$ be a number such that $p^{e(p)} \supseteq N \cdot R$ for each $p \in \pi$. Then $L \subseteq N^{-1} \cdot R_{(p)}L'$ for each $p \in \pi$, and therefore $L \subseteq \bigcap_{p \in \pi} N^{-1} \cdot R_{(p)}L' = N^{-1} \cdot R_\pi L'$, which is an $R_\pi$-lattice.

Now let us prove that $R_{(p)}L = L(p)$ for each $p \in \pi$. Clearly $R_{(p)}L \subseteq L(p)$. On the other hand, if $v \in L(p)$, then there is an integer $N$ such that $N \cdot v \in L(q)$, for all $q \in \pi$ with $q \neq p$, and $N \not\equiv 0 \pmod{p}$ (we can take $N$ to be contained in a product of sufficiently large powers of the maximal ideals in $\pi$ different from $p$). By definition, we now have $N \cdot v \in L$, and since $N$ is invertible in $R_{(p)}$ we also have $v = N^{-1} \cdot N \cdot v \in R_{(p)}L$. This implies $L(p) \subseteq R_{(p)}L$, which completes the proof of the first point. For the second point see [Rei75, Exercise 18.3]. □

## 4. Locally free lattices and class groups

As in the previous section let $R$ be the ring of integers in an algebraic number field $K$. Let $A$ be a finite-dimensional semisimple $K$-algebra, and let $\Lambda$ be an $R$-order in $A$. Throughout this section we adopt the following notational convention: if $p$ is a maximal ideal of $R$, and $M$ is an $R$-module, then $M_p$ denotes the $p$-adic completion of $M$. In particular, $K_p$ is a complete field with valuation ring $R_p$, $A_p$ is a finite-dimensional $K_p$-algebra and $\Lambda_p$ is an $R_p$-order in $A_p$.

Let us first check that no information is lost in passing from the localisations considered in the previous section to the completions we are going to consider now. If we keep the notation $R_{(p)}$ for the localisation of $R$ at $p$ and $\Lambda_{(p)} = R_{(p)} \cdot \Lambda \subseteq A$, then $R_p$ and $\Lambda_p$ can also be viewed as the $p$-adic completions of $R_{(p)}$ and $\Lambda_{(p)}$, respectively.

**Proposition 4.1** ([CR87, Proposition 30.17])**.** *Let $M$ and $N$ be finitely generated $\Lambda_{(p)}$-modules. Then*

$$M \cong N \quad \textit{if and only if} \quad M_p \cong N_p$$

In particular, if $M$ and $N$ are finitely generated $\Lambda$-modules, then $M_{(p)} \cong N_{(p)}$ as $\Lambda_{(p)}$-modules if and only if $M_p \cong N_p$ as $\Lambda_p$-modules.

Now let us define the protagonist of this section: the locally free class group of $\Lambda$.

**Definition 4.2** (cf. [CR87, §49A])**.** *(1) A right $\Lambda$-lattice $L$ is called* locally free *of rank $n \in \mathbb{N}$ if*

$$L_p \cong \Lambda_p^{\oplus n}$$

*as right $\Lambda_p$-modules for all maximal ideals $p$ of $R$.*

*(2) If $L$ and $L'$ are right $\Lambda$-lattices, we say that $L$ and $L'$ are* stably isomorphic *if*

$$L \oplus \Lambda^{\oplus n} \cong L' \oplus \Lambda^{\oplus n}$$

*for some $n \in \mathbb{N}$.*

*(3) The* locally free class group *of $\Lambda$, denoted by $\mathrm{Cl}(\Lambda)$, is an additive group whose elements are the stable isomorphism classes $[X]$ of locally free right $\Lambda$-ideals in $A$. The group operation on $\mathrm{Cl}(\Lambda)$ is defined as follows: if $X$ and $Y$ are locally free right $\Lambda$-ideals in $A$, then there is a locally free right $\Lambda$-ideal $Z$ such that*

$$X \oplus Y \cong Z \oplus \Lambda$$

*as right $\Lambda$-modules. We define the sum $[X] + [Y]$ to be equal to $[Z]$.*

Note that the unit element of $\mathrm{Cl}(\Lambda)$ is $[\Lambda]$. For the purposes of this article, class groups serve as a means to prove that certain $\Lambda$-lattices are free. The reason this works is that most group algebras satisfy the Eichler condition relative to $\mathbb{Z}$, which guarantees that we can infer $X \cong \Lambda$ from $[X] = [\Lambda]$:

**Definition 4.3** (cf. [CR87, Remark 45.5 (i)])**.** *We say that $A$ satisfies the* Eichler condition *relative to $R$ if no simple component of $A$ is isomorphic to a totally definite quaternion algebra.*

**Theorem 4.4** (Jacobinski Cancellation Theorem [CR87, Theorem 51.24])**.** *If $A$ satisfies the Eichler condition relative to $R$, then any two locally free $\Lambda$-lattices which are stably isomorphic are isomorphic.*

**Theorem 4.5** ([CR87, Theorem 51.3])**.** *If $G$ is a finite group which does not have an epimorphic image isomorphic to either one of the following:*

*(1) A generalised quaternion group of order $4n$ where $n \geq 2$.*

*(2) The binary tetrahedral group of order* $24$.
*(3) The binary octahedral group of order* $48$.
*(4) The binary icosahedral group of order* $120$.
*then* $KG$ *satisfies the Eichler condition relative to* $R$.

We now turn our attention to the problem of deciding whether a given locally free $\Lambda$-ideal is trivial in $\mathrm{Cl}(\Lambda)$.

**Definition 4.6** ([CR87, (49.4)])**.** *(1) We define the idèle group of* $A$ *as*

$$J(A) = \left\{ (\alpha_p)_p \in \prod_p \mathcal{U}(A_p) \;\middle|\; \alpha_p \in \mathcal{U}(\Lambda_p) \text{ for all except finitely many } p \right\}$$

*where* $p$ *ranges over all maximal ideals of* $R$*. If* $\alpha = (\alpha_p)_p$ *and* $\beta = (\beta_p)_p$ *are two elements of* $J(A)$*, then their product* $\alpha \cdot \beta$ *in* $J(A)$ *is defined as* $(\alpha_p \cdot \beta_p)_p$.
*(2) We identify* $\mathcal{U}(A)$ *with the subgroup of* $J(A)$ *consisting of constant idèles.*
*(3) Define*

$$U(\Lambda) = \{\alpha \in J(A) \mid \alpha_p \in \mathcal{U}(\Lambda_p) \text{ for all } p\}$$

*This is also a subgroup of* $J(A)$.

Even though it is not immediately obvious from the definition, $J(A)$ does not depend on the order $\Lambda$ (in fact, if $\Gamma$ is another $R$-order in $A$, then $\Lambda_p = \Gamma_p$ for all except finitely many $p$).

**Theorem 4.7** (Special case of [CR87, Theorem 31.18])**.** *There is a bijection between the double cosets*

$$\mathcal{U}(A) \setminus J(A)/U(\Lambda)$$

*and isomorphism classes of locally free right* $\Lambda$*-ideals in* $A$ *given by*

$$\mathcal{U}(A) \cdot \alpha \cdot U(\Lambda) \mapsto A \cap \bigcap_p \alpha_p \Lambda_p$$

*where* $\alpha = (\alpha_p)_p \in J(A)$*. We denote the right hand side of this assignment by* $\alpha\Lambda$.

As shown in [CR87, Theorem 31.19] we have, for arbitrary $\alpha, \beta \in J(A)$, an isomorphism $\alpha\Lambda \oplus \beta\Lambda \cong \Lambda \oplus \alpha\beta\Lambda$. This shows that there is an epimorphism of groups

$$\theta : \; J(A) \twoheadrightarrow \mathrm{Cl}(\Lambda) : \; \alpha \mapsto [\alpha\Lambda]$$

Since $\mathrm{Cl}(\Lambda)$ is commutative by definition, we certainly have $[J(A), J(A)] \subseteq \mathrm{Ker}(\theta)$. In [Frö75], A. Fröhlich gave an explicit characterisation of the kernel of $\theta$, which will be very useful to us later.

**Definition 4.8** (Reduced norms)**.** *Let* $F$ *be a field, and let* $B$ *be a finite-dimensional semisimple* $F$*-algebra. Then there is a decomposition*

$$B = B_1 \oplus \ldots \oplus B_n$$

*where each* $B_i$ *is a simple* $F$*-algebra. We may view* $B_i$ *as a central simple algebra over its centre* $Z(B_i)$*. In each component we have a reduced norm map*

$$\mathrm{nr}_{B_i/Z(B_i)} : \; B_i \longrightarrow Z(B_i)$$

*obtained by embedding* $B_i$ *into* $E \otimes_{Z(B_i)} B_i$ *for some field extension* $E/Z(B_i)$ *which splits* $B_i$*, followed by mapping* $E \otimes_{Z(B_i)} B_i$ *isomorphically onto a full matrix ring over* $E$ *of the appropriate dimension and then taking the determinant. We can then define a reduced norm map on* $B$

*component-wise. This map will take values in* $Z(B_1) \oplus \ldots \oplus Z(B_n) = Z(B)$. *That is, we get a multiplicative map*

$$\mathrm{nr}_{B/Z(B)} : \ B \longrightarrow Z(B)$$

**Definition 4.9.** *Define*

$$J_0(A) = \{(\alpha_p)_p \in J(A) \mid \mathrm{nr}_{A_p/Z(A_p)}(\alpha_p) = 1 \textit{ for all } p\}$$

*This is a normal subgroup of* $J(A)$.

**Theorem 4.10** ([Frö75, Theorem 1 and subsequent remarks])**.** *The map*

$$\frac{J(A)}{J_0(A) \cdot \mathcal{U}(A) \cdot U(\Lambda)} \xrightarrow{\sim} \mathrm{Cl}(\Lambda) : \ \alpha \cdot J_0(A) \cdot \mathcal{U}(A) \cdot U(\Lambda) \mapsto [\alpha\Lambda]$$

*is an isomorphism of groups.*

For our purposes it will suffice to know that for any $\alpha \in J_0(A)$ the corresponding element $[\alpha\Lambda] \in \mathrm{Cl}(\Lambda)$ is trivial.

## 5. Semi-local counterexamples

After these general sections we will now start to work with a more concrete class of groups which will ultimately provide our counterexample. Let $G$ be a finite group of the form

$$G = N \rtimes A$$

where $N$ is an abelian group. Moreover, let $U = \langle c \rangle$ be a cyclic group such that the exponent of $N$ and the exponent of $U$ coincide. Let

$$\varepsilon : \ G \longrightarrow \mathbb{Z} : \ g \mapsto \varepsilon_{g^G}$$

be a class function which vanishes outside of $N$ (the notation for $\varepsilon$ is deliberately chosen to resemble our notation for partial augmentations). When we say that the partial augmentations of a unit $u \in \mathcal{U}(RG)$ are given by $\varepsilon$, for some commutative ring $R \supseteq \mathbb{Z}$, we mean that $\varepsilon_{g^G}(u) = \varepsilon_{g^G}$ for all $g \in G$. Define

$$\chi = \sum_{g^G} \varepsilon_{g^G} \cdot 1 \uparrow_{[g]}^{G \times U} \tag{3}$$

Note that, a priori, $\chi$ is only a virtual character of $G \times U$. Assume that all of the following hold:

- **(C.1)** $\sum_{g^G} \varepsilon_{g^G} = 1$.
- **(C.2)** If $\varepsilon_{n^G} \neq 0$ for some $n \in N$, then $C_G(n_p) \cap C_G(n_{p'}^g) = N$ for all $g \in G$ and all primes $p$ dividing the order of $N$.
- **(C.3)** For each prime $p$ dividing the order of $N$ we have a decomposition

$$\chi|_{N \times U} = \sum_{n \in N_p} \xi_n \otimes 1 \uparrow_{[n]_p}^{N_p \times U_p} \tag{4}$$

  where $\xi_n$ is a proper character of $N_{p'} \times U_{p'}$ for each $n \in N_p$.

The aim of this section is to prove the following theorem:

**Theorem 5.1.** *Let* $\pi$ *be a finite collection of primes. Then, under the above assumptions, there exists a* $G$*-regular* $\mathbb{Z}_\pi(G \times U)$*-lattice* $L$ *with character* $\chi$. *Moreover, the partial augmentations of the associated unit* $u_\pi \in \mathcal{U}(\mathbb{Z}_\pi G)$ *are given by* $\varepsilon$.

By [CW00, Theorem 3.3] the condition **(C.3)** actually implies that there exists a $\mathbb{Z}(N \times U)$-lattice which is locally free over $\mathbb{Z}N$. We will not use this fact, but it provided the original motivation for this construction. The condition is also studied in [MR17a].

**Remark 5.2.** In (4), the $\xi_n$ are uniquely determined. Namely,

$$\xi_n = \sum_{m \in N_{p'}} \varepsilon_{(m\cdot n)^G} \cdot 1 \uparrow_{[m]_{p'}}^{N_{p'} \times U_{p'}}$$

*Proof.* By Mackey decomposition we have

$$1 \uparrow_{[h]}^{G \times U} |_{N \times U} = [C_G(h) : N] \sum_{m \in h^G} 1 \uparrow_{[m]}^{N \times U}$$

for every $h \in N$. Thus we obtain

$$\chi|_{N \times U} = \sum_{h \in N} [C_G(h) : N] \cdot \varepsilon_{h^G} \cdot 1 \uparrow_{[h]}^{N \times U}$$

Note that our assumptions imply that $C_G(h) = C_G(h_p) \cap C_G(h_{p'})$ is equal to $N$ whenever $\varepsilon_{h^G} \neq 0$. Hence

$$\chi|_{N \times U} = \sum_{h \in N} \varepsilon_{h^G} \cdot 1 \uparrow_{[h]}^{N \times U}$$

So, setting

$$\xi_n = \sum_{m \in N_{p'}} \varepsilon_{(m\cdot n)^G} \cdot 1 \uparrow_{[m]_{p'}}^{N_{p'} \times U_{p'}}$$

for every $n \in N_p$ certainly ensures that (4) holds.

