TORSION UNITS IN INTEGRAL GROUP RINGS

ÁNGEL DEL RÍO

Abstract. We revise some problems on the study of finite subgroups of the group of units of integral group rings of finite groups and some techniques to attack them.

The study of the group of units $\mathcal{U}(\mathbb{Z}G)$ of the integral group ring of a finite group G was started by Higman in [Hig40] (see also [San81]) and has been an active subject of research since. Two basics references for this topic are the book of Sehgal [Seh93] and the two volumes book by Jespers and the author [JdR15a, JdR15b]. The aim of this note is to introduce the reader to the investigation of the finite subgroups of $\mathcal{U}(\mathbb{Z}G)$ and, in particular, of the torsion units in $\mathbb{Z}G$. For a more advanced and updated treatment of the topic see [MdR19].

1. Basic notation

All throughout G is a finite group, denoted multiplicatively, and $Z(G)$ denotes the center of G. The order of a set X is denoted $|X|$. We also use $|g|$ to denote the order of a torsion group element g, i.e. g has finite order.

Every ring R is assumed to have an identity and its center and group of units are denoted $Z(R)$ and $\mathcal{U}(R)$, respectively. If n is a positive integer then $M_n(R)$ denotes the ring of $n \times n$ matrices with entries in R and $\mathrm{GL}_n(R) = \mathcal{U}(M_n(R))$, the group of units of $M_n(R)$. If M is an R-module then $\mathrm{End}_R(M)$ denotes the ring of endomorphisms of M and $\mathrm{Aut}_R(M)$ denotes the group of automorphisms of M. If M is free of rank n then there is a natural isomorphism $\mathrm{End}_R(M) \to M_n(R)$ associating every homomorphism with its expression in a fixed basis, which restricts to a group isomorphism $\mathrm{Aut}_R(M) \to \mathrm{GL}_n(R)$. We will use these isomorphisms freely to identify endomorphisms and matrices.

The group ring of G with coefficients in R is denoted RG. It contains R as a subring an its group of units contains G as a subgroup which is also a basis of RG as a left R-module. Moreover the elements of R and G commute. The group ring is characterized by the following property, which we refer to as the *Universal Property of Group Rings*: For every ring homomorphism $f : R \to S$ and every group homomorphism $\phi : G \to \mathcal{U}(S)$ satisfying $f(r)\phi(g) = \phi(g)f(r)$ for every $r \in R$ and every $g \in G$ there is a unique ring homomorphism f' extending f and ϕ. In particular, if S is a ring containing R as subring then every group homomorphism $\phi : G \to \mathcal{U}(S)$ with image commuting with the elements of R extends uniquely to a ring homomorphism $RG \to S$, which we will also denote ϕ.

We will abuse slightly the notation so that any time that we write $r = \sum_{g\in G} r_g g \in RG$ we are implicitly assuming that each r_g belongs to R. The *support* of r is

$$\mathrm{Supp}(r) = \{g \in G : r_g \neq 0\}.$$

Partially supported by Ministerio de Economía y Competitividad project MTM2012-35240 and Fondos FEDER and Fundación Séneca of Murcia 04555/GERM/06.

2. The Berman-Higman Theorem

We start with a result with many consequences on the finite subgroups of $\mathcal{U}(\mathbb{Z}G)$.

Theorem 2.1 (Berman-Higman Theorem)**.** [Ber55, Hig40] *If $u = \sum_{g\in G} u_g g$ is a torsion unit of $\mathbb{Z}G$ then either $u = \pm 1$ or $u_1 = 0$.*

Proof. Consider the regular representation, i.e. the group homomorphism $G \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}G)$ associating $g \in G$ with the map $\rho(g) : x \mapsto gx$. Representing ρ_g in the basis G, we deduce that if $n = |G|$ then the trace of $\rho(1)$ is n and if $g \in G \setminus \{1\}$, then the trace of $\rho(g)$ is 0. Identifying $\mathrm{End}_{\mathbb{C}}(\mathbb{C}G)$ and $M_n(\mathbb{C})$ we have a group homomorphism $\rho : G \to \mathcal{U}(M_n(\mathbb{C})) = \mathrm{GL}_n(\mathbb{C})$. By the Universal Property of Group Rings, ρ extends to a $\mathbb{C}$-algebra homomorphism $\rho : \mathbb{C}G \to M_n(G)$.

Suppose that $u = \sum_{g\in G} u_g g$ is a torsion unit of $\mathbb{Z}G$, say of order m. By Problem 2a, $\rho(u)$ is diagonalizable and $|\mathrm{tr}(\rho(u))| \leq n$. As the trace map $\mathrm{tr} : M_n(\mathbb{C}) \to \mathbb{C}$ is $\mathbb{C}$-linear, we have $nu_1 = \sum_{g\in G} u_g \mathrm{tr}(\rho(g)) = \mathrm{tr}(\rho(u))$. Thus $n|u_1| = |\mathrm{tr}(\rho(u))| \leq n$. As u_1 is an integer either $u_1 = 0$ or $u_1 = \pm 1$. Moreover, by the second part of Problem 2a, in the second case $\rho(u)$ is a scalar matrix, i.e. $\rho(g) = aI$ for some complex root of unity a. But $nu_1 = na$, so that $\rho(u) = u_1 I = \pm I$. As ρ is an injective map we deduce that $u = \pm 1$, as desired. □

The most obvious torsion units of $\mathbb{Z}G$ are the elements of the form $\pm g$ with $g \in G$. They are called *trivial units* of $\mathbb{Z}G$.

As a consequence of the Berman-Higman Theorem (Theorem 2.1), one can describe all the torsion central units.

Corollary 2.2. *The torsion central units of $\mathbb{Z}G$ are the trivial units $\pm g$ with $g \in Z(G)$. In particular, if G is abelian then every finite subgroup of $\mathcal{U}(\mathbb{Z}G)$ is contained in $\pm G$.*

Proof. Let u be a torsion central unit of $\mathbb{Z}G$ and let $g \in \mathrm{Supp}(u)$. Then $v = ug^{-1}$ is a torsion unit with $1 \in \mathrm{Supp}(v)$. By Theorem 2.1, $v = \pm 1$, and so $u = \pm g$. □

The proof of Theorem 2.1 uses one of the main tools in the study of group rings, namely Representation Theory. Let R be a commutative ring and let M be a left RG-module. The map associating $g \in G$ to the R-endomorphism of M given by $m \mapsto gm$ is a group homomorphism $G \mapsto \mathrm{Aut}_R(M)$. Conversely, if M is an R-module then, by the Universal Property of Group Rings, every group homomorphism $G \to \mathrm{Aut}_R(M)$ extends to a ring homomorphism $RG \to \mathrm{End}_R(M)$ and this induces a structure of RG-module on M. Thus we can identify RG-modules with group homomorphism $G \to \mathrm{End}_R(M)$ with M an R-module.

An *R-representation* of G of *degree k* is a group homomorphism $\rho : G \to \mathrm{GL}_k(R)$. Our identification of $\mathrm{End}_R(R^k)$ and $M_k(R)$ allows to identify ρ with the RG-module whose underlying R-module is R^k and $gm = \rho(g)m$ for $g \in G$ and $m \in R^k$. The composition of ρ with the trace map $\mathrm{tr} : M_k(R) \to R$ is called *the character* afforded by ρ, or by the underlying RG-module. Observe that both ρ and the character afforded by ρ are R-linear maps defined not only on G but also on RG.

For example, the trivial map $G \to \mathcal{U}(R), g \mapsto 1$ is a character of degree 1 and its linear span to RG is called the *augmentation map*:

$$\begin{array}{rcl} \mathrm{aug}_G : RG & \to & R \\ \sum_{g\in G} r_g g & \mapsto & \sum_{g\in G} r_g. \end{array}$$

The kernel $\mathrm{Aug}(RG)$ of aug_G is called the *augmentation ideal* of RG. As the augmentation map is a ring homomorphism it restricts to a group homomorphism

$$\mathrm{aug}_G : \mathcal{U}(RG) \to \mathcal{U}(R).$$

The kernel of this group homomorphism is denoted $V(RG)$, i.e.

$$V(RG) = \{u \in \mathcal{U}(RG) : \mathrm{aug}_G(u) = 1\}^1.$$

The elements of $V(RG)$ are usually called *normalized units*. If R is commutative then $\mathcal{U}(RG) = \mathcal{U}(R) \times V(RG)$. In particular, $\mathcal{U}(\mathbb{Z}G) = \pm V(\mathbb{Z}G)$ and hence the study $\mathcal{U}(\mathbb{Z}G)$ and $V(\mathbb{Z}G)$ are equivalent.

