UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

On the Zassenhaus Conjecture for PSL(2,q), SL(2,q) and Direct Products

Sobre la Conjetura de Zassenhaus para PSL(2,q), SL(2,q) y Productos Directos

D. Mariano Serrano Sánchez
2018

Escuela Internacional de Doctorado
Universidad de Murcia
Tesis Doctoral

On the Zassenhaus Conjecture for PSL(2,q), SL(2,q) and direct products

Sobre la Conjetura de Zassenhaus para PSL(2,q), SL(2,q) y productos directos

Author: Mariano Serrano Sánchez

Tutor: Ángel del Río Mateos

April 19, 2018

Acknowledgments

I would like to express my sincere gratitude to Ángel del Río for his continuous support of my PhD, encouragement, unconditional dedication and his immense knowledge.

I am also really grateful to Wolfgang Kimmerle and Juan Jacobo Simón for the good advice and helpful conversations which helped me in all the time of this thesis.

I would like also to thank Andreas Bächle and Leo Margolis for their kind hospitality and important contribution to my mathematical background.

I would like to thank my fellow doctoral students of the Lázaro Cánovas Room for their feedback, cooperation and friendship.

I must also acknowledge Ministerio de Economía y Competitividad (MTM2012-35240 and MTM2016-77445-P), Fondos FEDER and Fundación Séneca of Murcia (19880/GERM/15), for making this study possible by providing me financial support.

To Cristina.
To my mum.

Contents

Resumen

Sean G un grupo y R un anillo. El anillo de grupo RG de G con coeficientes en R es el anillo que contiene a R como subanillo y a G como subgrupo de su grupo de unidades de tal forma que G es una base de RG como R-módulo y los elementos de R y de G conmutan. Si K es un cuerpo entonces el anillo de grupo KG se llama el álgebra de grupo de G con coeficientes en K. El estudio de los anillos de grupo y de las álgebras de grupo ha sido siempre un tema de mucha importancia dentro del álgebra abstracta, principalmente porque se ha usado como herramienta en la teoría de grupos, debido a su conexión con las representaciones de grupos, y también porque utiliza propiedades propias de la teoría de grupos y de anillos.

De entre todos los anillos de grupo, se muestra un especial interés en el estudio del anillo de grupo con coeficientes enteros $\mathbb{Z}G$ de un grupo finito G, y más concretamente, en las propiedades aritméticas y algebraicas del grupo de unidades de $\mathbb{Z}G$, el cual se denota por $\mathcal{U}(\mathbb{Z}G)$. En este caso también la teoría de números es de gran utilidad. Todo esto puede verse como un caso particular del estudio del grupo de unidades de un $\mathbb{Z}$-orden en un álgebra racional semisimple de dimensión finita. Este tipo de órdenes son conocidos como órdenes clásicos. Un ejemplo sería el anillo de enteros algebraicos de un cuerpo. En relación a esta línea de investigación, recomendamos la lectura del trabajo [Kle94].

Varios libros se han publicado sobre el estudio de los anillos de grupo [Pas85, Pas79]. En concreto, el estudio de $\mathcal{U}(\mathbb{Z}G)$ cobró mucho importancia después del trabajo de Higman [Hig40]. Además, los libros [Seh93, JdR16, RT92] recolectan muchos resultados y técnicas que se utilizan en esta investigación (recomendamos las recopilaciones de Jespers y Kimmerle [Jes98, Kim13]).

Uno de los principales problemas en el estudio de los anillos de grupo con coeficientes enteros es el Problema del Isomorfismo, el cual pregunta si el anillo de

grupo determina al grupo salvo isomorfismos:

> **(IP):** Dados un anillo R y grupos finitos G y H, ¿$RG \simeq RH$ implica $G \simeq H$?

De hecho, es fácil encontrar respuestas negativas para (IP) con $R = \mathbb{C}$. Por ejemplo, si G y H son grupos abelianos finitos entonces $\mathbb{C}G \simeq \mathbb{C}H$ si y solo si G y H tienen el mismo cardinal. Sin embargo, (IP) tiene respuesta positiva con $R = \mathbb{Q}$ y con $R = \mathbb{Z}$ si G es un grupo abeliano finito. Esto es consecuencia del Teorema de Perlis-Walker [PMS02, Teorema 3.5.4].

Una respuesta negativa muy general al (IP) para álgebras de grupo fue proporcionada por Dade [Dad71], el cual mostró dos grupos finitos no isomorfos G y H con $FG \simeq FH$ para todo cuerpo F. En relación al (IP) para $R = \mathbb{Z}$, Withcomb obtuvo una respuesta positiva para grupos metabelianos en 1968 [Whi68]. Además, Roggenkamp y Scott dieron respuestas positivas para grupos nilpotentes en 1987 [RS87]. La primera respuesta negativa al (IP) para $R = \mathbb{Z}$ fue anunciada en 1997 por Hertweck [Her01].

Un caso particular del (IP) para el cual todavía no se conoce respuesta negativa es el llamado Problema del Isomorfismo Modular:

> **(MIP):** Dados p-grupos finitos G y H, y $\mathbb{F}_p$ el cuerpo con p elementos, ¿$\mathbb{F}_pG \simeq \mathbb{F}_pH$ implica $G \simeq H$?

Este problema ha sido estudiado por muchos autores [Pas65, HS06, San85, Bov98, NS17] y tiene respuesta positiva para p-grupos de orden como mucho p^5, para 2-grupos de orden como mucho 2^9 y 3-grupos de orden como mucho 3^6 (para más detalles consultar [EK11, Introducción]).

Otro problema relevante consiste en describir los automorfismos de $\mathbb{Z}G$. De hecho, hay dos subgrupos naturales del grupo de automorfismos de $\mathbb{Z}G$. El primero de ellos está formado por las extensiones lineales de automorfismos de G, que denotamos por $\mathrm{Aut}(G)$, y el segundo es el grupo de los automorfismos internos de $\mathbb{Z}G$, el cual es denotado por $\mathrm{Inn}(\mathbb{Z}G)$. Más aún, denotamos por $\mathrm{Inn}_{\mathbb{Q}}\,\mathbb{Z}G$ al grupo formado por los automorfismos de $\mathbb{Z}G$ que se pueden obtener como restricción a $\mathbb{Z}G$ de un automorfismo interno de $\mathbb{Q}G$, o sea dados por la conjugación de unidades de $\mathbb{Q}G$ que normalizan $\mathbb{Z}G$. Consideramos $\mathrm{Aut}(G)$ incluido en $\mathrm{Aut}(\mathbb{Z}G)$ por extensiones lineales y usando que $\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$ es un subgrupo normal de $\mathrm{Aut}(\mathbb{Z}G)$ deducimos que $\mathrm{Aut}(G)\,\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$ es un subgrupo de $\mathrm{Aut}(\mathbb{Z}G)$. De hecho, todo elemento de $\mathrm{Aut}(G)\,\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$ preserva aumentos y el Problema del Automorfismo pregunta precisamente por el recíproco:

> **(AUT):** ¿Todo automorfismo de $\mathbb{Z}G$ que preserve aumentos pertenece a $\mathrm{Aut}(G)\,\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$?

Una respuesta negativa para (AUT) fue obtenida por Roggenkamp y Scott [Rog91, Sco92]. También hay respuestas negativas de Klinger [Kli91] y de Hertweck [Her02].

En los años 1960, Zassenhaus propuso el problema de describir las unidades de torsión de $\mathcal{U}(\mathbb{Z}G)$ (es decir, las unidades con orden finito) y más generalmente el problema de describir los subgrupos finitos de $\mathcal{U}(\mathbb{Z}G)$. Denotamos por $\mathrm{V}(\mathbb{Z}G)$ al grupo de las unidades con aumento uno de $\mathbb{Z}G$ (son las llamadas unidades normalizadas), esto es

$$\mathrm{V}(\mathbb{Z}G) = \left\{ \sum_{g\in G} u_g g \in \mathcal{U}(\mathbb{Z}G) : \sum_{g\in G} u_g = 1 \right\}.$$

Entonces $\mathrm{V}(\mathbb{Z}G)$ es un subgrupo de índice 2 en $\mathcal{U}(\mathbb{Z}G)$ y de hecho se tiene que $\mathcal{U}(\mathbb{Z}G) = \pm\mathrm{V}(\mathbb{Z}G)$. Esta es la razón por la que a la hora de estudiar $\mathcal{U}(\mathbb{Z}G)$ es suficiente con estudiar $\mathrm{V}(\mathbb{Z}G)$ y, en particular, para describir las unidades de torsión de $\mathbb{Z}G$ es suficiente con considerar las unidades normalizadas.

Sea G un grupo finito. Las unidades de torsión más obvias de $\mathrm{V}(\mathbb{Z}G)$ son los elementos de G. Si G es abeliano entonces los elementos de G son las únicas unidades de torsión normalizadas, gracias a un resultado de Higman [Seh93, Proposición 1.4]. Sin embargo, esto no se puede extender a grupos no abelianos porque los conjugados de los elementos de G son unidades de torsión normalizadas y normalmente G no es invariante por conjugación. Una manera obvia de producir unidades de torsión normalizadas de $\mathbb{Z}G$ es tomando inversos de los elementos de G. Por lo tanto, una pregunta natural sería si éstas son todas las unidades de torsión normalizadas. Hughes y Pearson demostraron en [HP72] que $\mathrm{V}(\mathbb{Z}S_3)$ tiene dos clases de conjugación de elementos de orden 2 (donde S_3 denota el grupo simétrico en 3 símbolos). Sin embargo, todas las unidades normalizadas de orden

2 de $\mathcal{U}(\mathbb{Z}G)$ son conjugadas en $\mathbb{Q}S_3$. Esto sugiere una modificación del problema, siendo G un grupo finito, el cual tomó la forma de las siguientes tres conjeturas conocidas por el nombre de las Conjeturas de Zassenhaus [Zas74] (ver [Seh93, Section 37] para más detalles):

> **(ZC1):** Todo elemento de torsión de $\mathrm{V}(\mathbb{Z}G)$ es conjugado de un elemento de G en $\mathbb{Q}G$.
>
> **(ZC2):** Todo subgrupo finito de $\mathrm{V}(\mathbb{Z}G)$ con el mismo cardinal que G es conjugado de G en $\mathbb{Q}G$.
>
> **(ZC3):** Todo subgrupo finito de $\mathrm{V}(\mathbb{Z}G)$ es conjugado de un subgrupo de G en $\mathbb{Q}G$.

Diremos que dos elementos de $\mathbb{Z}G$ son conjugados racionales si son conjugados en las unidades de $\mathbb{Q}G$. Por lo tanto, (ZC1) se verifica para $\mathbb{Z}G$ si y solo si todo elemento de torsión de $\mathrm{V}(\mathbb{Z}G)$ es conjugado racional de un elemento de G.

Claramente (ZC1) y (ZC2) son casos particulares de (ZC3). Además, (ZC2) está muy relacionada con (IP) y con (AUT). Esto es porque un subgrupo de unidades de $\mathbb{Z}G$ que tenga el mismo cardinal que G es un grupo base de $\mathbb{Z}G$ y por supuesto isomorfismos entre anillos envían grupos base a grupos base. Utilizando esto se puede demostrar que

$$\text{(ZC2)} \iff \text{(IP)} + \text{(AUT)}.$$

Esto implica que las respuestas negativas para (AUT) dadas por Roggenkamp y Scott, Klingler y Hertweck, y la respuesta negativa para (IP) también dada por Hertweck, son todas contraejemplos para (ZC2) (y por lo tanto también para (ZC3)). Además, las tres conjeturas mencionadas anteriormente se verifican para clases importantes de grupos. Por ejemplo para grupos nilpotentes [Wei91].

Hoy día, (ZC1) es considerada como un problema muy importante en este área y su progreso ha dado lugar a técnicas muy profundas. Recopilamos a continuación varios resultados positivos sobre las Conjeturas de Zassenhaus.

A raíz de los cálculos de Hughes y Pearson, mencionados anteriormente donde ellos demuestran (ZC1) para S_3, varios autores empezaron a estudiar (ZC1) para grupos particulares. En 1987, Fernandes demostró (ZC1) para S_4 [Fer87], también fue demostrada para A_5 en 1989 por Luthar y Passi [LP89], y para S_5 en 1991 por Luthar y Trama [LT91]. Dokuchaev, Juriaans y Polcino Milies demostraron (ZC1) para $\mathrm{SL}(2,5)$ en 1997 [DJMP97]. En 2008, Hertweck demostró (ZC1) para A_6 [Her08c] y Bovdi y Hertweck la demostraron para extensiones centrales de S_5 [BH08].

Roggenkamp y Scott demostraron el primer resultado importante sobre la Conjetura de Zassenhaus para clases más grandes de grupos. Ellos demostraron (ZC2) para grupos nilpotentes en 1987 [RS87]. Además, Weiss demostró (ZC3) para p-grupos [Wei88] y más tarde también para grupos nilpotentes [Wei91].

El estudio de (ZC1) para grupos metacíclicos recibió mucha atención desde 1980 y fue demostrada para varios casos particulares [MRSW87, LB83, LS98, LT90, PMRS86, PMS84, SW86, dRS06]. La demostración general para esta clase de grupos fue conseguida por Hertweck en 2008 [Her08b]. De hecho, Hertweck demostró (ZC1) para grupos de la forma $G = AB$ con A un subgrupo normal cíclico de G y B un subgrupo abeliano de G. Este resultado ha sido extendido en [CMdR13] para grupos cíclico-por-abeliano. Además, (ZC1) ha sido verificada para varios grupos no resolubles [BKM18, KK17].

En contraste con los resultados mencionados anteriormente para los cuales se demuestra (ZC1) para grandes clases de grupos resolubles, al comienzo de este trabajo (ZC1) no se había demostrado para ninguna familia infinita de grupos no resolubles. De hecho, (ZC1) había sido demostrada solo para 13 grupos simples (ver [BM17b]).

Recopilando todos los resultados conocidos hasta ahora, (ZC1) ha sido verificada para todos los grupos de orden como mucho 144 [BHK$^+$17, BHK04, HK06]. La mejor herramienta para demostrar (ZC1) para estos grupos ha sido el llamado Método HeLP, el cual podría ser resumido como sigue (para más detalles ver Sección 1.4): Sea G un grupo finito y sea u un elemento de orden n en $\mathrm{V}(\mathbb{Z}G)$. Para un elemento $g \in G$, usaremos la notación $\varepsilon_g(u)$ para referirnos a la suma de todos los coeficientes de u con respecto a la clase de conjugación de g. A esta suma se la conoce como el aumento parcial de u con respecto a g. La relevancia de los aumentos parciales para el estudio de (ZC1) viene dada por un resultado de Marciniak, Ritter, Sehgal y Weiss, los cuales demostraron que u es conjugada racional de un elemento de G si y solo si todos los aumentos parciales de las potencias de u son no negativos. La idea básica del Método HeLP consiste en producir restricciones sobre los posibles aumentos parciales de las potencias de u utilizando la siguiente fórmula para todo carácter χ de G y todo entero ℓ:

$$\frac{1}{n}\sum_{g\in T}\sum_{d|n}\varepsilon_g(u^d)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(g)\zeta_n^{-\ell d}),$$

donde T denota un conjunto de representantes de las clases de conjugación de G y ζ_n denota una raíz n-ésima compleja primitiva de la unidad. Este método ha sido implimentado en GAP [GAP16] por Bächle y Margolis [BM15].

Durante la elaboración de esta tesis, un contraejemplo metabeliano para (ZC1) fue anunciado por Eisele y Margolis [EM17]. En vista de este contraejemplo, versiones más débiles (también podríamos decir sustitutas) de (ZC1) han adquirido relevancia en esta línea de investigación (ver recopilación en [MdR17]). Mencionamos a continuación algunas de ellas.

Recordamos que el espectro de un grupo G es el conjunto de los órdenes de sus elementos de torsión. El grafo primo de G es el grupo no dirigido $\Gamma(G)$ que tiene como vértices aquellos primos p para los cuales hay un elemento de orden p en G y dos vértices p y q están conectados siempre que haya un elemento de orden pq en G. Claramente, si (ZC1) se verifica para G entonces G y $\mathrm{V}(\mathbb{Z}G)$ tienen el mismo espectro y si G y $\mathrm{V}(\mathbb{Z}G)$ tienen el mismo espectro entonces también tienen el mismo grafo. Esto dio lugar a los siguientes problemas: El primero de ellos es conocido como el Problema del Espectro (ver [Seh93, Problem 8]) y el segundo de ellos es la Pregunta del Grafo Primo (ver [Ari07, Problem 21]):

(SP): Dado un grupo finito G, ¿tienen G y $\mathrm{V}(\mathbb{Z}G)$ el mismo espectro?

(PQ): Dado un grupo finito G, ¿tienen G y $\mathrm{V}(\mathbb{Z}G)$ el mismo grafo primo?

Se conocen respuestas positivas para (SP) y (PQ) para clases de grupos más grandes que para los que se ha demostrado (ZC1). Por ejemplo, (SP) se verifica para todos los grupos resolubles [Her08a]. Además, (PQ) se verifica para muchos grupos simples esporádicos [BKL11] y para algunas series infinitas de grupos casi simples [BM17a].

Hay un teorema de reducción del (PQ) demostrado por Kimmerle y Konovalov en [KK17, Teorema 2.1], el cual afirma que (PQ) tiene una respuesta positiva para G siempre que éste sea el caso para todos sus imágenes casi simples (recordamos que un grupo A es casi simple si hay un grupo simple no abeliano que verifica $\mathrm{Inn}(S) \leq A \leq \mathrm{Aut}(S)$).

Otro problema de relevancia ha sido propuesto en [Ari07, Pregunta 22] y es conocido como el Problema de Kimmerle:

> **(KP):** Dado un elemento de torsión u en $\mathrm{V}(\mathbb{Z}G)$, ¿hay un grupo finito H que contenga a G como subgrupo tal que u es conjugado en $\mathbb{Q}H$ de un elemento de G?

El siguiente problema fue estudiado por Bovdi [Bov87, p. 26] y es conocido como el Problema de Bovdi, mientras que su generalización es conocida como el Problema de Bovdi Generalizado (ver [Seh93, Problema 44]). Para enunciar ambos problemas necesitamos introducir algo de notación. Para un elemento $u \in \mathrm{V}(\mathbb{Z}G)$ y un entero positivo m, denotamos por $\varepsilon_{G[m]}(u)$ a la suma de los coeficientes de u con respecto a todos los elementos de G que tengan orden m.

> **(BP):** Sea u un elemento de $\mathrm{V}(\mathbb{Z}G)$ con orden p^n y p un número primo. ¿Se tiene que $\varepsilon_{G[p^k]}(u) = 0$ para todo $k \neq n$ y $\varepsilon_{G[p^n]}(u) = 1$?

> **(Gen-BP):** Sea u un elemento de $\mathrm{V}(\mathbb{Z}G)$ con orden n. ¿Se tiene que $\varepsilon_{G[m]}(u) = 0$ para todo $m \neq n$?

En [MdR17] se demuestra que (KP) y (Gen-BP) son equivalentes. De hecho, en lo referido a (KP) es de interés el construir H suficientemente pequeño de tal forma que se verifique (ZC1).

Resumimos en el siguiente diagrama las relaciones lógicas entre los problemas mencionados anteriormente (ver [MdR17, Proposición 2.1]):

$$\text{(ZC1)} \implies \text{(KP)} \iff \text{(Gen-BP)} \implies \text{(SP)} \implies \text{(PQ)}.$$

Describimos a continuación los resultados de la tesis. Nuestro primer logro consiste en mostrar las limitaciones del Método HeLP en el estudio de (ZC1) para grupos proyectivos especiales lineales. Más concretamente, por resultados de Hertweck [Her07] y Margolis [Mar16] es conocido que si $G = \mathrm{PSL}(2, q)$ con $q = p^f$ y p un número primo, y u un elemento de $\mathrm{V}(\mathbb{Z}G)$ con orden n, entonces u es conjugado racional de un elemento de G en los siguientes casos:

- n es potencia de un primo no divisible por p.
- $f \leq 2$ y n es divisible por p.
- $n = 6$ y $\gcd(6, p) = 1$.