To prove that the $\xi_n$'s are uniquely determined as virtual characters, it suffices to show that they can be recovered from $\chi|_{N \times U}$. Let $m, n \in N_p$. Then

$$1 \uparrow_{[m]_p}^{N_p \times U_p} ((n, c_p)) = \begin{cases} 0 & \text{if } n \neq m \\ |N_p| & \text{otherwise} \end{cases}$$

Hence, if $h \in N_{p'}$ and $n \in N_p$, then

$$\chi((h \cdot n, c)) = |N_p| \cdot \xi_n((h, c_{p'}))$$

which shows that $\xi_n$ is determined uniquely by $\chi|_{N \times U}$. □

**Definition 5.3.** *For a group $X$ we define*

$$e(X) = \frac{1}{|X|} \sum_{x \in X} x$$

**Definition 5.4.** *Assume that $p$ is a prime dividing the order of $N$ and let $q$ be any prime not dividing the order of $N_{p'}$ (in particular, $q = p$ is a possible choice for $q$). Let $X \leq N \times U$ be a subgroup such that $(N_{p'} \times U_{p'})/X_{p'}$ is cyclic. Let $e$ denote the primitive idempotent in the rational group algebra $\mathbb{Q}((N_{p'} \times U_{p'})/X_{p'})$ corresponding to the unique faithful irreducible representation of $(N_{p'} \times U_{p'})/X_{p'}$ over $\mathbb{Q}$, and denote its preimage in $\mathbb{Q}(N_{p'} \times U_{p'})$ by $\widehat{e}$ (we may choose $\widehat{e}$ in such a way that $\widehat{e} \cdot e(X_{p'}) = \widehat{e}$).*

*We define a $\mathbb{Z}_{(q)}(N \times U)$-lattice*

$$M_0(X, p, q) = \mathbb{Z}_{(q)} \uparrow_{X_p}^{N_p \times U_p} \otimes \left( \mathbb{Z}_{(q)} \uparrow_{X_{p'}}^{N_{p'} \times U_{p'}} \cdot \widehat{e} \right)$$

*as well as a $\mathbb{Z}_{(q)}(G \times U)$-lattice*

$$M(X,p,q) = M_0(X,p,q) \uparrow_{N\times U}^{G\times U}$$

**Proposition 5.5.** *The character of the $\mathbb{Z}_{(q)}(N \times U)$-lattice $M_0(X,p,q)$ is equal to*

$$\psi_{M_0(X,p,q)} = 1 \uparrow_{X_p}^{N_p\times U_p} \otimes\varphi$$

*where $\varphi$ is the unique irreducible rational character of $N_{p'} \times U_{p'}$ with kernel $X_{p'}$.*

*Proof.* This follows immediately from the fact that $\varphi$ is afforded by the $\mathbb{Z}_{(q)}(N_{p'} \times U_{p'})$-lattice $\mathbb{Z}_{(q)} \uparrow_{X_{p'}}^{N_{p'}\times U_{p'}} \cdot\widehat{e}$. □

**Remark 5.6.** The following description of the character of $M(X,p,q)$ for certain $X$ is useful for explicit computations, even though we do not use it in this article:

(1) If $X_{p'} = N_{p'} \times U_{p'}$, then

$$\psi_{M(X,p,q)} = 1 \uparrow_X^{G\times U}$$

(2) If $(N_{p'} \times U_{p'})/X_{p'}$ is cyclic of order $r$ for some prime $r$, then

$$\psi_{M(X,p,q)} = 1 \uparrow_X^{G\times U} -1 \uparrow_{X\cdot(N_{p'}\times U_{p'})}^{G\times U}$$

**Proposition 5.7.** *If $(X \cap G)_q = \{1\}$, then $M(X,p,q)|_G$ is projective.*

*Proof.* This follows from the Mackey formula, as $M(X,p,q)$ is a direct summand of $\mathbb{Z}_{(q)} \uparrow_X^{G\times U}$:

$$\mathbb{Z}_{(q)} \uparrow_X^{G\times U} |_G \cong \bigoplus_{(g,u)} \mathbb{Z}_{(q)} \uparrow_{X^{(g,u)}\cap G}^G = \bigoplus_{(g,u)} \mathbb{Z}_{(q)} \uparrow_{(X\cap G)^{(g,u)}}^G$$

where the summation index $(g,u)$ runs over a transversal of the double cosets $X \setminus (G \times U)/G$. Each summand on the right hand side is induced from a $q'$-subgroup of $G$, and therefore is projective. □

**Lemma 5.8.** *Let $p$ be a prime dividing the order of $N$ and let $n \in N_p$ be some $p$-element of $N$. Let $\chi_n$ be the following character of $N \times U$:*

$$\chi_n = \sum_{C_G(n)\cdot g\in C_G(n)\backslash G} 1 \uparrow_{[n^g]_p}^{N_p\times U_p} \otimes\xi_n^g$$

*where $\xi_n$ is the character of $N_{p'} \times U_{p'}$ defined in the beginning of this section (in particular $\xi_n$ is stabilised by $C_G(n)$).*

*Then, for any prime $q$ not dividing the order of $N_{p'}$, $\chi_n$ is the restriction to $N \times U$ of the character of the $\mathbb{Z}_{(q)}(G \times U)$-lattice*

$$L = \bigoplus_{\varphi\in \mathrm{Irr}_{\mathbb{Q}}(N_{p'}\times U_{p'})/C_G(n)} M([n]_p \times \mathrm{Ker}(\varphi), p, q)^{\oplus\mu(\varphi,n)}$$

*with*

$$\mu(\varphi,n) = \frac{(\varphi,\xi_n)}{(\varphi,\varphi)} \cdot \frac{1}{[C_G(n) \cap N_G(\mathrm{Ker}(\varphi)) : N]} \in \mathbb{Z}_{\geq 0}$$

*Moreover, the restriction of $L$ to $G$ is a projective $\mathbb{Z}_{(q)}G$-lattice.*

*Proof.* We need to prove three things:

(1) The $\mu(\varphi,n)$ as defined above are (non-negative) integers.

(2) The lattice $L$ defined in Lemma 5.8 restricted to $G$ is projective.
(3) The restriction to $N \times U$ of the character of $L$ is equal to $\chi_n$.

Recall that

$$\xi_n = \sum_{m \in N_{p'}} \varepsilon_{(m\cdot n)^G} \cdot 1 \uparrow_{[m]_{p'}}^{N_{p'} \times U_{p'}}$$

Take some $\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{p'} \times U_{p'})$. Then $\varphi$ is the sum over the Galois conjugacy class of some $\varphi_0 \in \mathrm{Irr}_{\mathbb{C}}(N_{p'} \times U_{p'})$. In particular, $(\varphi, \varphi) = \varphi(1)$ and $(\varphi, \xi_n) = \varphi(1) \cdot (\varphi_0, \xi_n)$, since $\varphi_0$ is linear and $\xi_n$ rational. By Frobenius reciprocity

$$\begin{aligned}(\varphi_0, \xi_n) &= \sum_{m \in N_{p'}} \varepsilon_{(m\cdot n)^G} \cdot \left(\varphi_0, 1 \uparrow_{[m]_{p'}}^{N_{p'} \times U_{p'}}\right) \\ &= \sum_{m \in N_{p'}} \varepsilon_{(m\cdot n)^G} \cdot \left(\varphi_0|_{[m]_{p'}}, 1_{[m]_{p'}}\right).\end{aligned} \tag{5}$$

Now,

$$\left(\varphi_0|_{[m]_{p'}}, 1_{[m]_{p'}}\right) = \begin{cases} 1 & \text{if } (m, c_{p'}) \in \mathrm{Ker}(\varphi_0) = \mathrm{Ker}(\varphi), \\ 0 & \text{otherwise} \end{cases}$$

So for $g \in C_G(n) \cap N_G(\mathrm{Ker}(\varphi))$ we have

$$\varepsilon_{(m\cdot n)^G} \cdot \left(\varphi_0|_{[m]_{p'}}, 1_{[m]_{p'}}\right) = \varepsilon_{(m^g\cdot n)^G} \cdot \left(\varphi_0|_{[m^g]_{p'}}, 1_{[m^g]_{p'}}\right)$$

Hence grouping together elements conjugate by $C_G(n) \cap N_G(\mathrm{Ker}(\varphi))$ we can write

$$(\varphi_0, \xi_n) = \sum_{\substack{m^{C_G(n)\cap N_G(\mathrm{Ker}(\varphi))}, \\ m \in N_{p'}}} [C_G(n) \cap N_G(\mathrm{Ker}(\varphi)) : N] \cdot \varepsilon_{(m\cdot n)^G} \cdot \left(\varphi_0|_{[m]_{p'}}, 1_{[m]_{p'}}\right)$$

where we use our assumption that $C_G(n)/N$ acts semiregularly on $m^G$ whenever $\varepsilon_{(m\cdot n)^G} \neq 0$ (that is Condition **(C.2)**). It follows that $\mu(\varphi, n)$ is an integer.

The fact that $L|_G$ is projective follows immediately from Proposition 5.7, since $[n]_p \cap G = \{1\}$ and for each $\varphi$

$$([n]_p \times \mathrm{Ker}(\varphi)) \cap G = ([n]_p \cap G) \times (\mathrm{Ker}(\varphi) \cap G) = \mathrm{Ker}(\varphi) \cap G$$

is a subgroup of $N_{p'}$, and therefore a $q'$-group.

Now let us prove that the character of $L|_{N\times U}$ is equal to $\chi_n$. Recall from Proposition 5.5 that for any $\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{p'} \times U_{p'})$ and any $g \in G$

$$\psi_{M_0([n^g]_p \times \mathrm{Ker}(\varphi), p, q)} = 1 \uparrow_{[n^g]_p}^{N_p \times U_p} \otimes \varphi$$

We can therefore write $\chi_n$ as follows:

$$\begin{aligned}
\chi_n &= \frac{1}{[C_G(n):N]} \sum_{gN \in G/N} 1 \uparrow_{[n^g]_p}^{N_p \times U_p} \otimes \xi_n^g \\
&= \frac{1}{[C_G(n):N]} \sum_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{p'} \times U_{p'})} \frac{(\varphi, \xi_n)}{(\varphi, \varphi)} \sum_{gN \in G/N} \psi_{M_0([n^g]_p \times \mathrm{Ker}(\varphi)^g, p, q)} \\
&= \frac{1}{[C_G(n):N]} \sum_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{p'} \times U_{p'})} \frac{(\varphi, \xi_n)}{(\varphi, \varphi)} \cdot \psi_{M([n]_p \times \mathrm{Ker}(\varphi), p, q)}|_{N \times U} \\
&= \sum_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{p'} \times U_{p'})/C_G(n)} \frac{(\varphi, \xi_n)}{(\varphi, \varphi)} \cdot \frac{[C_G(n) : C_G(n) \cap N_G(\mathrm{Ker}(\varphi))]}{[C_G(n):N]} \cdot \psi_{M([n]_p \times \mathrm{Ker}(\varphi), p, q)}|_{N \times U} \\
&= \sum_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{p'} \times U_{p'})/C_G(n)} \frac{(\varphi, \xi_n)}{(\varphi, \varphi)} \cdot \frac{1}{[C_G(n) \cap N_G(\mathrm{Ker}(\varphi)) : N]} \cdot \psi_{M([n]_p \times \mathrm{Ker}(\varphi), p, q)}|_{N \times U} \\
&= \sum_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{p'} \times U_{p'})/C_G(n)} \mu(\varphi, n) \cdot \psi_{M([n]_p \times \mathrm{Ker}(\varphi), p, q)}|_{N \times U}
\end{aligned}$$

The latter is clearly the character of $L|_{N \times U}$. Going from the third to the fourth line we made use of the fact that $(\varphi, \xi_n)$ is constant on the $C_G(n)$-orbit of $\varphi$, as $\xi_n$ is assumed to be $C_G(n)$-invariant. □

We need one last proposition before proceeding to the proof of Theorem 5.1.

**Proposition 5.9.** *Let $X$ be a group and let $Y \trianglelefteq X$ be a normal subgroup. If $\chi$ and $\psi$ are virtual characters of $Y$, then $\chi \uparrow^X = \psi \uparrow^X$ if and only if $\chi \uparrow^X |_Y = \psi \uparrow^X |_Y$.*

*Proof.* We claim that $\chi \uparrow^X |_Y \uparrow^X = [X : Y] \cdot \chi \uparrow^X$ (same for $\psi$). This would clearly imply the assertion, and it is an easy application of the Mackey formula (note that $Y \setminus X / Y = X/Y$ in this case):

$$(\chi \uparrow^X |_Y) \uparrow^X = \left( \sum_{xY} \chi^x|_{Y^x \cap Y} \uparrow^Y \right) \uparrow^X = \sum_{xY} \chi^x \uparrow^X = [X : Y] \cdot \chi \uparrow^X$$

□

We now prove the main result of this section.

*Proof of Theorem 5.1.* Let $p$ be a prime dividing the order of $N$. For $n \in N_p$ define

$$\chi_n = \sum_{C_G(n) \cdot g \in C_G(n) \backslash G} 1 \uparrow_{[n^g]_p}^{N_p \times U_p} \otimes \xi_n^g$$

By formula (4) we then have

$$\chi|_{N \times U} = \sum_{n^G, n \in N_p} \chi_n$$

By applying Lemma 5.8 to the individual $\chi_n$ we get, for any prime $q$ not dividing the order of $N_{p'}$, a $\mathbb{Z}_{(q)}(G \times U)$-lattice $L$ such that $L|_{N\times U}$ has character $\chi|_{N\times U}$ and $L|_G$ is projective. Furthermore, since all summands of $L$ are induced from $N \times U$, and similarly $\chi$ is induced from a (potentially virtual) character of $N \times U$, Proposition 5.9 implies that the character of $L$ is equal to $\chi$. In particular, this shows that $\chi$ is in fact a proper character of $G \times U$.

Since we can do the above for all primes $p$ dividing the order of $N$, we do in fact get a $\mathbb{Z}_{(q)}(G \times U)$-lattice $L(q)$ with character $\chi$ and projective restriction to $G$ for all prime numbers $q$. Moreover, Proposition 2.4 ensures that $\chi$ is the character of a $G$-regular $\mathbb{Q}(G \times U)$-module $V$, and that the partial augmentations of the associated unit are given by $\varepsilon$. We may assume without loss that the $L(q)$ are lattices in $V$. Using Proposition 3.1 it also follows that the $L(q)$ are $G$-regular. Now define

$$L = \bigcap_{q\in\pi} L(q)$$

Then $\mathbb{Z}_{(q)}L|_G = L(q)|_G \cong \mathbb{Z}_{(q)}G$ for all $q \in \pi$. Hence Proposition 3.2 implies that $L$ is a $G$-regular $\mathbb{Z}_\pi(G \times U)$ module with character $\chi$. This concludes the proof. □

**Remark 5.10.** While it has no bearing on the proof of Theorem 5.1, it still seems worth pointing out that for every prime $p$ dividing the order of $N$, there is at most one $G$-conjugacy class $n^G$ of elements in $N_p$ such that $\xi_n \neq 0$, or, equivalently, $\chi_n \neq 0$. This can be seen by considering the degree of $\xi_n$, which can be computed using the formula given in Remark 5.2. What we obtain is that $\xi_n(1)$ is equal to $|N_{p'}|$ times the sum over a certain subset of the $\varepsilon_{g^G}$. Since none of these sums can be negative, and the $\varepsilon_{g^G}$ are integers summing up to one, it follows that at most one of these sums can be non-zero.

In order to apply Theorem 5.1 later on we will need to verify the condition that the $\xi_n$ are proper characters. The following lemma, which was also proved in [MR17b, Corollary 3.5], helps with that.