More generally, if N is a normal subgroup of G then the natural map $G \to G/N \subseteq \mathcal{U}(R(G/N))$ extends linearly to a ring homomorphism

$$\begin{array}{rcl} \mathrm{aug}_{G,N} : RG & \to & R(G/N) \\ \sum_{g\in G} r_g g & \mapsto & \sum_{g\in G} r_g gN. \end{array}$$

We set $\mathrm{Aug}_N(RG) = \ker(\mathrm{aug}_{G,N})$. Furthermore, $V(RG, N)$ denotes the kernel of the restriction of $\mathrm{aug}_{G,N}$ to $\mathcal{U}(RG)$, considered as the homomorphism between the group of units of RG and $R(G/N)$ (see Problem 3).

One of the main questions on group rings is the so called Isomorphism Problem:

The Isomorphism Problem for group rings over a ring R: (ISO-R):

$$\text{Does } RG \cong RH \text{ imply } G \cong H?$$

(ISO) is an abbreviation of (ISO-$\mathbb{Z}$) and called the **Isomorphism Problem**. We say that (ISO) holds for a group G if and only if $\mathbb{Z}G$ is not isomorphic to $\mathbb{Z}H$ for every group H non-isomorphic to G.

Observe that $RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G$ and therefore if $\mathbb{Z}G \cong \mathbb{Z}H$ then $RG \cong RH$ for every ring R. Thus a negative solution for (ISO) is a negative solution for (ISO-R) for every ring R.

It is easy to find negative solutions for the Isomorphism Problem for group rings over the complex numbers using only abelian groups (see Problem 6). However this is not the case for $R = \mathbb{Z}$.

Corollary 2.3. *The Isomorphism Problem has a positive solution for finite abelian groups.*

Proof. Let G and H be finite groups and suppose that G is abelian and suppose that $\mathbb{Z}G$ and $\mathbb{Z}H$ are isomorphic. Then necessarily H is abelian (why?). By Problem 7 there is an isomorphism $f : \mathbb{Z}G \to \mathbb{Z}H$ which maps $V(\mathbb{Z}G)$ onto $V(\mathbb{Z}H)$. Moreover, by Corollary 2.2, the set of torsion units of $V(\mathbb{Z}G)$ and $V(\mathbb{Z}H)$ are G and H, respectively. Then f restricts to an isomorphism $f : G \to H$. □

Another consequence of the Berman-Higman Theorem is the following:

Corollary 2.4. *Every finite subgroup of $V(\mathbb{Z}G)$ is linearly independent over $\mathbb{Q}$ (equivalently, over $\mathbb{Z}$).*

[1]Some authors denote $V(RG)$ as $\mathcal{U}_1(RG)$

Proof. Let $H = \{u_1, \dots, u_n\}$ be a finite subgroup of $V(\mathbb{Z}G)$ and suppose that

$$c_1u_1 + \cdots + c_nu_n = 0$$

with $c_i \in \mathbb{Z}$. Then

$$c_1 + c_2u_2u_1^{-1} + \cdots + c_nu_nu_1^{-1} = 0$$

and each $u_iu_1^{-1}$, with $i = 2, \dots, n$ is a torsion element of $V(\mathbb{Z}G) \setminus \{1\}$. By the Berman-Higman Theorem (Theorem 2.1), $1 \notin \mathrm{Supp}(u_iu_1^{-1})$ for every $i \neq 1$ and therefore, comparing the coefficients of 1 in both sides of the previous equality, we deduce that $c_1 = 0$. This shows that each $c_i = 0$. □

An obvious consequence of Corollary 2.4 is that if H is a finite subgroup of $V(\mathbb{Z}G)$ then the subring $\mathbb{Z}[H]$ of $\mathbb{Z}G$ H is isomorphic to the group ring $\mathbb{Z}H$. Clearly H is a basis of $\mathbb{Q}[H]$ over $\mathbb{Q}$. Actually, it is also a basis of $\mathbb{Z}[H]$ over $\mathbb{Z}$ (see Problem 8). Using this one can prove that (ISO) holds for G if and only if all the subgroup of $V(\mathbb{Z}G)$ with the same order as G are isomorphic .

Using the same technique as for the proof of the Berman-Higman Theorem one can obtain the following:

Lemma 2.5. *Let K be a field extension of $\mathbb{Q}$ and let $e = \sum_{g\in G} e_g g \in KG$ with $e^2 = e \notin \{0, 1\}$. Then e_1 is a rational number in the interval $(0, 1)$.*

Proof. Let ρ be the regular representation of G and χ the character afforded by ρ. By Problem 2b, $\rho(e)$ is diagonalizable and all the eigenvalues of $\rho(e)$ are 0 or 1 and $\chi(e)$ is the multiplicity of 1 as eigenvalue of $\rho(e)$. As $e \notin \{0, 1\}$ and ρ is injective, $\chi(e) \in \{1, \dots, |G| - 1\}$ and $e_1 = \frac{\chi(e)}{|G|}$. □

Corollary 2.6. *The order of every finite subgroup of $V(\mathbb{Z}G)$ divides $|G|$.*

Proof. Let ρ be the regular representation and let χ be the character afforded by ρ.

Let H be a finite subgroup of $V(\mathbb{Z}G)$ and let $e = \widehat{H} = \frac{\sum_{h\in H} h}{|H|}$. Then e is an idempotent of $\mathbb{Q}G$ and hence $r = \chi(e)$, where r is the rank of $\rho(e)$. On the other hand $\chi(h) = |G|c_h$ where c_h is the coefficient of 1 in h. By the Berman-Higman Theorem, $c_h = 0$ unless $h = 1$. Therefore $r = \chi(e) = \frac{|G|}{|H|}$, is an integer and thus $|H|$ divides $|G|$. □

3. Problems on finite subgroups of $\mathcal{U}(\mathbb{Z}G)$

In this section we collect some of the main problems on the finite groups of units of $\mathbb{Z}G$. The results of the previous sections suggests that there is a strong connection between the finite subgroups H of $V(\mathbb{Z}G)$ and the subgroups of G. For example, the elements of H are linearly independent over $\mathbb{Q}$ (Corollary 2.4) and the order of H divides the order of G (Corollary 2.6). Moreover, if G is abelian then the torsion elements of $V(\mathbb{Z}G)$ are just the elements of G (Corollary 2.2). We cannot expect that the latter generalizes to non-abelian groups because conjugates of G in $\mathcal{U}(\mathbb{Z}G)$ are not included in G. So the most that we can expect is that the finite subgroups of $V(\mathbb{Z}G)$ are conjugate to subgroups of G or at least isomorphic to subgroups of G. Already Higman knew that $V(\mathbb{Z}S_3)$ has torsion units which are not conjugate in the units of $\mathbb{Z}S_3$ to any element of G. However, Hughes and Pearson proved that every torsion element of $V(\mathbb{Z}S_3)$ is conjugate in the units of $\mathbb{Q}S_3$ to an element of S_3 (see Problem 10).

Two subgroups or elements of $\mathcal{U}(\mathbb{Z}G)$ are said to be *rationally conjugate* if they are conjugate within the units of $\mathbb{Q}G$.

The results of Hughes and Pearson on the torsion elements of $V(\mathbb{Z}S_3)$ suggested the following problems which were proposed as conjecture by Hans Zassenhaus [Zas74].

The Zassenhaus Problems[2]: Given a finite group G:

(ZP1) Is every torsion element of $V(\mathbb{Z}G)$ rationally conjugate to an element of G?
(ZP2) Is every finite subgroup of $V(\mathbb{Z}G)$, with the same order as G, rationally conjugate to G?
(ZP3) Is every finite subgroup of $V(\mathbb{Z}G)$ rationally conjugate to a subgroup of G?

Clearly a positive solution for (ZP3) implies a positive solution for (ZP1) and (ZP2). Moreover a positive solution for (ZP2) implies a positive solution for the Isomorphisms Problem, or more precisely if (ZP2) has a positive solution for a finite group G and $\mathbb{Z}G \cong \mathbb{Z}H$ for another group H then $G \cong H$.

The following proposition shows that in the Zassenhaus Problems one can replace $\mathbb{Q}$ by any field of characteristic 0. For its proof we need some notation.

If F is a field, A is a finite dimensional F-algebra and $a \in A$ then the *norm* of a over F is $\mathrm{Nr}_{A/F}(a) = \det(\rho(a))$ where $\rho : A \to \mathrm{End}_F(A)$ is the regular representation of A, i.e. $\rho(a)(b) = ab$, for $a, b \in A$. Observe that if B is a basis of A over F then $\mathrm{Nr}_{A/F}(a) = \det(\rho_B(a))$, where $\rho_B(a)$ is the matrix representation of $\rho(a)$ in the basis B. Moreover, if E is a field containing F as a subfield then B is also a basis of $E \otimes_F A$ over E and hence, considering A embedded in $E \otimes_F A$ via the map $a \mapsto 1 \otimes a$, we have $\mathrm{Nr}_{B/E}(a) = \det(\rho_G(a)) = \mathrm{Nr}_{A/F}(a)$ for every $a \in A$.