Estos resultados han sido todos obtenidos usando el Método HeLP. De hecho, Hertweck expresó que "quizás se pueda esperar más cuando la versión p-modular del Método de Luthar-Passi se use más rigurosamente" para demostrar (ZC1) para $\mathrm{PSL}(2, q)$ [Her07]. Desafortunadamente, éste no es el caso como nuestro primer resultado muestra (ver Teorema 3.2.1). En este resultado calculamos cómo de lejos podemos llegar después de aplicar el Método HeLP para unidades en $\mathbb{Z}\,\mathrm{PSL}(2, q)$ con orden $2t$ con q potencia de un primo impar y t un número primo que sea coprimo con $2q$. Por otro lado, como segundo logro hemos conseguido demostrar que toda unidad de torsión de $\mathbb{Z}\,\mathrm{PSL}(2, q)$ con orden coprimo con $2q$ es conjugada racional de un elemento de $\mathrm{PSL}(2, q)$ (ver Teorema 3.3.1). Para ello hemos introducido una variación del Método HeLP que se adapta mucho mejor a los caracteres del grupo $\mathrm{PSL}(2, q)$ dado que el Método HeLP clásico hubiera implicado muchas distinciones de casos. Ésta es la razón por la que podríamos considerar esta nueva versión del método como un atajo adaptado para el estudio de (ZC1) para $\mathrm{PSL}(2, q)$. Como consecuencia de este resultado hemos conseguido demostrar (ZC1) para $\mathrm{PSL}(2, p)$ con p un primo de Fermat o de Mersenne (ver Teorema 3.3.2). Este resultado aumenta el número de grupos simples no-abelianos para los cuales se verifica (ZC1) de 13 hasta al menos 62 grupos. Además, utilizando la misma técnica mencionada anteriormente, hemos obtenido algunos avances sobre (ZC1) para grupos especiales lineales. Más concretamente, hemos demostrado como tercer logro que toda unidad de torsión de $\mathbb{Z}\,\mathrm{SL}(2, q)$ con orden coprimo con q es conjugada racional de un elemento de $\mathrm{SL}(2, q)$ (ver Teorema 4.2.2). Como consecuencia de este resultado, hemos conseguido demostrar (ZC1) para $\mathrm{SL}(2, p^f)$

con p un número primo y $f \leq 2$ (ver Teorema 4.2.1). Ésta es la primera familia infinita de grupos no resolubles para los cuales se ha demostrado (ZC1).

Otra importante contribución de esta tesis ha sido la respuesta positiva del (KP) en el caso en que G tenga un subgrupo normal de Hall que sea producto directo de subgrupos de Sylow, con complemento abeliano (ver Teorema 5.1.2). Aquí G se encuentra incluido dentro de un producto directo adecuado de grupos Sylow-por-abelianos para los cuales (ZC1) se cumple (ver Corolario 5.1.3). Esto demuestra (KP), en particular, para los contraejemplos de (ZC1) construidos por Eisele y Margolis en [EM17] y muestra que la propiedad (ZC1) no es cerrada para subgrupos. En contraste con esto, (KP) sí es cerrada para subgrupos. Además, demostramos que (KP) se verifica cuando G es un grupo con una torre de Sylow (ver Teorema 5.1.6). En particular también se tiene para la clase de los grupos superresolubles.

Nos centramos a continuación en el estudio de (ZC1) para productos directos. Más concretamente, consideramos el siguiente problema:

> **Problema:** Sean G y H dos grupos finitos. Supongamos que (ZC1) se verifica para G y para H. ¿(ZC1) se verifica para $G \times H$?

Muy poco es conocido sobre este problema. Si H es un 2-grupo abeliano elemental entonces este problema tiene respuesta afirmativa, la cual fue obtenida por Höfert y Kimmerle [HK06]. Además, Hertweck demostró que (ZC1) se verifica para $G \times H$ siempre que H sea un grupo nilpotente y G sea un grupo finito arbitrario para el que se verifica (ZC1) y cuyo orden es coprimo con el orden de H [Her08a, Proposición 8.1].

Otra importante contribución de esta tesis es la demostración de (ZC1) para el producto directo de un grupo de Frobenius finito con complementos metacíclicos, y de un grupo abeliano finito (ver Proposición 5.2.5). Además, demostramos que (KP) tiene respuesta positiva para el producto directo de un grupo de Frobenius con un grupo abeliano finito (ver Teorema 6.2.7).

La situación en la cual tenemos grupos de la forma $G \times A$ donde (ZC1) se verifica para G y A es un grupo abeliano finito, da lugar naturalmente al problema de considerar el análogo de (ZC1) para anillos de grupo $\mathcal{O}G$ donde $\mathcal{O}$ es un anillo de enteros algebraicos (ver Problema 6.1.2 y Proposición 6.1.1). En la Sección 6.1

extendemos el clásico Método HeLP para anillos de grupo $\mathcal{O}G$. Utilizando este nuevo método, hemos estudiado (ZC1) para el producto directo $G \times A$ donde G es un grupo de orden a lo sumo 95 y A es un grupo abeliano finito (ver Proposición 6.1.9) y hemos conseguido demostrar que (KP) tiene una respuesta positiva para estos grupos (ver Teorema 6.2.8).

Introduction

Given a group G and a ring R, the *group ring* RG of G with coefficients in R is the ring which contains R as a subring and G as a subgroup of its group of units in such a way that G is a basis of RG as R-module and the elements of R and G commute. If K is a field then the group ring KG is called the *group algebra* of G with coefficients in K. The study of group rings and group algebras has always been an important point of interest in abstract algebra because it is used as a tool in group theory, due to its connection with group representations, and also because it uses properties coming from group theory itself and ring theory.

Of special interest is the integral group ring $\mathbb{Z}G$ of a finite group G, and more precisely, the arithmetic and algebraic properties of the group of units of $\mathbb{Z}G$, which is denoted by $\mathcal{U}(\mathbb{Z}G)$. In this case also properties coming from number theory could be very useful. This could be seen as a particular case of the study of the unit group of a $\mathbb{Z}$-order in a semisimple rational algebra of finite dimension. This type of orders are known as classical orders. One example would be the ring of algebraic integers of a field. For this line of research we recommend the work [Kle94].

Several books have been published studying just group rings [Pas85, Pas79]. The study of $\mathcal{U}(\mathbb{Z}G)$ found much attention after Higman's work [Hig40]. The books [Seh93, JdR16, RT92] collect many results and techniques of this subject (see also the surveys of Jespers and Kimmerle [Jes98, Kim13]).

One of the main questions on the study of integral group rings is the *Isomorphism Problem*, which asks whether the group ring determines the group up to isomorphism:

> **(IP):** For a ring R and finite groups G and H, does $RG \simeq RH$ imply $G \simeq H$?

In fact, negative solutions for (IP) with $R = \mathbb{C}$ are easy to find. For example, if G and H are finite abelian groups then $\mathbb{C}G \simeq \mathbb{C}H$ if and only if G and H have the same cardinality. However, (IP) has a positive solution with $R = \mathbb{Q}$ and $R = \mathbb{Z}$ if G is finite abelian. This is a consequence of the Perlis-Walker Theorem [PMS02, Theorem 3.5.4].

A very general negative solution of (IP) for group algebras was provided by Dade [Dad71] who showed two non isomorphic finite groups G and H with $FG \simeq FH$ for every field F. Concerning (IP) for the case where $R = \mathbb{Z}$, Withcomb proved that (IP) has a positive solution for metabelian groups in 1968 [Whi68]. Roggenkamp and Scott also proved that (IP) has a positive solution for nilpotent groups in 1987 [RS87]. The first negative solution for (IP) for the case $R = \mathbb{Z}$ was announced in 1997 by Hertweck [Her01].

A particular case of (IP) for which no negative solution is known is the so called *Modular Isomorphism Problem*:

> **(MIP):** Given G and H finite p-groups and $\mathbb{F}_p$ the field with p elements, does $\mathbb{F}_pG \simeq \mathbb{F}_pH$ imply $G \simeq H$?

This problem has been studied for many authors [Pas65, HS06, San85, Bov98, NS17] and it has an affirmative answer for p-groups of order at most p^5, for 2-groups of order at most 2^9 and for 3-groups of order at most 3^6 (see [EK11, Introduction] for more details).

Another relevant question consists in describing the automorphisms of $\mathbb{Z}G$. Actually, there are two natural subgroups of the group of automorphisms of $\mathbb{Z}G$. The first one is formed by the linear extensions of automorphism of G, denoted by $\mathrm{Aut}(G)$, and the second one is the group of inner automorphism of $\mathbb{Z}G$ which is denoted by $\mathrm{Inn}(\mathbb{Z}G)$. Moreover, denote by $\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$ the group formed by the automorphism of $\mathbb{Z}G$ which could be obtained as a restriction to $\mathbb{Z}G$ of an inner automorphism of $\mathbb{Q}G$, i.e. they are given by conjugation of units which normalize $\mathbb{Z}G$. Considering $\mathrm{Aut}(G)$ embedded in $\mathrm{Aut}(\mathbb{Z}G)$ by linear extensions and using that $\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$ is a normal subgroup of $\mathrm{Aut}(\mathbb{Z}G)$ we deduce that $\mathrm{Aut}(G)\,\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$ is a subgroup of $\mathrm{Aut}(\mathbb{Z}G)$. In fact, every element of $\mathrm{Aut}(G)\,\mathrm{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$ preserves augmentation and the *Automorphism Problem* asks for the converse:

(AUT): Does every augmentation preserving automorphism of $\mathbb{Z}G$ belong to $\operatorname{Aut}(G)\operatorname{Inn}_{\mathbb{Q}}(\mathbb{Z}G)$?

A metabelian negative solution for (AUT) was obtained by Roggenkamp and Scott [Rog91, Sco92]. Other negative solutions are due to Klinger [Kli91] and Hertweck [Her02].

In the 1960s, Zassenhaus raised the problem of describing the *torsion units* of $\mathcal{U}(\mathbb{Z}G)$ (i.e. units with finite order) and more generally of how are the finite subgroups of $\mathcal{U}(\mathbb{Z}G)$. Let $\mathrm{V}(\mathbb{Z}G)$ denote the set of units of augmentation one of $\mathbb{Z}G$ (so called *normalized units*), that is

$$\mathrm{V}(\mathbb{Z}G) = \left\{ \sum_{g\in G} u_g g \in \mathcal{U}(\mathbb{Z}G) : \sum_{g\in G} u_g = 1 \right\}.$$

Then $\mathrm{V}(\mathbb{Z}G)$ is a subgroup of index 2 of $\mathcal{U}(\mathbb{Z}G)$ and actually $\mathcal{U}(\mathbb{Z}G) = \pm\mathrm{V}(\mathbb{Z}G)$. This is the ultimate reason why in order to study $\mathcal{U}(\mathbb{Z}G)$ it is enough to consider $\mathrm{V}(\mathbb{Z}G)$ and, in particular, to describe the torsion units of $\mathbb{Z}G$ we only regard the normalized units.

Assume that G is a finite group. The most obvious torsion elements of $\mathrm{V}(\mathbb{Z}G)$ are the elements of G. If G is abelian then these are the only normalized torsion units, by a result of Higman [Seh93, Proposition 1.4]. This cannot be extended to non-abelian groups because the conjugates of the elements of G are, of course, normalized torsion units and usually G is not invariant under conjugation. An obvious way to produce normalized torsion units of $\mathbb{Z}G$ is by taking conjugates of the elements of G. Therefore, a natural question is whether these are all the normalized torsion units. Hughes and Pearson showed in [HP72] that $\mathrm{V}(\mathbb{Z}S_3)$ has two conjugacy classes of elements of order 2 (here S_3 denotes the symmetric group on 3 symbols). However all normalized units of order 2 of $\mathcal{U}(\mathbb{Z}S_3)$ are conjugate in $\mathbb{Q}S_3$. This suggested a modification of the problem, for G a finite group, which took the form of the following three conjectures known as Zassenhaus Conjectures [Zas74] (see [Seh93, Section 37] for more details):

(ZC1): Every torsion element of $\mathrm{V}(\mathbb{Z}G)$ is conjugate to an element of G in $\mathbb{Q}G$.

(ZC2): Every finite subgroup of $\mathrm{V}(\mathbb{Z}G)$ with the same cardinality as G is conjugate to G in $\mathbb{Q}G$.

(ZC3): Every finite subgroup of $\mathrm{V}(\mathbb{Z}G)$ is conjugate to a subgroup of G in $\mathbb{Q}G$.

We say that two elements of $\mathbb{Z}G$ are *rationally conjugate* if they are conjugate in the units of $\mathbb{Q}G$. Thus, (ZC1) holds for $\mathbb{Z}G$ if and only if every torsion element of $\mathrm{V}(\mathbb{Z}G)$ is rationally conjugate to an element of G.

Clearly (ZC1) and (ZC2) are particular cases of (ZC3). Moreover (ZC2) is strongly linked to (IP) and (AUT). This is because a subgroup of units of $\mathbb{Z}G$ having the same cardinality than G is a group basis of $\mathbb{Z}G$ and of course isomorphisms between rings map group basis to group basis. Using this it can be shown that

$$\text{(ZC2)} \iff \text{(IP)} + \text{(AUT)}.$$

This implies that the negative solutions for (AUT) by Roggenkamp and Scott, Klingler and Hertweck and the negative solution for (IP) by the last author are all counterexamples for (ZC2) (and hence for (ZC3)). Moreover, all three conjectures stated above are true for important classes of groups, e.g. for nilpotent groups by a result of Weiss [Wei91].

Nowadays, (ZC1) is considered as an important question in this area and its progress has developed deep techniques. We now collect some positive results on the Zassenhaus Conjectures.

After the calculations of Hughes and Pearson mentioned above where they proved (ZC1) for S_3, several authors started studying (ZC1) for particular groups. In 1987, Fernandes proved (ZC1) for S_4 [Fer87], it was also verified for A_5 in 1989 by Luthar and Passi [LP89], and for S_5 in 1991 by Luthar and Trama [LT91]. Dokuchaev, Juriaans and Polcino Milies proved (ZC1) for $\mathrm{SL}(2,5)$ in 1997 [DJMP97]. In 2008, Hertweck proved (ZC1) for A_6 [Her08c] and Bovdi and Hertweck proved it for central extensions of S_5 [BH08].

Roggenkamp and Scott proved the first important result on the Zassenhaus Conjecture for large classes of groups. Namely, they proved (ZC2) for nilpotent groups in 1987 [RS87]. Moreover, Weiss proved (ZC3) for p-groups [Wei88] and later also for nilpotent groups [Wei91].

The study of (ZC1) for metacyclic groups received much attention since 1980 and it was proved in some particular cases [MRSW87, LB83, LS98, LT90, PMRS86, PMS84, SW86, dRS06]. It was finally proved for this class of groups by Hertweck in 2008 [Her08b]. Actually Hertweck proved (ZC1) for groups of the form $G = AB$ with A a normal cyclic subgroup of G and B an abelian subgroup of G. This result has been extended in [CMdR13] for cyclic-by-abelian groups. Furthermore, (ZC1) has been established as well for several non-solvable groups [BKM18, KK17].

In contrast with the results mentioned above which prove (ZC1) for large classes of solvable groups, at the starting point of this work (ZC1) was not proved for any infinite family of non-solvable groups. Special attention have received the simple groups. In fact, (ZC1) had been proved only for 13 simple groups (see [BM17b]).

Collecting all the results known at the moment, (ZC1) has been verified for all groups whose order is at most 144 [BHK$^+$17, BHK04, HK06]. The best tool used in proving (ZC1) for these groups is the so called HeLP Method which can be summarized as follows (for more details see Section 1.4): Let G be a finite group and let u be an element of order n in $\mathrm{V}(\mathbb{Z}G)$. For an element $g \in G$, denote by $\varepsilon_g(u)$ the sum of all the coefficients of u with respect to the conjugacy class of g. This sum is called the *partial augmentation* of u at g. The relevance of partial augmentations on the study of (ZC1) comes from a result of Marciniak, Ritter, Sehgal and Weiss, who proved that u is rationally conjugate to an element of G if and only if all but one of the partial augmentations of the powers of u vanish. The basic idea of the HeLP Method is to produce restrictions on the possible partial augmentations of the powers of u using the following formula for every character χ of G and every integer ℓ

$$\frac{1}{n}\sum_{g\in T}\sum_{d\mid n}\varepsilon_g(u^d)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(g)\zeta_n^{-\ell d}),$$

where T denotes a set of representatives of the conjugacy classes of G and ζ_n denotes a complex primitive n-th root of unity. This method has been implemented in GAP [GAP16] by Bächle and Margolis [BM15].

During the preparation of this thesis, a metabelian counterexample for (ZC1) was announced by Eisele and Margolis [EM17]. In view of this counterexample, weaker versions (you may also say substitutes) of (ZC1) are gaining relevance in this line of research (see [MdR17] for a recent overview). We mention here some of them.

Recall that the *spectrum* of a group G is the set of orders of its torsion elements. The *prime graph* of G is the undirected graph $\Gamma(G)$ having as vertices those primes p for which there exists an element of order p in G and two vertices p and q are connected whenever there is an element of order pq in G. Clearly, if (ZC1) holds for G then G and $\mathrm{V}(\mathbb{Z}G)$ have the same spectrum and if G and $\mathrm{V}(\mathbb{Z}G)$ have the same spectrum then they have the same graph. This yields the following problems. The first one is the *Spectrum Problem* (see [Seh93, Problem 8]) and the second one is the *Prime Graph Question* (see [Ari07, Problem 21]):

> **(SP):** Given a finite group G, do G and $\mathrm{V}(\mathbb{Z}G)$ have the same spectrum?

> **(PQ):** Given a finite group G, do G and $\mathrm{V}(\mathbb{Z}G)$ have the same prime graph?

There are positive answers for (SP) and (PQ) for much wider classes than the Zassenhaus Conjectures. For example, (SP) holds for all solvable groups [Her08a]. Moreover, (PQ) holds for many sporadic simple groups [BKL11] and for some infinite series of almost simple groups [BM17a].

There is a reduction theorem for (PQ) proved by Kimmerle and Konovalov in [KK17, Theorem 2.1] which states that (PQ) has an affirmative answer for G provided this is the case for all its almost simple images (recall that a group A is almost simple if there is a non-abelian simple group S satisfying $\mathrm{Inn}(S) \leq A \leq \mathrm{Aut}(S)$).

Another relevant problem has been posed in [Ari07, Question 22] and it is known as the *Kimmerle Problem*:

> **(KP):** Given a torsion element u in $\mathrm{V}(\mathbb{Z}G)$, is there a finite group H containing G as subgroup such that u is conjugate in $\mathbb{Q}H$ to an element of G?

The following problem was stated by Bovdi [Bov87, p. 26] and it is known as the *Bovdi Problem*, whereas its generalization is called the *General Bovdi Problem* (see

[Seh93, Problem 44]). To state both problems we need to introduce some notation. For an element $u \in \mathrm{V}(\mathbb{Z}G)$ and a positive integer m we denote by $\varepsilon_{G[m]}(u)$ the sum of the coefficients of u at all elements of order m of G.

> **(BP):** Let u be an element of $\mathrm{V}(\mathbb{Z}G)$ of prime power order p^n. Is $\varepsilon_{G[p^k]}(u) = 0$ for every $k \neq n$ and $\varepsilon_{G[p^n]}(u) = 1$?
>
> **(Gen-BP):** Let u be an element of $\mathrm{V}(\mathbb{Z}G)$ of order n. Is $\varepsilon_{G[m]}(u) = 0$ for all $m \neq n$?

In [MdR17] it is shown that (KP) and (Gen-BP) are equivalent. Certainly, concerning (KP) it is of interest to construct H sufficiently small and satisfying (ZC1).

We collect in the following diagram the logical connections of the previous problems (see [MdR17, Proposition 2.1]):

$$\text{(ZC1)} \implies \text{(KP)} \iff \text{(Gen-BP)} \implies \text{(SP)} \implies \text{(PQ)}.$$

We now describe the achievements of this thesis. Our first achievement consists in showing the limitations of the HeLP Method on the study of (ZC1) for projective special linear groups. More precisely, by results of Hertweck [Her07] and Margolis [Mar16] it is known that if $G = \mathrm{PSL}(2, q)$ with $q = p^f$ and p a prime integer, and u is an element of $\mathrm{V}(\mathbb{Z}G)$ of order n, then u is rationally conjugate to an element of G in the following cases:

- n is a prime power not divisible by p.
- $f \leq 2$ and n is divisible by p.
- $n = 6$ and $\gcd(6, p) = 1$.