**Lemma 5.11.** *Let $p$ be a prime dividing the order of $N$ and let $\varphi$ be an irreducible complex character of $N_{p'} \times U_{p'}$.*

*(1) If $\varphi$ is the trivial character then*

$$(\xi_n, \varphi) = [C_G(n) : N] \cdot \sum_{(n\cdot m)^G, m\in N_{p'}} \varepsilon_{(n\cdot m)^G}$$

*(2) If there is no $m_0 \in N_{p'}$ such that $(m_0, c_{p'}) \in \mathrm{Ker}(\varphi)$ then*

$$(\xi_n, \varphi) = 0$$

*(3) Otherwise set $K = \mathrm{Ker}(\varphi) \cap N_{p'}$ and let $m_0 \in N_{p'}$ be chosen such that $(m_0, c_{p'}) \in \mathrm{Ker}(\varphi)$. Then*

$$(\xi_n, \varphi) = \sum_{m^{C_G(n)}, m\in N_{p'}} \left| m^{C_G(n)} \cap m_0 \cdot K \right| \cdot \varepsilon_{(n\cdot m)^G}$$

*In particular, $\xi_n$ is a proper character of $N_{p'} \times U_{p'}$ if and only if for all subgroups $K$ of $N_{p'}$ such that $N_{p'}/K$ is cyclic and for all $m_0 \in N_{p'}$ we have*

$$\sum_{m^{C_G(n)}, m\in N_{p'}} \left| m^{C_G(n)} \cap m_0 \cdot K \right| \cdot \varepsilon_{(n\cdot m)^G} \geq 0$$

*Proof.* As in formula (5) we have

$$(\xi_n, \varphi) = \sum_{m \in N_{p'}} \varepsilon_{(n\cdot m)^G} \cdot \left(\varphi|_{[m]_{p'}}, 1_{[m]_{p'}}\right) \tag{6}$$

and $(\varphi|_{[m]_{p'}}, 1_{[m]_{p'}})$ is equal to one if $(m, c_{p'}) \in \mathrm{Ker}(\varphi)$ and equal to zero otherwise.

So for $\varphi$ equal to the the trivial character we have

$$(\xi_n, \varphi) = \sum_{m \in N_{p'}} \varepsilon_{(n\cdot m)^G} = \sum_{(n\cdot m)^G, m \in N_{p'}} \left| m^{C_G(n)} \right| \cdot \varepsilon_{(n\cdot m)^G} = [C_G(n) : N] \sum_{(n\cdot m)^G, m \in N_{p'}} \varepsilon_{(n\cdot m)^G}$$

where we used that the centraliser of $m$ in $C_G(n)$ is equal to $C_G(m) \cap C_G(n) = N$ whenever $\varepsilon_{(n\cdot m)^G} \neq 0$.

If there is no $m_0 \in N_{p'}$ such that $(m_0, c_{p'}) \in \mathrm{Ker}(\varphi)$ then all summands on the right hand side of (6) are zero, which implies the second assertion.

Finally the third case follows directly by grouping together summands in (6) for which $m$ is in the same $C_G(n)$-conjugacy class. All one has to use here is that an $m \in N_{p'}$ satisfies $(m, c_{p'}) \in \mathrm{Ker}(\varphi)$ if and only if $m \in m_0 \cdot K$ by definition of $m_0$ and $K$. □

## 6. A local-global principle for certain torsion units

In this section we will show that by making only slightly stronger assumptions on $G$ and $\chi$, the semi-local units $u_\pi \in \mathcal{U}(\mathbb{Z}_\pi G)$ constructed in Theorem 5.1 can be shown to be conjugate to elements of $\mathcal{U}(\mathbb{Z}G)$. This follows from a general local-global principle which might also prove useful for other problems which have a "double action" formulation (such as subgroup conjugation questions for $\mathcal{U}(\mathbb{Z}G)$). In essence, the argument boils down to the following: if $u \in \mathcal{U}(\mathbb{Q}G)$ is a torsion unit which has an eigenvalue equal to one in each simple component of $\mathbb{Q}G$, then any unit in $\mathcal{U}(Z(\mathbb{Q}_pG))$ (for any $p$) can be realised as the reduced norm of an element of the centraliser of $u$ in $\mathcal{U}(\mathbb{Q}_pG)$. It follows that if $u$ is conjugate to an element of $\mathcal{U}(\mathbb{Z}_pG)$, then it can be conjugated into $\mathcal{U}(\mathbb{Z}_pG)$ by means of an element of reduced norm one. This holds true for all $p$, and in this situation the strong approximation theorem for the kernel of the reduced norm (see [CR87, Theorem 51.13]) guarantees the existence of an element in $\mathcal{U}(\mathbb{Q}G)$ of reduced norm one which conjugates $u$ into $\mathbb{Z}_pG$ for all $p$ simultaneously, that is, it conjugates $u$ into $\mathbb{Z}G$.

**Lemma 6.1.** *Let $R$ be the ring of integers in an algebraic number field $K$, let $B$ be a finite dimensional $K$-algebra and let $A \subseteq B$ be a semisimple $K$-subalgebra of $B$ satisfying the Eichler condition relative to $R$. Moreover, let $\Lambda$ be an $R$-order in $A$ and let $\Gamma$ be an $R$-order in $B$ containing $\Lambda$. By $\pi$ we denote the set of maximal ideals $p$ of $R$ such that $\Lambda_p$ is not a maximal order, and we assume that $V$ is a $B$-module such that*

1. *$V|_A$ is free of rank one as an $A$-module.*
2. *There is an idempotent $e \in \mathrm{End}_A(V|_A)$ such that $e \cdot \mathrm{End}_A(V|_A) \cdot e \subseteq \mathrm{End}_B(V)$ and $e \cdot \eta \neq 0$ for all primitive idempotents $\eta \in Z(\mathrm{End}_A(V|_A))$.*

*Then our claim is the following: for every $R_\pi\Gamma$-lattice $L(\pi) \leq V$ such that $L(\pi)|_{R_\pi\Lambda}$ is free of rank one as a $R_\pi\Lambda$-module there is a $\Gamma$-lattice $L \leq V$ such that $L|_\Lambda$ is free of rank one as a $\Lambda$-module and $R_\pi \cdot L \cong L(\pi)$.*

*Proof.* Fix an isomorphism of right $A$-modules $\varphi : V|_A \xrightarrow{\sim} A$. We may identify $\mathrm{End}_A(A)$ with $A$, where $a \in A$ is identified with the endomorphism of $A$ induced by left multiplication by $a$ (our notational conventions ensure that we do not have to consider the opposite ring of $A$

here, as one is often compelled to do in similar situations). Hence $\alpha \mapsto \varphi \circ \alpha \circ \varphi^{-1}$ induces an isomorphism between $\mathrm{End}_A(V|_A)$ and $\mathrm{End}_A(A) = A$. Let $f$ denote the image of $e$ under this isomorphism. Then the algebra $C = fAf$ is contained in the image of $\mathrm{End}_B(V)$, and $C$ is again a semisimple $K$-algebra with the additional property that $C \cdot \eta \neq \{0\}$ for all primitive idempotents $\eta \in Z(A)$. The latter ensures that the map $Z(A) \longrightarrow Z(C) : \ z \mapsto z \cdot f$ is an isomorphism. If $p$ is a maximal ideal of $R$, we also have that $C_p$ is contained in the image of $\mathrm{End}_{B_p}(V_p)$, and multiplication by $f$ again induces an isomorphism between $Z(A)_p$ and $Z(C)_p$ (note that $Z(A_p) = Z(A)_p$, and the same holds for $C$). Moreover, it follows immediately from the definition of reduced norms that $\mathrm{nr}_{C_p/Z(C_p)}(c) = \mathrm{nr}_{A_p/Z(A_p)}((1-f)+c) \cdot f$ for any $c \in \mathcal{U}(C_p)$.

By [CR81, Theorem 7.45]

$$\mathrm{nr}_{C_p/Z(C_p)}(\mathcal{U}(C_p)) = \mathcal{U}(Z(C_p))$$

for each maximal ideal $p$ of $R$. Hence we can find, for each $a \in \mathcal{U}(Z(A_p))$, a $c \in \mathcal{U}(C_p)$ such that

$$\mathrm{nr}_{A_p/Z(A_p)}((1-f)+c) = a$$

Of course, the element $(1-f)+c$ also lies in the image of $\mathrm{End}_{B_p}(V_p)$.

Next let us pick an arbitrary $\Gamma$-lattice $L' \leq V$ with the property that $R_\pi L' = L(\pi)$ (for instance, we could take $L'$ to be the $\Gamma$-lattice generated by some $R_\pi\Gamma$-generating set of $L(\pi)$). Then for each prime $p \in \pi$ the completion $L'_p$ is isomorphic to $(L(\pi))_p$, which is free of rank one as a $\Lambda_p$-lattice by definition of $L(\pi)$. For every $p \notin \pi$ the order $\Lambda_p$ is maximal, and therefore $L'_p$ restricted to $\Lambda_p$ is free of rank one since $K_pL'$ restricted to $A_p$ is free of rank one (this is by virtue of [Rei75, Theorem 18.10]). We conclude that $L'$ restricted to $\Lambda$ is locally free. Therefore we can write

$$\varphi(L') = \alpha'\Lambda = \bigcap_p \alpha'_p\Lambda_p$$

for some idèle $\alpha' = (\alpha'_p)_p \in J(A)$. Since $\alpha'_p \in \mathcal{U}(\Lambda_p)$ for all except finitely many $p$, we may as well assume that $\alpha'_p = 1$ for all except finitely many $p$. By the arguments above we can find elements $c_p \in C_p$ (one for each maximal ideal $p$ of $R$) such that $\mathrm{nr}_{C_p/Z(C_p)}(c_p) = \mathrm{nr}_{A_p/Z(A_p)}(\alpha'_p) \cdot f$. We can assume without loss that $c_p = f$ whenever $\alpha'_p = 1$. Then $\alpha = (\alpha_p)_p = (((1-f)+c_p)^{-1} \cdot \alpha'_p)_p$ is an element of $J_0(A)$, which means that

$$L = \varphi^{-1}(\alpha\Lambda)$$

is stably free by Theorem 4.10. Since $A$ satisfies the Eichler condition relative to $R$ we know that $L$ is free of rank 1 as a $\Lambda$-module by Theorem 4.4. All we need to show now is that $L$ is a $\Gamma$-lattice and $L_p \cong (L(\pi))_p$ for all $p \in \pi$. But, for any maximal ideal $p$ of $R$, multiplication by $((1-f)+c_p)$ from the left induces an isomorphism between $\alpha_p\Lambda_p$ and $\alpha'_p\Lambda_p$. By definition, $((1-f)+c_p)$ lies in the image of $\mathrm{End}_{B_p}(V_p)$. That is, there is a $\gamma_p \in \mathrm{End}_{B_p}(V_p)$ such that $\gamma_p(L_p) = \gamma_p(\varphi^{-1}(\alpha_p\Lambda_p)) = \varphi^{-1}(((1-f)+c_p) \cdot \alpha_p\Lambda_p) = \varphi^{-1}(\alpha'_p\Lambda') = L'_p$. This shows that each $L_p$ is a $\Gamma_p$-lattice of the desired isomorphism type, and since $L$ is the intersection of the $L_p$'s, it also follows that $L$ is a $\Gamma$-lattice. □

**Theorem 6.2.** *Assume we are in the setting of Theorem 5.1, and suppose that the Conditions* ***(C.1)****,* ***(C.2)*** *and* ***(C.3)*** *hold. If in addition to that the following conditions are satisfied:*

- ***(C.4)*** *$G$ does not have an epimorphic image isomorphic to either one of the following:*
  - *(a) A generalised quaternion group of order $4n$ where $n \geq 2$.*
  - *(b) The binary tetrahedral group of order $24$.*
  - *(c) The binary octahedral group of order $48$.*
  - *(d) The binary icosahedral group of order $120$.*

***(C.5)*** $(\chi, \eta \otimes 1_U) \neq 0$ *for every* $\eta \in \mathrm{Irr}_{\mathbb{C}}(G)$.

*Then there exists a* $G$*-regular* $\mathbb{Z}(G \times U)$*-lattice* $L$ *with character* $\chi$*. The partial augmentations of the associated unit* $u \in \mathcal{U}(\mathbb{Z}G)$ *are given by* $\varepsilon$*.*

*Proof.* Theorem 5.1 ensures that there is a $G$-regular $\mathbb{Z}_\pi(G \times U)$-lattice $L(\pi)$ in a $\mathbb{Q}(G \times U)$-module $V$ with character $\chi$, where $\pi$ is the set of all prime divisors of the order of $G$. Our assertion will follow once we show that there is a $G$-regular $\mathbb{Z}(G \times U)$-lattice $L \leq V$ with $\mathbb{Z}_\pi L \cong L(\pi)$. Note that by Proposition 2.2 we may assume without loss that $L(\pi) = {}_{u_\pi}(\mathbb{Z}_\pi G)_G$ and $V = {}_{u_\pi}(\mathbb{Q}G)_G$ for a unit $u_\pi \in \mathcal{U}(\mathbb{Z}_\pi G)$ of order $n$.

Now if $\eta$ is a primitive idempotent in $Z(\mathbb{Q}G)$ corresponding to a character $\varphi \in \mathrm{Irr}_{\mathbb{Q}}(G)$, then

$$\eta_{G\times U} = \eta \cdot \frac{1}{n} \sum_{i=1}^{n} c^i \in Z(\mathbb{Q}(G \times U))$$

is the primitive idempotent in $Z(\mathbb{Q}(G \times U))$ belonging to the character $\varphi \otimes 1_U$. Since $(\chi, \varphi_0 \otimes 1_U) \neq 0$ for all irreducible complex characters $\varphi_0$ occurring in $\varphi$, it follows that $V \cdot \eta_{G\times U} \neq 0$.