Proposition 3.1. *Let E/F be an extension of infinite fields, let A be a finite dimensional F-algebra and let $B = E \otimes_F A$. Let M and N be finite subsets of A which are conjugate within B. Then they are also conjugate within A.*

Proof. Fix an F-basis $\{b_1, \ldots, b_d\}$ of A. Let u be a unit of B such that $M^u = N$. For every $m \in M$ let $n_m = u^{-1}mu$. So the system of equations $Xn_m = mX$ has a solution in the units of B. Expressing this in terms of the F-basis $b_1, \ldots, b_d$ of A we obtain a system of homogeneous linear equations in d unknowns, with coefficients in F which has a solution $(e_1, \ldots, e_d)$ in E such that $e_1b_1 + \cdots + e_nb_d$ is a unit of B. Let $v_1, \ldots, v_k$ be an F-basis of the set of solutions and consider the polynomial $f(X_1, \ldots, X_k) = \mathrm{Nr}_{A/F}(X_1v_1 + \cdots + X_kv_k) = \mathrm{Nr}_{B/E}(X_1v_1 + \cdots + X_kv_k)$. By elementary linear algebra $v_1, \ldots, v_k$ is also an E-basis of the set of solutions in E. Thus $e_1b_1 + \cdots + e_kb_k = x_1v_1 + \cdots + x_kv_k$ for some $x_1, \ldots, x_k \in E$ and hence $f(x_1, \ldots, x_k) \neq 0$. This implies that f is not the zero polynomial. Then $f(y_1, \ldots, y_k) \neq 0$ for some $y_1, \ldots, y_k \in F$, since F is infinite. Therefore $v = y_1v_1 + \cdots + y_kv_k$ is an element of A with $\mathrm{Nr}_{A/F}(v) \neq 0$ and $vn_m = mv$ for each $m \in M$. The first implies that $v \in \mathcal{U}(A)$ and the second that $M^v = N$. Thus M and N are conjugate within A. □

Applying Proposition 3.1 to $A = \mathbb{Q}G$ and F a field containing $\mathbb{Q}$, and having in mind that $FG \cong F \otimes_{\mathbb{Q}} G$, we get the following:

Corollary 3.2. *Let H be a finite subgroup of $V(\mathbb{Z}G)$ and let F be a field containing $\mathbb{Q}$ then H is rationally conjugate to a subgroup of G if and only if it is conjugate in FG to a subgroup of G.*

Corollary 3.3. *Let H_1 and H_2 be subgroups of $\mathcal{U}(\mathbb{Z}G)$. Then H_1 and H_2 are rationally conjugate if and only if there is an isomorphism $\phi : H_1 \to H_2$ such that $\chi(h) = \chi(\phi(h))$ for every $h \in H_1$ and every $\chi \in \mathrm{Irr}(G)$.*

[2]These problems have been known for a long time as the Zassenhaus Conjectures although counterexamples for the last two are known since the beginning of the 1990s. Since we also know now counterexamples for the first one, I prefer to call them problems now.

Proof. The necessary condition is obvious. Suppose that $\phi : H_1 \to H_2$ is an isomorphism satisfying the condition. For every $\chi \in \mathrm{Irr}(G)$ fix a representation ρ_χ affording χ. Then $\Phi = (\rho_\chi)_{\chi\in\mathrm{Irr}} : \mathbb{C}G \to \prod_{\chi\in\mathrm{Irr}(G)} M_{\chi(1)}(\mathbb{C})$ is an isomorphism of $\mathbb{C}$-algebras. Moreover $\rho_\chi|_{H_1}$ and $\rho_\chi|_{H_2} \circ \phi$ are representations of H_1 affording the same character, namely $\chi_{H_1} = \chi_{H_2}\circ\phi$. Thus $\rho_\chi|_{H_1}$ and $\rho_\chi|_{H_2}\circ\phi$ are equivalent as $\mathbb{C}$-representations, i.e. there is $U_\chi \in \mathcal{M}_{\chi(1)}(\mathbb{C})$ such that $\rho_\chi\phi(h) = U^{-1}\rho_\chi(h)U$ for every $h \in H_1$. Hence $u = \Phi((U_\chi)_{\chi\in\mathrm{Irr}(G)})$ is a unit of $\mathbb{C}G$ such that $u^{-1}hu = \phi(h)$ for every $h \in H_1$. Thus $u^{-1}H_1u = \phi(H_1) = H_2$, i.e. H_1 and H_2 are conjugate in $\mathbb{C}G$. Thus H_1 and H_2 are conjugate in $\mathbb{Q}G$, by Corollary 3.2. □

The set of orders of the torsion elements of a group Γ is call the *spectrum* of Γ. If (ZP1) has a positive solution then G and $V(\mathbb{Z}G)$ have the same spectra. This suggests the following problem.

The Spectrum Problem: (SpP) Do G and $V(\mathbb{Z}G)$ have the same spectra?

A weaker version of the Spectrum Problem is the Prime Graph Question which was proposed by Kimmerle. The *prime graph* of Γ is the undirected graph whose vertices are the prime integers p with $p = |g|$ for some $g \in \Gamma$ and the edges are the pairs $\{p, q\}$ of different primes p and q with $pq = |g|$ for some $g \in \Gamma$, i.e. with pq in the spectrum of G.

The Prime Graph Question: (PGQ) Do G and $V(\mathbb{Z}G)$ have the same prime graph?

By the Cohn-Livingstone Theorem (Problem 12), the spectra of G and $V(\mathbb{Z}G)$ contain the same prime powers and in particular the prime graphs of G and $V(\mathbb{Z}G)$ have the same vertices. However whether (ZP1) has a positive solution for units of prime power order is still unknown.

Another weaker version of the Zassenhaus Problem (ZP1) was proposed by Kimmerle.

The Kimmerle Problem: (KP) Is every torsion element of $V(\mathbb{Z}G)$ conjugate to an element of G in $\mathbb{Q}H$ for some finite group H containing G as subgroup?

A final question related with these problems is the Automorphism Problem which tries to predicts how are the automorphisms of $\mathbb{Z}G$ which preserves the augmentation. They form a subgroup of the group $\mathrm{Aut}(\mathbb{Z}G)$ of all autormorphisms of $\mathbb{Z}G$, which we denote by $\mathrm{Aut}_*(\mathbb{Z}G)$. Every automorphism of G extends uniquely to an element of $\mathrm{Aut}_*(\mathbb{Z}G)$. We can identify the latter with the group $\mathrm{Aut}(G)$ of automorphisms of G so we see $\mathrm{Aut}(G)$ as a subgroup of $\mathrm{Aut}_*(\mathbb{Z}G)$. Also, the inner automorphisms of $\mathbb{Z}G$ belong to $\mathrm{Aut}_*(\mathbb{Z}G)$. More generally, the inner automorphisms of $\mathbb{Q}G$ leaving $\mathbb{Z}G$ invariant form another normal subgroup of $\mathrm{Aut}_*(\mathbb{Z}G)$. We denote this group $\mathrm{Inn}_{\mathbb{Q}G}(\mathbb{Z}G)$. Then $\mathrm{Aut}(G)\mathrm{Inn}_{\mathbb{Q}G}(\mathbb{Z}G)$ is a subgroup of $\mathrm{Aut}_*(\mathbb{Z}G)$.

The Automorphism Problem (AUT) Is $\mathrm{Aut}_*(\mathbb{Z}G) = \mathrm{Aut}(G)\mathrm{Inn}_{\mathbb{Q}G}(\mathbb{Z}G)$?

Proposition 3.4. *(ZP2) has a positive solution for G if and only if (ISO) and (AUT) have a positive solution for G.*

Proof. Suppose that (ZP2) has a positive solution for G. Let H be a subgroup of $V(\mathbb{Z}G)$ with the same cardinality as G. By assumption H is rationally conjugate to G and hence $G \cong H$. Thus (ISO) has a positive solution for G. Let now $\alpha \in \mathrm{Aut}_*(\mathbb{Z}G)$. Then $H = \alpha(G)$ is a subgroup of $V(\mathbb{Z}G)$ with the same order as G. By assumption, there is a unit u of $\mathbb{Q}G$ such that $H = u^{-1}Gu$. Let β be the inner automorphism of $\mathbb{Q}G$ defined by u. Then $\beta(\mathbb{Z}G) = \mathbb{Z}H \subseteq \mathbb{Z}G$ and therefore

$\beta \in \mathrm{Inn}_{\mathbb{Q}G}(\mathbb{Z}G)$. Moreover, $\beta^{-1}\alpha \in \mathrm{Aut}(G)$. Thus $\alpha \in \mathrm{Aut}(G)\mathrm{Inn}_{\mathbb{Q}G}(\mathbb{Z}G)$. We conclude that (AUT) has a positive solution for G.