These results have been all obtained using the HeLP Method. Actually, Hertweck expressed that "perhaps more can be expected when the p-modular version of the Luthar-Passi Method is used more rigorously" to prove (ZC1) for $\mathrm{PSL}(2, q)$ [Her07]. Unfortunately, this is not the case as our first result shows (see Theorem 3.2.1). It calculates how far one can go by applying the HeLP Method for units in $\mathbb{Z}\,\mathrm{PSL}(2, q)$ of order $2t$ with q an odd prime power and t a prime integer coprime with $2q$.

On the other hand, as a second achievement we prove that every torsion unit in $\mathbb{Z}\,\mathrm{PSL}(2,q)$ of order coprime with $2q$ is rationally conjugate to an element of $\mathrm{PSL}(2,q)$ (see Theorem 3.3.1). For that we have introduced a new variation of the HeLP Method which is more suitable for the characters of $\mathrm{PSL}(2,q)$ as the plain HeLP Method would involve to many case distinctions. That's why this new version should be seen as an adapted shortcut for studying (ZC1) for $\mathrm{PSL}(2,q)$. As a consequence of this result we prove (ZC1) for $\mathrm{PSL}(2,p)$ with p a Fermat or Mersenne prime (see Theorem 3.3.2). This result increases the number of non-abelian simple groups for which (ZC1) is known from thirteen to at least sixty-two groups. Moreover, using the same new technique explained above, we have obtained some advances on (ZC1) for special linear groups. Namely, we have proved as a third achievement that every torsion unit in $\mathbb{Z}\,\mathrm{SL}(2,q)$ of order coprime with q is rationally conjugate to an element of $\mathrm{SL}(2,q)$ (see Theorem 4.2.2). As a consequence of this result, we also prove (ZC1) for $\mathrm{SL}(2,p^f)$ with p a prime integer and $f \leq 2$ (see Theorem 4.2.1). This is the first infinite family of non-solvable groups for which (ZC1) has been proved.

As another contribution to this thesis, we give a positive answer to (KP) in the case when G has a normal Hall subgroup formed by the direct products of Sylow subgroups, with abelian complement (see Theorem 5.1.2). Here G is embedded into a suitable direct product of Sylow-by-abelian groups for which (ZC1) is valid (see Corollary 5.1.3). This proves, in particular, a positive answer for (KP) for the counterexamples to (ZC1) constructed by Eisele and Margolis in [EM17] and shows that the property (ZC1) is not closed under subgroups. In contrast, (KP) is inherited by subgroups. Moreover we show that (KP) holds when G is a Sylow tower group (see Theorem 5.1.6), so in particular it holds for the class of supersolvable groups.

We now turn our attention to the study of (ZC1) for direct products. Namely,

> **Problem:** Let G and H be finite groups. Assume that (ZC1) holds for G and H. Does (ZC1) hold for $G \times H$?

Very little is known about this problem. If H is an elementary abelian 2-group this was answered affirmatively by Höfert and Kimmerle [HK06]. Moreover, Hertweck proved that (ZC1) holds for $G \times H$ provided H is nilpotent and G is an arbitrary finite group for which (ZC1) holds and whose order is coprime to the order of H [Her08a, Proposition 8.1].

Another important contribution of this thesis is the proof of (ZC1) for the direct product of a Frobenius group with metacyclic complements and a finite abelian group (see Proposition 5.2.5). Moreover, we prove that (KP) holds for the direct product of a Frobenius group with any abelian finite group (see Theorem 6.2.7).

The case of groups of the form $G \times A$ where (ZC1) holds for G and A is a finite abelian group leads naturally to the problem of considering the analogue of (ZC1) for group rings $\mathcal{O}G$ where $\mathcal{O}$ is a ring of algebraic integers (see Problem 6.1.2 and Proposition 6.1.1). In Section 6.1 we extend the classical HeLP Method to group rings $\mathcal{O}G$. Using this new method we study (ZC1) for the direct product $G \times A$ where G is a group with order at most 95 and A is any abelian finite group (see Proposition 6.1.9) and we prove that (KP) holds for these groups (see Theorem 6.2.8).

We now explain the organization of the contents of this thesis. Chapter 1 is reserved to the preliminaries where we include the necessary definitions and recall some known facts. In Chapter 2 we prove some technical general results which will be used in the remaining chapters. In Chapter 3 and Chapter 4 we study (ZC1) for the groups $\mathrm{PSL}(2,q)$ and $\mathrm{SL}(2,q)$, respectively, with q a prime power. In Chapter 5 we study (ZC1) and (KP) for direct products. Finally in Chapter 6 we extend the HeLP Method to ring of algebraic integers in order to study (ZC1) and (KP) for the direct product of an abelian finite group with a group which is either a finite Frobenius group or its order is at most 95.

CHAPTER 1

Preliminaries

The necessary background is collected in this chapter. We also establish the notation, and introduce the basic concepts which will be used throughout this thesis. All material presented here is classical. Most of the results will be needed in the subsequences chapters, and the other are included to illustrate the chapter. Although not all proofs are included, we give references where they can be found.

We start fixing some general notation. The cardinality of a set X is denoted by $|X|$. As usual, φ denotes the *Euler's totient function* and μ denotes the *Möbius function*. For m an integer, p a prime (positive) integer and q a prime power, let

$v_p(m)$ = maximum non-negative integer k such that p^k divides m;

ζ_m = complex primitive m-th root of unity;

$\Phi_m(X)$ = m-th cyclotomic polynomial, i.e. the minimal polynomial of ζ_m over $\mathbb{Q}$;

$\mathbb{Z}_{\geq 0}$ = the set of non-negative integers;

$\mathbb{Z}_p$ = p-adic integers;

$\mathbb{F}_q$ = the field with q elements;

$P(m)$ = number of prime divisors of m.

1.1 Groups

In this section we establish the group theoretical notation which we are using throughout. The concepts and results presented in this section are taken mainly from [Rob82].

If G is a group, X and Y are non-empty subsets of G, and $g, h, g_1, \dots, g_n \in G$ then let

$$\begin{aligned}
Z(G) &= \textit{center} \text{ of } G; \\
G' &= \textit{commutator subgroup} \text{ of } G; \\
\exp(G) &= \textit{exponent} \text{ of } G; \\
\mathbb{Z}_{(G)} &= \text{subring of } \mathbb{Q} \text{ formed by the fractions } n/m \text{ with } \gcd(m, |G|) = 1; \\
|g| &= \text{order of } g; \\
g^h &= h^{-1}gh, \ \textit{conjugate} \text{ of } g \text{ by } h; \\
(g, h) &= g^{-1}h^{-1}gh, \text{commutator of } g \text{ and } h; \\
g^G &= \text{conjugacy class of } g \text{ in } G; \\
X^g &= \{g^{-1}xg : x \in X\}; \\
\langle X \rangle &= \text{subgroup generated by } X; \\
\langle g_1, \dots, g_n \rangle &= \text{subgroup generated by } \{g_1, \dots, g_n\}; \\
C_G(X) &= \{g \in G : (x, g) = 1 \text{ for every } x \in X\}, \textit{centralizer} \text{ of } X \text{ in } G; \\
N_G(X) &= \{g \in G : X^g \subseteq X\}, \textit{normalizer} \text{ of } X \text{ in } G.
\end{aligned}$$

Recall that the exponent of G is the smallest positive integer m such that $g^m = 1$ for every $g \in G$, in case such positive integer exists. Otherwise we set $\exp(G) = \infty$.

For g and h elements of G, we will write $g \sim_G h$ to express that g and h are conjugate. In case the group G is clear for the context, we will just write $g \sim h$.

We will use the notation $H \leq G$ to denote that H is a subgroup of G. In that case, i.e. if $H \leq G$, then we will also use the notation $H \trianglelefteq G$ (respectively $H \triangleleft G$) to denote that H is a normal subgroup (respectively proper normal subgroup) of G.

We will use the notation $G = \begin{array}{|c|}\hline Q \\ \hline N \\ \hline \end{array}$ to indicate that G has a normal subgroup

N such that $G/N \simeq Q$.

Let p be a prime integer and g an element of finite order in G. Then g is called a *torsion* element. Moreover, g can be written in a unique way as $g = g_p g_{p'}$ where $|g_p|$ is a power of p and $|g_{p'}|$ is coprime with p. We call g_p the *p-part* of g and $g_{p'}$ the *p'-part* of g.

Definition 1.1.1. *Let G be a finite group and let π be a non-empty set of primes.*

(i) A positive integer m is called a π-number *if each prime factor of m belongs to π, and a* π'-number *if no prime factor of m belongs to π.*

(ii) An element of G is called a π-element *or* π-singular *if its order is a π-number, and it is called a* π'-element *or* π-regular *if its order is a π'-number.*

(iii) G is called a π-group *if every element of G is a π-element.*

(iv) A π-subgroup H of G is called a Hall π-subgroup *if $[G : H]$ is a π'-number.*

When we have $\pi = \{p\}$ in the previous definition, we will say *p-elements*, *p-groups*, *p'-elements* and *p'-groups*.

If G is a finite nilpotent group then its Sylow p-subgroups are unique (see [Rob82, 5.2.4]). In case G is a finite group having a unique Sylow p-subgroup, this will be denoted by G_p. In particular, this applies to each nilpotent group. If G has a unique Hall p'-subgroup then it will be denoted by $G_{p'}$. Moreover, $O_\pi(G)$ (respectively $O_{\pi'}(G)$) denotes the unique maximal normal π-subgroup (respectively π'-subgroup) of G. Its existence and uniqueness follows from [Rob82, 9.1.1].

Theorem 1.1.2 (P. Hall)**.** *[Rob82, 9.1.7] Let π be a non-empty set of primes. If G is a finite solvable group then every π-subgroup of G is contained in a Hall π-subgroup of G. Moreover, all Hall π-subgroups of G are conjugate.*

On the other hand, we use the following constructions of groups:

$$\begin{aligned} G \times H &= \text{direct product of the groups } G \text{ and } H; \\ G \rtimes_n H &= \text{semidirect product of } H \text{ acting on } G \text{ with kernel of order } n; \end{aligned}$$

Some groups that we encounter in this thesis are:

$$\begin{aligned}
C_n &= \text{cyclic group of order } n;\\
S_n &= \text{symmetric group on } n \text{ symbols};\\
A_n &= \text{alternating group on } n \text{ symbols};\\
Q_{4n} &= \text{quaternion group of order } 4n;\\
\mathrm{SL}(n,q) &= \{a \in M_n(\mathbb{F}_q) : \det(a) = 1\}, \text{ as multiplicative group};\\
\mathrm{PSL}(n,q) &= \mathrm{SL}(n,q)/Z(\mathrm{SL}(n,q)).
\end{aligned}$$

Definition 1.1.3. *Let G be a finite group.*

(i) *A* Sylow tower *in G is a normal series $1 = P_0 \subseteq P_1 \subseteq \cdots \subseteq P_r = G$ satisfying that for every prime $p \mid |G|$ there is a unique k such that P_k/P_{k-1} is of order a power of p. G is called a* Sylow tower group *if it has a Sylow tower.*

(ii) *The* Fitting subgroup *of G is the unique largest normal nilpotent subgroup of G and it is denoted by $F(G)$.*

(iii) *G is called a* Frobenius group *if it has a subgroup $H < G$ such that $H \cap H^g = 1$ for every $g \in G \setminus H$, where $H^g = \{g^{-1}hg : h \in H\}$. In this situation, H is called the* Frobenius complement *of G.*

(iv) *G is called a Z-*group *if all its Sylow subgroups are cyclic.*

(v) *G is called a* Camina group *if $G \neq G'$ and $gG' = g^G$ for all $g \in G \setminus G'$.*

(vi) *G is called a* supersolvable group *if there is a series of normal subgroups of G with cyclic factors.*

(vii) *G is called a* metacyclic group *if there is a normal subgroup N of G such that both N and G/N are cyclic.*

(viii) *G is called a* metabelian group *if there is a normal subgroup A of G such that both A and G/A are abelian.*

If G is a Frobenius group with Frobenius complement H then, by Frobenius famous theorem, there is a normal subgroup N of G such that $G = HN$ and $H \cap N = 1$. In this situation N is called the *Frobenius kernel* of G.

We finish this section given the structure of Frobenius complements

Theorem 1.1.4. *[Pas68, §18] Let C be a finite Frobenius complement. Denote by $F = \mathrm{F}(C)$ the Fitting subgroup of C. Then the following statements hold:*

(1) If the Sylow 2-subgroup of C is cyclic then C is a Z-group.

(2a) If F_2 is cyclic then C is metabelian.

(2b) If $F_2 \cong Q_8$ then either

$$C = \begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,3) \times M \\ \hline \end{array} \; \text{or } C = \boxed{\mathrm{SL}(2,3) \times M} \; \text{or } C = \boxed{Q_8 \times M}\,,$$

where M is a metacyclic Z-group of odd order coprime to the order of $\mathrm{SL}(2,3)$ *and Q_8 respectively.*

(2c) If $F_2 \cong Q_{2^n}$ with $n \geq 4$ then

$$C \cong F_2 \times M,$$

where M is a metacyclic Z-group of odd order and the Sylow 2-subgroup of C is isomorphic to Q_{2^n}.

(3) If C is non-solvable then

$$C = \begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,5) \times M \\ \hline \end{array} \; \text{or } C = \boxed{\mathrm{SL}(2,5) \times M}\,,$$

where M is a metacyclic Z-group of odd order coprime to the order of $\mathrm{SL}(2,5)$.

1.2 Group rings

In this section we recall the notion of group ring. It will be the main algebraic structure in this work. The concepts collected in this section are mostly from

[Seh93, PMS02].

Definition 1.2.1. *Let G be a group and let R be a ring. The* group ring *of G over R, is the ring RG of all formal linear combinations of the form*

$$\sum_{g\in G} a_g g,$$

where $a_g \in R$ and $a_g = 0$ for almost all $g \in G$. By definition

$$\sum_{g\in G} a_g g = \sum_{g\in G} b_g g \quad \textit{if and only if} \quad a_g = b_g \textit{ for every } g \in G,$$

the sum is defined component-wise

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)\, g,$$

and the multiplication is given by

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} \left(\sum_{uv=g} a_u b_v\right) g.$$

The identity of RG is the element $1_R 1_G$, where 1_R and 1_G are the identities of the ring R and of the group G, respectively. We will denote $1_R 1_G$ by 1, as usual. In case R is a field then RG is called the group algebra *of G over R.*

One can regard G and R as subsets of RG through the maps $g \mapsto 1_R \cdot g$ for $g \in G$, and $a \mapsto a \cdot 1_G$ for $a \in R$, respectively. By these identifications, R is a subring of RG and hence RG has a structure of (R, R)-bimodule. Moreover G is a basis of RG over R both as left and right module, and $ag = ga$ for every $g \in G$ and $a \in R$.

Definition 1.2.2. *The homomorphism $\varepsilon : RG \to R$ given by*

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

is called the augmentation map *of* RG *and its kernel*

$$\Delta_R(G) = \left\{ \sum_{g \in G} a_g g \in RG : \sum_{g \in G} a_g = 0 \right\}$$

is called the augmentation ideal *of* RG.

One can show that the set $\{g - 1 : g \in G, g \neq 1\}$ is a basis of $\Delta_R(G)$ over R both as left and right module. Thus

$$\Delta_R(G) = \bigoplus_{g \in G \setminus \{1\}} R(g-1).$$

The following theorem provides the necessary and sufficient conditions on R and G for the group ring RG to be semisimple (see [PMS02, Theorem 3.4.7]).

Theorem 1.2.3 (Maschke Theorem). *The group ring* RG *is semisimple if and only if* R *is a semisimple ring,* G *is finite and the order of* G *is a unit in* R.

In particular, if G is a finite group and F is a field, then FG is semisimple if and only if the characteristic of F does not divide the order of G. In that case, by the Wedderburn-Artin Theorem one gets that $FG \simeq \sum_{i=1}^{r} M_{n_i}(D_i)$, where D_i is a division F-algebra.

In this thesis the group of units of $\mathbb{Z}G$, for a finite group G, will be the main ingredient.

For a ring R we denote by $\mathcal{U}(R)$ the group of units of R, i.e. the group of invertible elements of R. As mentioned before, in this thesis we will focus on the study of $\mathcal{U}(\mathbb{Z}G)$. The easiest example of units in $\mathbb{Z}G$ are the elements of the form $\pm g$ with $g \in G$. They are called *trivial units*. As the augmentation map $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ is a ring homomorphism, if $u \in \mathcal{U}(\mathbb{Z}G)$ then $\varepsilon(u) = \pm 1$. This implies that $\mathcal{U}(\mathbb{Z}G)) = \pm \mathrm{V}(\mathbb{Z}G)$, where $\mathrm{V}(\mathbb{Z}G)$ consists of all units of $\mathbb{Z}G$ with augmentation one (they are called *normalized units*). For any ring R, we will also use the notation $\mathrm{V}(RG)$ to denote the units of RG with augmentation one.

The group of units of $\mathbb{Z}G$ has been a subject of interest for a long time. However, it turns out that to obtain a complete description of $\mathcal{U}(\mathbb{Z}G)$ in terms of generators has become a very difficult problem. By a much more general result of Borel and Harish Chandra proved in [BHC62], it follows that $\mathcal{U}(\mathbb{Z}G)$ is finitely generated. Unfortunately, a finite set of generators is not known in general. On the other hand Hartley and Pickel proved in [HP80] that $\mathcal{U}(\mathbb{Z}G)$ contains a free subgroup of rank 2 provided that G is neither abelian nor isomorphic to $C_2^n \times Q_8$. This explains the difficulty of studying $\mathcal{U}(\mathbb{Z}G)$ in the majority of the cases.

As a consequence of a result of Higman [Hig40], it is known that if G is non-abelian then all central torsion units of $\mathcal{U}(\mathbb{Z}G)$ are trivial. This yields to the natural problem of describing all non-central torsion units of $\mathcal{U}(\mathbb{Z}G)$. An approach would be the so-called Zassenhaus Conjectures which intend to characterize this kind of units and also the finite subgroups of $\mathcal{U}(\mathbb{Z}G)$ up to rational conjugacy. See the Introduction for a more general discussion on the Zassenhaus Conjectures and other problems on torsion units of $\mathbb{Z}G$.

We now explain some results on torsion units of $\mathrm{V}(\mathbb{Z}G)$ and explain the relation between (ZC1) and partial augmentations.

Let G be a finite group. If α is an element of a group ring of G and α_g denotes the coefficient of an element g of G, then the *partial augmentation* of α at g is

$$\varepsilon_g(\alpha) = \sum_{h \in g^G} \alpha_h.$$

For a positive integer m, we denote by $\varepsilon_{G[m]}(\alpha)$ the sum of the coefficients of α at all elements of order m of G, i.e.

$$\varepsilon_{G[m]}(\alpha) = \sum_{\substack{g \in G \\ |g|=m}} \alpha_g.$$

Clearly, $\varepsilon_{G[m]}(\alpha)$ is just the sum over all partial augmentations of α at conjugacy classes containing elements of order m. This notion will be of special interest in Chapter 5.

The relevance of partial augmentations for the study of (ZC1) is provided by a result of Marciniak, Ritter, Sehgal and Weiss stated in Theorem 1.2.6. We include a proof of this result for completeness.

The following theorem collects known results about torsion units in $\mathrm{V}(\mathbb{Z}G)$ which will be used throughout.

Theorem 1.2.4. *Let G be a finite group and let u be an element of order n in $\mathrm{V}(\mathbb{Z}G)$. Then the following conditions hold:*

1. *[JdR16, Proposition 1.5.1] (Berman-Higman Theorem) If $g \in Z(G)$ and $u \neq g$ then $\varepsilon_g(u) = 0$.*
2. *[Seh93, 7.3] n divides the exponent of G.*
3. *[Her07, Theorem 2.3] If $\varepsilon_g(u) \neq 0$ then $|g|$ divides $|u|$.*
4. *[Her08a, Proposition 2.1] If N is a normal p-subgroup of G and u maps under the map $\mathbb{Z}G \to \mathbb{Z}G/N$ to 1, then u is a p-element.*

The following result can be found in [Seh93, Lemma 37.5].