Using the fact that the action of $G \times U$ on $V = {}_{u_\pi}(\mathbb{Q}G)_G$ is given explicitly, we get

$$\{0\} \neq V \cdot \eta_{G\times U} = \left(\frac{1}{n} \sum_{i=1}^{n} (u_\pi^\circ)^i\right) \cdot \mathbb{Q}G \cdot \eta = \eta \cdot \left(\frac{1}{n} \sum_{i=1}^{n} (u_\pi^\circ)^i\right) \cdot \mathbb{Q}G \tag{7}$$

Now define

$$e = \frac{1}{n} \sum_{i=1}^{n} (u_\pi^\circ)^i$$

and $C = e\mathbb{Q}Ge$. Clearly, left multiplication by elements of $C$ commutes with left multiplication by $u_\pi^\circ$, that is, left multiplication by elements of $C$ induces $\mathbb{Q}(G \times U)$-module endomorphisms of $V$. Since $V$ restricted to $G$ is just $\mathbb{Q}G$ viewed as a right module over itself, we may identify $\mathbb{Q}G$ with $\mathrm{End}_{\mathbb{Q}G}(V|_G)$. Concretely, an element $a \in \mathbb{Q}G$ may be identified with the $\mathbb{Q}G$-endomorphism of $V$ induced by left multiplication with $a$. To summarise, what we have shown is that

$$e \cdot \mathrm{End}_{\mathbb{Q}G}(V|_G) \cdot e \subseteq \mathrm{End}_{\mathbb{Q}(G\times U)}(V)$$

and $e \cdot \eta \neq 0$ for all primitive idempotents $\eta$ in $\mathrm{End}_{\mathbb{Q}G}(V|_G)$ by (7) above. Moreover, by Theorem 4.5 our first condition implies that $\mathbb{Q}G$ satisfies the Eichler condition relative to $\mathbb{Z}$. Hence we may apply Lemma 6.1 to obtain a $G$-regular $\mathbb{Z}(G \times U)$-lattice $L \leq V$ with $\mathbb{Z}_\pi L \cong L(\pi)$. This completes the proof. □

## 7. The counterexample

We will now restrict our attention to a specific family of metabelian groups, consisting of the groups $G(p, q; d; \alpha, \beta)$ defined in the introduction, where the parameters $p$ and $q$ are two different primes, $d$ is a common divisor of $p^2 - 1$ and $q^2 - 1$ which divides neither $p + 1$ nor $q+1$, and $\alpha$ and $\beta$ are primitive elements in $\mathbb{F}_{p^2}$ and $\mathbb{F}_{q^2}$, respectively. Groups of this type were recently studied, in a related context, in [MR17a]. This work provided the motivation to look at these groups as potential counterexamples to the Zassenhaus conjecture.

Our first aim is to reformulate the conditions under which Theorems 5.1 and 6.2 yield semilocal and global units, respectively, in elementary terms for the $G(p, q; d; \alpha, \beta)$'s. This reformulation is stated in Theorem 7.2 below. The proof of this theorem is spread out over several propositions and lemmas, each corresponding, more or less, to one of the conditions of Theorems 5.1 and 6.2. The proofs of the main theorems of this article, the fact that $G(7, 19; 3; \alpha, \beta)$

(with $\alpha$ a root of $X^2 - X + 3$ over $\mathbb{F}_7$ and $\beta$ a root of $X^2 - X + 2$ over $\mathbb{F}_{19}$) is a counterexample to the Zassenhaus conjecture and so are infinitely many more $G(p, q; d; \alpha, \beta)$, are then a quick application of the aforementioned Theorem 7.2.

Whenever we use the group $G(p, q; d; \alpha, \beta)$ below we will tacitly assume the entire notation used in the definition of this group, i.e. the subgroups $N$ and $A$, as well as the generators $a, b, c$ of $A$. Since the definition of $G(p, q; d; \alpha, \beta)$ is symmetric in $p$ and $q$ (of course interchanging $\alpha$ and $\beta$ as well) all statements we make below have an analogue with the roles of $p$ and $q$ reversed. We do not always state this analogue explicitly.

We will often use the fact that

$$|A| = \frac{(p^2 - 1) \cdot (q^2 - 1)}{d}$$

as well as the facts that $C_A(N_p) = \langle b \rangle$ and $C_A(N_q) = \langle a \rangle$. Moreover $G(p, q; d; \alpha, \beta)$ is a metabelian group.

**Notation 7.1.** *For $G = G(p, q; d; \alpha, \beta)$ we define the following subset of $\mathbb{F}_{p^2} \times \{0\} = N_p$*

$$K_p = \{(\alpha + x, 0) \mid x \in \mathbb{F}_p\}$$

*Moreover, for any $i \in \mathbb{Z}$, set*

$$r_i(p) = \left| \left\{ 1 \leq t \leq \frac{p^2 - 1}{d} \;\middle|\; (\alpha^{i+t \cdot d}, 0) \in K_p \right\} \right|$$

*Notice that $r_i(p) = r_j(p)$ if $i \equiv j \bmod d$.*

The first goal of this section is to prove the following theorem:

**Theorem 7.2.** *Let $G = G(p, q; d; \alpha, \beta)$ and let $\varepsilon : G \longrightarrow \mathbb{Z} : \; g \mapsto \varepsilon_{g^G}$ be a class function such that*

*(1) $\sum_{g^G} \varepsilon_{g^G} = 1$*
*(2) If $\varepsilon_{g^G} \neq 0$ for some $g \in G$, then $g \in N$ and the order of $g$ is $p \cdot q$*
*(3) For every $j \in \{0, \ldots, d-1\}$ the inequalities*

$$\sum_{i=1}^{d} r_{j+i}(p) \cdot \varepsilon_{(\alpha^i, 1)^G} \geq 0 \tag{8}$$

*and*

$$\sum_{i=1}^{d} r_{j+i}(q) \cdot \varepsilon_{(1, \beta^i)^G} \geq 0 \tag{9}$$

*hold.*

*Then there is a unit $u \in \mathcal{U}(\mathbb{Z}G)$ of order $p \cdot q$ whose partial augmentations are given by the class function $\varepsilon$. If $\varepsilon_{(\alpha^i, 1)^G} \neq 0$ for more than one $i \in \{1, \ldots, d\}$, then $u$ is not conjugate in $\mathcal{U}(\mathbb{Q}G)$ to an element of the form $\pm g$ with $g \in G$.*

Once we have done that we will verify the conditions of this theorem for one concrete choice of values of $p$, $q$ and $d$ and a concrete class function $\varepsilon$. That bit, which is of course at the same time the proof of Theorem A, is ultimately just a simple calculation (albeit a tedious one). The proof of Theorem B is an application of the following corollary.

**Corollary 7.3.** *Fix an $M \in \mathbb{N}$ and let $G = G(p, q; d; \alpha, \beta)$. Assume that both $p$ and $q$ are greater than or equal to*

$$\frac{d^4 \cdot M^2}{1 - |\cos(2\pi/d)|}$$

*Let $\varepsilon : G \longrightarrow \mathbb{Z} :\ g \mapsto \varepsilon_{g^G}$ be a class function such that*

*(1) $\sum_{g^G} \varepsilon_{g^G} = 1$*
*(2) $|\varepsilon_{g^G}| \leq M$ for all $g \in G$.*
*(3) If $\varepsilon_{g^G} \neq 0$ for some $g \in G$, then $g \in N$ and the order of $g$ is $p \cdot q$.*

*Then there is a unit $u \in \mathcal{U}(\mathbb{Z}G)$ of order $p \cdot q$ whose partial augmentations are given by $\varepsilon$.*

*Proof.* We just need to check that the inequalities (8) and (9) are satisfied. The situation is symmetric in $p$ and $q$, so we will just prove that (8) holds. For brevity write $r_i$ instead of $r_i(p)$.

First note that $\alpha^{p+1}$ is a primitive element of $\mathbb{F}_p$. Let $\zeta_d$ be a primitive $d$-th root of unity in $\mathbb{C}$, and define a multiplicative character

$$\chi :\ \mathbb{F}_p \longrightarrow \mathbb{Q}(\zeta_d) :\ \alpha^{p+1} \mapsto \zeta_d$$

where we adopt the convention $\chi(0) = 0$. Set $f(X) = X^2 + (\alpha + \alpha^p) \cdot X + \alpha^{p+1} \in \mathbb{F}_p[X]$. Then, for any $x \in \mathbb{F}_p$, we have $\chi(f(x)) = \chi((\alpha + x) \cdot (\alpha + x)^p) = \chi((\alpha + x)^{p+1})$. So, if $\alpha + x$ can be written as $\alpha^i$ for some $i$, then $\chi(f(x)) = \chi((\alpha^i)^{p+1}) = \zeta_d^i$. By definition, $r_i$ is the number of $x \in \mathbb{F}_p$ such that $\alpha + x = \alpha^{i+t \cdot d}$ for some $t \in \mathbb{Z}$. Hence $r_i$ is exactly the number of $x \in \mathbb{F}_p$ such that $\chi(f(x)) = \zeta_d^i$. This means that

$$\sum_{x \in \mathbb{F}_p} \chi(f(x)) = \sum_{i=1}^{d} r_i \cdot \zeta_d^i$$

On the other hand, by [LN97, Theorems 5.39 and 5.40], the left hand side of this equation is equal to a complex number $\omega$ of absolute value $\sqrt{p}$. If we write $\delta_i = r_i - \frac{p}{d}$ and use that fact that $\zeta_d + \zeta_d^2 + \ldots + \zeta_d^d = 0$, we get

$$\omega = \sum_{i=1}^{d} \delta_i \cdot \zeta_d^i$$

and thus

$$p = \left( \sum_{i=1}^{d} \delta_i \cdot \zeta_d^i \right) \cdot \left( \sum_{i=1}^{d} \delta_i \cdot \zeta_d^{-i} \right) = \sum_{i=1}^{d} \delta_i^2 + \sum_{1 \leq i < j \leq d} (\zeta_d^{i-j} + \zeta_d^{j-i}) \cdot \delta_i \cdot \delta_j$$

Note that $\zeta_d^{i-j} + \zeta_d^{j-i} = 2 \cdot \mathrm{Re}(\zeta_d^{i-j})$, and the absolute value of this number is bounded above by $2 \cdot |\cos(2\pi/d)|$. Hence

$$p \geq \sum_{i=1}^{d} \delta_i^2 - 2 \cdot |\cos(2\pi/d)| \cdot \left| \sum_{1 \leq i < j \leq d} \delta_i \cdot \delta_j \right| = (1 - |\cos(2\pi/d)|) \cdot \sum_{i=1}^{d} \delta_i^2$$

In the second step we used the fact that $\delta_1 + \ldots + \delta_d = 0$ (a consequence of $r_1 + \ldots + r_d = p$). We conclude that

$$\delta_i \leq \sqrt{\frac{p}{1 - |\cos(2\pi/d)|}}$$

Now, for each $j \in \{0, \dots, d-1\}$, the left hand side of the inequality (8) can be bounded below as follows:

$$\sum_{i=1}^{d} r_{j+i} \cdot \varepsilon_{(\alpha^i,1)^G} = \frac{p}{d} + \sum_{i=1}^{d} \delta_{j+i} \cdot \varepsilon_{(\alpha^i,1)^G} \geq \frac{p}{d} - d \cdot \sqrt{\frac{p}{1 - |\cos(2\pi/d)|}} \cdot M$$

Our assumed lower bound on $p$ ensures that the right hand side of this is non-negative, which proves that the inequality (8) is satisfied for each $j$. □

**Remark 7.4.** The combination of Corollary 7.3 for fixed $d$ and Dirichlet's theorem on arithmetic progressions clearly provides an infinite number of counterexamples to the Zassenhaus conjecture, with arbitrary prescribed partial augmentations for the elements of order $p \cdot q$, and hence a proof of Theorem B. However, it does not yield counterexamples of particularly small order. The smallest choice of parameters for which Corollary 7.3 applies is $M = 1$, $d = 3$, $p = 163$ and $q = 167$. The resulting counterexample has order $2^7 \cdot 3^4 \cdot 7 \cdot 41 \cdot 83 \cdot 163^2 \cdot 167^2$.

To prove Theorem 7.2 we first collect elementary properties of the group $G(p, q; d; \alpha, \beta)$.

**Proposition 7.5.** *Let $G = G(p, q; d; \alpha, \beta)$. Then the following hold:*

1. *Let $g \in N$ be of order $p \cdot q$. Then $C_G(g) = N$.*
2. *For a non-trivial element $n \in N_p$ we have $C_G(n) = C_G(N_p)$.*
3. *Representatives of the $G$-conjugacy classes of element of order $p \cdot q$ in $N$ are given by $(1,1)$, $(\alpha,1)$, $(\alpha^2,1), \dots, (\alpha^{d-1},1)$. Moreover, for a non-trivial element $n \in N_q$ the $C_G(n)$-conjugacy classes of elements of order $p$ in $N$ are given by $(1,0)$, $(\alpha,0), \dots, (\alpha^{d-1},0)$.*
4. *$G$ acts transitively (by conjugation) on the set of cyclic subgroups of order $p \cdot q$ in $N$.*
5. *$G/C_G(N_p)$ acts regularly on the set of non-trivial cosets of cyclic groups of order $p$ in $N_p$, that is, the set*

$$\{n \cdot X \mid X \leq N_p \text{ has order } p \text{ and } n \in N_p, n \notin X\}$$

   *This set has cardinality $p^2 - 1$.*
6. *$C_A(N_q)$ acts semiregularly on the set of non-trivial cosets of cyclic groups of order $p$ in $N_p$.*
7. *$C_G(N_q)$ acts transitively on the set of cyclic groups of order $p$ in $N_p$.*

*Proof.* (1) Let $(\alpha^i, \beta^j) \in N$ be some element of order $p \cdot q$ and $r, s, t \in \mathbb{Z}$. Then

$$(\alpha^i, \beta^j)^{a^r b^s c^t} = (\alpha^i, \beta^j) \Leftrightarrow rd \equiv -t \bmod (p^2 - 1),\ sd \equiv -t \bmod (q^2 - 1).$$

This implies that $t$ is divisible by $d$ and hence $c^t \in \langle a, b \rangle$. But then also $a^r b^s c^t = 1$.

(2) This follows directly since multiplication is a regular action on $\mathbb{F}_{p^2}^{\times}$.

(3) First note that two elements of the form $(\alpha^i, 1)$ and $(\alpha^j, 1)$, for some $i, j \in \mathbb{Z}$, are $G$-conjugate if and only if they are $C_G((0,1))$-conjugate. This follows since $(0,1)$ is the $q$-part of both elements. But $C_G((0,1)) = \langle a \rangle$ and since for any $t \in \mathbb{Z}$ we have

$$(\alpha^i, 1)^{a^t} = (\alpha^{i+d \cdot t}, 1)$$

we get that $(\alpha^i, 1)$ and $(\alpha^j, 1)$ are $G$-conjugate if and only if $i \equiv j \bmod d$. In particular the elements $(1,1), \dots, (\alpha^{d-1}, 1)$ are pairwise non-conjugate and contain representatives of the conjugacy classes of all elements of the form $(\alpha^i, 1)$. Now any element of order $p \cdot q$ in $N$ is of the form $(\alpha^j, \beta^k)$, for certain $j$ and $k$, and since $(\alpha^j, \beta^k)^{c^{-k}} = (\alpha^{j-k}, 1)$, any element of order $p \cdot q$ in $N$ is conjugate to an element of the form $(\alpha^i, 1)$.

Moreover any element of order $p$ in $N$ is of the form $(\alpha^i, 0)$ and since $C_G(n) = \langle a \rangle$ for a non-trivial $n \in N_q$ we can argue as above to see that $(1,0)$, ..., $(\alpha^{d-1}, 0)$ are the $C_G(n)$-conjugacy classes of elements of order $p$ in $N$.