Conversely, suppose that (ISO) and (AUT) have a positive solution for G. Let H be a subgroup of $V(\mathbb{Z}G)$ with the same order as G. By the Universal Property of Group Rings there is a ring homomorphism $\beta : \mathbb{Z}H \to \mathbb{Z}G$ whose restriction to H is the identity of H. As G and H have the same order, β is an isomorphism and hence there is an isomorphism $\alpha : G \to H$. Applying again the Universal Property of Group Rings there is a ring isomorphism $\mathbb{Z}G \to \mathbb{Z}H$ extending α, which we also denote α. Then $\beta\alpha \in \mathrm{Aut}_*(\mathbb{Z}G)$ and by assumption $\beta\alpha = \delta\gamma$ for some $\gamma \in \mathrm{Aut}(G)$ and $\delta \in \mathrm{Inn}_{\mathbb{Q}G}(\mathbb{Z}G)$. Then $H = \beta(H) = \delta\gamma\alpha^{-1}(H) = \delta(G)$. Therefore H is rationally conjugate to G. This proves that (ZP2) has a positive solution for G. □

We list here a few relevant results on them. See [MdR19] for a more extensive list of results.

Negative results:

- Roggenmkamp and Scott constructed metabelian[3] negative solutions to (AUT) [Rog91] and Klingler discovered a simpler one [Kli91]. This provides metabelian negative solutions to (ZP2) and (ZP3).
- Hertweck constructed a solvable negative solution to (ISO) [Her01]. Of course this is another negative solution for (ZP2) but it is more complicated than the counterexamples of Roggenkamp and Scott and Klingler.
- Recently Eisele and Margolis found a metabelian negative solution to (ZP1) [EM18].
- Dade found two metabelian groups G and H such that $FG \cong FH$ for every field F [Dad71].

Positive solutions for (ZP3): (ZP3) has a positive solution (and hence all the problems mentioned in this Section) for the following groups.

- nilpotent groups [Wei91].
- split metacyclic groups $A \rtimes X$ with A and X cyclic of coprime order [Val94]. The proof of this result is based in a previous proof in [PMS84] of a positive solution for (ZP1) for this class of groups.

Positive solutions for (ZP1): Besides the groups in the previous list positive solutions for (ZP1) has been proved for the following families of groups:

- All the groups of order at most 143 [BHK$^+$17].
- groups with a normal Sylow subgroup with abelian complement [Her06].
- cyclic-by-abelian groups [CMdR13].
- $\mathrm{PSL}(2, q)$ for q either a Fermat or Mersenne prime or $q \in \{8, 9, 11, 13, 16, 19, 23, 25, 32\}$ [LP89, Her06, Her07, Her08b, KK17, BM17, MdRS19].

Positive solutions for (ISO): Withcomb proved (ISO) for metabelian groups, i.e. groups whose derived subgroup is abelian [Whi68].

Results for (SpP). Hertweck proved that the Spectrum Problem has a positive solution for solvable groups [Her08a]. No negative solution is known.

Results for (PGQ): Kimmerle and Konovalov have proved that the Prime Graph Question has a positive solution for a group if and only if it has a positive solution for every almost simple epimorphic image of G [KK17]. Many positive results for simple and almost simple groups have been obtained in the latter years.

[3]A group is said to be metabelian if its derived subgroup is abelian, or equivalent if it has an abelian normal subgroup with abelian quotient.

Results for (KP). We know that the Kimmerle Problem has a positive solution for torsion units in $V(\mathbb{Z}G, N)$ with N a nilpotent normal subgroup of G [MdR18]. Observe that the counterexample to the Zassenhaus Conjecture by Eisele and Margolis belongs to $V(\mathbb{Z}G, A)$ for A an abelian normal subgroup of G. No negative solution is known.

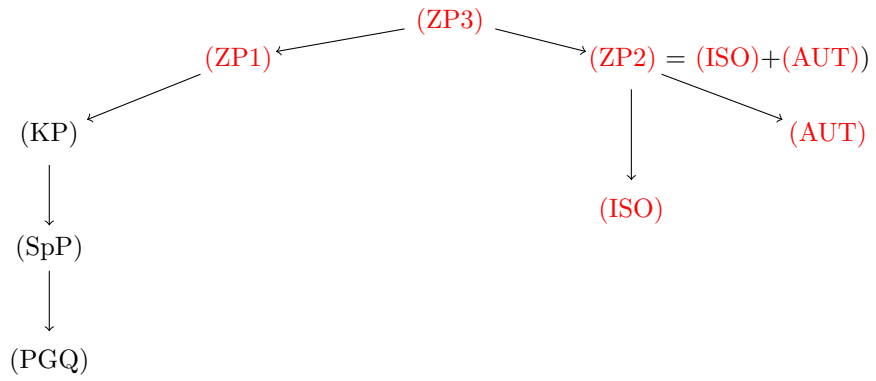

FIGURE 1. Logical implications between problems on finite subgroups of $V(\mathbb{Z}G)$. Red means that some negative solution is known.

4. Additive commutators and partial augmentations

Let R be a ring. Then $[R, R]$ denotes the additive subgroup of R generated by the Lie brackets

$$[x, y] = xy - yx, \quad (x, y \in R).$$

If S is a subring of the center of R then $R \times R \to R, (x, y) \mapsto [x, y]$ is an S-bilinear map. Therefore $[R, R]$ is an S-submodule of R. If moreover, $R = SX$, i.e. R is generated by X as S-module then $[R, R]$ is generated by $\{[x, y] : x, y \in X\}$ as S-module. In particular, if R is commutative then $[RG, RG]$ is generated by $\{[g, h] : g, h \in G\}$ as R-module.

Given $a = \sum_{g \in G} a_g g \in RG$, with $a_g \in R$ for every $g \in G$ and a subset X of G we set

$$\varepsilon_X(a) = \sum_{x \in X} a_x.$$

This notation will be used mostly with X a conjugacy class of G and with the sets of the form

$$G[n] = \{g \in G : |g| = n\}.$$

If $g \in G$ then g^G denotes the conjugacy class of g in G and the *partial augmentation* of a at g is $\varepsilon_{g^G}(a)$. When the group G is clear from the context we simplify the notation by writing $\varepsilon_g(a)$ rather than $\varepsilon_{g^G}(a)$. The Berman-Higman Theorem states that if u is a non-trivial torsion element of $V(\mathbb{Z}G)$ then $\varepsilon_1(u) = 0$.

Lemma 4.1. *If R is a commutative ring and G is a group then*

$$[RG, RG] = \sum_{g,h \in G} R[g, h] = \{a \in RG : \varepsilon_C(a) = 0, \textit{for each conjugacy class } C \textit{ of } G\}.$$

Proof. That the first two sets are equal was already mentioned at the beginning of this section. That the second is included in the third follows because ε_C is R-linear and $\varepsilon_C([g,h])$ for every $g,h \in G$. To finish the proof observe that if a belong to the third set then a is a sum of elements of the form $x = \sum_{t\in T} x_t g^t$ for $g \in G$, T a right transversal of $C_G(g)$ in G and $x_t \in R$ with $\sum_{t\in T} x_t = 0$. For such x we have $x = \sum_{t\in T} x_t g^t - (\sum_{t\in T} x_t)g = \sum_{t\in T} x_t(g^t - g) = \sum_{t\in T} x_t[t^{-1}g, t] \in [RG, RG]$. Thus a is a sum of elements in $[RG, RG]$, so that $a \in [RG, RG]$. □

Using Lemma 4.1 it easily follows that if T is a set of representatives of the conjugacy classes of G then

$$[RG, RG] = \bigoplus_{t\in T, g\in t^G\setminus\{t\}} R(g-t).$$

Therefore $RG/[RG, RG]$ is a free R-module with rank the number of conjugacy classes of G. Moreover, if S is a subring of R then

$$[SG, SG] = SG \cap [RG, RG].$$

Lemma 4.2. *The following conditions are equivalent for a finite subgroup H of $V(\mathbb{Z}G)$.*

1. *H is rationally conjugate to a subgroup of G;*
2. *there is a homomorphism $\phi : H \to G$ such that for every $h \in H$ and every $g \in G \setminus \phi(h)^G$, $\varepsilon_g(h) = 0$.*
3. *there is a homomorphism $\phi : H \to G$ such that $\varepsilon_g(h) = \varepsilon_g(\phi(h))$ for every $h \in H$ and $g \in G$.*

Proof. (1) implies (2). Suppose that $u^{-1}Hu \leq G$ with $u \in \mathcal{U}(\mathbb{Q}G)$ and consider the group homomorphism $\phi : H \to G, h \mapsto u^{-1}hu$. Then

$$h - \phi(h) = [hu, u^{-1}] \in \mathbb{Z}G \cap [\mathbb{Q}G, \mathbb{Q}G] = [\mathbb{Z}G, \mathbb{Z}G].$$

Thus, if $g \in G \setminus \phi(h)^G$ then

$$0 = \varepsilon_g(h - \phi(h)) = \varepsilon_g(h).$$

(2) implies (3). Suppose that $\phi : H \to G$ is a group homomorphism satisfying the condition in (2). Then

$$\varepsilon_g(h) = \begin{cases} \mathrm{aug}(h) = 1, & \text{if } g \in \phi(h)^G; \\ 0, & \text{if } g \notin \phi(h)^G. \end{cases}$$

Thus $\varepsilon_g(h) = \varepsilon_g(\phi(h))$ for every $h \in H$ and $g \in G$, i.e. ϕ satisfies (3).