Lemma 1.2.5. *Let $K \geq k$ be infinite fields and let G be a finite group. Suppose that H_1 and H_2 are finite subgroups of units in kG. Then H_1 and H_2 are conjugate in KG if and only if they are conjugate in kG.*

For the proof of the following result we need to introduce first the following notation. For a commutative ring R and an R-algebra, we denote by $[A, A]$ the additive subgroup of A generated by the *Lie products* $[a, b] = ab-ba$. If $A = M_n(F)$ with F a field, then $[A, A]$ is a vectorial subspace of $M_n(F)$ and it is formed by the matrices over F whose trace is 0.

Theorem 1.2.6. *[MRSW87, Theorem 2.5] Let G be a finite group and let u be an element of order n in $\mathrm{V}(\mathbb{Z}G)$. Then the following statements are equivalent:*

1. *u is rationally conjugate to an element of G.*
2. *$\varepsilon_g(u^d) \geq 0$ for all $g \in G$ and all divisors d of n.*

Proof. Suppose that (1) holds. Then there are $g_0 \in G$ and $\alpha \in \mathcal{U}(\mathbb{Q}G)$ such that $u = \alpha^{-1} g_0 \alpha$. Then $[\alpha g_0, \alpha^{-1}] = \alpha g_0 \alpha^{-1} - \alpha^{-1}\alpha g_0 = u - g_0$. This implies that $u - g_0 = [\alpha g_0, \alpha^{-1}] \in [\mathbb{Q}G, \mathbb{Q}G] \cap \mathbb{Z}G = [\mathbb{Z}G, \mathbb{Z}G]$ and hence $\varepsilon_g(u - g_0) = 0$ for every $g \in G$. Thus (2) follows.

Suppose that (2) holds. Then there is $g_0 \in G$ such that u^d and g_0^d have the same partial augmentations for every $d \mid n$. As the multiplicity of each complex root of unity of order dividing n as an eigenvalue of $\rho(u)$, for any complex representation ρ of G, could be express in terms of the partial augmentations of u^d (see [LP89] or (1.1) for more details), it follows that the images of u and g_0 by all the complex representations of G have the same eigenvalues with the same multiplicities. Hence u and g_0 are conjugate in $\mathbb{C}G$ and also in $\mathbb{Q}G$ by Lemma 1.2.5. □

As (KP) has a positive answer for a finite group G if and only if (Gen-BP) have a positive answer for G [MdR17], we have the analogous of Theorem 1.2.6 for (KP):

Theorem 1.2.7. *Let G be a finite group. Then the following conditions are equivalent:*

1. *(KP) has a positive answer for G.*
2. *For every torsion element u of $\mathrm{V}(\mathbb{Z}G)$ we have that $\varepsilon_{G[m]}(u) = 0$ for every integer m different to the order of u.*

1.3 Representations and characters

Representation Theory and Character Theory provide powerful tools for studying finite groups. The purpose of this section is to revise the needed background about these topics. Our sources have been [CR81, Isa76, Ser78].

Let F be a field with characteristic $p \geq 0$ and let A be an F-algebra. An *F-representation* of A is an homomorphism of F-algebras $A \to M_n(F)$ where n is a positive integer called the *degree* of the representation. Two F-representations ρ and ρ' of A are *equivalent* if they have the same degree, say n, and there is $U \in \mathrm{GL}_n(F)$ such that $U\rho(a) = \rho'(a)U$ for every $a \in A$.

There is a one to one correspondence between isomorphic classes of left A-modules of finite dimension over F and equivalent classes of F-representations of A. More precisely, associated to a left A-module M of finite dimension over F there is an F-algebra homomorphism $\rho : A \to \mathrm{End}_F(M)$ given by $\rho(a) = \rho_a$, where $\rho_a(m) = am$ for every $a \in A$ and $m \in M$. For every F-base B of M and every $a \in A$, let $\rho_B(a)$ denote the matrix expression of ρ_a with respect to the basis B. Then ρ_B is a representation of A of degree $\dim_F(M)$ and it is called the representation of A with respect to the basis B. The map $M \to \rho_B$ induces the desired one to one correspondence.

Let G be a group. An F-representation of G is a group homomorphism $\rho : G \to \mathrm{GL}_n(F)$, where n is a positive integer called the degree of the representation. Two F-representations of G, ρ and ρ' are equivalent if they have the same degree, say n, and there is $U \in \mathrm{GL}_n(F)$ such that $U\rho(g) = \rho'(g)U$ for every $g \in G$.

An F-representation ρ of G of degree n can be extended uniquely to an homomorphism of F-algebras $\bar{\rho} : FG \to M_n(F)$. Moreover, if ρ' is another representation of G then ρ and ρ' are equivalent if and only if $\bar{\rho}$ and $\bar{\rho}\,'$ are equivalent. Thus, we deduce that an F-representation of G and a representation of FG define the same mathematical notion. We will identify equivalent classes of F-representations of G with isomorphic classes of FG-modules of finite dimension over F.

Suppose now that G is a finite group and let ρ be a representation of G of degree n. We define the *character* of G afforded by ρ as the map $\chi : G \to F$ given by $\chi(g) = \mathrm{tr}(\rho(g))$, where $\mathrm{tr}(\rho(g))$ denotes the trace of the matrix $\rho(g)$. As ρ is an homomorphism, it is clear that $\chi(1_G) = n$ and that $\chi(gh) = \chi(hg)$ for every $g, h \in G$.

An F-character of G is, by definition, the character of G afforded by a F-representation of G. In terms of FG-modules, if M is an FG-module then the character afforded by M is the character afforded by a representation with respect to any basis. Therefore, the character χ afforded by ρ is the same as the character of the FG-module M afforded by ρ.

An F-representation of G afforded by a simple FG-module is called an *irreducible representation* of G. Moreover, if χ is the character afforded by an irreducible F-representation of G then χ is called an *irreducible character* of G. If ρ is a $\mathbb{C}$-representation of G then ρ is called a *complex representation* (or *ordinary representation*) of G. In the same way, if χ is the character afforded by a complex representation of G, then χ is called a *complex character* (or *ordinary character*) of G.

It is well known that if F is an algebraic closed field of characteristic p coprime with $|G|$, then the number of irreducible F-representations of G, up to isomorphism, coincides with the number of conjugacy classes of p-regular elements of G. Suppose that this number is k and that $F = \mathbb{C}$. Let $\{1 = g_1, g_2, \ldots, g_k\}$ be a set of representatives of the conjugacy classes of G and let $\mathrm{Irr}(G) = \{1_G = \chi_1, \chi_2, \dots, \chi_k\}$ be the set of all irreducible characters of G, where 1_G is the *trivial character*. We define the *character table* of G as the square matrix $(\chi_i(g_j))_{1 \leq i,j \leq k}$.

We now introduce the Brauer characters.

Let G be a finite group and let p be a prime integer. Write $\exp(G) = p^k m$ with $p \nmid m$. Fix a field F of characteristic p containing a primitive m-th root of unity ξ. Let ρ be an F-representation of G of degree n. For each p-regular element $g \in G_{p'}$, all the eigenvalues of $\rho(g)$ are m-th roots of unity in F, and hence $\rho(g)$ is conjugate to $\mathrm{diag}(\xi^{i_1}, \xi^{i_2}, \dots, \xi^{i_n})$ for some integers $i_1, i_2, \dots, i_n$. Then the F-character Ψ afforded by ρ satisfies $\Psi(g) = \xi^{i_1} + \xi^{i_2} + \cdots + \xi^{i_n}$. Therefore, the *p-Brauer character* of G is the map $\chi : G_{p'} \to \mathbb{C}$ given by $\chi(g) = \zeta^{i_1} + \zeta^{i_2} \cdots + \zeta^{i_n}$, where ζ denotes a complex primitive m-th root of unity. It follows from the definition that $\chi(1_{G_{p'}}) = n$ and that χ is constant on the conjugacy classes of $G_{p'}$ (i.e. it is a class function on $G_{p'}$).

Let $\{E_1, \dots, E_l\}$ be a set of representatives of the isomorphic conjugacy classes of simples FG-modules. Then we define $\mathrm{IBr}(G) = \{\chi_{E_1}, \dots, \chi_{E_l}\}$ to be the set of all *irreducible Brauer characters* of G. Let $\{x_1, x_2, \dots, x_l\}$ be a set of representatives of the conjugacy classes of $G_{p'}$. Then $|\mathrm{IBr}(G)| = l$. Let $\{\Psi_1, \dots, \Psi_h\}$ be the ordinary irreducible K-characters of G and let $\{\chi_1, \dots, \chi_l\}$ be the irreducible K-Brauer characters of G module p. We define the Brauer character table of G module p as the square matrix $(\chi_i(x_j))_{1 \leq i,j \leq l}$. Moreover, it is known that the restriction of each Ψ_i to $G_{p'}$ could be expressed as a linear combination with non-negative integral coefficients of the irreducible K-Brauer characters of G module p [Ser78, Section 15.2]. The coefficients of these linear combinations could be saved into a matrix which is called the *decomposition matrix* of G relative to p. We denote this matrix by $D = (d_{ij})$. We define the *Cartan matrix* as the matrix $C = D^t D$. It is known that C is symmetric and positive defined [Ser78, Chapter 15]. Therefore, if u is a p-regular torsion element then for every $i = 1, \dots, h$ we have $\Psi_i(u) = \sum_{j=1}^{l} d_{ij} \chi_j(u)$. In this situation we define the *p-modular constituents* of the character Ψ_i as the Brauer characters $\{\chi_j\}_j$ for which $d_{ij} \neq 0$.

We finish this section quoting the following result on Brauer characters which will be used in the remainder of this thesis.

Theorem 1.3.1. *[Her07, Theorem 3.2] Let G be a finite group and let u be an element of $\mathrm{V}(\mathbb{Z}G)$ of order n. Let p be a prime not dividing n and let χ be a p-Brauer character of G. Then, with $g_1, ..., g_k$ representatives of the p-regular conjugacy classes of G, we have*

$$\chi(u) = \sum_{i=1}^{k} \varepsilon_{g_i}(u)\chi(g_i).$$

1.4 The HeLP Method

In this section we explain the HeLP Method which will be very useful in the following chapters.

Recall that for a positive integer n we always use ζ_n to denote a complex primitive n-th root of unity. If F/K is an extension of number fields then $\mathrm{Tr}_{F/K} : F \to K$ denotes the trace map, i.e. $\mathrm{Tr}(a)$ is the sum of the images of a by the K-homomorphisms of F in $\mathbb{C}$.

Let G be a finite group and let ρ be a representation of G affording the character χ. Let u be a torsion unit in $\mathbb{C}G$. If $z \in \mathbb{C}$ then the multiplicity of z as an eigenvalue of $\rho(u)$ only depends on the character χ and it is denoted by $\mu(z, u, \chi)$.

The following theorem states the main ingredient of the HeLP Method.

Theorem 1.4.1. *[LP89, Her07] Let G be a finite group and let u be an element of order n in $\mathrm{V}(\mathbb{Z}G)$. Let F be a field of characteristic $t \geq 0$ with $t \nmid n$. Let ρ be an F-representation of G. If $t \neq 0$ then let ξ_n be a primitive n-th root of unity in F, so that if $t = 0$ then $\xi_n = \zeta_n$. Let T be a set of representatives of the conjugacy classes of t-regular elements of G (all the conjugacy classes if $t = 0$). Let χ denote the character afforded by ρ if $t = 0$, and the t-Brauer character of G afforded by ρ if $t > 0$ (using a group isomorphism associating ξ_n to ζ_n). Then for every integer ℓ, the multiplicity of ξ_n^ℓ as eigenvalue of $\rho(u)$ is*

$$\mu(\xi_n^\ell, u, \chi) = \frac{1}{n} \sum_{x \in T} \sum_{d \mid n} \varepsilon_x(u^d)\, \mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(x)\zeta_n^{-\ell d}). \tag{1.1}$$

Observe that the right side of (1.1) makes sense because if $\varepsilon_x(u^d) \neq 0$ then $x^{\frac{n}{d}} = 1$, by Theorem 1.2.4.(3), and hence $\chi(x) \in \mathbb{Q}(\zeta_n^d)$.

We will often use the notation $\sum_{x^G}$ to simplify the sum $\sum_{x\in T}$ where T is a set of representatives of the conjugacy classes of G.

Let n be a positive integer. A distribution of *virtual partial augmentations* of order n for G is a list $\Upsilon = (\Upsilon_d)_{d|n}$, indexed by the divisors of n, where each Υ_d is a class function of G taking values on $\mathbb{Z}$, and the following conditions hold:

(V1) $\sum_{x^G} \Upsilon_d(x) = 1$;

(V2) if $d \neq n$ then $\Upsilon_d(1) = 0$;

(V3) if $\frac{n}{d}$ is not multiple of $|x|$ then $\Upsilon_d(x) = 0$;

(V4) if χ is either an ordinary character of G or a Brauer character of G modulo a prime not dividing n and $l \in \mathbb{Z}$ then

$$\frac{1}{n}\sum_{x^G}\sum_{d|n}\Upsilon_d(x)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(x)\zeta_n^{-ld})$$

is a positive integer which we denote by $\mu(\zeta_n^l, \Upsilon, \chi)$.

As for (1.1), the right side of the previous formula makes sense because, by (V3), if $\Upsilon_d(x) \neq 0$ then the order of x divides $\frac{n}{d}$ and hence x is p-regular and $\chi(x) \in \mathbb{Q}(\zeta_n^d)$. Let

$$\mathrm{VPA}_n(G) = \{\text{Distributions of virtual partial augmentations of order } n \text{ for } G\}.$$

For example, by Theorem 1.2.4.(1), Theorem 1.2.4.(3) and (1.1), each element u of order n in $\mathrm{V}(\mathbb{Z}G)$ defines a distribution of virtual partial augmentations of order n for G by the following formula:

$$\Upsilon_d(g) = \varepsilon_g(u^d) \quad \text{for } d \mid n \text{ and } g \in G.$$

This is called the *distribution of partial augmentations* of u. Let $\mathrm{PA}_n(G)$ denote the set formed by the distributions of partial augmentations of elements of order n in $\mathrm{V}(\mathbb{Z}G)$ and $\mathrm{TPA}_n(G)$ denotes the set of distributions of partial augmentations of trivial units. So we have

$$\mathrm{TPA}_n(G) \subseteq \mathrm{PA}_n(G) \subseteq \mathrm{VPA}_n(G).$$

Calculating $\mathrm{TPA}_n(G)$ is very easy:

$$\begin{aligned}\mathrm{TPA}_n(G) &= \big\{(\Upsilon_d)_{d\mid n} : \text{there is } g \in G \text{ with } \Upsilon_d(h) = 1 \text{ if } h \in (g^d)^G \\ &\qquad \text{and } \Upsilon_d(h) = 0 \text{ otherwise}\big\} \\ &= \big\{(\Upsilon_d)_{d\mid n} : \Upsilon_d(g) \geq 0 \text{ for every } d \mid n \text{ and } g \in G\big\}.\end{aligned}$$

Moreover, if $\mathrm{VPA}_n(G) = \mathrm{TPA}_n(G)$ then all elements of $\mathrm{V}(\mathbb{Z}G)$ of order n are rationally conjugate to elements of G by Theorem 1.2.6. Unfortunately, calculating $\mathrm{PA}_n(G)$ is usually difficult. The HeLP Method consists in calculating $\mathrm{VPA}_n(G)$. In case $\mathrm{VPA}_n(G) = \mathrm{TPA}_n(G)$ then all elements of $\mathrm{V}(\mathbb{Z}G)$ of order n are rationally conjugate to elements of G and if this holds for all the possible orders n, then (ZC1) holds for G. The HeLP Method fails to verify (ZC1) when $\mathrm{VPA}_n(G) \neq \mathrm{TPA}_n(G)$ for some n. Nevertheless, each element of $\mathrm{VPA}_n(G) \setminus \mathrm{TPA}_n(G)$ provides relevant information of a possible counterexample to (ZC1). Indeed, it determines a conjugacy class in the normalized units of $\mathbb{Q}G$ formed by elements with integral partial augmentations. Actually, using the representation theory of $\mathbb{Q}G$ one can find a concrete representative of this class. With this information at hand, to prove (ZC1) one should prove that none of these conjugacy classes contains an element with integral coefficients and to disprove it one should find an element in this class with integral coefficients.

The HeLP Method was introduced by Luthar and Passi in [LP89] for ordinary characters to prove (ZC1) for A_5. Its name was coined by Konovalov based on the authors' names who developed the method: **He**rtweck**L**uthar**P**assi.

We will often argue by induction on n (respectively, on the order of the torsion unit $u \in \mathrm{V}(\mathbb{Z}G)$) and because of this we will assume that $\mathrm{VPA}_d(G) = \mathrm{TPA}_d(G)$ for every proper divisor d of n (respectively, that u^d is rationally conjugate to an element of G for every d dividing of the order of u and $d \neq 1$). This will simplify our arguments reducing the summands in (V4) (respectively, in (1.1)).

Actually, the HeLP Method is not applied exactly as explained above. Observe that the bulk of the HeLP Method is (1.1) and hence the only genuine HeLP conditions are (V1) and (V4). However, in practice one uses all the available information which one has at hand. This new information will be included in the HeLP Method making it into a dynamic method (in the sense explained in [MdR17]). For example, we use (V2) by the Berman-Higman Theorem. Observe that the equivalent condition of (V3) for units is Theorem 1.2.4.(3) which was proved in 2007 [Her07] and the plain HeLP Method was used for the first time in 1989 [LP89]. On the other hand, in some particular cases one can use even more information. For example, if G is a solvable group then the only non-zero partial augmentations of a torsion unit u in $\mathrm{V}(\mathbb{Z}G)$ are those at conjugacy classes of elements with the same order as u [Her08a].

We finish this section collecting other results which could be included in the HeLP Method in some particular cases and which will be very useful in the following chapters.

In several papers Hertweck considered the behavior of torsion units of integral group rings mapping to the identity under the map $\mathbb{Z}G \to \mathbb{Z}G/N$, where N is a normal p-subgroup of G. His main results are the following (see [Her13, Theorem B], [Mar17] for a proof, [Her08b, Lemma 2.2], and [Her06, Theorem 5.6] respectively):

Theorem 1.4.2. *Let N be a normal p-subgroup of a finite group G. Then any torsion unit in $\mathbb{Z}G$ which maps to the identity under the natural map $\mathbb{Z}G \to \mathbb{Z}G/N$ is conjugate to an element of N by a unit in $\mathbb{Z}_pG$.*

Proposition 1.4.3. *Let G be a finite group and p a prime integer. Let R be a p-adic ring and u a torsion unit of RG with augmentation one. Suppose that the p-part of u is conjugate to an element x of G in the units of RG and g is an element of G such that the p-parts of x and g are not conjugate in G. Then $\varepsilon_g(u) = 0$.*

Theorem 1.4.4. *Suppose that the finite group G has a normal Sylow p-subgroup with abelian complement. Then any torsion unit of the group ring $\mathbb{Z}_{(G)}G$ is rationally conjugate to a trivial unit.*

For the case of finite Frobenius groups, we also have the following information which could be added to the HeLP Method:

Theorem 1.4.5. *[Her12] Let G be a finite Frobenius group with Frobenius kernel N. Then any torsion unit in $\mathbb{Z}_{(G)}G$ which maps to the identity under the natural ring homomorphism $\mathbb{Z}_{(G)}G \to \mathbb{Z}_{(G)}G/N$ is conjugate to an element of G by a unit in $\mathbb{Z}_{(G)}G$.*

Theorem 1.4.6. *[JPM00, Theorem 2.1] Let G be a finite Frobenius group with Frobenius kernel N and a Frobenius complement C. If u is a torsion element of $\mathrm{V}(\mathbb{Z}G)$ then the order of u divides either $|N|$ or $|C|$.*

CHAPTER 2

Preliminary general results

In this chapter we prove several general results which we use through this thesis. The results of Section 2.1 appeared in [dRS17] and those of Section 2.2 in [MdRS17]. In Section 2.3 we recall the representation theory of $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$, collect some properties of these groups and state known results on torsion units. The results of this section appeared in [dRS17].

2.1 General results for virtual partial augmentations

In this section we collect some technical general results that will be used in the next chapter.