(4) Let $(\alpha^i, \beta^j)$ be some element of order $p \cdot q$ in $N$. We will show that there are $r, s, t \in \mathbb{Z}$ such that $(\alpha^i, \beta^j)^{a^r b^s c^t} \in \langle (1,1) \rangle = \mathbb{F}_p \times \mathbb{F}_q$. This is the case if and only if

$$i + dr + t \equiv 0 \bmod (p+1),\ j + ds + t \equiv 0 \bmod (q+1).$$

These congruences can be solved for any given $i$ and $j$ since $d$ is by assumption coprime to $p+1$ and $q+1$, so we just need to bring $i$, $j$ and $t$ over to the right hand side, and then divide by $d$.

(5) $G/C_G(N_p)$ acts on $N_p = \mathbb{F}_{p^2} \times \{0\}$ by multiplication by elements of $\mathbb{F}_{p^2}^\times$. There are $p+1$ cyclic subgroups in $N_p$ each of which has $p-1$ non-trivial cosets. So as $|G/C_G(N_p)| = p^2 - 1$ it is enough to show that it acts semiregularly. Let $K$ be a cyclic group of order $p$ in $N_p$ and let $m_0 \in N_p \setminus K$. Then we can write $m_0 \cdot K$ as a subset of $N_p$ as $(\alpha^i + \alpha^j \cdot \mathbb{F}_p, 0)$ for certain $i$ and $j$. We can understand this as an affine line in the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^2}$. If multiplication by an element $\alpha^r$ stabilises this coset it also stabilises $\alpha^j \cdot \mathbb{F}_p$, which means $\alpha^r \in \mathbb{F}_p$. Hence we get

$$\alpha^i + \alpha^j \cdot \mathbb{F}_p = \alpha^r \cdot \alpha^i + \alpha^j \cdot \mathbb{F}_p \Leftrightarrow \alpha^i \cdot (1 - \alpha^r) \in \alpha^j \cdot \mathbb{F}_p \Leftrightarrow \alpha^i \in \alpha^j \cdot \mathbb{F}_p,$$

contradicting the assumption that $m_0 \cdot K$ is a non-trivial coset.

(6) Since $C_A(N_q) = \langle a \rangle$, and $a$ acts on $N_p$ by multiplication by an element of order $\frac{p^2-1}{d}$ in $\mathbb{F}_{p^2}^\times$ we can argue as in the proof of (5).

(7) Clearly $\langle \alpha \rangle = \mathbb{F}_{p^2}^\times$ acts transitively on the set of cyclic groups of order $p$ in $N_p$, since it acts transitively on the set of non-trivial elements. Multiplying by an element in $\mathbb{F}_p^\times = \langle \alpha^{p+1} \rangle$ stabilises any subgroup of order $p$, since they are of the form $\alpha^i \cdot \mathbb{F}_p$, for some $i$. We have $C_G(N_q) = \langle a \rangle$, and $a$ acts by multiplication by $\alpha^d$ on $\mathbb{F}_{p^2}$. To show that $C_G(N_q)$ acts transitively on subgroups of order $p$ it suffices to show that $\alpha^d$ together with $\alpha^{p+1}$ generates all of $\mathbb{F}_{p^2}^\times$, since $\alpha^{p+1}$ acts trivially on the set of subgroups of order $p$ of $N_p$ anyway. Since $\gcd(d, p+1) = 1$ by assumption, we have $\langle \alpha^d, \alpha^{p+1} \rangle = \langle \alpha \rangle = \mathbb{F}_{p^2}^\times$, which completes the proof.

□

We proceed to describe the irreducible complex characters of $G(p, q; d; \alpha, \beta)$. We do this the elementary way, but it could also be done using, for instance, the theory of strong Shoda pairs, cf. [JR16, Section 3.5].

**Proposition 7.6.** *Let $G = G(p, q; d; \alpha, \beta)$. Fix an arbitrary irreducible complex character $\varphi_p \in \mathrm{Irr}_{\mathbb{C}}(N)$ with kernel $\langle (1,0), (0,y) \mid y \in \mathbb{F}_{q^2} \rangle$ and an arbitrary irreducible complex character $\varphi_q \in \mathrm{Irr}_{\mathbb{C}}(N)$ with kernel $\langle (x,0), (0,1) \mid x \in \mathbb{F}_{p^2} \rangle$. Then the irreducible complex characters of $G$ are given as follows:*

*(1) The characters induced from the linear characters of $N$ which have kernel $\langle (1,1) \rangle$.*
*(2) The characters induced from linear characters of $C_G(N_p)$ whose restriction to $N$ is $\varphi_p$.*
*(3) The characters induced from linear characters of $C_G(N_q)$ whose restriction to $N$ is $\varphi_q$.*
*(4) The linear characters of $G$. The kernels of these always contains $N$.*

*In particular, each irreducible character of $G$ is induced from a linear character of a subgroup of $G$, and the kernels of these linear characters always contain $\langle (1,1) \rangle$.*

*Proof.* If $\psi$ is a linear characters of $N$ with kernel of order $p \cdot q$, then

$$(\psi \uparrow_N^G, \psi \uparrow_N^G) = (\psi, \psi \uparrow_N^G |_N) = \sum_{x \in A} (\psi, \psi^x) \tag{10}$$

by the Mackey formula. The character $\psi^x$ is again an irreducible character of $N$, and $\psi^x = \psi$ if and only if $\mathrm{Ker}(\psi)^x = \mathrm{Ker}(\psi)$ and $n \cdot \mathrm{Ker}(\psi) = x^{-1}nx \cdot \mathrm{Ker}(\psi)$ for all $n \in N$. This only happens if $n \cdot \mathrm{Ker}(\psi)_p = (n \cdot \mathrm{Ker}(\psi)_p)^x$ for every $n \in N_p$ and $n \cdot \mathrm{Ker}(\psi)_q = (n \cdot \mathrm{Ker}(\psi)_q)^x$ for every $n \in N_q$. By the regularity assertions of Proposition 7.5 (5) this implies that $x \in C_A(N_p) \cap C_A(N_q) = \{1\}$. Looking again at the right hand side of (10) we conclude that $(\psi \uparrow_N^G, \psi \uparrow_N^G) = 1$, that is, $\psi \uparrow_N^G$ is irreducible.

If $\psi'$ is another irreducible character of $N$ with kernel of order $p \cdot q$, then $(\psi \uparrow_N^G, \psi' \uparrow_N^G)$ is either zero or one, and, to be more precise, it follows from Mackey's formula that $(\psi \uparrow_N^G, \psi' \uparrow_N^G) = 1$ if and only if $\psi' = \psi^x$ for some $x \in A$. Hence the number of irreducible characters of $G$ we have constructed so far is the number of $G$-orbits of characters of $N$ with kernel of order $p \cdot q$, and all of these characters have degree $[G : N] = |A|$.

Now we will show that the number of $G$-orbits of characters of $N$ with kernel of order $p \cdot q$ is equal to $d$. Denote by $\zeta_{p \cdot q}$ a primitive $p \cdot q$-th root of unity. A character $\psi$ of $N$ with kernel of order $p \cdot q$ is uniquely determined by the fibre $\psi^{-1}(\{\zeta_{p \cdot q}\})$, which can be written as a coset $n_\psi \cdot \mathrm{Ker}(\psi)$ for some $n_\psi \in N$ of order $p \cdot q$ such that $(n_\psi)_p \notin \mathrm{Ker}(\psi)_p$ and $(n_\psi)_q \notin \mathrm{Ker}(\psi)_q$. The coset $n_\psi \cdot \mathrm{Ker}(\psi)$ is equal to the product of the coset $(n_\psi)_p \cdot \mathrm{Ker}(\psi)_p$ and $(n_\psi)_q \cdot \mathrm{Ker}(\psi)_q$. Conversely, a pair of cosets $n_1X_1$ and $n_2X_1$, with $X_1 \leq N$ of order $p$, $n_1 \in N_p$ not contained in $X_1$, $X_2 \leq N_q$ of order $q$ and $n_2 \in N_q$ not contained in $X_2$ determines a character $\psi$ of $N$ with kernel of order $p \cdot q$. The group $G/C_G(N_p) \times G/C_G(N_q)$ acts regularly on the set of such pairs by Proposition 7.5 (5), and $G/N$ embeds diagonally into $G/C_G(N_p) \times G/C_G(N_q)$ since $C_G(N_p) \cap C_G(N_q) = N$. The index of the image of this embedding is $[A : C_A(N_p)] \cdot [A : C_A(N_q)] \cdot |A|^{-1} = d$. Therefore $G$ has exactly $d$ orbits on such pairs of cosets, and therefore also on characters of $N$ with kernel of order $p \cdot q$.

Next let us show that if $\psi$ is a linear character of $C_G(N_p)$ whose restriction to $N$ is $\varphi_p$ then $\psi \uparrow_{C_G(N_p)}^G$ is irreducible. By Frobenius reciprocity and Mackey we have

$$(\psi \uparrow_{C_G(N_p)}^G, \psi \uparrow_{C_G(N_p)}^G) = \sum_{x \in A/C_A(N_p)} (\psi, \psi^x)$$

Denote by $\zeta_p$ a primitive $p$-th root of unity. We have $\psi^{-1}(\{\zeta_p\}) \cap N_p = \varphi_p^{-1}(\{\zeta_p\})$, which is a coset of $\mathrm{Ker}(\varphi_p)$, a group of order $p$. Since $A/C_A(N_p)$ acts regularly on the set of non-trivial cosets of subgroups of order $p$ in $N_p$ by Proposition 7.5 (5) it follows that $(\psi^x)^{-1}(\{\zeta_p\}) \cap N_p = (\psi^{-1}(\{\zeta_p\}) \cap N_p)^x \neq \psi^{-1}(\{\zeta_p\}) \cap N_p$ (and therefore $\psi \neq \psi^x$) whenever $x \in A$ such that $x \notin C_A(N_p)$. The irreducibility of $\psi \uparrow_{C_G(N_p)}^G$ now follows. Moreover, if we have another linear character $\psi'$ of $C_G(N_p)$ such that $\psi'|_N = \varphi_p$ and $\psi' \neq \psi$, then $\psi(x) \neq \psi'(x)$ for some $x \in C_A(N_p)$. But $\psi \uparrow_{C_G(N_p)}^G |_A = \psi \uparrow_{C_A(N_p)}^A$, which restricted to $C_A(N_p)$ is just $[A : C_A(N_p)] \cdot \psi$. Since the same holds for $\psi'$ it follows that $\psi \uparrow_{C_G(N_p)}^G (x) \neq \psi' \uparrow_{C_G(N_p)}^G (x)$. We have $|C_G(N_p)/N_p| = |C_A(N_p)|$ possibilities for $\psi$ in total, and the degree of $\psi \uparrow_{C_G(N_p)}^G$ is $[G : C_G(N_p)] = [A : C_A(N_p)]$.

Analogously we get $|C_A(N_q)|$ characters of the form given in the third point of the statement, and their degrees are $[A : C_A(N_q)]$. As for the linear characters, there are $|G/N| = |A|$ irreducible characters with $N$ in their kernel.

These four families of irreducible characters of $G$ are disjoint owing to the fact that the intersection of the kernel of a character with $N$ is something different depending on the family

the character comes from (it is either $\{1\}$, $N_q$, $N_p$ or $N$). So all that is left to do now is check that the sum of the squares of the degrees of the characters we have constructed is equal to $|G|$:

$$\begin{aligned} & d \cdot |A|^2 + |C_A(N_p)| \cdot [A : C_A(N_p)]^2 + |C_A(N_q)| \cdot [A : C_A(N_q)]^2 + |A| \cdot 1^2 \\ = \;& |A| \cdot (d \cdot |A| + [A : C_A(N_p)] + [A : C_A(N_q)] + 1) \\ = \;& |A| \cdot ((p^2-1) \cdot (q^2-1) + (p^2-1) + (q^2-1) + 1) \\ = \;& |A| \cdot p^2 \cdot q^2 = |G| \end{aligned}$$

□

**Proposition 7.7.** *Let $G = G(p, q; d; \alpha, \beta)$ and let $U = \langle c \rangle$ be a cyclic group of order $p \cdot q$. Let $\varepsilon : G \longrightarrow \mathbb{Z} : \; g \mapsto \varepsilon_{g^G}$ be a class function with $\sum_{g^G} \varepsilon_{g^G} = 1$ and $\varepsilon_{g^G} \neq 0$ only for elements $g \in G$ of order $p \cdot q$. Define*

$$\chi = \sum_{g^G} \varepsilon_{g^G} \cdot 1 \uparrow_{[g]}^{G \times U}$$

*Then*

$$(\chi, \eta \otimes 1_U) \neq 0 \quad \textit{for all } \eta \in \mathrm{Irr}_{\mathbb{C}}(G)$$

*Proof.* By Proposition 7.5 (4) we can choose $g_1, \ldots, g_k \in \langle (1,1) \rangle$ such that $g_i^G \neq g_j^G$ whenever $i \neq j$ and $\varepsilon_{g^G} \neq 0$ for some $g \in G$ if and only if $g^G = g_i^G$ for some $i$. Our assumptions ensure that each $g_i$ has order $p \cdot q$, which implies that it generates $\langle (1,1) \rangle$. Now, if $\eta \in \mathrm{Irr}_{\mathbb{C}}(G)$ then

$$(\chi, \eta \otimes 1_U) = \sum_{i=1}^{k} \varepsilon_{g_i^G} \cdot \left( 1 \uparrow_{[g_i]}^{G \times U}, \eta \otimes 1_U \right)$$

We claim that the value of $\left( 1 \uparrow_{[g_i]}^{G \times U}, \eta \otimes 1_U \right)$ is independent of $i$, which would imply that $(\chi, \eta \otimes 1_U) = (1 \uparrow_{[g_1]}^{G \times U}, \eta \otimes 1_U)$ (of course we could have used any $g_i$ here instead of $g_1$). By Frobenius reciprocity we have

$$\left( 1 \uparrow_{[g_i]}^{G \times U}, \eta \otimes 1_U \right) = \left( 1_{[g_i]}, (\eta \otimes 1_U)|_{[g_i]} \right) = \frac{1}{p \cdot q} \cdot \sum_{j=1}^{p \cdot q} \eta(g_i^j)$$

The value of the right hand side manifestly only depends on the group generated by $g_i$, which is $\langle (1,1) \rangle$ independent of the value of $i$.