(3) implies (1) Suppose that $\phi : H \to G$ satisfies condition (3). Therefore, $\varepsilon_g(\phi(h) - h) = 0$ for each $g \in G$ and hence $\phi(h) - h \in [\mathbb{Z}G, \mathbb{Z}G]$, by Lemma 4.1. Moreover, ϕ is injective, because if $\phi(h) = 1$ then $\varepsilon_1(h) = 1$. Thus $h = 1$ by the Berman-Higman Theorem. Therefore ϕ is an isomorphism from H to $\phi(H)$ and the latter is a subgroup of G. If $\chi \in \mathrm{Irr}(G)$ then $\chi([\mathbb{Z}G, \mathbb{Z}G]) = 0$ and hence $\chi(h) = \chi(\phi(h))$. By Corollary 3.3, H and $\phi(H)$ are conjugate in $\mathbb{Q}G$. □

Lemma 4.3. *Let $v \in V(\mathbb{Z}G)$, let p be a prime integer and let $x, y \in G$ such that $\varepsilon_g(v) = 0$ for every $g \in G \setminus x^G$ and $\varepsilon_g(v^p) = 0$ for every $g \in G \setminus y^G$. Then x^p and y are conjugate in G.*

Proof. Indeed, as $\varepsilon_g(v) = \varepsilon_g(x)$ and $\varepsilon_g(v^p) = \varepsilon_g(y)$ for each $g \in G$ and $\mathrm{aug}(v) = \mathrm{aug}(v^p) = 1$, it follows from Lemma 4.1 that $v \equiv x \mod [\mathbb{Z}G, \mathbb{Z}G]$ and $v^p \equiv y \mod [\mathbb{Z}G, \mathbb{Z}G]$. Then $x^p \equiv v^p \equiv y \mod ([\mathbb{Z}G, \mathbb{Z}G] + p\mathbb{Z}G)$, by Problem 11. Therefore taking images in $\mathbb{F}_pG$ we deduce that $x^p \equiv y \mod [\mathbb{F}_pG, \mathbb{F}_pG]$. Therefore, by Lemma 4.1, we have $\varepsilon_g(x^p) \equiv \varepsilon_g(y) \mod p$ for every $g \in G$. In particular $1 = \varepsilon_{x^p}(x^p) \equiv \varepsilon_{x^p}(y) \mod p$. As $\varepsilon_{x^p}(y) = 0$ if x^p and y are not conjugate in G we deduce that x^p and y are conjugate in G, as desired. □

Theorem 4.4 (Marciniak-Ritter-Sehgal-Weiss [MRSW87])**.** *Let u be an element of order n of $V(\mathbb{Z}G)$. Then the following are equivalent:*

(1) *u is conjugate in $\mathbb{Q}G$ to an element of G.*
(2) *For every $i = 1, \dots, n-1$, there is exactly one conjugacy class C of G with $\varepsilon_C(u^i) \neq 0$.*
(3) *$\varepsilon_C(u^i) \geq 0$, for every $i = 1, \dots, n-1$ and every conjugacy class C of G.*

Proof. (1) $\Rightarrow$ (2) is obvious and (2) $\Leftrightarrow$ (3) follows easily from the fact that the sum of the partial augmentations $\varepsilon_C(u)$ of u is $\mathrm{aug}(u) = 1$.

Suppose that (2) holds. For every $i = 1, \dots, n$ let $g_i \in G$ such that $\varepsilon_{g^G}(u^i) = 0$ for every $g \in G \setminus g_i^G$. By the Berman-Higman Theorem $g_i = 1$ if and only if $u^i = 1$ if and only if $i = n$.

We now prove by induction on the number of primes in the factorization of i that g_i is conjugate to g_1^i for every $i = 1, \dots, n$. This is clear if the number of primes is 0, i.e. if $i = 1$. So suppose that $i = pj$ with p prime. By the induction hypothesis g_j and g_1^j are conjugate in G. Let $v = u^j$. By the previous paragraph $\varepsilon_g(v) = 0$ for every $g \in G \setminus g_j^G = G \setminus (g_1^j)^G$ and $\varepsilon_g(v^p) = 0$ for every $g \in G \setminus g_i^G$. This implies that g_i is conjugate to g_j^p in G, by Lemma 4.3. Thus g_i is conjugate to g_1^i, as desired.

Thus, if $1 \leq i \leq n$ then $g_1^n = 1$ if and only $g_i = 1$ if and only $i = n$, i.e. g_1 has order n and hence $u^i \to g_1^i$ defines a group isomorphism $\langle u \rangle \to \langle g_1 \rangle$ with $\varepsilon_g(u^i) = 0$ for each $g \in G \setminus (g_1^i)^G$. Then $\langle u \rangle$ is rationally conjugate to a subgroup of G, by Theorem 4.2, and hence u is rationally conjugate to an element of G, as desired. □

5. Double action

In this section we rewrite the Zassenhaus Problems in terms of isomorphisms between certain modules.

In the remainder G and H are finite groups and R is a commutative ring. Fix a group homomorphism

$$\alpha : H \to V(RG).$$

Then we define a left $R(H \times G)$-module $R[\alpha]$ as follows: As an R-module $R[\alpha] = RG$ and the multiplication by elements of $H \times G$ is given by the following formula:

$$(h, g)v = \alpha(h) v g^{-1}, \quad (h \in H, g \in G, v \in RG). \tag{5.1}$$

We consider G as a subgroup of $H \times G$ via the projection on the second component. Let $\alpha, \beta : H \to \mathcal{U}(RG)$ be two group homomorphism. Then $R[\alpha]$ and $R[\beta]$ are isomorphic as RG-modules and every isomorphism between them as RG-module is given as follows

$$\begin{array}{rccc} \rho_u : RG & \to & RG \\ x & \mapsto & ux \end{array}$$

for some $u \in \mathcal{U}(RG)$. Moreover ρ_u is an isomorphism of $R(H \times G)$-modules if and only if $\beta(h) = u\alpha(h)u^{-1}$ for every $h \in H$. This proves the following:

Proposition 5.1. *Let $\alpha, \beta : H \to \mathcal{U}(RG)$ be group homomorphisms. Then $R[\alpha] \cong R[\beta]$ if and only if there is $u \in \mathcal{U}(RG)$ such that $\beta(h) = u\alpha(h)u^{-1}$ for every $h \in H$.*

The connection of Proposition 5.1 with the Zassenhaus Problems is now clear:

Corollary 5.2. *The following are equivalent for a group homomorphism $\alpha : H \to V(RG)$:*

(1) *There is $u \in \mathcal{U}(RG)$ and a group homomorphism $\sigma : H \to G$ such that $\alpha(h) = u^{-1}\sigma(h)u$ for every $h \in H$.*
(2) *$\alpha(H)$ is conjugate within $\mathcal{U}(RG)$ to a subgroup of G*

(3) $R[\alpha] \cong R[\sigma]$ *for some group homomorphism* $\sigma : H \to G$.

Furthermore, if R *is a field of characteristic zero then the above conditions are equivalent to the following:*

(4) *The character afforded by* $R[\alpha]$ *is equal to the character afforded by* $R[\sigma]$ *for some group homomorphism* $\sigma : H \to G$.

Corollary 5.2 suggests to calculate the character χ_α afforded by the module $R[\alpha]$. Using G as a basis of $R[\alpha]$ as R-module one easily obtains the following

$$\chi_\alpha(h, g) = |C_G(g)|\varepsilon_g(\alpha(h)). \tag{5.2}$$

We need the following proposition whose proof is beyond the scope of these notes.

Proposition 5.3 (Hertweck)**.** *Let* u *be a torsion element of* $V(\mathbb{Z}G)$ *and let* $g \in G$. *If* $|g|$ *does not divide* $|u|$ *then* $\varepsilon_g(u) = 0$.

Let $\mathrm{Cl}(G)$ denote the set of conjugacy classes of G. If $C \in \mathrm{Cl}(G)$ and $g \in C$ then, by definition, the order of C is the order of g and for every integer k, C^k denotes the conjugacy class of C in G containing g^k. Let $\mathrm{Cl}_m(G)$ be the set of conjugacy classes of G of order dividing m.

Lemma 5.4. *Let* u *be a torsion element of order* n *in* $V(\mathbb{Z}G)$, *let* k *be a positive integer coprime with* n *and let* C *be a conjugacy class in* G. *Then*

$$\varepsilon_C(u) = \sum_{\substack{D \in \mathrm{Cl}(G) \\ D^k = C}} \varepsilon_D(u). \tag{5.3}$$

Proof. Let $C \in \mathrm{Cl}(G)$ and let m denote the order of C. If $m \nmid n$ then the order of every $D \in \mathrm{Cl}(G)$ with $D^k = C$ does not divide n and hence, by Lemma 5.3, we have $\varepsilon_C\left(u^k\right) = \varepsilon_D\left(u\right) = 0$ for every such D. Then (5.3) holds.