The following well known formula, for k and d integers with $k > 0$, will be used in several situations:

$$\sum_{i=0}^{k-1} \zeta_k^{-id} = \begin{cases} 0, & \text{if } k \nmid d; \\ k, & \text{otherwise.} \end{cases} \tag{2.1}$$

In the remainder of the section G is a finite group, n is a positive integer and $\Upsilon \in \mathrm{VPA}_n(G)$ (see the definition of $\mathrm{VPA}_n(G)$ in page 34). If m divides n then we define

$$\Upsilon^{\frac{n}{m}} = ((\Upsilon^{\frac{n}{m}})_d)_{d|m} \quad \text{with} \quad (\Upsilon^{\frac{n}{m}})_d(g) = \Upsilon_{d\frac{n}{m}}(g) \quad \text{for} \quad g \in G.$$

Observe that if Υ is the distribution of partial augmentations of an element u in $\mathrm{V}(\mathbb{Z}G)$ of order n then $\Upsilon^{\frac{n}{m}}$ is the distribution of partial augmentations of $u^{\frac{n}{m}}$.

Moreover,

$$\text{if } \Upsilon \in \mathrm{VPA}_n(G) \text{ and } m \mid n \text{ then } \Upsilon^{\frac{n}{m}} \in \mathrm{VPA}_m(G). \tag{2.2}$$

Indeed, that $\Upsilon^{\frac{n}{m}}$ satisfies (V1), (V2) and (V3) is elementary and (V4) follows from the following lemma.

Lemma 2.1.1. *Let G be a finite group. Let n and m be positive integers with $m \mid n$, let $l \in \mathbb{Z}$ and let $\Upsilon \in \mathrm{VPA}_n(G)$. Let χ be either an ordinary character of G or a Brauer character of G module a prime not dividing n. Then*

$$\mu(\zeta_m^l, \Upsilon^{\frac{n}{m}}, \chi) = \sum_{\xi, \xi^{\frac{n}{m}} = \zeta_m^l} \mu(\xi, \Upsilon, \chi).$$

Proof. Let $k = \frac{n}{m}$ and fix $\xi_0 \in \mathbb{C}$ with $\xi_0^k = \zeta_m^l$. Then $\xi^k = \zeta_m^l$ if and only if $(\xi\xi_0^{-1})^k = 1$ if and only if $\xi = \xi_0 \zeta_k^i$ for some $i \in \{0, 1, \dots, k-1\}$. Then

$$\begin{aligned} \sum_{\xi, \xi^k = \zeta_m^l} \mu(\xi, \Upsilon, \chi) &= \frac{1}{n} \sum_{x^G} \sum_{d \mid n} \Upsilon_d(x) \operatorname{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}} \left(\chi(x) \xi_0^{-d} \sum_{i=0}^{k-1} \zeta_k^{-id} \right) \\ &= \frac{1}{m} \sum_{x^G} \sum_{d \mid n, k \mid d} \Upsilon_d(x) \operatorname{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}} (\chi(x) \xi_0^{-d}), \end{aligned}$$

where the last equality is a consequence of (2.1). Furthermore $\{d : d \mid n, k \mid d\} = \{kd_1 : d_1 \mid m\}$ and ζ_n^k has order m. Thus

$$\sum_{\xi, \xi^k = \zeta_m^l} \mu(\xi, \Upsilon, \chi) = \frac{1}{m} \sum_{x^G} \sum_{d_1 \mid m} (\Upsilon^{\frac{n}{m}})_{d_1}(x) \operatorname{Tr}_{\mathbb{Q}(\zeta_m^{d_1})/\mathbb{Q}} (\chi(x) \zeta_m^{-ld_1}) = \mu(\zeta_m^l, \Upsilon^{\frac{n}{m}}, \chi).$$

□

Proposition 2.1.2. *Let G be a finite group and let n be a positive integer. If $\mathrm{VPA}_n(G) \neq \emptyset$ then every prime divisor of n divides $|G|$.*

Proof. Let p be a prime not dividing $|G|$ and let $\Upsilon \in \mathrm{VPA}_p(G)$. By (V2) and (V3), $\Upsilon_1(g) = 0$ for every $g \in G$ and this is in contradiction with (V1). This shows that if p does not divides the order of G then $\mathrm{VPA}_p(G) = \emptyset$. Now, if $\Upsilon \in \mathrm{VPA}_n(G)$, with p a prime divisor of n then $\Upsilon^{\frac{n}{p}} \in \mathrm{VPA}_p(G)$ by (2.2), and hence p divides the order of G, by the previous sentence. □

Let χ be either an ordinary character of G or a Brauer character of G module a prime p not dividing n and let m be a divisor of n. Let

$$\mu_m^-(\Upsilon, \chi) = \frac{1}{n}\sum_{x^G}\sum_{d\in\mathcal{X}_{n,m}} \Upsilon_d(x)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(x)),$$

where $\mathcal{X}_{n,m} = \{d \mid n : m \mid d\}$. By (V4), for every $l \in \mathbb{Z}$, we have

$$0 \le \mu(\zeta_m^l, \Upsilon, \chi) = \mu_m^-(\Upsilon, \chi) + \frac{1}{n}\sum_{x^G}\sum_{\substack{d\mid n\\ d\notin\mathcal{X}_{n,m}}} \Upsilon_d(x)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(x)\zeta_m^{-dl}).$$

Combining this with (2.1) we obtain

$$\begin{aligned} 0 &\le \mu(1, \Upsilon, \chi) = \mu_m^-(\Upsilon, \chi) + \frac{1}{n}\sum_{x^G}\sum_{\substack{d\mid n\\ d\notin\mathcal{X}_{n,m}}} \Upsilon_d(x)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(x)) \\ &= \mu_m^-(\Upsilon, \chi) - \frac{1}{n}\sum_{l=1}^{m-1}\sum_{x^G}\sum_{\substack{d\mid n\\ d\notin\mathcal{X}_{n,m}}} \Upsilon_d(x)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_n^d)/\mathbb{Q}}(\chi(x)\zeta_m^{-dl}) \le m\mu_m^-(\Upsilon, \chi). \end{aligned}$$

We record this for future use:

$$0 \le \mu(1, \Upsilon, \chi) \le m\mu_m^-(\Upsilon, \chi). \tag{2.3}$$

2.2 Number theoretical results

In this section we prove two number theoretical results which are essential for the remaining chapters of this thesis. They appeared in [MdRS17] and they might also have interest on themselves. Our first proof of Proposition 2.2.2 below was too long. We include a proof which was given to us by Hendrik Lenstra. We are very thankful to him for his simple and nice proof.

Lemma 2.2.1. *If n, m and p are positive integers with p a prime then $\Phi_{np^m}(\zeta_n) \in p\,\mathbb{Z}[\zeta_n]$.*

Proof. We argue by induction on $v_p(n)$. Suppose first that $p \nmid n$ and let S denote the set of primitive p^m-th roots of unity. Then $\zeta_n\xi$ is a root of $\Phi_{np^m}(X)$ for every

$\xi \in S$ and hence $\prod_{\xi \in S}(X - \zeta_n \xi)$ divides $\Phi_{np^m}(X)$ in $\mathbb{Z}[\zeta_n][X]$. Therefore

$$\Phi_{np^m}(\zeta_n) \in \prod_{\xi \in S}(\zeta_n - \zeta_n \xi)\, \mathbb{Z}[\zeta_n] = \prod_{\xi \in S}(1 - \xi)\, \mathbb{Z}[\zeta_n] = \Phi_{p^m}(1)\, \mathbb{Z}[\zeta_n] = p\, \mathbb{Z}[\zeta_n].$$

Suppose that $p \mid n$ and assume that the lemma holds with n replaced by $\frac{n}{p}$. Then $\Phi_{np^{m-1}}(\zeta_n^p) = \Phi_{\frac{n}{p}p^m}(\zeta_n^p) \in p\, \mathbb{Z}[\zeta_n^p] \subseteq p\, \mathbb{Z}[\zeta_n]$. As $\Phi_{np^m}(X) = \Phi_{np^{m-1}}(X^p)$ and ζ_n^p is a primitive $\frac{n}{p}$-th root of unity, we have $\Phi_{np^m}(\zeta_n) = \Phi_{np^{m-1}}(\zeta_n^p) \in p\, \mathbb{Z}[\zeta_n]$. □

Proposition 2.2.2. *Let n be a positive integer. Let $A_0, A_1, \ldots, A_{n-1}$ be integers and for every positive integer i set*

$$\omega_i = \sum_{j=0}^{n-1} A_j \zeta_n^{ij}.$$

Let d be a divisor of n such that $\omega_{\frac{d}{q}} = 0$ for every prime power q dividing d with $q \neq 1$. Then $\omega_d \in d\, \mathbb{Z}[\zeta_n]$.

Proof. Let $k = \frac{n}{d}$ and consider the polynomial $f(X) = \sum_{j=0}^{n-1} A_j X^j$. We can take $\zeta_k = \zeta_n^d$, so that $\omega_d = f(\zeta_k)$. By hypothesis, for every prime p and every positive integer m with p^m dividing d we have $f(\zeta_{kp^m}) = 0$, or equivalently $\Phi_{kp^m}(X)$ divides $f(X)$ in $\mathbb{Z}[X]$. Thus $\prod_{p \mid d} \prod_{m=1}^{v_p(d)} \Phi_{kp^m}(X)$ divides $f(X)$ in $\mathbb{Z}[X]$. Therefore

$$\omega_d = f(\zeta_k) \in \prod_{p \mid d} \prod_{m=1}^{v_p(d)} \Phi_{kp^m}(\zeta_k)\, \mathbb{Z}[\zeta_k].$$

By Lemma 2.2.1, each $\Phi_{kp^m}(\zeta_k)\, \mathbb{Z}[\zeta_k] \subseteq p\, \mathbb{Z}[\zeta_k] \subseteq p\, \mathbb{Z}[\zeta_n]$. As $d = \prod_{p \mid d} \prod_{m=1}^{v_p(d)} p$ we deduce that $\omega_d \in d\, \mathbb{Z}[\zeta_n]$, as desired. □

For a positive integer n and a subfield F of $\mathbb{Q}(\zeta_n)$, let Γ_F denote a set of representatives of equivalence classes of the following equivalence relation defined on $\mathbb{Z}$:

$$x \sim y \quad \text{if and only if} \quad \zeta_n^x \text{ and } \zeta_n^y \text{ are conjugate in } \mathbb{Q}(\zeta_n) \text{ over } F.$$

Corollary 2.2.3. *Let n be a positive integer, let F be a subfield of $\mathbb{Q}(\zeta_n)$ and let R be the ring of integers of F. For every $x \in \Gamma_F$ let B_x be an integer and for every* *integer i define*

$$\omega_i = \sum_{x\in\Gamma_F} B_x \operatorname{Tr}_{\mathbb{Q}(\zeta_n)/F}(\zeta_n^{ix}).$$

Let d be a divisor of n such that $\omega_{\frac{d}{q}} = 0$ for every prime power q dividing d with $q \neq 1$. Then $\omega_d \in d\,R$.

Proof. Apply Proposition 2.2.2 to the integers $A_x = B_{\overline{x}}$ with $\overline{x}$ denoting the class in Γ_F containing x. □

In the remainder of this section we reserve the letter p to denote positive prime integers. We now introduce some notation for a positive integer n which will be fixed throughout. First we set

$$n' = \prod_{p\mid n} p \quad \text{and} \quad n_p = p^{v_p(n)}.$$

If moreover $x \in \mathbb{Z}$ then we set

$$\begin{array}{rcl}
(x:n) & = & \text{representative of the class of } x \text{ modulo } n \text{ in the interval } \left(-\frac{n}{2},\frac{n}{2}\right]; \\
|x:n| & = & \text{the absolute value of } (x:n); \\
\gamma_n(x) & = & \displaystyle\prod_{\substack{p\mid n \\ |x:n_p|<\frac{n_p}{2p}}} p \quad \text{and} \quad \bar{\gamma}_n(x) = \prod_{\substack{p\mid n \\ |x:n_p|\le\frac{n_p}{2p}}} p = \begin{cases} 2\gamma_n(x), & \text{if } |x:n_2| = \frac{n_2}{4}; \\ \gamma_n(x), & \text{otherwise.} \end{cases}
\end{array}$$

The following lemma collects two elementary arithmetic properties of these objects whose proofs are direct consequences of the definitions.

Lemma 2.2.4. *Let p be a prime dividing n and let $x, y \in \mathbb{Z}$. Then the following conditions hold:*

1. *If $p \mid \bar{\gamma}_n(x)$ then $\left(x : \frac{n_p}{p}\right) \equiv x \bmod n_p$.*
2. *Let $d \mid n'$ such that $x \equiv y \bmod \frac{n}{d}$. If d divides both $\bar{\gamma}_n(x)$ and $\bar{\gamma}_n(y)$ then $x \equiv y \bmod n$.*

For integers x and y we define the following equivalence relation on $\mathbb{Z}$:

$$x \sim_n y \quad \Leftrightarrow \quad x \equiv \pm y \bmod n.$$

We denote by Γ_n a set of representatives of these equivalence classes. Without loss of generality one may assume that $\Gamma_n = \Gamma_{\mathbb{Q}(\zeta_n+\zeta_n^{-1})}$.

If x, y and n are integers with $n > 0$ then let

$$\delta_{x,y}^{(n)} = \begin{cases} 1, & \text{if } x \sim_n y; \\ 0, & \text{otherwise;} \end{cases} \quad \text{and} \quad \kappa_x^{(n)} = \begin{cases} 2, & \text{if } x \equiv 0 \bmod n \text{ or } x \equiv \frac{n}{2} \bmod n; \\ 1, & \text{otherwise.} \end{cases}$$

For an integer x (or $x \in \Gamma_n$) we set

$$\alpha_x^{(n)} = \zeta_n^x + \zeta_n^{-x}.$$

Moreover, $\mathbb{Q}(\alpha_1^{(n)})$ is the maximal real subfield of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Z}[\alpha_1^{(n)}]$ is the ring of integers of $\mathbb{Q}(\alpha_1^{(n)})$. If $n \neq n_2$ then let p_0 denote the smallest odd prime dividing n. Let

$$\begin{aligned} \mathbb{B}_n \quad = \quad & \Big\{ x \in \mathbb{Z}/n\mathbb{Z} : \text{ for every } p \mid n, \text{ either } |x : n_p| > \frac{n_p}{2p} \text{ or} \\ & \qquad p = 2, n \neq n_2, |x : n_2| = \frac{n_2}{4}, n_{p_0} \nmid x \text{ and } (x : n_2) \cdot (x : n_{p_0}) > 0 \Big\} \end{aligned}$$

and

$$\mathcal{B}_n = \begin{cases} \{\alpha_b^{(n)} : b \in \mathbb{B}_n\}, & \text{if } n \neq n_2; \\ \{1\} \cup \{\alpha_b^{(n)} : b \in \mathbb{B}_n\}, & \text{otherwise.} \end{cases}$$

For $b \in \mathbb{B}_n$ and $x \in \mathbb{Z}$ let

$$\beta_{b,x}^{(n)} = \begin{cases} -1, & \text{if } n \neq n_2, |x : n_2| = \frac{n_2}{4} \text{ and } (x : n_2) \cdot (b : n_{p_0}) < 0; \\ 1, & \text{otherwise.} \end{cases}$$

In the following proposition we prove that $\mathcal{B}_n$ is a $\mathbb{Q}$-basis of $\mathbb{Q}[\alpha_1^{(n)}]$. For $x \in \mathbb{Q}[\alpha_1^{(n)}]$ and $b \in \mathcal{B}_n$, we use

$$C_b(x) = \text{coefficient of } \alpha_b^{(n)} \text{ in the expression of } x \text{ in the basis } \mathcal{B}_n.$$

Proposition 2.2.5. *Let n be a positive integer. Then*

1. *$\mathcal{B}_n$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha_1^{(n)}]$.*

2. *If* $b \in \mathbb{B}_n$ *and* $i \in \mathbb{Z}$ *then* $C_b(\alpha_i^{(n)}) = \kappa_i^{(n)} \cdot \mu(\gamma(i)) \cdot \beta_{b,i}^{(n)} \cdot \delta_{b,i}^{(n/\bar{\gamma}(i))}$.

Proof. We only prove the proposition in the case $n \neq n_2$, as the proof in the case $n = n_2$ is similar (actually simpler). It is easy to see that $|\mathcal{B}_n| \leq \frac{\varphi(n)}{2} = [\mathbb{Q}(\alpha_1^{(n)}) : \mathbb{Q}]$. Thus it is enough to prove the following equality:

$$\alpha_i^{(n)} = \kappa_i^{(n)}\, \mu(\gamma(i)) \sum_{b \in \mathbb{B}_n, b \sim_{n/\bar{\gamma}(i)} i} \beta_{b,i}^{(n)}\, \alpha_b^{(n)}.$$

Actually we will show that

$$\zeta_n^i = \mu(\gamma(i)) \sum_{\substack{b \equiv i \bmod n/\bar{\gamma}(i) \\ b \in \mathbb{B}_n}} \beta_{b,i}^{(n)}\, \zeta_n^b$$

which easily implies the desired expression of $\alpha_i^{(n)}$. Indeed, for every $p \mid n$ let ζ_{n_p} denote the p-th part of ζ_n, i.e. ζ_{n_p} is a primitive n_p-th root of unity and $\zeta_n = \prod_{p|n} \zeta_{n_p}$. Let J be the set of tuples $(j_p)_{p|\bar{\gamma}(i)}$ satisfying the following conditions:

- If $p \mid \gamma(i)$ then $j_p \in \{1, \ldots, p-1\}$.

- If $p = 2$ and $|i : n_2| = \frac{n_2}{4}$ then $j_2 = \begin{cases} 1, & \text{if } (i : n_2) \cdot \left(i + j_{p_0} \frac{n_{p_0}}{p_0} : n_{p_0}\right) < 0; \\ 0, & \text{otherwise.} \end{cases}$.

For every $j \in J$ let $b_j \in \mathbb{Z}/n\mathbb{Z}$ given by

$$b_j \equiv \begin{cases} i + j_p \frac{n_p}{p} \mod n_p, & \text{if } p \mid \bar{\gamma}(i); \\ i \mod n_p, & \text{otherwise.} \end{cases}$$

Then $\{b_j : j \in J\}$ is the set of elements in $\mathbb{B}_n$ satisfying $i \equiv b \bmod \frac{n}{\bar{\gamma}(i)}$. From

$$0 = \zeta_{n_p}^i \left(1 + \zeta_{n_p}^{\frac{n_p}{p}} + \zeta_{n_p}^{\frac{2n_p}{p}} + \ldots + \zeta_{n_p}^{\frac{(p-1)n_p}{p}}\right)$$

we obtain $\zeta_{n_p}^i = -\sum_{j_p=1}^{p-1} \zeta_{n_p}^{i+j_p\frac{n_p}{p}}$. Therefore, if $|i:n_2| \neq \frac{n_2}{4}$ then $\gamma(i) = \bar{\gamma}(i)$ and

$$\zeta_n^i = \prod_{\substack{p|n\\ p\nmid\gamma(i)}} \zeta_{n_p}^i \prod_{\substack{p|n\\ p|\gamma(i)}} \left(-\sum_{j_p=1}^{p-1}\zeta_{n_p}^{i+j_p\frac{n_p}{p}}\right) = \mu(\gamma(i))\sum_{j\in J}\zeta_n^{b_j} = \mu(\gamma(i)) \sum_{\substack{b\equiv i \bmod n/\bar{\gamma}(i)\\ b\in\mathbb{B}_n}} \zeta_n^b.$$

This gives the desired equality because in this case $\beta_{b,i}^{(n)} = 1$ for every $b \in \mathbb{B}_n$. Suppose otherwise that $|i:n_2| = \frac{n_2}{4}$. Then $\zeta_{n_2}^i = \beta_{b_j,i}^{(n)}\zeta_{n_2}^{b_j}$ for every $j \in J$ and a small modification of the argument in the case where $|i:n_2| \neq \frac{n_2}{4}$ gives

$$\begin{aligned}\zeta_n^i &= \zeta_{n_2}^i \prod_{\substack{p|n\\ p\nmid\gamma(i)}} \zeta_{n_p}^i \prod_{\substack{p|n\\ p|\gamma(i)}} \left(-\sum_{j_p=1}^{p-1}\zeta_{n_p}^{i+j_p\frac{n_p}{p}}\right) = \mu(\gamma(i))\sum_{j\in J}\beta_{b,i}^{(n)}\,\zeta_n^{b_j} = \\ &= \mu(\gamma(i)) \sum_{\substack{b\equiv i \bmod n/\bar{\gamma}(i)\\ b\in\mathbb{B}_n}} \beta_{b,i}^{(n)}\,\zeta_n^b.\end{aligned}$$

□

We finish this section quoting the following result which will be very useful in the next chapters:

Lemma 2.2.6. *[Mar16, Lemma 2.1] If n and d are positive integers with $d \mid n$ then*

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_d) = \mu(d)\frac{\varphi(n)}{\varphi(d)}.$$

2.3 Group theoretical properties of PSL(2,q) and SL(2,q)

In this section we collect the group theoretical properties of $\mathrm{PSL}(2,q)$ and $\mathrm{SL}(2,q)$, and their representation theory as well as some results on their integral group rings relevant for our purposes.