It remains to be seen that $(1 \uparrow_{[g_1]}^{G \times U}, \eta \otimes 1_U)$ is non-zero for every $\eta$. By Proposition 7.6 any $\eta \in \mathrm{Irr}_{\mathbb{C}}(G)$ can be written as $\varphi \uparrow_K^G$ where $\langle (1,1) \rangle \leq K \leq G$ and $\varphi$ is a linear character of $K$ whose kernel contains $\langle (1,1) \rangle = \langle g_1 \rangle$. Hence

$$\begin{aligned} (1 \uparrow_{[g_1]}^{G \times U}, \eta \otimes 1_U) &= (1 \uparrow_{[g_1]}^{G \times U}, (\varphi \otimes 1_U) \uparrow_{K \times U}^{G \times U}) = (1_{[g_1]}, (\varphi \otimes 1_U) \uparrow_{K \times U}^{G \times U} |_{[g_1]}) \\ &= \sum_{x \in K \times U \backslash G \times U / [g_1]} \left( 1_{[g_1]}, (\varphi \otimes 1_U) \uparrow_{(K \times U)^x \cap [g_1]}^{[g_1]} \right) \\ &= \left( 1_{[g_1]}, (\varphi \otimes 1_U)|_{[g_1]} \right) + \text{(other terms)} = (1_{[g_1]}, 1_{[g_1]}) + \text{(other terms)} \end{aligned}$$

which is clearly greater than zero. □

**Lemma 7.8.** *Let $G = G(p, q; d; \alpha, \beta)$, let $\varepsilon : G \to \mathbb{Z}$ be a class function which is non-vanishing only on elements of $N$ of order $p \cdot q$ such that*

$$\sum_{g^G} \varepsilon_{g^G} = \sum_{i=1}^{d} \varepsilon_{(\alpha^i,1)^G} = 1$$

*and let $U = \langle c \rangle$ be a cyclic group of order $p \cdot q$. Set $n = (0, 1) \in N_q$. Recall also the definition of $K_p$ and the $r_i(p)$'s from Notation 7.1. We will write $r_i$ instead of $r_i(p)$ below.*

*(1) The character*

$$\xi_n = \sum_{m \in N_p} \varepsilon_{(m \cdot n)^G} \cdot 1 \uparrow_{[m]_p}^{N_p \times U_p} \qquad \textit{(same as in Remark 5.2)}$$

*is a proper character of $N_p \times U_p$ if and only if*

$$\begin{pmatrix} r_1 & r_2 & \dots & r_d \\ r_2 & r_3 & \dots & r_1 \\ \vdots & \vdots & \ddots & \vdots \\ r_d & r_1 & \dots & r_{d-1} \end{pmatrix} \begin{pmatrix} \varepsilon_{(\alpha,1)^G} \\ \varepsilon_{(\alpha^2,1)^G} \\ \vdots \\ \varepsilon_{(\alpha^d,1)^G} \end{pmatrix} \geq 0.$$

*(2) Let $\varphi$ be an irreducible rational character of $N_p \times U_p$. Let*

$$K = \mathrm{Ker}(\varphi) \cap N_p$$

*Then the values of*

$$\mu(\varphi, n) = \frac{(\varphi, \xi_n)}{(\varphi, \varphi)} \cdot \frac{1}{[C_G(n) \cap N_G(\mathrm{Ker}(\varphi)) : N]} \qquad \textit{(same as in Lemma 5.8)}$$

*are as follows:*

*(a) If $\varphi$ is the trivial character then $\mu(\varphi, n) = 1$.*
*(b) If there is no element $m_0 \in N_p$ such that $(m_0, c_p) \in \mathrm{Ker}(\varphi)$ then $\mu(\varphi, n) = 0$.*
*(c) Otherwise choose an $m_0 \in N_p$ such that $(m_0, c_p) \in \mathrm{Ker}(\varphi)$.*
*(i) If $m_0 \in K$ then $\mu(\varphi, n) = 1$.*
*(ii) If $m_0 \notin K$ we can choose a $g \in G$ such that $(m_0 \cdot K)^g = (\alpha + \mathbb{F}_p, 0)$ by Proposition 7.5 (5). Choose $\ell(g) \in \mathbb{Z}$ such that $(1, 0)^g = (\alpha^{\ell(g)}, 0)$. Then we have*

$$\mu(\varphi, n) = \sum_{i=0}^{d-1} r_{\ell(g)+i} \cdot \varepsilon_{(\alpha^i,1)^G}$$

*If we reverse the roles of $p$ and $q$ as well as $\alpha$ and $\beta$ then the same statements also hold for $\xi_n$ with $n = (1, 0) \in N_p$.*

*Proof.* For every $j \in \{0, \dots, d-1\}$ the inequalities holding by assumption can be understood as follows:

$$0 \leq \sum_{i=1}^{d} r_{j+i} \cdot \varepsilon_{(\alpha^i,1)^G} = \sum_{i=1}^{d} |\{(\alpha^{j+i}, 0)^{\langle a \rangle} \cap K_p\}| \cdot \varepsilon_{(\alpha^i,1)^G} \tag{11}$$

$$= \sum_{i=1}^{d} |\{(\alpha^{j+i}, 0)^{\langle a \rangle} \cap (\alpha + \mathbb{F}_p, 0)\}| \cdot \varepsilon_{(\alpha^i,1)^G}$$

Furthermore, for any fixed $i$ we have

$$\left|(\alpha^i,0)^{\langle a\rangle}\cap(\mathbb{F}_p,0)\right| = \left|\left\{1\le t\le\frac{p^2-1}{d}\;\middle|\;\alpha^{i+td}\in\mathbb{F}_p\right\}\right| \tag{12}$$
$$= \left|\left\{1\le t\le\frac{p^2-1}{d}\;\middle|\;i+td\equiv 0 \bmod (p+1)\right\}\right| = \frac{p-1}{d}$$

where the last equality follows since $d$ and $p+1$ are coprime.

Now $C_G(n)=\langle a\rangle$ and representatives of the $C_G(n)$-conjugacy classes in $N_p\setminus\{(0,0)\}$ are given by $(\alpha,0),(\alpha^2,0),...,(\alpha^d,0)$ by Proposition 7.5 (3). So by Lemma 5.11 we know that $\xi_n$ is a proper character of $N_p\times U_p$ if and only if for every subgroup $K=(\mathbb{F}_p\cdot\alpha^s,0)$ of order $p$ in $N_p$, where $s\in\{1,\dots,p^2-1\}$, and every $(m_0,0)\in N_p$ we have

$$\sum_{i=0}^{d-1}\left|\left\{(\alpha^i,0)^{\langle a\rangle}\cap(m_0+\mathbb{F}_p\cdot\alpha^s,0)\right\}\right|\cdot\varepsilon_{(\alpha^i,1)^G}\ge 0.$$

If $m_0\notin\mathbb{F}_p\cdot\alpha^s$ then by Proposition 7.5 (5) there exists a $g\in G$ such that $(m_0+\mathbb{F}_p\cdot\alpha^s,0)^g=(\alpha+\mathbb{F}_p,0)$. Pick an $\ell(g)$ such that $(1,0)^g=(\alpha^{\ell(g)},0)$. So the condition we have to verify can be formulated as

$$\sum_{i=0}^{d-1}\left|\left\{(\alpha^{i+\ell(g)},0)^{\langle a\rangle}\cap(\alpha+\mathbb{F}_p,0)\right\}\right|\cdot\varepsilon_{(\alpha^i,1)^G}\ge 0$$

and this holds by (11) with $j=\ell(g)$.

So assume $m_0\in\mathbb{F}_p\cdot\alpha^s$ and let $g\in C_G(n)$ be chosen such that $(\mathbb{F}_p\cdot\alpha^s,0)^g=(\mathbb{F}_p,0)$, which exists by Proposition 7.5 (7). Then by (12) we have

$$\sum_{i=0}^{d-1}\left|\left\{(\alpha^i,0)^{\langle a\rangle}\cap(m_0+\mathbb{F}_p\cdot\alpha^s,0)\right\}\right|\cdot\varepsilon_{(\alpha^i,1)^G}=\sum_{i=0}^{d-1}\left|\left\{(\alpha^i,0)^{g\langle a\rangle}\cap(\mathbb{F}_p\cdot\alpha^s,0)^g\right\}\right|\cdot\varepsilon_{(\alpha^i,1)^G}$$
$$=\sum_{i=0}^{d-1}\left|\left\{(\alpha^{i+\ell(g)},0)^{\langle a\rangle}\cap(\mathbb{F}_p,0)\right\}\right|\cdot\varepsilon_{(\alpha^i,1)^G}=\sum_{i=0}^{d-1}\frac{p-1}{d}\cdot\varepsilon_{(\alpha^i,1)^G}=\frac{p-1}{d}$$

This finishes the proof of the first claim.

Let $\varphi_0$ be an irreducible complex character of $N_p\times U_p$ such that $\varphi$ is the sum of the Galois-conjugates of $\varphi_0$. We can reformulate the definition of $\mu(\varphi,n)$ as

$$\mu(\varphi,n)=\frac{(\varphi_0,\xi_n)}{[C_G(n)\cap N_G(\mathrm{Ker}(\varphi)):N]}$$

If $\varphi$ is the trivial character then $C_G(n)\cap N_G(\mathrm{Ker}(\varphi))=C_G(n)$. Using Lemma 5.11 we get

$$(\varphi_0,\xi_n)=[C_G(n):N]\cdot\sum_{(n\cdot m)^G,m\in N_p}\varepsilon_{(n\cdot m)^G}=[C_G(n):N]$$

which shows that $\mu(\varphi,n)$ is as desired.

Next, if there is no element $m_0\in N_p$ such that $(m_0,c_p)\in\mathrm{Ker}(\varphi)$ then Lemma 5.11 implies that $(\varphi_0,\xi_n)=0$, and again $\mu(\varphi,n)$ is as desired.

So let us assume that we have an $m_0\in N_p$ such that $(m_0,c_p)\in\mathrm{Ker}(\varphi)$. Then by Lemma 5.11

$$(\varphi_0,\xi_n)=\sum_{m^{C_G(n)},m\in N_p}\left|m^{C_G(n)}\cap m_0\cdot K\right|\cdot\varepsilon_{(n\cdot m)^G}$$

If $m_0 \in K$ then $\mathrm{Ker}(\varphi) = K \times U$, and therefore $N_G(\mathrm{Ker}(\varphi)) = N_G(K)$. Since $C_G(n)$ acts transitively on the set of cyclic groups of order $p$ in $N_p$ (by Proposition 7.5 (7)), and $N_G(\mathrm{Ker}(\varphi))$ is the stabiliser in $G$ of one of these cyclic groups of order $p$ (namely $K$), it follows that $[C_G(n) : C_G(n) \cap N_G(\mathrm{Ker}(\varphi))]$ is equal to the number of cyclic subgroups of order $p$ of $N_p$, which is $p+1$. By the regularity asserted in Proposition 7.5 (5) $[G : C_G(n)] = [G : C_G(N_q)] = q^2 - 1$. Therefore

$$\begin{aligned}[C_G(n) \cap N_G(\mathrm{Ker}(\varphi)) : N] &= \frac{[G:N]}{[G : C_G(n)] \cdot [C_G(n) : C_G(n) \cap \mathrm{Ker}(\varphi)]} \\ &= \frac{(p^2-1)\cdot(q^2-1)}{d} \cdot \frac{1}{q^2-1} \cdot \frac{1}{p+1} = \frac{p-1}{d}\end{aligned}$$

By Proposition 7.5 (7) we can also find a $g \in G$ such that $K^g = (\mathbb{F}_p, 0)$. So

$$\begin{aligned}\mu(\varphi, n) &= \frac{d}{p-1} \cdot \sum_{m^{C_G(n)}, m \in N_p} \left| m^{C_G(n)} \cap K \right| \cdot \varepsilon_{(n\cdot m)^G} \\ &= \frac{d}{p-1} \cdot \sum_{i=0}^{d-1} \left| (\alpha^i, 0)^{\langle a \rangle} \cap (\mathbb{F}_p, 0) \right| \cdot \varepsilon_{(\alpha^i,1)^G} = \frac{d}{p-1} \cdot \sum_{i=0}^{d-1} \frac{p-1}{d} \cdot \varepsilon_{(\alpha^i,1)^G} = 1\end{aligned}$$

where we used (12) to compute the cardinalities. This settles the case $m_0 \in K$.

Finally assume $m_0 \notin K$. Since $C_G(n)$ acts semiregularly on the non-trivial cosets of cyclic groups of order $p$ in $N_p$ and $N_G(\mathrm{Ker}(\varphi))$ fixes the coset $m_0 \cdot K$ we have $C_G(n) \cap N_G(\mathrm{Ker}(\varphi)) = N$. It follows that $\mu(\varphi, n) = (\varphi_0, \xi_n)$. We may again choose a $g \in G$ such that $(m_0 \cdot K)^g = (\alpha + \mathbb{F}_p, 0)$, and we can define $\ell(g)$ as before. Hence

$$\begin{aligned}(\varphi_0, \xi_n) &= \sum_{m^{C_G(n)}, m \in N_p} \left| m^{C_G(n)} \cap (m_0 \cdot K) \right| \cdot \varepsilon_{(m\cdot n)^G} \\ &= \sum_{i=0}^{d-1} \left| (\alpha^i, 0)^{\langle a \rangle} \cap (m_0 \cdot K) \right| \cdot \varepsilon_{(\alpha^i,1)^G} = \sum_{i=0}^{d-1} \left| (\alpha^{i+\ell(g)}, 0)^{\langle a \rangle} \cap (\alpha + \mathbb{F}_p, 0) \right| \cdot \varepsilon_{(\alpha^i,1)^G} \\ &= r_{\ell(g)} \cdot \varepsilon_{(1,1)^G} + r_{\ell(g)+1} \cdot \varepsilon_{(\alpha,1)^G} + \ldots + r_{\ell(g)+d-1} \cdot \varepsilon_{(\alpha^{d-1},1)^G}\end{aligned}$$

as claimed. □

*Proof of Theorem 7.2.* First we need to check that $\varepsilon$ satisfies the conditions of Theorem 5.1, that is, **(C.1)**-**(C.3)**.

(1) Condition **(C.1)** is satisfied by definition of $\varepsilon$.
(2) Condition **(C.2)** is satisfied by Proposition 7.5 (1).
(3) Condition **(C.3)** holds by Lemma 7.8.

This furnishes us with a unit of order $p \cdot q$ in $\mathcal{U}(\mathbb{Z}_\pi G)$ having the desired partial augmentations. Now let us check the conditions of Theorem 6.2, that is, **(C.4)** and **(C.5)**.

(1) We need to show that $G$ does not have an epimorphic image isomorphic to one of the groups in the list given in Theorem 6.2. Since all groups in that list are non-commutative subgroups of the real quaternions they all have an irreducible complex character of degree two. It follows from Proposition 7.6 that the degrees of the irreducible characters of $G$ are

$$\left\{1,\ p^2-1,\ q^2-1,\ \frac{(p^2-1)\cdot(q^2-1)}{d}\right\}$$

All of these numbers, except for 1, are greater than or equal to $2^2 - 1 = 3$, so clearly $G$ cannot surject onto a group which has an irreducible complex character of degree two.

(2) We need to check that $(\chi, \varphi \otimes 1_U) \neq 0$ for all $\varphi \in \mathrm{Irr}_{\mathbb{C}}(G)$, where $U$ is cyclic group of order $p \cdot q$ and $\chi$ is obtained from $\varepsilon$ via formula (3). This follows by Proposition 7.7.