Suppose otherwise that $m \mid n$ and let l be an integer such that $kl \equiv 1 \mod n$. Then C^l is the unique element D of $\mathrm{Cl}(G)$ with $D^k = C$. Thus we have to prove that $\varepsilon_C\left(u^k\right) = \varepsilon_{C^l}\left(u\right)$. Let $\alpha : \langle u \rangle \to V(\mathbb{Z}G)$ denote the inclusion map. The representation ρ of $\langle u \rangle \times G$ associated to the module $\mathbb{Z}[\alpha]$ has degree $|G|$ and affords the character $\chi = \chi_\alpha$. Let $g \in C$. By assumption the order of (u^k, g) is n. Let ζ_n denote a complex primitive n-th root of unity. Then $\rho(u^k, g)$ is conjugate to $\mathrm{diag}(\zeta_n^{i_1}, \ldots, \zeta_n^{i_{|G|}})$ for some integers $i_1, \ldots, i_{|G|}$ and $\rho(u, g^l)$ is conjugate to $\mathrm{diag}(\zeta_n^{li_1}, \ldots, \zeta_n^{li_{|G|}})$. As $\gcd(l, n) = 1$, there is an automorphism σ of $\mathbb{Q}(\zeta_n)$ given by $\sigma(\zeta_n) = \zeta_n^l$. Moreover, $\chi(u^k, g) \in \mathbb{Z}$, by (5.2). Then $\chi(u^k, g) = \sigma(\chi(u^k, g)) = \sum_{j=1}^{|G|} \zeta_n^{li_j} = \chi(u, g^l)$. Applying again (5.2) and $C_G(g) = C_G(g^l)$ we have $\varepsilon_C\left(u^k\right) = \varepsilon_g\left(u^k\right) = \varepsilon_{g^l}\left(u\right) = \varepsilon_{C^l}\left(u\right)$, as desired. □

Using Lemma 5.4 and Theorem 4.4 one can obtain the following simplified version of the latter.

Corollary 5.5. *Let* u *be an element of* $V(\mathbb{Z}G)$ *of order* n. *Then the following are equivalent.*

(1) u *is rationally conjugate to an element of* G.
(2) *For every* $d \mid n$, *there is* $g_d \in G$ *with* $\varepsilon_g(u^d) = 0$ *for every* $g \in G \setminus g_d^G$.
(3) $\varepsilon_g(u^d) \geq 0$, *for every* $d \mid n$ *and* $g \in G$.

Proof. By Theorem 4.4, it is enough to show that if (3) holds then $\varepsilon_C(u^i) \geq 0$ for every positive integer i and every $C \in \mathrm{Cl}(G)$. Indeed, suppose that (3) holds, let i be a positive integer and let $d = \gcd(i, n)$ and $k = \frac{i}{d}$. Then $\frac{n}{d} = |u^d|$ and $\gcd(k, \frac{n}{d}) = 1$. Then, by Lemma 5.4, we have $\varepsilon_C\left(u^i\right) = \sum_{\substack{D \in \mathrm{Cl}(G) \\ D^k = C}} \varepsilon_D\left(u^d\right) \geq 0$. □

We finish this section with an application of Corollary 5.5 to (KP) which provides an specific "bigger" group in the statement of (KP).

Theorem 5.6. [MdR18] *Let G be a finite group and consider G as subgroup of S_G via the homomorphism $G \to S_G$ mapping $g \in G$ to the permutation of G given by $x \mapsto gx$. The following are equivalent for a finite group G.*

1. *(KP) has a positive solution for G.*
2. *Every torsion element of $V(\mathbb{Z}G)$ is conjugate in $\mathbb{Q}S_G$ to an element of G.*
3. *For every element of order n in $V(\mathbb{Z}G)$ and every positive integer $m \neq n$ we have $\varepsilon_{G[m]}(u) = 0$.*

Proof. (2) implies (1) is clear.

(1) implies (3). Assume that (KP) has a positive solution for G and let u be an element of order n in $V(\mathbb{Z}G)$. By assumption, G is contained as a subgroup in a finite group H such that u is conjugate to an element of G in $\mathbb{Q}H$. Since the support of u clearly consists only of elements in G and $G[m] = G \cap H[m]$, we have $\varepsilon_{G[m]}(u) = \varepsilon_{H[m]}(u) = 0$ for any integer $m \neq n$.

(3) implies (2). Suppose that (3) holds. Let u be an element of order n in $V(\mathbb{Z}G)$. The cycle type of an element of order k in G viewed as an element of S_G is given as $|G|/k$ cycles of length k. So two elements of G of the same order are conjugate in S_G. In particular all conjugacy classes of elements of the same order in G fuse into one conjugacy class in S_G. Then, applying (3) to any power u^k of u we deduce that there exists exactly one conjugacy class C, consisting of elements of the same order as u^k, in S_G such that $\varepsilon_C(u^k) = 1$ and $\varepsilon_{C'}(u^k) = 0$ for any other conjugacy class C'. Thus u is conjugate in $\mathbb{Q}S_G$ to an element h of S_G, by Theorem 5.5. If h is not conjugate in S_G to any element of G then $\varepsilon_g(u) = 0$ for every $g \in G$ and hence $1 = \mathrm{aug}(u) = 0$, a contradiction. Thus h is conjugate in S_G to an element g of G and hence u is conjugate in $\mathbb{Q}S_G$ to g. □

6. The HeLP Method

Let ζ_n denote a complex primitive n-th root of unity and set $F = \mathbb{Q}(\zeta_n)$. Then every automorphism of F is given by $\sigma_i(\zeta_n) = \zeta_n^i$ with i an integer coprime with n. Consider the Vandermonde matrix

$$V = V(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}) = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \dots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^{2^2} & \dots & \zeta_n^{2(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \zeta_n^{(n-1)} & \zeta_n^{2(n-1)} & \dots & \zeta_n^{(n-1)^2} \end{pmatrix}$$

and its complex conjugate

$$\overline{V} = V(1, \overline{\zeta_n}, \overline{\zeta_n}^2, \dots, \overline{\zeta_n}^{n-1}) = V(1, \zeta_n^{-1}, \zeta_n^{-2}, \dots, \zeta_n^{1-n}).$$

The (i,j)-th entry of $V\overline{V}$ is

$$\sum_{k=0}^{n-1} \zeta_n^{k(i-j)} = \begin{cases} n, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}.$$

Therefore

$$V^{-1} = \frac{1}{n}\overline{V}.$$

Let $U \in M_k(\mathbb{C})$ with $U^n = 1$. Then the eigenvalues of U are of the form ζ_n^i with $i = 0, 1, \ldots, n-1$. Let μ_i denote the multiplicity of ζ_n^i as eigenvalue of U, i.e. U is conjugate in $M_k(\mathbb{C})$ to a diagonal matrix where each ζ_n^i appears μ_i times in the diagonal. We denote this diagonal matrix as

$$\mathrm{diag}(1 \times \mu_0, \zeta_n \times \mu_1, \ldots, \zeta_n^{n-1} \times \mu_{n-1}).$$

Then U^j is conjugate in $\mathcal{M}_k(\mathbb{C})$ to $\mathrm{diag}(1 \times \mu_i, \zeta_n^j \times \mu_1, \ldots, \zeta_n^{j(n-1)} \times \mu_{n-1})$. Therefore

$$\mathrm{tr}(U^j) = \mu_0 + \mu_1\zeta_n^j + \mu_2\zeta_n^{2j} + \cdots + \mu_{n-1}\zeta_n^{(n-1)j}, \tag{6.4}$$

for all j, or equivalently

$$\begin{pmatrix} \mathrm{tr}(U^0) \\ \mathrm{tr}(U) \\ \mathrm{tr}(U^2) \\ \vdots \\ \mathrm{tr}(U^{n-1}) \end{pmatrix} = V \begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \vdots \\ \mu_{n-1} \end{pmatrix}.$$

Thus

$$\begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \vdots \\ \mu_{n-1} \end{pmatrix} = \frac{1}{n}\overline{V} \begin{pmatrix} \mathrm{tr}(U^0) \\ \mathrm{tr}(U) \\ \mathrm{tr}(U^2) \\ \vdots \\ \mathrm{tr}(U^{n-1}) \end{pmatrix},$$

or equivalently

$$\mu_i = \frac{1}{n}\sum_{j=0}^{n-1} \mathrm{tr}(U^j)\zeta_n^{-ij}. \tag{6.5}$$

If $d = \gcd(j, n)$ then $\sigma_{\frac{j}{d}} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n^d)/\mathbb{Q})$ and $\zeta_n^{-ij} = \sigma_{\frac{j}{d}}(\zeta_n^{-id})$. Combining this with (6.4), we deduce that $\mathrm{tr}(U^j) = \sigma_{\frac{j}{d}}(\mathrm{tr}(U^d))$ and hence, grouping the summands in the right side of (6.5) with the same greatest common divisor with n, we have

$$\mu_i = \frac{1}{n}\sum_{d|n} \mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\mathrm{tr}(U^d)\zeta_n^{-id}). \tag{6.6}$$