We fix $q = p^f$ for an odd prime p and a positive integer f. Denote by $\bar{\pi} : \mathrm{SL}(2,q) \to \mathrm{PSL}(2,q)$ the natural projection, which we extend by linearity to a ring homomorphism $\bar{\pi} : \mathbb{Z}\,\mathrm{SL}(2,q) \to \mathbb{Z}\,\mathrm{PSL}(2,q)$.

We collect in the following proposition some properties of $\mathrm{SL}(2,q)$, $\mathrm{PSL}(2,q)$ and $\mathbb{Z}\,\mathrm{PSL}(2,q)$.

Proposition 2.3.1. *1. [Hup67, Hauptsatz 8.27] The order of* $\mathrm{PSL}(2,q)$ *is* $(q-1)q(q+1)/d$*, where* $d=\gcd(2,q-1)$*. The orders of elements in* $\mathrm{PSL}(2,q)$ *are exactly* p *and the divisors of* $(q+1)/d$ *and* $(q-1)/d$*. Two cyclic subgroups of* $\mathrm{PSL}(2,q)$ *are conjugate in* $\mathrm{PSL}(2,q)$ *if and only if they have the same order. If* g *is an element of* $\mathrm{PSL}(2,q)$ *of order not divisible by* p*, then the only conjugates of* g *in* $\langle g\rangle$ *are* g *and* g^{-1}*. In particular a conjugacy class of elements of order coprime with* p *is a real conjugacy class.*

2. Let u *be an element of order* n *in* $\mathrm{V}(\mathbb{Z}\,\mathrm{PSL}(2,q))$*. If* $\gcd(n,q)=1$ *or* q *is prime then* $\mathrm{PSL}(2,q)$ *has an element of order* n *[Her07, Proposition 6.7]. In the following cases* u *is rationally conjugate to an element of* $\mathrm{PSL}(2,q)$*:*

(a) [Mar16, Theorem 1] n *is a prime power not divisible by* p*.*

(b) [Her07, Proposition 6.1, Proposition 6.3] [Mar16] $f\le 2$ *and* n *is divisible by* p *(hence in this case* $n=p$*).*

(c) [Her07, Proposition 6.6] $n=6$ *and* $\gcd(6,p)=1$*.*

3. [Dor71, Theorem 38.1] $\mathrm{SL}(2,q)$ *has a unique element* J *of order* 2 *and* $q+4$ *conjugacy classes. More precisely, two of the classes are formed by elements of order* p*, another two are formed by elements of order* $2p$ *and* q *classes are formed by elements of order dividing* $q+1$ *or* $q-1$*. Furthermore, if* g *and* h *are* p*-regular elements of* $\mathrm{SL}(2,q)$ *and* $|h|$ *divides* $|g|$ *then* h *is conjugate in* $\mathrm{SL}(2,q)$ *to an element of* $\langle g\rangle$ *and two elements of* $\langle g\rangle$ *are conjugate in* $\mathrm{SL}(2,q)$ *if and only if they are equal or mutually inverse.*

4. [Dor71, Theorem 38.1] Let C *be a conjugacy class of* $\mathrm{PSL}(2,q)$ *formed by elements of order* n*. If* $n=2$ *then* $\bar{\pi}^{-1}(C)$ *is the only conjugacy class of* $\mathrm{SL}(2,q)$ *formed by elements of order* 4*. Otherwise,* $\bar{\pi}^{-1}(C)$ *is the union of two conjugacy classes* C_1 *and* C_2 *of* $\mathrm{SL}(2,q)$ *with* $C_2=JC_1$*. Furthermore, if* n *is multiple of* 4 *then the elements of* C_1 *and* C_2 *have order* $2n$ *while if* n *is not multiple of* 4 *then one of the classes* C_1 *or* C_2 *is formed by elements of order* n*.*

The following proposition collects some consequences of these facts.

Proposition 2.3.2. *Let u be a torsion element of $\mathrm{V}(\mathbb{Z}G)$ of order n with $p \nmid n$. Then the following statements hold:*

1. *J is the unique element of order 2 in $\mathrm{V}(\mathbb{Z}\,\mathrm{SL}(2,q))$.*
2. *$|\bar{\pi}(u)| = \frac{n}{\gcd(2,n)}$.*
3. *If $\gcd(n,q)=1$ then $\mathrm{SL}(2,q)$ has an element of order n.*
4. *If ρ is a representation of $\mathrm{SL}(2,q)$ and ζ is a root of unity of order dividing n then ζ and ζ^{-1} have the same multiplicity as eigenvalues of $\rho(u)$.*

Proof. (1) is a direct consequence of Theorem 1.2.4.(1) and Proposition 2.3.1.(3).

(2) By Theorem 1.4.2, if $\bar{\pi}(u)=1$ then $u^2=1$ and hence either $u=1$ or $u=J$, by (1). Then (2) follows.

(3) is a consequence of (2) and Proposition 2.3.1.(2).

(4) is a consequence of Proposition 2.3.1.(3) and (1.1). □

We describe the ordinary characters of $\mathrm{PSL}(2,q)$ and some Brauer characters of $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$ which will be used in the remainder of the thesis. First we display the character table of $\mathrm{PSL}(2,q)$ for q an odd prime power where δ stands for the Kronecher symbol [Her07]:

Table 2.1: Character Table of $\mathrm{PSL}(2,q)$ with $q \equiv \epsilon \bmod 4$ where $\epsilon = \pm 1$.

class of	1	c	d	a^l	b^m
order	1	p	p	$\lvert a\rvert = (q-1)/2$	$\lvert b\rvert = (q+1)/2$
1	1	1	1	1	1
ψ	1	0	0	1	-1
χ_i	$q+1$	1	1	$\zeta_{q-1}^{il} + \zeta_{q-1}^{-il}$	0
θ_j	$q-1$	-1	-1	0	$-(\zeta_{q+1}^{jm} + \zeta_{q+1}^{-jm})$
η_1	$\frac{1}{2}(q+\epsilon)$	$\frac{1}{2}(\epsilon+\sqrt{\epsilon q})$	$\frac{1}{2}(\epsilon-\sqrt{\epsilon q})$	$(-1)^l\delta_{\epsilon,1}$	$(-1)^m\delta_{\epsilon,-1}$
η_2	$\frac{1}{2}(q+\epsilon)$	$\frac{1}{2}(\epsilon-\sqrt{\epsilon q})$	$\frac{1}{2}(\epsilon+\sqrt{\epsilon q})$	$(-1)^l\delta_{\epsilon,1}$	$(-1)^m\delta_{\epsilon,-1}$

If $\epsilon = 1$ then $1 \le i \le \frac{1}{4}(q-5),\ 1 \le j,l,m \le \frac{1}{4}(q-1)$;
If $\epsilon = -1$ then $1 \le i,j,l \le \frac{1}{4}(q-3),\ 1 \le m \le \frac{1}{4}(q+1)$.

Suppose that $g_0 \in \mathrm{PSL}(2,q)$ and $h_0 \in \mathrm{SL}(2,q)$ both of order m with $p \nmid m$. If h is an integer then let $\phi_h, \psi_h : \langle g_0 \rangle \to \mathbb{C}$ be defined as follows:

$$\phi_h(g_0^i) = \begin{cases} q+\epsilon, & \text{if } m \mid i; \\ \epsilon(\zeta_m^{hi} + \zeta_m^{-hi}), & \text{otherwise;} \end{cases} \qquad \psi_h(g_0^i) = \begin{cases} q-\epsilon, & \text{if } m \mid i; \\ 0, & \text{otherwise.} \end{cases}$$

Given $R = (r_0, r_1, \ldots, r_k) \in \mathbb{Z}^{k+1}$, let

$$\mathcal{Y}_R = \{(s_0, s_1, \ldots, s_k) \in \mathbb{Z}^{k+1} : -r_j \leq s_j \leq r_j \text{ and } 2 \mid r_j - s_j \text{ for each } j\},$$

and let $\Psi_{r_0,r_1,\ldots,r_k} : \langle h_0 \rangle \to \mathbb{C}$ be defined by

$$\Psi_{r_0,r_1,\ldots,r_k}(h_0^i) = \sum_{(s_0,s_1,\ldots,s_k)\in\mathcal{Y}_R} \zeta_m^{i\sum_{j=0}^k s_j p^j}.$$

If moreover $r_0 + \cdots + r_k$ is even then let

$$V_{R;h} = \left\{ (s_0, s_1, \ldots, s_k) \in \mathcal{Y}_R \setminus \{(0,\ldots,0)\} : \frac{\sum_{j=0}^k s_j p^j}{2} \equiv \pm h \bmod m \right\}, \quad (2.4)$$

and let $\chi_{r_0,r_1,\ldots,r_k} : \langle g_0 \rangle \to \mathbb{C}$ be defined by

$$\chi_{r_0,r_1,\ldots,r_k}(g_0^i) = \sum_{(s_0,s_1,\ldots,s_k)\in\mathcal{Y}_R} \zeta_m^{i\frac{\sum_{j=0}^k s_j p^j}{2}}.$$

Lemma 2.3.3. *Let g_0 and h_0 be p-regular elements of $\mathrm{PSL}(2,q)$ and $\mathrm{SL}(2,q)$, respectively, both of order m. Then the following statements hold for $s \in \mathbb{Z}$ and $R = (r_0, r_1, \ldots, r_k) \in \mathbb{Z}^{k+1}$:*

1. *If $m \nmid s$ then both ϕ_s and ψ_s are the restriction to $\langle g_0 \rangle$ of ordinary characters of $\mathrm{PSL}(2,q)$.*

2. *$\Psi_{r_0,r_1,\ldots,r_k}$ is the restriction to $\langle h_0 \rangle$ of a Brauer character of $\mathrm{SL}(2,q)$ modulo p. Moreover, if $r_0 + r_1 + \cdots + r_k$ is even then $\chi_{r_0,r_1,\ldots,r_k}$ is the restriction to $\langle g_0 \rangle$ of a Brauer character of $\mathrm{PSL}(2,q)$ modulo p.*

3. *If χ is an irreducible Brauer character of $\mathrm{SL}(2,q)$ (respectively $\mathrm{PSL}(2,q)$)*

modulo p then the restriction of χ *to* $\langle h_0\rangle$ *(respectively* $\langle g_0\rangle$*) equals* $\Psi_{r_0,r_1,\ldots,r_{f-1}}$ *(respectively* $\chi_{r_0,r_1,\ldots,r_{f-1}}$*) for some integers* $0 \leq r_0, r_1, \ldots, r_{f-1} \leq p-1$ *(respectively* $0 \leq r_0, r_1, \ldots, r_{f-1} \leq p-1$ *with* $r_0 + r_1 + \cdots + r_{f-1}$ *even).*

4. *If* $r_0 + r_1 + \cdots + r_k$ *is even then*

$$\chi_{r_0,r_1,\ldots,r_k} = \begin{cases} (1+2n_0)1_{\mathrm{PSL}(2,q)} + \epsilon \sum_{h=1}^{\frac{m}{2}} n_h\left(\phi_h - \psi_h\right), & \text{if } 2 \mid r_j \text{ for all } j; \\ 2n_0 1_{\mathrm{PSL}(2,q)} + \epsilon \sum_{h=1}^{\frac{m}{2}} n_h\left(\phi_h - \psi_h\right), & \text{otherwise}; \end{cases}$$

where $2n_h = |V_{R;h}|$ *and* $1_{\mathrm{PSL}(2,q)}$ *denotes the trivial character of* $\mathrm{PSL}(2,q)$*.*

Proof. (1) To prove that ϕ_s and ψ_s are the restriction to $\langle g_0\rangle$ of ordinary characters of $\mathrm{PSL}(2,q)$ we simply express them in terms of the irreducible characters η_1, η_2, θ_i and χ_i of $\mathrm{PSL}(2,q)$ as described in Table 2.1. If $s \equiv \pm s' \bmod m$ then $\phi_s = \phi_{s'}$ and $\psi_s = \psi_{s'}$. Therefore we may assume that $1 \leq s \leq \frac{m}{2}$. Firstly, if m is even then $\phi_{\frac{m}{2}}$ is the restriction of $\eta_1 + \eta_2$, and $\psi_{\frac{m}{2}}$ is the restriction of any θ_j if $\epsilon = 1$, and the restriction of any χ_i if $\epsilon = -1$. This covers the case $s = \frac{m}{2}$. Suppose otherwise that $1 \leq s < \frac{m}{2}$. If $\epsilon = 1$ then ϕ_s is the restriction of $\chi_{s\frac{q-1}{2m}}$ and ψ_s is the restriction of $\theta_{s\frac{q-1}{2m}}$, while if $\epsilon = -1$ then ϕ_s is the restriction of $\theta_{s\frac{q+1}{2m}}$ and ψ_s is the restriction of $\chi_{s\frac{q+1}{2m}}$.

(2) Let K be a field of characteristic p. The following defines an action by K-automorphisms on the group $\mathrm{SL}(2,q)$ on the ring of polynomials $K[X,Y]$[Alp86, Pages 14–16]:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} X = aX + bY, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} Y = cX + dY.$$

If n is a positive integer then the vector space V_n formed by the homogenous polynomials of degree n is invariant under this action and, if moreover n is even then $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ acts trivially on V_n. Therefore $\mathrm{PSL}(2,q)$ acts on V_n provided that n is even.

Let us fix integers $0 \leq r_0, r_1, \ldots, r_k \leq p-1$ and let $n = r_0 + r_1 p + \cdots + r_k p^k$. Observe that if $r_0 + r_1 + \cdots + r_k$ is even then n is also even. Let $W_{r_0,r_1,\ldots,r_k}$ be the subspace of V_n generated by the polynomials of the form $X^i Y^{n-i}$ with

$i = i_0 + i_1 p + \cdots + i_k p^k$ and $0 \leq i_j \leq r_j$ for every j. For such s we have

$$\begin{aligned}
\begin{pmatrix} a & b \\ c & d \end{pmatrix} X^i Y^{n-i} &= (aX+bY)^i (cX+dY)^{n-i} \\
&= \prod_{h=0}^{k} \left(a^{p^h} X^{p^h} + b^{p^h} Y^{p^h}\right)^{i_h} \left(c^{p^h} X^{p^h} + d^{p^h} Y^{p^h}\right)^{r_h - i_h} \\
&= \prod_{h=0}^{k} \left(\sum_{u=0}^{i_h} \alpha_{h,u} X^{up^h} Y^{(i_h-u)p^h} \right) \left(\sum_{v=0}^{r_h - i_h} \beta_{h,v} X^{vp^h} Y^{(r_h - i_h - v)p^h} \right) \\
&= \prod_{h=0}^{k} \left(\sum_{j=0}^{r_h} \gamma_{h,j} X^{jp^h} Y^{(r_h-j)p^h} \right) \\
&= \sum_{\substack{j = j_0 + j_1 p + \cdots + j_k p^k \\ 0 \leq j_h \leq r_h}} \delta_j X^j Y^{n-j} \in W_{r_0,\ldots,r_k}.
\end{aligned}$$

Therefore, $W_{r_0,r_1,\ldots,r_k}$ is invariant by the action of $\mathrm{SL}(2,q)$ (respectively $\mathrm{PSL}(2,q)$ if $r_0 + r_1 + \cdots + r_k$ is even) and hence it is a $K\,\mathrm{SL}(2,q)$-module (respectively $K\,\mathrm{PSL}(2,q)$-module). Let ρ denote the K-representation of $\mathrm{SL}(2,q)$ (respectively $\mathrm{PSL}(2,q)$) given by $W_{r_0,r_1,\ldots,r_k}$ and let χ be the Brauer character associated to the p-modular character afforded by ρ. If $\epsilon = 1$ then $\overline{\zeta_{2m}}$ belongs to the field with q elements, so that the diagonal matrix $D = \mathrm{diag}(\overline{\zeta_{2m}}, \overline{\zeta_{2m}}^{-1})$ belongs to $\mathrm{SL}(2,q)$. After a suitable election of ζ_{2m} we may assume that $g_0 = D$ because g_0 is conjugate to a power of D in $\mathrm{PSL}(2,q)$. Then each base element $X^s Y^{n-s}$ is an eigenvector of $\rho(g_0)$ with eigenvalue $\overline{\zeta_{2m}}^{2i-n} = \overline{\zeta_{2m}}^{s} = \overline{\zeta_m}^{\frac{s}{2}}$ for $s = s_0 + s_1 p + \cdots + s_k p^k$, $-r_j \leq s_j \leq r_j$ and $2 \mid r_j - s_j$ for each j. Therefore $\Psi_{r_0,r_1,\ldots,r_k}$ (respectively $\chi_{r_0,r_1,\ldots,r_k}$) coincides with the restriction of χ to $\langle h_0 \rangle$ (respectively $\langle g_0 \rangle$). Suppose that $\epsilon = -1$. Then $D \in \mathrm{SL}(2,q^2)$ and this group acts on $W_{r_0,r_1,\ldots,r_k}$ in the same way. Again the same argument finishes the proof.

(3) The absolutely irreducible characters in characteristic p of $\mathrm{SL}(2,q)$ have been described in [BN41] (see also [Sri64]). After lifting these characters to $\mathrm{SL}(2,q)$ we obtain that if $0 \leq r_0, r_1, \ldots, r_{f-1} \leq p-1$ then $\chi_{r_0,r_1,\ldots,r_{f-1}}$ is the restriction to $\langle g_0 \rangle$ of an irreducible Brauer character of $\mathrm{SL}(2,q)$ modulo p and, conversely, the restriction to $\langle g_0 \rangle$ of any irreducible Brauer character of $\mathrm{SL}(2,q)$ modulo p is of this form. Observe that the result for $\mathrm{PSL}(2,q)$ is just a consequence of the one

for $\mathrm{SL}(2,q)$.

(4) Straightforward. □

Notation 2.3.4. *In the following chapters we will often encounter some fixed element g_0 of $\mathrm{SL}(2,q)$ or of $\mathrm{PSL}(2,q)$. Then we will use the complex valuated functions defined on g_0: $\Psi_{r_0,r_1,\ldots,r_k}, \phi_h, \psi_h, \chi_{r_0,r_1,\ldots,r_k}$ and we will abuse the notation by referring to them as the ordinary or p-Brauer characters of $\mathrm{SL}(2,q)$ or $\mathrm{PSL}(2,q)$, rather as the restriction to $\langle g_0\rangle$ of such an ordinary or p-Brauer character. This will be harmless because we will use only these restrictions.*

CHAPTER 3

On the Zassenhaus Conjecture for PSL(2,q)

In this chapter we study (ZC1) for projective special linear groups $\mathrm{PSL}(2,q)$ with q a prime power. The results appeared in [dRS17] and [MdRS17].

Along this chapter

$$p \text{ is a prime integer, } q = p^f \text{ for a positive integer } f \text{ and } G = \mathrm{PSL}(2,q).$$

Let u be an element of order n in $\mathrm{V}(\mathbb{Z}G)$. Hertweck proved that u is rationally conjugate to an element of G provided that n is prime different from p, or $n = p$ and $f \leq 2$, or $n = 6$ [Her07]. The first case was extended by Margolis to p-regular elements of prime power order [Mar16]. The main tool used to prove these results was the HeLP Method (see Section 1.4).