This yields a unit $u \in \mathcal{U}(\mathbb{Z}G)$, which also has partial augmentations given by $\varepsilon$. It follows immediately from the double action formalism (Propositions 2.2 and 2.3) that if $\varepsilon$ is non-vanishing on more than one conjugacy class, then $u$ is not conjugate in $\mathcal{U}(\mathbb{Q}G)$ to an element of the form $\pm g$ for $g \in G$. □

*Proof of Theorem A.* Set $G = G(7, 19; 3; \alpha, \beta)$, where $\alpha$ is a root of the polynomial $X^2 - X + 3$ over $\mathbb{F}_7$ and $\beta$ is a root of $X^2 - X + 2$ over $\mathbb{F}_{19}$. Let $U = \langle c \rangle$ be a cyclic group of order $7 \cdot 19$. Note that representatives of the conjugacy classes of elements of order $7 \cdot 19$ in $G$ are given by $(1,1)$, $(1,\beta)$, $(1,\beta^2)$, or, alternatively, $(1,1)$, $(\alpha,1)$, $(\alpha^2,1)$. We will need to use both systems of representatives, and to avoid confusion we should note that $(1,\beta)$ is conjugate to $(\alpha^2,1)$ since $(1,\beta)^{c^{-1}\cdot a} = (\alpha^{-1},1)^a = (\alpha^2,1)$.

Define a class function $\varepsilon : G \to \mathbb{Z}$ vanishing everywhere except on the conjugacy classes of $(1,1)$ and $(1,\beta^2)$. Let the values of $\varepsilon$ on these two classes be given by

$$\varepsilon_{(1,1)^G} = 2 \quad \text{and} \quad \varepsilon_{(1,\beta^2)^G} = -1$$

All we have to do now is check that $\varepsilon$ satisfies the inequalities (8) and (9). Theorem 7.2 then shows that this $G$ does indeed constitute a counterexample to the Zassenhaus conjecture.

First assume that $n = (0,1) \in N_{19}$. As in Notation 7.1 set $K_7 = (\alpha + \mathbb{F}_7, 0)$. For $1 \leq i \leq 3$ define

$$A_i = \left\{ 1 \leq t \leq \frac{p^2-1}{d} \;\middle|\; (\alpha^{i+3\cdot t}, 0) \in K_7 \right\}$$

That is, $|A_i| = r_i(7)$. Denote by $\mathrm{Nr}$ the usual Galois norm of $\mathbb{F}_{7^2}$ over $\mathbb{F}_7$. Then for $x \in \mathbb{F}_7$ we have

$$\mathrm{Nr}(\alpha + x) = x^2 + (\alpha + \alpha^p)x + \alpha^{p+1} = x^2 + x + 3$$

where the last equality follows from the fact that $\alpha^p + \alpha$ is the trace of $\alpha$ over $\mathbb{F}_7$ and $\alpha^{p+1}$ its norm. Those are just the coefficients occurring in the minimal polynomial of $\alpha$, where the trace is taken negatively. We have $\mathrm{Nr}(\alpha^{i+3\cdot t}) = (\alpha^{p+1})^{i+3\cdot t} = 3^{i+3\cdot t} = (-1)^t \cdot 3^i$. So $\alpha + x \in A_i$ if and only if $\mathrm{Nr}(\alpha + x) \in \{\pm 3^i\}$. Computing these norms for every $x \in \mathbb{F}_7$ we get the values in Table 1. We conclude $r_1(7) = 2$, $r_2(7) = 4$ and $r_3(7) = 1$. The inequalities (8) from Theorem 7.2,

TABLE 1. Computation of $A_i$ for $\mathbb{F}_7$

| $x \in \mathbb{F}_7$: | 0 | 1 | 2 | 3 | $-3$ | $-2$ | $-1$ |
|---|---|---|---|---|---|---|---|
| $\mathrm{Nr}(\alpha + x)$: | 3 | $-2$ | 2 | 1 | 2 | $-2$ | 3 |
| $i$ such that $\alpha + x \in A_i$: | 1 | 2 | 2 | 3 | 2 | 2 | 1 |

written in matrix form, now read as follows

$$\begin{pmatrix} 2 & 4 & 1 \\ 4 & 1 & 2 \\ 1 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} \varepsilon_{(\alpha,1)^G} \\ \varepsilon_{(\alpha^2,1)^G} \\ \varepsilon_{(1,1)^G} \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 \\ 4 & 1 & 2 \\ 1 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} \geq 0$$

and they clearly hold.

Now let $n = (1,0) \in N_7$. We will argue similarly as above. Let $\mathrm{Nr}$ be the norm of $\mathbb{F}_{19^2}$ over $\mathbb{F}_{19}$. Define subsets $A_1, A_2, A_3 \subseteq K_{19}$ as before. Then for $x \in \mathbb{F}_{19}$ we have $\mathrm{Nr}(\beta + x) = x^2 + x + 2$. Moreover $\mathrm{Nr}(\beta^{i+3\cdot t}) = 2^{i+3\cdot t}$, so

$$\mathrm{Nr}(A_i) \subseteq \{8^t \cdot 2^i \mid 1 \leq t \leq 6\} = \{2^i, 8\cdot 2^i, 7\cdot 2^i, -1\cdot 2^i, -8\cdot 2^i, -7\cdot 2^i\}$$

Hence

$$\mathrm{Nr}(A_1) \subseteq \{2, -3, -5, -2, 3, 5\}$$
$$\mathrm{Nr}(A_2) \subseteq \{4, -6, 9, -4, 6, -9\}$$
$$\mathrm{Nr}(A_3) \subseteq \{8, 7, -1, -8, -7, 1\}$$

Computing the norms of elements in $\beta + \mathbb{F}_{19}$ we obtain the values in Table 2. So $r_1(19) = 9$,

TABLE 2. Computation of $A_i$ for $\mathbb{F}_{19}$

| $x \in \mathbb{F}_{19}$: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | −9 | −8 | −7 | −6 | −5 | −4 | −3 | −2 | −1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{Nr}(\alpha + x)$: | 2 | 4 | 8 | −5 | 3 | −6 | 6 | 1 | −2 | −3 | −2 | 1 | 6 | −6 | 3 | −5 | 8 | 4 | 2 |
| $i$ such that $\alpha + x \in A_i$: | 1 | 2 | 3 | 1 | 1 | 2 | 2 | 3 | 1 | 1 | 1 | 3 | 2 | 2 | 1 | 1 | 3 | 2 | 1 |

$r_2(19) = 6$ and $r_3(19) = 4$. Hence the inequalities (9) from Theorem 7.2, written in matrix form, are

$$\begin{pmatrix} 9 & 6 & 4 \\ 6 & 4 & 9 \\ 4 & 9 & 6 \end{pmatrix} \cdot \begin{pmatrix} \varepsilon_{(1,\beta)^G} \\ \varepsilon_{(1,\beta^2)^G} \\ \varepsilon_{(1,1)^G} \end{pmatrix} = \begin{pmatrix} 9 & 6 & 4 \\ 6 & 4 & 9 \\ 4 & 9 & 6 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -1 \\ 2 \end{pmatrix} \geq 0$$

and these also hold. This completes the proof, as all of our assertions now follow from Theorem 7.2. □

**Remark 7.9.** Theorems A and B assert the existence of certain units $u \in \mathcal{U}(\mathbb{Z}G)$ for $G = G(p, q; d; \alpha, \beta)$. To do this we prove the existence of a double action module with the appropriate character. Describing the double action module ${}_u(\mathbb{Z}G)_G$ and the unit $u$ explicitly would be difficult, but in principle even this could be done. However, due to the size of $G$, this might not be feasible in practice and there is no guarantee that the resulting description would be "nice".

By contrast, the construction of the $p$-local double action modules ${}_u(\mathbb{Z}_{(p)}G)_G$ for arbitrary prime numbers $p$ is perfectly explicit. We will do this in Proposition 7.11 below for the situation described in Theorem A. The lattices constructed in Proposition 7.11 become projective upon restriction to $G$ by definition, and one can use Remark 5.6 to compute their characters (on a computer rather than by hand). One can then go on to verify the conditions of Theorems 5.1 and 6.2 directly, avoiding the various technical lemmas and cumbersome computations of this section.

**Lemma 7.10.** *Let $G = G(p, q; d; \alpha, \beta)$, $U = \langle c \rangle$ a cyclic group of order $p \cdot q$ and $n = (0, 1) \in N_q$. Then representatives for the elements of $\mathrm{Irr}_{\mathbb{Q}}(N_p \times U_p)/C_G(n)$ are given by*

*(1) The trivial character*
*(2) A character whose kernel equals $N_p$*
*(3) A non-trivial character whose kernel contains $U_p$*
*(4) For every $0 \leq i \leq d-1$ a non-trivial character $\varphi_i$ whose kernel is*

$$\langle ((1,0),1), (\alpha^{i\cdot(p+1)} \cdot \alpha, 0), c_p) \rangle$$

*Proof.* A rational character $\varphi$ of $N_p \times U_p$, an elementary-abelian group of rank three, is determined by its kernel. The kernel can be the whole group, which happens if and only if $\varphi$ is the trivial character, or an elementary abelian group of rank two. There are $\frac{p^3-1}{p-1} = p^2+p+1$ cyclic groups of order $p$ in $N_p \times U_p$ and as many subgroups of order $p^2$ by duality. Clearly $N_p$ is a subgroup invariant under the action of $C_G(n) = \langle a \rangle$. Furthermore $C_G(n)$ acts transitively on the cyclic subgroups of $N_p$ by Proposition 7.5 (7) and therefore also on the groups of the form $\langle m \rangle \times U_p$ with $m$ a non-trivial element of $N_p$. All rational characters which have any of these groups as their kernel are therefore conjugate under the action of $C_G(n)$.

Since the number of cyclic subgroups of $N_p$ is equal to $p+1$ this leaves $p^2+p+1-1-(p+1) = p^2-1$ possible kernels of irreducible characters. Such a kernel is generated by an element $m$ in $N_p$ and an element of the form $(m_0, c)$ with $m_0$ a non-trivial element in $N_p$ such that $m_0 \notin \langle m \rangle$. Hence this kernel is determined by the non-trivial coset $m_0 \cdot \langle m \rangle$. By Proposition 7.5 (6) the group $C_A(n)$ acts semiregularly on these cosets, and since $a$ has order $\frac{p^2-1}{d}$ the action of $C_A(n)$ partitions the remaining possible kernels into $d$ orbits.

It remains to show that cosets of the form $(\alpha^{i\cdot(p+1)} \cdot \alpha + \mathbb{F}_p, 0)$ and $(\alpha^{j\cdot(p+1)} \cdot \alpha + \mathbb{F}_p, 0)$ are not $C_G(n)$-conjugate for any $0 \leq i, j \leq d-1$ with $i \neq j$. If $x \in G$ is an element conjugating $(\alpha^{i\cdot(p+1)} \cdot \alpha + \mathbb{F}_p, 0)$ into $(\alpha^{j\cdot(p+1)} \cdot \alpha + \mathbb{F}_p, 0)$ then $x$ stabilises $(\mathbb{F}_p, 0)$ and hence corresponds to multiplication by an element in $\mathbb{F}_p^\times$. The subgroup of $\langle a \rangle$ acting by multiplication by elements of $\mathbb{F}_p^\times$ is generated by $a^{p+1}$, since $a$ acts by multiplication by $\alpha^d$, $\mathbb{F}_p^\times = \langle \alpha^{p+1} \rangle$ and $\gcd(d, p+1) = 1$ by assumption. But $a^{p+1}$ acts by multiplication by $\alpha^{(p+1)\cdot d}$, so an $x$ lying in the group generated by $a^{p+1}$ could not possibly conjugate $(\alpha^{i\cdot(p+1)} \cdot \alpha + \mathbb{F}_p, 0)$ into $(\alpha^{j\cdot(p+1)} \cdot \alpha + \mathbb{F}_p, 0)$. □

**Proposition 7.11.** *Assume we are in the situation of Theorem A. Let $q$ be a prime different from 19. Then the $\mathbb{Z}_{(q)}(G \times U)$-lattice*

$$\begin{aligned} L(19,q) \;=\;& M([(1,0)]_7 \times N_{19} \times U_{19}, 7, q) \\ \oplus\;& M([(1,0)]_7 \times \langle ((0,1),1), ((0,0), c_{19}) \rangle, 7, q) \\ \oplus\;& M([(1,0)]_7 \times \langle ((0,1),1), ((0,\beta), c_{19}) \rangle, 7, q)^{\oplus 2} \\ \oplus\;& M([(1,0)]_7 \times \langle ((0,1),1), ((0,2\beta), c_{19}) \rangle, 7, q)^{\oplus 14} \\ \oplus\;& M([(1,0)]_7 \times \langle ((0,1),1), ((0,4\beta), c_{19}) \rangle, 7, q)^{\oplus 3} \end{aligned}$$

*is $G$-regular with character $\chi$ as defined in formula (3). Here the $M(X,p,q)$ are as defined in Definition 5.4.*

*In the same vein, if $q$ is a prime different from 7, then the $\mathbb{Z}_{(q)}(G \times U)$-lattice*

$$\begin{aligned} L(7,q) \;=\;& M([(0,1)]_{19} \times N_7 \times U_7, 19, q) \\ \oplus\;& M([(0,1)]_{19} \times \langle ((1,0),1), ((0,0), c_7) \rangle, 19, q) \\ \oplus\;& M([(0,1)]_{19} \times \langle ((1,0),1), ((9\alpha,0), c_7) \rangle, 19, q)^{\oplus 7} \end{aligned}$$

*is $G$-regular with character $\chi$.*

*Proof.* By Lemma 5.8 we have $G$-regular lattices

$$L(7,q) = \bigoplus_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_7 \times U_7)^{C_G((0,1))}} M([(0,1)]_{19} \times \mathrm{Ker}(\varphi), 19, q)^{\oplus \mu(\varphi, (0,1))}$$

and

$$L(19,q) = \bigoplus_{\varphi \in \mathrm{Irr}_{\mathbb{Q}}(N_{19} \times U_{19})^{C_G((1,0))}} M([(1,0)]_7 \times \mathrm{Ker}(\varphi), 7, q)^{\oplus \mu(\varphi, (1,0))}$$

both of which have character $\chi$. We just need to verify that these coincide with the definition of $L(7,q)$ and $L(19,q)$ made in the statement of the proposition. The $\varphi$ over which these direct

sums range were described in Lemma 7.10 and the $\mu(\varphi,(1,0))$ and $\mu(\varphi,(0,1))$ can be computed using their definition in Lemma 7.8. We will now do this explicitly.