Suppose now that u is an element of order n of $\mathcal{U}(\mathbb{C}G)$ and ρ is a representation of G affording the character χ. Applying (6.6) to $U = \rho(u)$ we deduce that the multiplicity of ζ_n^i as an eigenvalue of $\rho(u)$ is

$$\mu(\zeta_n^i, u, \chi) := \frac{1}{n}\sum_{d|n} \mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(u^d)\zeta_n^{-id}).$$

We are going to use that χ is constant on conjugacy classes to consider χ as a map defined on $\mathrm{Cl}(G)$, i.e. we denote $\chi(C) = \chi(g)$ whenever $C = g^G$ with $g \in G$. By the linearity of χ, for every $a \in \mathbb{C}G$ we have

$$\chi(a) = \sum_{C \in \mathrm{Cl}(G)} \varepsilon_C(a)\chi(C).$$

Therefore

$$\mu(\zeta_n^i, u, \chi) = \frac{1}{n}\sum_{d|n}\sum_{C \in \mathrm{Cl}(G)} \varepsilon_C(u^d)\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(C)\zeta_n^{-id}). \tag{6.7}$$

Observe that $\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(C)\zeta_n^{-id})$ makes sense in summands where $\varepsilon_C(u^d) \neq 0$. This is a consequence of Proposition 5.3 because in that case the order of C divides $\frac{n}{d}$ and hence $\chi(C) \in \mathbb{Q}(\zeta_n^d)$. Thus, in the previous formula it is enough to run on the conjugacy classes C in $\mathrm{Cl}_{\frac{n}{d}}(G)$. As each $\mu(\zeta_n^i, u, \chi)$ is a non-negative integer we deduce:

Proposition 6.1 (Luthar-Passi [LP89])**.** *Let $u \in \mathcal{U}(\mathbb{Z}G)$ with $u^n = 1$ and let χ be an ordinary character of G. Then*

$$\frac{1}{n}\sum_{d|n}\sum_{C\in \mathrm{Cl}_{\frac{n}{d}}(G)} \varepsilon_C(u^d)\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(C)\zeta_n^{-id}) \in \mathbb{Z}^{\geq 0}. \tag{6.8}$$

The Luthar-Passi Method uses (6.8) to describe the possible partial augmentations of powers of u for an element of order n. More precisely, suppose that we want to prove the Zassenhaus Conjecture for a group G. By the Cohn-Livingstone Theorem (Problem 12) we know that if $V(\mathbb{Z}G)$ has an element of order n then n divides the exponent of G. So we first calculate the exponent of G and we consider all the possible divisors n of this exponent. For each of these n we calculate all the tuples $(\varepsilon_{d,C})_{d|n, C\in \mathrm{Cl}_{\frac{n}{d}}(G)}$ of integers satisfying $\sum_{C\in \mathrm{Cl}_{\frac{n}{d}}(G)} \varepsilon_{d,C} = 1$ for every $d \mid n$ and the following conditions:

$$\frac{1}{n}\sum_{d|n}\sum_{C\in \mathrm{Cl}_{\frac{n}{d}}(G)} \varepsilon_{d,C}\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(g)\zeta_n^{-id}) \in \mathbb{Z}^{\geq 0}.$$

We consider the $\varepsilon_{d,C}$ as the partial augmentations $\varepsilon_C(u^d)$ for a unit u of order n. By Corollary 5.5, if all the tuples satisfying these conditions are formed by non-negative integers for all the possible values of n then (ZP1) has a positive solution for G. In that case we say that the Luthar-Passi Method gives a positive solution of (ZP1) for G.

Hertweck extended (6.7) to Brauer characters. We recall the definition of Brauer characters. Let p be a prime integer. Let $G_{p'}$ denote the set formed by the *p-regular* elements of G, i.e. those of order coprime with p. Let m be the least common multiple of the elements of $G_{p'}$ and fix ζ_m a complex primitive m-th root of unity and ξ_m a primitive m-th root of unity in a field F of characteristic p. Let ρ be an F-representation of G and let $g \in G_{p'}$. Then $\rho(g)$ is conjugate to $\mathrm{diag}(\xi_m^{i_1}, \dots, \xi_m^{i_k})$ for some integers $i_1, \dots, i_k$. Thus the character afforded by ρ maps g to $\xi_m^{i_1} + \cdots + \xi_m^{i_k}$. By definition, the Brauer character afforded by ρ is the map $\chi : G_{p'} \to \mathbb{C}$ associating g with $\zeta_m^{i_1} + \cdots + \zeta_m^{i_k}$. Composing ρ with the natural projection $\mathbb{Z}G \to \mathbb{F}_pG \subseteq FG$ we obtain a ring homomorphism $\rho : \mathbb{Z}G \to M_n(F)$. Then (6.7) gives the multiplicity of ξ_n^i as an eigenvalue of $\rho(u)$ [Her07]. This provides more constrains to the possible partial augmentations of a p-regular units. This has been used to obtain positive solutions for (ZP1) for cases where the equations provided by ordinary characters are not sufficient. However, for solvable groups, by the Fong-Swan-Rulokain Theorem [CR87, 22.1] the Brauer characters does not add additional constrains.

7. Problems

(1) Prove that if A and B are $n \times n$ matrices with entries in a commutative ring R then $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. Deduce that if A and B are conjugate in $M_n(R)$ then $\mathrm{tr}(A) = \mathrm{tr}(B)$.
(2) Let A be an $m \times m$ matrix with entries in the field of complex numbers. Prove that
   (a) If $A^n = I$ then A is diagonalizable and the eigenvalues of A are n-th roots of unity. Deduce that $|\mathrm{tr}(A)| \leq m$ and if the equality holds then A is a scalar matrix.
   (b) If $A^2 = A$ then A is diagonalizable and every eigenvalue of A is either 1 or 0. Deduce that $\mathrm{tr}(A)$ is the rank of A.

(3) Let R be a ring, G be a group and let N, N_1 and N_2 be normal subgroups of G with $N_1 \subseteq N_2$. Let $\Phi : RG/N_2 \to R\left(\frac{G/N_1}{N_2/N_1}\right)$ be the R-linear extension of the natural isomorphism $G/N_2 \cong \frac{G/N_1}{N_2/N_1}$. Prove the following statements:
   (a) $\mathrm{Aug}_N(RG) = RG\,\mathrm{Aug}(RN) = \mathrm{Aug}(RN)RG$.
   (b) $\mathrm{Aug}(RG) = \bigoplus_{g\in G\setminus\{1\}} R(g-1)$.
   (c) $\Phi \circ \mathrm{aug}_{G,N_2} = \mathrm{aug}_{G/N_1,N_2/N_1} \circ \mathrm{aug}_{G,N_1}$.
   (d) $\mathrm{Aug}_{N_1}(RG) \subseteq \mathrm{Aug}_{N_2}(RG)$.
   (e) $V(RG, G) = V(RG)$, $V(RG, 1) = 1$ and $V(RG, N_1) \subseteq V(RG, N_2)$.

(4) Let F be a field of characteristic $p > 0$ and let G be a group. Prove the following statements:
   (a) If G is a p-group then $\mathrm{Aug}(FG)$ is the Jacobson radical of FG.
   (b) If P is a normal p-subgroup of G then $\mathrm{Aug}_P(FG)$ is nilpotent.

(5) Let G be a finite group, let p be a prime integer and let P be a normal p-subgroup of G. Prove that every torsion element of $V(\mathbb{Z}G, P)$ is a p-element.

(6) Prove that A and B are two abelian finite groups then $\mathbb{C}A \cong \mathbb{C}B$ if and only if A and B have the same cardinality.

(7) Let R be a commutative ring and let G and H be groups. Let $f : RG \to RH$ be a ring homomorphism. Prove that there is a unique ring homomorphism $f' : RG \to RH$ such that $f'(g) = \mathrm{aug}(f(g))^{-1}f(g)$ for every $g \in G$ and $\mathrm{aug}(f(x)) = \mathrm{aug}(x)$ for every $x \in RG$. Show that if f is an isomorphism then so is f'.

(8) Prove that the following statements are equivalent for a finite group G and a finite subgroup H of $V(\mathbb{Z}G)$:
   (a) $|H| = |G|$.
   (b) $\mathbb{Z}G = \mathbb{Z}[H]$. (Recall that $\mathbb{Z}[H]$ denotes the additive sugroup of $\mathbb{Z}G$ generated by H.)
   (c) H is an basis of $\mathbb{Z}G$ over $\mathbb{Z}$.