In Section 3.1 we calculate the sums $\Upsilon_d(G[m]) = \sum_{g^G, |g|=m} \Upsilon_d(g)$ for $\Upsilon \in \mathrm{VPA}_{rt}(G)$ for r and t two different primes not dividing q, $d \mid rt$ and m a positive integer. In Section 3.2 we show that the HeLP Method fails to prove (ZC1) for the next natural case to consider, namely when $n = 2t$ with t a prime integer greater than 4. On the positive side, the main result of this section (Theorem 3.2.1) provides significant information on a possible counterexample to (ZC1) of this kind.

As mentioned in the Introduction, (ZC1) has only been proved for very few non-solvable groups. The proofs of the results for solvable groups often argue by induction on the order of the group. In this way one may assume that the conjecture holds for proper quotients of the original group. The first step in a similar argument for non-solvable groups should consist in proving the conjecture for simple groups. Although this has been studied by some authors, see e.g. [LP89, Her07, Her08c, BKL08, BM17b, BC17], the conjecture is still only known for exactly thirteen non-abelian simple groups (see [BM17a, Proof of Theorem C] for an overview), all being isomorphic to some $\mathrm{PSL}(2,q)$ for some particular small prime power q. The aim of Section 3.3 is to extend this knowledge by proving that any torsion unit of $\mathbb{Z}G$ of order coprime with $2p$ is rationally conjugate to an element of G (see Theorem 3.3.1). We prove this result employing a variation of the HeLP Method, since the plain HeLP Method would imply too many case distinctions, in a way suitable for the character theory of $\mathrm{PSL}(2,q)$. As a direct application of this result and the results of Hertweck and Margolis mentioned above, we prove (ZC1) for $\mathrm{PSL}(2,p)$ with p a Fermat or Mersenne prime (see Theorem 3.3.2). This result increases the number of simple groups for which (ZC1) has been proved from thirteen to sixty-two, namely the groups $\mathrm{PSL}(2,q)$ with $q \in \{8,9,11,13,16,19,23,25,32\}$ or one of the four known Fermat primes different from 3 or one of the forty-nine known Mersenne primes different from 3 [Calb]. Actually, Theorem 3.3.2 proves the conjecture for probably infinitely many simple groups because, based on heuristic evidences, it has been conjectured that there are infinitely many Mersenne primes [Cala]. Lenstra, Pomerance and Wagstaff have proposed independently a conjecture on the growth of the number of Mersenne primes smaller than a given integer [Pom81, Wag83].

As a consequence of the results of Section 2.3 and Section 3.1, and looking on the orders of elements in G, cf. Proposition 2.3.1, one should not expect a better result for (ZC1) for G when applying only this method. Thus, as so often in Arithmetics and Group Theory, the prime 2 behaves very differently than the other primes.

Throughout this chapter we will often use Notation 2.3.4 and Lemma 2.2.6.

3.1 Virtual partial augmentations of order the product of at most two primes

We first describe $\mathrm{VPA}_r(G)$ with r a prime different from p and then we calculate the sums $\Upsilon_d(G[m])$ for $\Upsilon \in \mathrm{VPA}_{rt}(G)$ with r and t two different primes such that

$q \equiv \pm 1 \bmod 2rt$ (see the definition at the Introduction of this chapter).

The following proposition is another proof of the result of Hertweck for units of prime order [Her07, Proposition 6.4].

Proposition 3.1.1. *Let* $G = \mathrm{PSL}(2, q)$ *with* q *an odd prime power and let* r *be a prime not dividing* q*. Then* $\mathrm{TPA}_r(G) = \mathrm{VPA}_r(G)$*.*

Proof. The result is trivial if $q \not\equiv \pm 1 \bmod 2r$ because in such case r does not divides $|G|$ and hence $\mathrm{VPA}_r(G) = \emptyset = \mathrm{TPA}_r(G)$, by Proposition 2.1.2. The result is also trivial if $r = 2$ because, by Proposition 2.3.1, all the elements of G of order 2 are conjugate. So suppose that r is odd and $q \equiv \pm 1 \bmod 2r$.

Let $\Upsilon \in \mathrm{VPA}_r(G)$. To prove the lemma we fix an element $g_0 \in G$ of order r and use (V4) with the Brauer character χ_2. We have that $\left\{g_0^i : i = 1, \dots, \frac{r-1}{2}\right\}$ is a set of representatives of the conjugacy classes of G of elements of order r. Then, by (V1), (V2) and (V3), we have $\sum_{j=1}^{\frac{r-1}{2}} \Upsilon_1(g_0^j) = 1$. Using Lemma 2.2.6, for each $l, i \in \{1, \dots, \frac{r-1}{2}\}$ we have

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\chi_2(g_0^i)\zeta_r^{-l}) &= \mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r^{-l}) + \mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r^{i-l}) + \mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r^{-i-l}) \\ &= \begin{cases} r-3, & \text{if } i \equiv \pm l \bmod r; \\ -3, & \text{otherwise.} \end{cases} \end{aligned}$$

Hence, using the formula in (V4) we obtain

$$\mu(\zeta_r^l, \Upsilon, \chi_2) = \frac{1}{r}\left((r-3)\Upsilon_1(g_0^l) - 3\sum_{j=1, j\neq l}^{\frac{r-1}{2}} \Upsilon_1(g_0^j) + 3\right) = \Upsilon_1(g_0^l) \in \mathbb{Z}_{\geq 0}.$$

Therefore, there is an integer i in the interval $\left[1, \frac{r-1}{2}\right]$ such that $\Upsilon_1(g_0^i) = 1$ and $\Upsilon_1(h) = 0$ for every $h \in G \setminus (g_0^i)^G$. Then Υ is the distribution of partial augmentations of g_0^i. We conclude that $\Upsilon \in \mathrm{TPA}_r(G)$. □

Corollary 3.1.2. *Let* $G = \mathrm{PSL}(2, q)$ *with* q *an odd prime power and let* m *be a positive integer. Assume that* $q \equiv \pm 1 \bmod 2m$ *and let* $\Upsilon \in \mathrm{VPA}_m(G)$*. Then* G

has an element g_0 of order m such that for every prime divisor t of m we have

$$\Upsilon_{\frac{m}{t}}(g) = \begin{cases} 1, & \textit{if } g \in \left(g_0^{\frac{m}{t}}\right)^G; \\ 0, & \textit{otherwise.} \end{cases} \tag{3.1}$$

Proof. Fix $g_1 \in G$ of order m. By (2.2) and Proposition 3.1.1, if t is a prime divisor of m then $\Upsilon^{\frac{m}{t}} \in \mathrm{VPA}_t(G) = \mathrm{TPA}_t(G)$. As every element of order t in G is conjugate in G to an element of $\langle g_1^{\frac{m}{t}} \rangle$ by Proposition 2.3.1, we deduce that there is an integer i_t coprime with t such that $\Upsilon^{\frac{m}{t}}$ is the distribution of partial augmentations of $g_1^{\frac{m}{t} i_t}$. Let i be an integer with $i \equiv \pm i_t \mod t$ for every prime t dividing m and let $g_0 = g_1^i$. Then $g_0^{\frac{m}{t}} = g_1^{\frac{m}{t} i_t}$ for every prime t and this implies that $\Upsilon^{\frac{m}{t}}$ is the distribution of partial augmentations of $g_0^{\frac{m}{t}}$. In particular, (3.1) holds for every prime t. □

In the remainder of the section r and t are different primes such that $q \equiv \pm 1 \mod 2rt$ and $\Upsilon \in \mathrm{VPA}_{rt}(G)$. By Corollary 3.1.2, G has an element g_0 of order rt, which will be fixed throughout, such that

$$\Upsilon_r(g) = \begin{cases} 1, & \text{if } g \in (g_0^r)^G; \\ 0, & \text{otherwise;} \end{cases} \quad \text{and} \quad \Upsilon_t(g) = \begin{cases} 1, & \text{if } g \in (g_0^t)^G; \\ 0, & \text{otherwise.} \end{cases} \tag{3.2}$$

As every element of G of order divisible by rt is conjugate to an element of $\langle g_0 \rangle$, we have that $\Upsilon_1(g) = 0$ for every $g \in G$ which is not conjugate to an element of $\langle g_0 \rangle \setminus \{1\}$. This will simplify the expression in (V4), as in the following lemma.

For a general finite group G, an element $\Upsilon = (\Upsilon_d)_{d|n}$ of $\mathrm{VPA}_n(G)$ and a positive integer m we define

$$\Upsilon_d(G[m]) = \sum_{g^G, |g|=m} \Upsilon_d(g).$$

Lemma 3.1.3. *Let χ be either an ordinary character or a Brauer character of G module p. Then*

$$\begin{aligned} \mu(1, \Upsilon, \chi) \quad = \quad & \frac{1}{rt} \left[\Upsilon_1(G[rt]) \operatorname{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi(g_0)) + \Upsilon_1(G[t]) \operatorname{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi(g_0^r)) + \right. \\ & \Upsilon_1(G[r]) \operatorname{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi(g_0^t)) + \operatorname{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\chi(g_0^t)) + \\ & \left. \operatorname{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\chi(g_0^r)) + \chi(1) \right] \end{aligned}$$

and

$$0 \leq \mu(1, \Upsilon, \chi) \leq \frac{1}{t}\left[\chi(1) + \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\chi(g_0^r))\right].$$

Proof. If x and y are elements of G with the same order, then x is conjugate in G to a power of y by Proposition 2.3.1. This implies that if e is a multiple of this common order then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q})$ such that $\chi(x) = \sigma(\chi(y))$. (If χ is a Brauer character modulo p then one assume that x and y are p-regular elements of G.) Thus $\mathrm{Tr}_{\mathbb{Q}(\zeta_e)/\mathbb{Q}}(\chi(x)) = \mathrm{Tr}_{\mathbb{Q}(\zeta_e)/\mathbb{Q}}(\chi(y))$. Combining this with (V4) we obtain the expression for $\mu(1, \Upsilon, \chi)$ in the lemma. Moreover, $\mu_r^-(\Upsilon, \chi) = \frac{1}{rt}(\chi(1) + \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\chi(g_0^r)))$, by (3.2). The inequality is then a consequence of (2.3) for $n = rt$ and $m = r$. □

The specialization of the following lemma to the case where Υ is the distribution of partial augmentations of a torsion element of $\mathrm{V}(\mathbb{Z}G)$ is a particular case of a result of Wagner [Wag95, BM15].

Lemma 3.1.4. *t divides $\Upsilon_1(G[t])$ and r divides $\Upsilon_1(G[r])$.*

Proof. By symmetry we only have to prove $t \mid \Upsilon_1(G[t])$. We will give one proof for the case when t is odd and another one for the case when r is odd. This cover all the cases because r and t are different primes. Write $q = \epsilon + 2rth$ with $\epsilon = \pm 1$ and h an integer. We will use Lemma 3.1.3 and (V4) with the ordinary character ϕ_t (relative to the element g_0 of order $m = rt$ fixed above).

Using Lemma 2.2.6, for any j we have:

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\phi_t(g_0^j)) = \begin{cases} 2\epsilon(r-1)(t-1), & \text{if } r|j; \\ 2\epsilon(1-t), & \text{if } r \nmid j. \end{cases}$$

Clearly, we have $\mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\phi_t(g_0^j)) = 2\epsilon(t-1)$ if $\gcd(rt, j) = r$, and $\mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\phi_t(g_0^j)) = -2\epsilon$ if $\gcd(rt, j) = t$. By (V1) we have $\Upsilon_1(G[r]) + \Upsilon_1(G[t]) + \Upsilon_1(G[rt]) = 1$. Combining this with Lemma 3.1.3 we get

$$rt\mu(1, \Upsilon, \phi_t) = 2r\epsilon(t-1)\Upsilon_1(G[t]) + 2rth.$$

Thus, if t is odd then t divides $\Upsilon_1(G[t])$.

Suppose r odd. Let $1 \leq j \leq \frac{r-1}{2}$ be an integer. We have for every integer i that

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\phi_t(g_0^i)\zeta_{rt}^{-jt}) = \begin{cases} \epsilon(r-2)(t-1), & \text{if } i \equiv \pm j \bmod r; \\ 2\epsilon(1-t), & \text{if } i \not\equiv \pm j \bmod r. \end{cases} \tag{3.3}$$

For every $1 \leq i \leq \frac{r-1}{2}$ we denote $x_i = \sum_{1 \leq k \leq \frac{rt}{2}, k \equiv \pm i \bmod r} \Upsilon_1(g_0^k)$. Then $\Upsilon_1(G[t]) + \sum_{i=1}^{\frac{r-1}{2}} x_i = 1$. By (3.3), we obtain

$$\begin{aligned} \sum_{1 \leq k \leq \frac{rt}{2}} \Upsilon_1(g_0^k)\,\mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\phi_t(g_0^k)\zeta_{rt}^{-jt}) &= \epsilon(t-1)\left((r-2)x_j - 2\Upsilon_1(G[t]) - 2\sum_{i \neq j} x_i\right) \\ &= \epsilon(t-1)(rx_j - 2). \end{aligned}$$

Moreover, we have $\mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\phi_t(g_0^r)\zeta_{rt}^{-jtr}) = 2\epsilon(t-1)$ and

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\phi_t(g_0^t)\zeta_{rt}^{-jt^2}) = \epsilon w_j \quad \text{with} \quad w_j = \begin{cases} (r-2), & \text{if } jt \equiv \pm 1 \bmod r; \\ -2, & \text{if } jt \not\equiv \pm 1 \bmod r. \end{cases}$$

Applying condition (V4) with the character ϕ_t and $l = jt$ we deduce that

$$\epsilon(t-1)(rx_j - 2) + 2\epsilon(t-1) + \epsilon w_j + 2rth + 2\epsilon = 2hrt + \epsilon(rx_j(t-1) + 2 + w_j)$$

is a multiple of rt. In particular, t divides $2 + w_j - rx_j$ for every $j = 1, \dots, \frac{r-1}{2}$. Summing for $j = 1, \dots, \frac{r-1}{2}$ and taking into account that $\sum_{j=1}^{\frac{r-1}{2}} w_j = 1$ we obtain that t divides $r\left(1 - \sum_{j=1}^{\frac{r-1}{2}} x_j\right) = r\Upsilon_1(G[t])$. Therefore $t \mid \Upsilon_1(G[t])$, as desired. □

Proposition 3.1.5. *Let Υ be an element of $\mathrm{VPA}_{rt}(G)$, where $G = \mathrm{PSL}(2,q)$ for an odd prime power q and r and t are different primes with $\gcd(rt,q) = 1$. Then*

$$\Upsilon_1(G[r]) = \Upsilon_1(G[t]) = 0 \quad \textit{and} \quad \Upsilon_1(G[rt]) = 1.$$

Proof. By symmetry we may assume that $r < t$. We first prove that $\Upsilon_1(G[t]) = 0$. For that we use Lemma 3.1.3 applied to the Brauer character χ_{2r}. Using Lemma 2.2.6 we have

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi_{2r}(g_0)) = (t-1)(r-1),$$

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi_{2r}(g_0^t)) = (t-1)(r-1), \quad \mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi_{2r}(g_0^r)) = (r-1)(t-1-2r),$$

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\chi_{2r}(g_0^t)) = r-1 \quad \text{and} \quad \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\chi_{2r}(g_0^r)) = t-1-2r.$$

Combining these equalities with $\Upsilon_1(G[r]) + \Upsilon_1(G[t]) + \Upsilon_1(G[rt]) = 1$, we obtain by straightforward calculations that $\mu(1, \Upsilon, \chi_{2r}) = 1 - 2\frac{\Upsilon_1(G[t])}{t}$ and $\chi_{2r}(1) + \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\chi_{2r}(g_0^r)) = t$. Using Lemma 3.1.3, we conclude that $0 \le \frac{\Upsilon_1(G[t])}{t} \le \frac{1}{2}$. By Lemma 3.1.4, we know that $\frac{\Upsilon_1(G[t])}{t}$ is an integer, hence $\Upsilon_1(G[t]) = 0$ as desired.

Then $\Upsilon_1(G[r]) + \Upsilon_1(G[rt]) = 1$ and it remains only to show that $\Upsilon_1(G[r]) = 0$. For that we use Lemma 3.1.3 with the Brauer character χ_2. In this case we have

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi_2(g_0)) = tr - r - t + 3,$$

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi_2(g_0^t)) = tr - r - 3t + 3, \quad \mathrm{Tr}_{\mathbb{Q}(\zeta_{rt})/\mathbb{Q}}(\chi_2(g_0^r)) = tr - 3r - t + 3,$$

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\chi_2(g_0^t)) = r-3 \quad \text{and} \quad \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\chi_2(g_0^r)) = t-3.$$

Therefore, we have that $\mu(1, \Upsilon, \chi_2) = 1 - 2\frac{\Upsilon_1(G[r])}{r}$ and $\chi_2(1) + \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}(\chi_2(g_0^r)) = t$. Applying Lemma 3.1.3 we obtain $0 \le \frac{\Upsilon_1(G[r])}{r} \le \frac{1}{2}$ and the result follows, since, by Lemma 3.1.4, $\frac{\Upsilon_1(G[r])}{r}$ is an integer. □

3.2 Virtual partial augmentations of order 2t

Recall that $G = \mathrm{PSL}(2, q)$ with $q = p^f$ an odd prime power and that we are using Notation 2.3.4. Let t be an odd prime. By Proposition 2.3.1.(2), $\mathrm{V}(\mathbb{Z}G)$ has elements of order $2t$ if and only if so does G if and only if $q \equiv \pm 1 \bmod 4t$. Thus we assume that $q \equiv \pm 1 \bmod 4t$. For $g_0 \in G$ with $|g_0| = 2t$ and $t \ge 5$ let $\Upsilon^{(g_0)}$ denote the list of class functions $(\Upsilon_1^{(g_0)}, \Upsilon_2^{(g_0)}, \Upsilon_t^{(g_0)}, \Upsilon_{2t}^{(g_0)})$ of G defined as follows:

$$\Upsilon_d^{(g_0)}(g) = \begin{cases} 1, & \text{if } (d, g^G) \in \big\{(2t, 1^G), (t, (g_0^t)^G), (2, (g_0^2)^G), \\ & \qquad (1, (g_0^{\frac{t-1}{2}})^G), (1, (g_0^{\frac{t+1}{2}})^G)\big\}; \\ -1, & \text{if } (d, g^G) = (1, (g_0^{t-1})^G); \\ 0, & \text{otherwise.} \end{cases} \tag{3.4}$$

Hertweck proved (ZC1) for units of order 6 in $\mathrm{PSL}(2, q)$ (see Proposition 2.3.1.(2)).

This result is also a consequence of the the equality $\mathrm{VPA}_6(G) = \mathrm{TPA}_6(G)$ stated in the following theorem.

Theorem 3.2.1. *Let t be an odd prime, let q be a prime power such that $q \equiv \pm 1 \bmod 4t$ and let $G = \mathrm{PSL}(2,q)$. Then $\mathrm{VPA}_6(G) = \mathrm{TPA}_6(G)$ and if $t \geq 5$ then*

$$\mathrm{VPA}_{2t}(G) = \mathrm{TPA}_{2t}(G) \cup \{\Upsilon^{(g_0)} : g_0 \in G, |g_0| = 2t\}.$$

Proof. If $t = 3$ then G has a unique conjugacy class of elements of order 3 and a unique one of elements of order 6 by Proposition 2.3.1. Combining this with Proposition 3.1.5 we deduce that $\mathrm{VPA}_6(G) = \mathrm{TPA}_6(G)$. So in the remainder we assume that $t \geq 5$. We set $n = \frac{t-1}{2}$.

We first prove the inclusion $\mathrm{VPA}_{2t}(G) \subseteq \mathrm{TPA}_{2t}(G) \cup \{\Upsilon^{(g_0)} : g_0 \in G, |g_0| = 2t\}$. For that we take an element $\Upsilon = (\Upsilon_1, \Upsilon_2, \Upsilon_t, \Upsilon_{2t})$ of $\mathrm{VPA}_{2t}(G)$ and we show that there is an element g_0 of order $2t$ in G such that either $\Upsilon = \varepsilon^*$ or $\Upsilon = \Upsilon^{(g_0)}$, where ε^* is the distribution of partial augmentations of g_0 and $\Upsilon^{(g_0)}$ is as in (3.4). By (V3), if g is an element of G of order not dividing $2t$ then $\Upsilon_d(g) = 0$ for each $d \mid 2t$. By the results of Section 3.1, there exists $g_0 \in G$ of order $2t$ such that Υ_t and Υ_2 are as in (3.2) with $r = 2$. This shows that $\Upsilon_t = \Upsilon_t^{(g_0)} = \varepsilon_t^*$ and $\Upsilon_2 = \Upsilon_2^{(g_0)} = \varepsilon_2^*$. As, clearly $\Upsilon_{2t} = \Upsilon_{2t}^{(g_0)} = \varepsilon_{2t}^*$, it remains to show that Υ_1 is either ε_1^* or $\Upsilon_1^{(g_0)}$.