By Lemma 7.10 there are $3+d=6$ elements in $\mathrm{Irr}_{\mathbb{Q}}(N_7\times U_7)/C_G((0,1))$ and $\mathrm{Irr}_{\mathbb{Q}}(N_{19}\times U_{19})/C_G((1,0))$. For $p\in\{7,19\}$ define the following characters of $N_p\times U_p$, which are representatives of the classes of interest: $1_p$ is the trivial character, $\eta_p$ a non-trivial character with kernel $N_p$, $\psi_p$ a non-trivial character such that $U_p$ is in the kernel of $\psi_p$ and $\varphi_{p,i}$ a non-trivial character such that the kernel of $\varphi_{p,i}$ is $\langle((1,0),1),((\alpha^{8\cdot i}\cdot\alpha,0),c_7)\rangle$ and $\langle((0,1),1),((0,\beta^{20\cdot i}\cdot\beta),c_{19})\rangle$ respectively, where $0\leq i\leq 2$. This shows that the kernels of the various $\varphi$'s are as claimed, and it remains to compute the $\mu(\varphi,n)$'s.

For convenience let $n=(0,1)$ for $p=7$ and $n=(1,0)$ for $p=19$. Then by Lemma 7.8 we know $\mu(1_p,n)=1$, $\mu(\eta_p,n)=0$ and $\mu(\psi_p,n)=1$, for either $p$. Recall that $\alpha^8=3$ and $\beta^{20}=2$. By Lemma 7.8 we need to determine elements $g_1,g_2,h_1,h_2\in G$ such that

$$(3\alpha+\mathbb{F}_7)^{g_1}=\alpha+\mathbb{F}_7,(9\alpha+\mathbb{F}_7)^{g_2}=\alpha+\mathbb{F}_7,(2\beta+\mathbb{F}_{19})^{h_1}=\beta+\mathbb{F}_{19}\text{ and }(4\beta+\mathbb{F}_{19})^{h_2}=\beta+\mathbb{F}_{19}.$$

Since all of these elements must stabilise $\mathbb{F}_7$ or $\mathbb{F}_{19}$, respectively, we get $g_1,g_2\in\langle c^8\rangle$ (the subgroup of $\langle c\rangle$ corresponding to multiplication by elements of $\mathbb{F}_7^\times$) and $h_1,h_2\in\langle c^{20}\rangle$. Now $c^8$ acts as $\alpha^8=3$ on $N_7$ and $c^{20}$ acts as $\beta^{20}=2$ on $\mathbb{F}_{19}$. We have the following congruences:

$$3\cdot 3^5\equiv 9\cdot 3^4\equiv 1 \bmod 7 \text{ and } 2\cdot 2^{17}\equiv 4\cdot 2^{16}\equiv 1 \bmod 19.$$

So we can choose $g_1=c^{5\cdot 8}$, $g_2=c^{4\cdot 8}$, $h_1=c^{17\cdot 20}$ and $h_2=c^{16\cdot 20}$. This gives

$$(1,0)^{g_1}=(\alpha^{40},0),(1,0)^{g_2}=(\alpha^{32},0),(0,1)^{h_1}=(0,\beta^{340})\text{ and }(0,1)^{h_2}=(0,\beta^{320},0)$$

In the notation of Lemma 7.8 we get

$$\begin{array}{rcl}\ell(g_1)&=&40\equiv 1 \bmod 3\\ \ell(g_2)&=&32\equiv 2 \bmod 3\\ \ell(h_1)&=&340\equiv 1 \bmod 3\\ \ell(h_2)&=&320\equiv 2 \bmod 3\end{array}$$

Note that $\ell(1)=0$. So by Lemma 7.8 we obtain

$$\begin{pmatrix}\mu(\varphi_{7,0},n)\\ \mu(\varphi_{7,1},n)\\ \mu(\varphi_{7,2},n)\end{pmatrix}=\begin{pmatrix}r_3(7)&r_1(7)&r_2(7)\\ r_1(7)&r_2(7)&r_3(7)\\ r_2(7)&r_3(7)&r_1(7)\end{pmatrix}\begin{pmatrix}\varepsilon_{(1,1)^G}\\ \varepsilon_{(\alpha,1)^G}\\ \varepsilon_{(\alpha^2,1)^G}\end{pmatrix}=\begin{pmatrix}1&2&4\\ 2&4&1\\ 4&1&2\end{pmatrix}\begin{pmatrix}2\\ -1\\ 0\end{pmatrix}=\begin{pmatrix}0\\ 0\\ 7\end{pmatrix}$$

and

$$\begin{pmatrix}\mu(\varphi_{19,0},n)\\ \mu(\varphi_{19,1},n)\\ \mu(\varphi_{19,2},n)\end{pmatrix}=\begin{pmatrix}r_3(19)&r_1(19)&r_2(19)\\ r_1(19)&r_2(19)&r_3(19)\\ r_2(19)&r_3(19)&r_1(19)\end{pmatrix}\begin{pmatrix}\varepsilon_{(1,1)^G}\\ \varepsilon_{(1,\beta)^G}\\ \varepsilon_{(1,\beta^2)^G}\end{pmatrix}=\begin{pmatrix}4&9&6\\ 9&6&4\\ 6&4&9\end{pmatrix}\begin{pmatrix}2\\ 0\\ -1\end{pmatrix}=\begin{pmatrix}2\\ 14\\ 3\end{pmatrix}$$

This shows that the $\mu(\varphi,n)$'s are as claimed, which concludes the proof. □

## ACKNOWLEDGEMENTS

We would like to thank Á. del Río, whose research helped pave the way for this counterexample. We would also like to express our gratitude to Rob who helped start this collaboration.

## REFERENCES


[AH80] P. J. Allen and C. Hobby. A characterization of units in $\mathbf{Z}[A_4]$. *J. Algebra*, 66(2):534–543, 1980.

[BH08] V. Bovdi and M. Hertweck. Zassenhaus conjecture for central extensions of $S_5$. *J. Group Theory*, 11(1):63–74, 2008.

[BHK04] V. Bovdi, C. Höfert, and W. Kimmerle. On the first Zassenhaus conjecture for integral group rings. *Publ. Math. Debrecen*, 65(3-4):291–303, 2004.

[BHK+17] A. Bächle, A. Herman, A. Konovalov, L. Margolis, and G. Singh. The status of the Zassenhaus conjecture for small groups. *Experimental Mathematics*, page 6 pages, 2017. doi:10.1080/10586458.2017.1306814.

[BKM16] A. Bächle, W. Kimmerle, and L. Margolis. Algorithmic aspects of units in group rings. *to be published in a proceedings volume of the DFG priority program 1489, arxiv.org/abs/1612.06171*, page 21, 2016.

[BM16] A. Bächle and L. Margolis. On the Prime Graph Question for Integral Group Rings of 4-primary groups II. *preprint, arxiv.org/abs/1606.01506*, page 17 pages, 2016.

[BM17] A. Bächle and L. Margolis. Rational conjugacy of torsion units in integral group rings of non-solvable groups. *Proc. Edinb. Math. Soc. (2)*, page 22 pages, 2017. doi:10.1017/S0013091516000535.

[CMR13] M. Caicedo, L. Margolis, and Á. del Río. Zassenhaus conjecture for cyclic-by-abelian groups. *J. Lond. Math. Soc. (2)*, 88(1):65–78, 2013.

[CR81] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1981.

[CR87] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. II*. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1987.

[CW00] G. Cliff and A. Weiss. Finite groups of matrices over group rings. *Trans. Amer. Math. Soc.*, 352(1):457–475, 2000.

[Dad71] E. C. Dade. Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps. *Math. Z.*, 119:345–348, 1971.

[DJ96] M. A. Dokuchaev and S. O. Juriaans. Finite subgroups in integral group rings. *Canad. J. Math.*, 48(6):1170–1179, 1996.

[DJPM97] M. A. Dokuchaev, S. O. Juriaans, and C. Polcino Milies. Integral group rings of Frobenius groups and the conjectures of H. J. Zassenhaus. *Comm. Algebra*, 25(7):2311–2325, 1997.

[Fer87] N. A. Fernandes. Torsion units in the integral group ring of $S_4$. *Bol. Soc. Brasil. Mat.*, 18(1):1–10, 1987.

[Frö75] A. Fröhlich. Locally free modules over arithmetic orders. *J. Reine Angew. Math.*, 274/275:112–124, 1975.

[Gil13] J. Gildea. Zassenhaus conjecture for integral group ring of simple linear groups. *J. Algebra Appl.*, 12(6):1350016, 10, 2013.

[Her04] M. Hertweck. Contributions to the integral representation theory of groups. Habilitationsschrift, Universität Stuttgart, 2004.

[Her06] M. Hertweck. On the torsion units of some integral group rings. *Algebra Colloq.*, 13(2):329–348, 2006.

[Her07] M. Hertweck. Partial augmentations and Brauer character values of torsion units in group rings. arXiv:0612429v2 [math.RA], 2004 - 2007.

[Her08a] M. Hertweck. Torsion units in integral group rings of certain metabelian groups. *Proc. Edinb. Math. Soc. (2)*, 51(2):363–385, 2008.

[Her08b] M. Hertweck. Zassenhaus conjecture for $A_6$. *Proc. Indian Acad. Sci. Math. Sci.*, 118(2):189–195, 2008.

[HK06] C. Höfert and W. Kimmerle. On torsion units of integral group rings of groups of small order. In *Groups, rings and group rings*, volume 248 of *Lect. Notes Pure Appl. Math.*, pages 243–252. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[HP72] I. Hughes and K. R. Pearson. The group of units of the integral group ring $ZS_3$. *Canad. Math. Bull.*, 15:529–534, 1972.

[HS15] A. Herman and G. Singh. Revisiting the Zassenhaus conjecture on torsion units for the integral group rings of small groups. *Proc. Indian Acad. Sci. Math. Sci.*, 125(2):167–172, 2015.

[JPM00] S. O. Juriaans and C. Polcino Milies. Units of integral group rings of Frobenius groups. *J. Group Theory*, 3(3):277–284, 2000.

[JR16] E. Jespers and Á. del Río. *Group ring groups. Volume 1: Orders and generic constructions of units*. Berlin: De Gruyter, 2016.

[KK17] W. Kimmerle and A. Konovalov. On the Gruenberg-Kegel graph of integral group rings of finite groups. *Internat. J. Algebra Comput.*, 27(6):619–631, 2017.

[Kli91] L. Klingler. Construction of a counterexample to a conjecture of Zassenhaus. *Comm. Algebra*, 19(8):2303–2330, 1991.

[LB83] I. S. Luthar and A. K. Bhandari. Torsion units of integral group rings of metacyclic groups. *J. Number Theory*, 17(2):270–283, 1983.

[LN97] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[LP89] I. S. Luthar and I. B. S. Passi. Zassenhaus conjecture for $A_5$. *Proc. Indian Acad. Sci. Math. Sci.*, 99(1):1–5, 1989.

[LP92] I. S. Luthar and I. B. S. Passi. Torsion units in matrix group rings. *Comm. Algebra*, 20(4):1223–1228, 1992.

[LS98] I. S. Luthar and P. Sehgal. Torsion units in integral group rings of some metacyclic groups. *Res. Bull. Panjab Univ. Sci.*, 48(1-4):137–153 (1999), 1998.

[LT90] I. S. Luthar and P. Trama. Zassenhaus conjecture for certain integral group rings. *J. Indian Math. Soc. (N.S.)*, 55(1-4):199–212, 1990.

[LT91] I. S. Luthar and P. Trama. Zassenhaus conjecture for $S_5$. *Comm. Algebra*, 19(8):2353–2362, 1991.

[Mit86] T. Mitsuda. On the torsion units of integral dihedral group rings. *Comm. Algebra*, 14(9):1707–1728, 1986.

[MR17a] L. Margolis and Á. del Río. An algorithm to attack a problem of Sehgal on torsion units of integral group rings. *preprint, arxiv.org/abs/1710.05629*, page 21 pages, 2017.

[MR17b] L. Margolis and Á. del Río. Cliff-Weiss inequalities and the Zassenhaus Conjecture. *preprint, arxiv.org/abs/1706.02483*, page 21 pages, 2017.

[MR17c] L. Margolis and Á. del Río. Partial augmentations power property: A Zassenhaus Conjecture related problem. *preprint, arxiv.org/abs/1706.04787*, page 13 pages, 2017.

[MRS16] L. Margolis, Á. del Río, and M. Serrano. Zassenhaus conjecture on torsion units holds for $\mathrm{PSL}(2,p)$ with $p$ a Fermat or Mersenne prime. *preprint, arxiv.org/abs/arXiv:1608.05797*, page 32 pages, 2016.

[MRSW87] Z. Marciniak, J. Ritter, S. K. Sehgal, and A. Weiss. Torsion units in integral group rings of some metabelian groups II. *J. Number Theory*, 25(3):340–352, 1987.

[PM73] C. Polcino Milies. The group of units of the integral group ring $\mathbf{Z}D_4$. *Bol. Soc. Brasil. Mat.*, 4(2):85–92, 1973.

[PMRS86] C. Polcino Milies, J. Ritter, and S. K. Sehgal. On a conjecture of Zassenhaus on torsion units in integral group rings. II. *Proc. Amer. Math. Soc.*, 97(2):201–206, 1986.

[PMS84] C. Polcino Milies and S. K. Sehgal. Torsion units in integral group rings of metacyclic groups. *J. Number Theory*, 19(1):103–114, 1984.

[Rei75] I. Reiner. *Maximal Orders*. Academic Press Inc., 1975.

[RS83] J. Ritter and S. K. Sehgal. On a conjecture of Zassenhaus on torsion units in integral group rings. *Math. Ann.*, 264(2):257–270, 1983.

[RS06] Á. del Río and S. K. Sehgal. Zassenhaus conjecture (ZC1) on torsion units of integral group rings for some metabelian groups. *Arch. Math. (Basel)*, 86(5):392–397, 2006.

[Sco92] L. L. Scott. On a conjecture of Zassenhaus, and beyond. In *Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989)*, volume 131 of *Contemp. Math.*, pages 325–343. Amer. Math. Soc., Providence, RI, 1992.

[Seh93] S. K. Sehgal. *Units in integral group rings*, volume 69 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993. With an appendix by Al Weiss.

[SW86] S. K. Sehgal and A. Weiss. Torsion units in integral group rings of some metabelian groups. *J. Algebra*, 103(2):490–499, 1986.

[Wei88] A. Weiss. Rigidity of $p$-adic $p$-torsion. *Ann. of Math. (2)*, 127(2):317–332, 1988.

[Wei91] A. Weiss. Torsion units in integral group rings. *J. Reine Angew. Math.*, 415:175–187, 1991.

[Whi68] A. Whitcomb. *The group ring problem*. ProQuest LLC, Ann Arbor, MI, 1968. Thesis (Ph.D.)–The University of Chicago.

[Zas74] H. J. Zassenhaus. On the torsion units of finite group rings. In *Studies in mathematics (in honor of A. Almeida Costa) (Portuguese)*, pages 119–126. Instituto de Alta Cultura, Lisbon, 1974.

Florian Eisele
Department of Mathematics, City, University of London, Northampton Square, London EC1V 0HB, United Kingdom
E-mail address: Florian.Eisele@city.ac.uk

Leo Margolis
Departamento de Matemàticas, Universidad de Murcia, 30100 Murcia, Spain
E-mail address: leo.margolis@um.es