(9) Prove that the Isomorphism Problem holds for a finite group G if and only if every subgroup of $V(\mathbb{Z}G)$ with the same cardinality as G is isomorphic to G.

(10) Consider $S_3 = \langle a\rangle \rtimes \langle b\rangle$, the symmetric group on three symbols, where $a = (1, 2, 3)$ and $b = (1, 2)$. Prove the following:
   (a) $\rho(a) = \begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix}$ and $\rho(b) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$ defines an irreducible representation of S_3. (Hint: Let χ denote the character afforded by ρ. By Character Theory, ρ is irreducible if and only if $\sum_{g\in S_3} \chi(g)\chi(g^{-1}) = |S_3|$.)
   (b) Let $\phi : \mathbb{C}S_3 \to \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$ be the unique linear map with $\phi(g) = (1, \mathrm{sgn}(g), \rho(g))$ for $g \in S_3$. Then ϕ is a isomorphism of complex algebras and
$$\phi(\mathbb{Z}S_3) = \left\{ \left(x, y, \begin{pmatrix} a & 3b \\ c & d \end{pmatrix}\right) : x, y, a, b, c, d \in \mathbb{Z}, \begin{array}{c} x \equiv y \bmod 2, \\ x \equiv a \bmod 3, \\ y \equiv d \bmod 3 \end{array} \right\}.$$
   (c) $V(\mathbb{Z}S_3)$ contains an element u of order 2 with $\phi(u) = (1, -1, \mathrm{diag}(1, -1))$.
   (d) u is not conjugate in the units of $\mathbb{Z}S_3$ to any element of S_3.
   (e) Every torsion element of $V(\mathbb{Z}S_3)$ is conjugate in the units of $\mathbb{Q}S_3$ to an element of S_3.

(11) Let p and n be positive integers with p prime integer. Prove the following statements:
   (a) If x and y are elements of a ring R then
$$(x + y)^{p^n} \equiv x^{p^n} + y^{p^n} \mod (pR + [R, R]).$$
   Moreover, if $x \in [R, R]$ then $x^p \in pR + [R, R]$.

(b) If G is a finite group and u is a torsion element of $V(\mathbb{Z}G)$ then $|u| = p^n$ if and only if $\varepsilon_{G[p^n]}(u) \not\equiv 0 \mod p$.

(12) [Cohn-Livingstone [CL65]] If G is a finite group then $V(\mathbb{Z}G)$ and G have the same primary spectrum, i.e. for every prime and every positive integer G contains an element of order p^n if and only if so does $V(\mathbb{Z}G)$. In particular, the least common multiple of the orders of the torsion elements of $V(\mathbb{Z}G)$ is the exponent of G, i.e. the smallest positive integer e such that $g^e = 1$ for every $g \in G$.

(13) Let G a finite group and let u be an element of prime order p in $V(\mathbb{Z}G)$. Prove that if all the elements of order p in G are conjugate then u is rationally conjugate to an element of G. Conclude that, in general, G is a subgroup of a group H such that u is conjugate in $\mathbb{Q}H$ to an element of G.

(14) Use the Luthar-Passi Method to prove that (ZP1) has a positive solution for S_3, A_4, S_4 and A_5.

(15) Prove that the Luthar-Passi Method does not provide a positive answer to (ZP1) for A_6. (Hint: First prove that every torsion element of $V(\mathbb{Z}A_6)$ of order 2 or 3 is rationally conjugate to an element of A_6 and then apply the Luthar-Passi Method to units of order 6.)

References

[Ber55] S. D. Berman, *On the equation $x^m = 1$ in an integral group ring*, Ukrain. Mat. Ž. **7** (1955), 253–261. MR 0077521 (17,1048g)

[BHK+17] A. Bächle, A. Herman, A. Konovalov, L. Margolis, and G. Singh, *The status of the zassenhaus conjecture for small groups*, Experimental Mathematics (2017), 1–6.

[BM17] A. Bächle and L. Margolis, *Rational conjugacy of torsion units in integral group rings of non-solvable groups*, Proc. Edinb. Math. Soc. (2) **60** (2017), no. 4, 813–830. MR 3715687

[CL65] J. A. Cohn and D. Livingstone, *On the structure of group algebras. I*, Canad. J. Math. **17** (1965), 583–593. MR 0179266

[CMdR13] M. Caicedo, L. Margolis, and Á. del Río, *Zassenhaus conjecture for cyclic-by-abelian groups*, J. Lond. Math. Soc. (2) **88** (2013), no. 1, 65–78. MR 3092258

[CR87] Ch. W. Curtis and I. Reiner, *Methods of representation theory. Vol. II*, Pure and Applied Mathematics (New York), John Wiley & Sons Inc., New York, 1987, With applications to finite groups and orders, A Wiley-Interscience Publication. MR 892316 (88f:20002)

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

[EM18] F. Eisele and L. Margolis, *A counterexample to the first Zassenhaus conjecture*, Adv. Math. **339** (2018), 599–641.

[Her01] M. Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. **154** (2001), 115–138.

[Her06] ———, *On the torsion units of some integral group rings*, Algebra Colloq. **13** (2006), no. 2, 329–348. MR 2208368 (2006k:16049)

[Her07] ———, *Partial augmentations and Brauer character values of torsion units in group rings*, http://arXiv:math/0612429v2 (2007).

[Her08a] ———, *The orders of torsion units in integral group rings of finite solvable groups*, Comm. Algebra **36** (2008), no. 10, 3585–3588. MR 2458394

[Her08b] ———, *Zassenhaus conjecture for A_6*, Proc. Indian Acad. Sci. Math. Sci. **118** (2008), no. 2, 189–195. MR 2423231 (2009c:20010)

[Hig40] G. Higman, *Units in group rings*, 1940, Thesis (Ph.D.)–Univ. Oxford.

[JdR15a] E. Jespers and Á. del Río, *Group ring groups*, vol. 1: Orders and generic constructions of units, Walter De Gruyter, 2015.

[JdR15b] ———, *Group ring groups*, vol. 2: Structure theorems on unit groups, Walter De Gruyter, 2015.

[KK17] W. Kimmerle and A. Konovalov, *On the Gruenberg-Kegel graph of integral group rings of finite groups*, Internat. J. Algebra Comput. **27** (2017), no. 6, 619–631. MR 3708045

[Kli91] L. Klingler, *Construction of a counterexample to a conjecture of Zassenhaus*, Comm. Algebra **19** (1991), no. 8, 2303–2330. MR 1123126

[LP89] I.S. Luthar and I.B.S. Passi, *Zassenhaus conjecture for* A_5, Proc. Indian Acad. Sci. Math. Sci. **99** (1989), no. 1, 1–5. MR 1004634 (90g:20007)

[MdR18] L. Margolis and Á. del Río, *Partial augmentations power property: A Zassenhaus Conjecture related problem*, J. Pure Appl. Algebra, https://doi.org/10.1016/j.jpaa.2018.12.018 (2018), 1–13.

[MdR19] ———, *Finite subgroups of group rings: A survey*, To appear in Advances in Group Theory and Applications. Preprint, arxiv.org/abs/1809.00718 (2019), 20 pages.

[MdRS19] 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*, Journal of Algebra **531** (2019), 320–335.

[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** (1987), no. 3, 340–352. MR 880467 (88k:20019)

[PMS84] C. Polcino Milies and S.K. Sehgal, *Torsion units in integral group rings of metacyclic groups*, J. Number Theory **19** (1984), no. 1, 103–114. MR 751167 (86i:16009)

[Rog91] K. Roggenkamp, *Observations on a conjecture of Hans Zassenhaus*, Groups—St. Andrews 1989, Vol. 2, London Math. Soc. Lecture Note Ser., vol. 160, Cambridge Univ. Press, Cambridge, 1991, pp. 427–444. MR 1123997

[San81] R. Sandling, *Graham Higman's thesis "Units in group rings"*, Integral representations and applications (Oberwolfach, 1980), Lecture Notes in Math., vol. 882, Springer, Berlin-New York, 1981, pp. 93–116. MR 646094

[Seh93] S. K. Sehgal, *Units in integral group rings*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 69, Longman Scientific & Technical, Harlow, 1993. MR 1242557 (94m:16039)

[Val94] A. Valenti, *Torsion units in integral group rings*, Proc. Amer. Math. Soc. **120** (1994), no. 1, 1–4. MR 1186996

[Wei91] A. Weiss, *Torsion units in integral group rings*, J. Reine Angew. Math. **415** (1991), 175–187. MR 1096905 (92c:20009)

[Whi68] A. Whitcomb, *The group ring problem*, ProQuest LLC, Ann Arbor, MI, 1968, Thesis (Ph.D.)–The University of Chicago. MR 2611595

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

Ángel del Río, Departamento de Matemáticas, Universidad de Murcia, 30100, Murcia, Spain
E-mail address: adelrio@um.es