Let Odd denote the set of odd integers in the interval $[1, t-1]$ and for each $l \in [1, t-1]$ let

$$i_l = \begin{cases} l, & \text{if } l \in \mathrm{Odd}; \\ t - l, & \text{otherwise}; \end{cases} \qquad w_l = \begin{cases} 1, & \text{if } l \in \{1, t-1\}; \\ 0, & \text{otherwise}; \end{cases}$$

and

$$W_l = \begin{cases} 1, & \text{if } l \in \{1, 2, t-2, t-1\}; \\ 0, & \text{otherwise.} \end{cases}$$

Observe that i_l is the unique element $j \in \mathrm{Odd}$ with $j \equiv \pm l \bmod t$ and i_{nl} is the unique element $j \in \mathrm{Odd}$ with $2j \equiv \pm l \bmod t$. Moreover, $i_l \neq i_{nl}$ because $n \not\equiv \pm 1 \bmod t$, as $t \geq 5$.

We also use the notation $T = \mathrm{Tr}_{\mathbb{Q}(\zeta_{2t})/\mathbb{Q}} = \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathbb{Q}}$. Observe that $\{g_0^i : i \in \mathrm{Odd}\}$ and $\{g_0^{t-i} : i \in \mathrm{Odd}\}$ are sets of representatives of the conjugacy classes of elements of G of orders $2t$ and t, respectively. By Proposition 3.1.5 we have

$$\Upsilon_1(g_0^t) = \sum_{i \in \text{Odd}} \Upsilon_1\left(g_0^{t-i}\right) = 0 \quad \text{and} \quad \sum_{i \in \text{Odd}} \Upsilon_1\left(g_0^i\right) = 1. \tag{3.5}$$

By (V4) and Lemma 2.3.3.(2) if m is an even integer and $l \in \mathbb{Z}$ then the following is a non-negative integer:

$$\frac{1}{2t}\left[\chi_m(1) + \chi_m\left(g_0^t\right)(-1)^l + T\left(\chi_m\left(g_0^2\right)\zeta_{2t}^{-2l}\right)\right.$$
$$\left. + \sum_{i \in \text{Odd}} \left(\Upsilon_1\left(g_0^i\right) T\left(\chi_m\left(g_0^i\right)\zeta_{2t}^{-l}\right) + \Upsilon_1\left(g_0^{t-i}\right) T\left(\chi_m\left(g_0^{t-i}\right)\zeta_{2t}^{-l}\right)\right)\right]. \tag{3.6}$$

We will use this with $l \in \{1, \dots, t-1\}$ and $m \in \{2, 4\}$. To facilitate the calculations we collect the following equalities which are all direct application of Lemma 2.2.6:

$$\begin{array}{l} \chi_2(1) = 3, \quad \chi_2\left(g_0^t\right) = -1 \qquad \chi_4(1) = 5, \quad \chi_4\left(g_0^t\right) = 1, \\ T\left(\chi_2\left(g_0^2\right)\zeta_{2t}^{-2l}\right) = tw_l - 3, \quad T\left(\chi_4\left(g_0^2\right)\zeta_{2t}^{-2l}\right) = tW_l - 5. \end{array}$$

Moreover, if $i \in$ Odd then

$$T\left(\chi_2\left(g_0^i\right)\zeta_{2t}^{-l}\right) = \begin{cases} (1-t)(-1)^l, & \text{if } i = i_l; \\ (-1)^l, & \text{otherwise;} \end{cases}$$

$$T\left(\chi_2\left(g_0^{t-i}\right)\zeta_{2t}^{-l}\right) = \begin{cases} (t-3)(-1)^l, & \text{if } i = i_l; \\ (-3)(-1)^l, & \text{otherwise;} \end{cases}$$

$$T\left(\chi_4\left(g_0^i\right)\zeta_{2t}^{-l}\right) = \begin{cases} (t+1)(-1)^{l+1}, & \text{if } i = i_l; \\ (t-1)(-1)^l, & \text{if } i = i_{nl}; \\ (-1)^{l+1}, & \text{otherwise;} \end{cases}$$

and

$$T\left(\chi_4\left(g_0^{t-i}\right)\zeta_{2t}^{-l}\right) = \begin{cases} (t-5)(-1)^l, & \text{if } i \in \{i_l, i_{nl}\}; \\ (-5)(-1)^l, & \text{oherwise.} \end{cases}$$

Plugging this information into (3.6) for $m = 2$ and $m = 4$ and using (3.5), we obtain

$$\frac{1}{2}\left((-1)^l\left(\Upsilon_1\left(g_0^{t-i_l}\right)-\Upsilon_1\left(g_0^{i_l}\right)\right)+w_l\right)\ \in\ \mathbb{Z}_{\geq 0} \tag{3.7}$$

and

$$\frac{1}{2}\left((-1)^l\left(\Upsilon_1\left(g_0^{i_{nl}}\right)+\Upsilon_1\left(g_0^{t-i_{nl}}\right)-\Upsilon_1\left(g_0^{i_l}\right)+\Upsilon_1\left(g_0^{t-i_l}\right)\right)+W_l\right)\ \in\ \mathbb{Z}_{\geq 0}. \tag{3.8}$$

Using (3.7) with l and with $t-l$ we obtain $\left|\Upsilon_1(g_0^l)-\Upsilon_1(g_0^{t-l})\right| \leq w_l$ if $l \in \text{Odd}$. In particular,

$$\Upsilon_1(g_0^l)=\Upsilon_1(g_0^{t-l}),\ \text{if } l \in \text{Odd}\setminus\{1\}. \tag{3.9}$$

This together with (3.5) yields

$$\Upsilon_1(g_0)=1-\sum_{l\in\text{Odd}\setminus\{1\}}\Upsilon_1(g_0^l)=1-\sum_{l\in\text{Odd}\setminus\{1\}}\Upsilon_1(g_0^{t-l})=1+\Upsilon_1(g_0^{t-1}). \tag{3.10}$$

We now combine (3.9) and (3.10) with (3.8) for l and $t-l$. When we take $l=1$ we obtain

$$\Upsilon_1(g_0^{i_n})=\Upsilon_1(g_0^{t-i_n})\in\{0,1\};$$

and taking $l \in \text{Odd}\setminus\{1,t-2\}$ we have

$$\Upsilon_1(g_0^{i_{nl}})=\Upsilon_1(g_0^{t-i_{nl}})=0, \quad \text{if } l\in\text{Odd}\setminus\{1,t-2\}.$$

As $l \mapsto i_{nl}$ defines a bijection Odd → Odd mapping $t-2$ to 1, the latter is equivalent to

$$\Upsilon_1(g_0^l)=\Upsilon_1(g_0^{t-l})=0, \quad \text{for all } l\in\text{Odd}\setminus\{i_n,1\}.$$

Thus

$$\Upsilon_1(g_0)=1+\Upsilon_1(g_0^{t-1})=1-\sum_{l\in\text{Odd}\setminus\{1\}}\Upsilon_1(g_0^{t-l})=1-\Upsilon_1(g_0^{t-i_n})=1-\Upsilon_1(g_0^{i_n})\in\{0,1\}.$$

Since $\{i_n,t-i_n\}=\{n,n+1\}$, we conclude that either $\Upsilon_1(g_0)=1$ and $\Upsilon_1(g_0^l)=0$ for every $2\leq l\leq t-1$, or $\Upsilon_1(g_0^{t-1})=-1$, $\Upsilon_1(g_0^n)=\Upsilon_1(g_0^{n+1})=1$ and $\Upsilon_1(g_0^l)=0$ for every integer l in $[1,t-1]\setminus\{n,n+1,t-1\}$. In the first case $\Upsilon_1=\varepsilon_1^*$ and in the latter case $\Upsilon_1 = \Upsilon_1^{(g_0)}$, as desired. This finishes the necessary part of the proof.

To finish the proof of the theorem it remains to prove that if g_0 is an element of G of order $2t$ then $\Upsilon^{(g_0)} \in \mathrm{VPA}_{2t}(G)$. That $\Upsilon^{(g_0)}$ satisfies conditions (V1), (V2) and (V3) follows by straightforward arguments. So it remains to show that the following is a non-negative integer for every ordinary or Brauer character of G:

$$\begin{aligned}\mu\left(\zeta_{2t}^l, \Upsilon^{(g_0)}, \chi\right) \quad = \quad & \frac{1}{2t}\left[\chi(1) + \chi\left(g_0^t\right)(-1)^l + \right.\\ & \left. T\left(\chi\left(g_0^2\right)\zeta_{2t}^{-2l} + \left(\chi\left(g_0^n\right) + \chi\left(g_0^{n+1}\right) - \chi\left(g_0^{t-1}\right)\right)\zeta_{2t}^{-l}\right)\right].\end{aligned}$$

Actually, it suffices to consider Brauer characters module the prime p dividing q. This is a consequence of the following remark, which was brought to our attention by Leo Margolis.

Remark 3.2.2. *Let $G = \mathrm{PSL}(2, q)$, with q a power of a prime p and let n be an integer coprime to p. Let $\Upsilon = (\Upsilon_d)_{d|n}$ be a list of class functions of G satisfying conditions (V1), (V2) and (V3). Then $\Upsilon \in \mathrm{VPA}_n(G)$ if and only if it satisfies (V4) for every irreducible Brauer character of G modulo p.*

Proof. Suppose that $\Upsilon \in \mathrm{VPA}_n(G)$ satisfies (V4) for the irreducible Brauer characters of G modulo p. Observe that $\mu(\zeta_n^l, \Upsilon, \chi)$ is $\mathbb{Z}$-linear in the last argument. This implies that if condition (V4) holds for the class functions $f_1, \dots, f_k$ then it also holds for each linear combination $\chi = a_1 f_1 + \cdots + a_k f_k$ with $a_1, \dots, a_k$ non-negative integers. This is also valid for class functions defined on the t-regular elements of G for a given prime t. Therefore, to verify (V4) it is enough to consider irreducible ordinary characters and irreducible Brauer characters of G. Moreover, as n is coprime with p, by (V3), each non-zero summand in the expression of $\mu(\zeta_n^l, \Upsilon, \chi)$ correspond to p-regular elements, for any ordinary or Brauer character of G. Thus we only have to consider the restriction of each ordinary character of G to the p-regular elements and the restriction of Brauer characters of G modulo a prime t to the $\{p, t\}$-regular elements. If t is a prime integer then the restriction to the t-regular elements of G of an irreducible ordinary character of G is a linear combination of the irreducible Brauer characters of G modulo t with coefficients in the decomposition matrix relative to t and these coefficients are non-negative integers (see Section 1.3 or [Ser78, Section 15.2]). Using the expression of the ordinary characters of G on the p-regular elements in terms of the Brauer characters of G modulo p we deduce that (V4) holds for all the ordinary characters of G. Let now t be a prime different from p. The decomposition matrix A of G relative to t is described in [Bur76]. Every non-zero column of A contains an entry equal to 1 in a row on which all the other entries are 0. This implies that each Brauer character of G modulo t equals the restriction to the t-regular elements of an ordinary character of G. Hence (V4) also holds for Brauer characters of G modulo t. □

Using Lemma 2.3.3.(3) and Remark 3.2.2, it remains to prove that if $r_0, \dots, r_k$ are in $\mathbb{Z}_{\geq 0}$ with $r_0 + \cdots + r_k$ even and l is an integer then $\mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, \chi_{r_0,r_1,\dots,r_k}) \in \mathbb{Z}_{\geq 0}$. For that we use that the map $\chi \mapsto \mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, \chi)$ is linear and the expression of $\chi_{r_0,r_1,\dots,r_k}$ obtained in Lemma 2.3.3.(4) in terms of the ordinary characters 1_G, ϕ_h and ψ_h for $h \in \{1, \dots, t\}$. Hence we start considering the latter characters.

In the remainder of the proof l is an integer, $h \in \{1, \dots, t\}$ and $\epsilon = \pm 1$ with $q \equiv \epsilon \bmod 4t$. We will use Lemma 2.2.6 without specific mention. An easy calculation shows that

$$\mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, \psi_h) = \frac{q-\epsilon}{2t} \quad \text{and} \quad \mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, 1_G) = \begin{cases} 1, & \text{if } 2t \mid l; \\ 0, & \text{otherwise.} \end{cases} \tag{3.11}$$

Now we calculate $\mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, \phi_h)$. For that we introduce the following notation:

$$\vartheta_{h,l} = \begin{cases} 1, & \text{if } h \equiv \pm 2l \bmod 2t, \text{ or } h \equiv \pm l \bmod t \text{ and } 2 \nmid l; \\ 0, & \text{otherwise;} \end{cases}$$

and

$$\gamma_{i,l} = \begin{cases} t, & \text{if } hi \equiv \pm l \bmod t; \\ 0, & \text{if } hi \not\equiv \pm l \bmod t; \end{cases}$$

for each $1 \leq i \leq t-1$. Clearly, we have $\phi_h(g_0^t) = 2\epsilon(-1)^h$, $T(\phi_h(g_0^i)\zeta_{2t}^{-l}) = (\gamma_{i,l} - 2)\epsilon(-1)^{hi+l}$, $\gamma_{n,l} = \gamma_{n+1,l}$, $\gamma_{2,2l} = \gamma_{t-1,l} = \gamma_{1,l}$ and

$$\gamma_{1,l}(1 - (-1)^l) + \gamma_{n,l}(-1)^{hn+l}(1 + (-1)^h) = 2t\vartheta_{h,l}.$$

Therefore

$$T\left(\phi_h\left(g_0^2\right)\zeta_{2t}^{-2l} - \phi_h\left(g_0^{t-1}\right)\zeta_{2t}^{-l}\right) = \epsilon(\gamma_{1,l}-2)(1-(-1)^l)$$

and

$$\begin{aligned} T\left(\left(\phi_h\left(g_0^n\right) + \phi_h\left(g_0^{n+1}\right)\right)\zeta_{2t}^{-l}\right) &= \epsilon(\gamma_{n,l}-2)(-1)^{hn+l}(1+(-1)^h)) \\ &= \begin{cases} 2\epsilon(\gamma_{n,l}-2)(-1)^l, & \text{if } 2 \mid h; \\ 0, & \text{if } 2 \nmid h. \end{cases} \end{aligned}$$

Hence

$$\begin{aligned} \mu\left(\zeta_{2t}^l, \Upsilon^{(g_0)}, \phi_h\right) &= \frac{q-\epsilon+\epsilon(\gamma_{1,l}(1-(-1)^l)+\gamma_{n,l}(-1)^{hn+l}(1+(-1)^h))}{2t} \\ &= \frac{q-\epsilon}{2t} + \epsilon\,\vartheta_{h,l}. \end{aligned} \tag{3.12}$$

Let $R = (r_0, r_1, \ldots, r_k) \in \mathbb{Z}^{k+1}$ with $r_0 + r_1 + \cdots + r_k$ even, and let $2n_h$ be the cardinality of the set $V_{R;h}$ defined in (2.4). Observe that $\mu(\xi, \Upsilon, \chi)$ is linear in the third argument. Then, using Lemma 2.3.3.(4), (3.11) and (3.12) we obtain

$$\mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, \chi_{r_0,\ldots,r_k}) = k_0\mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, 1_G) + \sum_{h=1}^{t} n_h\vartheta_{h,l}, \tag{3.13}$$

where k_0 is either $2n_0$ or $1+2n_0$. This finishes the proof of the theorem, as the expression in (3.13) is a non-negative integer because $\mu(\zeta_{2t}^l, \Upsilon^{(g_0)}, 1_G)$ is either 0 or 1 by (3.11), and all the n_h are non-negative integers. □

Suppose that $t \geq 5$ and let g_0 be an element of order $2t$ in $G = \mathrm{PSL}(2, q)$. Then $\Upsilon^{(g_0)}$ is the distribution of partial augmentations of the elements of a conjugacy class C in the units of $\mathbb{Q}G$ of an element of order $2t$ in $\mathrm{V}(\mathbb{Q}G)$ with integral partial augmentations. To settle (ZC1) in this case it remains to decide whether C contains an element u with integral coefficients. If not, (ZC1) holds in this case and otherwise u provides a counterexample for (ZC1). The smallest example of this situation is encountered for $q = 19$ and $t = 5$. However, Bächle and Margolis have proved (ZC1) for this example with a technique which they called the Lattice

Method [BM17b]. Unfortunately, the Lattice Method does not apply for the next cases ($q = 27$ and $q = 29$ and $t = 7$) basically because the representation type appearing in these cases is wild.

3.3 (ZC1) holds for units of order coprime to 2q in PSL(2,q)

In this section we prove the following theorem:

Theorem 3.3.1. *Let $G = \mathrm{PSL}(2, q)$ for some prime power q. Then any torsion unit of $\mathbb{Z}G$ of order coprime with $2q$ is rationally conjugate to an element of G.*

Suppose that $G = \mathrm{PSL}(2, p)$ with p a Fermat or Mersenne prime (i.e. $p = 2^k \pm 1$) and let u be an element in $\mathrm{V}(\mathbb{Z}G)$ of order n. Then by Proposition 2.3.1 we deduce that either $n = p$ or $p \nmid n$ and $n \mid \frac{p\pm1}{2}$. If n is a prime power then u is rationally conjugate to an element of G by Proposition 2.3.1.(2). On the other hand, if $n \mid \frac{p\pm1}{2}$ and n is not a prime power then n is coprime with $2p$ and hence, by Theorem 3.3.1, u is also rationally conjugate to an element of G. Therefore we have proved the following:

Theorem 3.3.2. *Let p be a Fermat or Mersenne prime. Then (ZC1) holds for $\mathrm{PSL}(2, p)$.*

Observe that a result as Theorem 3.3.2 for $\mathrm{PSL}(2, p^f)$ with $f \geq 2$ could not be possible to achieve only using the HeLP Method. In this case we will have to consider units of even order and in that situation we already know that the HeLP Method is not enough to prove that these units are rationally conjugate to elements of $\mathrm{PSL}(2, p^f)$ (see Theorem 3.2.1 as an example).

We now focus on proving Theorem 3.3.1. For that we will use the notation of Section 2.2. We will prove that any element u of order n in $\mathrm{V}(\mathbb{Z}G)$, where n is greater than 1 and coprime with $2p$, is rationally conjugate to an element of G. By Proposition 2.3.1.(2) we may also assume that n is not a prime power.

As the order n of u is fixed throughout, we simplify the notation of Section 2.2 by setting

$$\gamma = \gamma_n = \bar{\gamma}_n, \quad \alpha_x = \alpha_x^{(n)}, \quad \beta_{b,x}^{(n)} = 1, \quad \kappa_x = \kappa_x^{(n)} = \begin{cases} 2, & \text{if } x \equiv 0 \bmod n; \\ 1, & \text{otherwise.} \end{cases}$$

$$\mathbb{B} = \mathbb{B}_n = \left\{ x \in \mathbb{Z}/n\mathbb{Z} : |x : n_r| > \frac{n_r}{2r} \text{ for every prime } r \mid n \right\}$$

and

$$\mathcal{B} = \mathcal{B}_n = \{\alpha_b^{(n)} : b \in \mathbb{B}\}.$$

We argue by induction on n. So we assume that u^d is rationally conjugate to an element of G for every divisor d of n with $d \neq 1$.

By Lemma 2.3.3 (or by [Mar16, Lemma 1.2]), we deduce that there is a primitive n-th root of unity α in a field of characteristic p such that for every positive integer m, there is a p-modular representation Θ_{2m} of G of degree $1+2m$ such that

$$\Theta_{2m}(g) \text{ is conjugate to } \operatorname{diag}\left(1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}, \dots, \alpha^m, \alpha^{-m}\right).$$

We denote by χ_{2m} the p-Brauer character associated with Θ_{2m}. As usual in modular representation theory, a bijection between the complex roots of unity of order coprime with p and the roots of unity of the same order in a field of characteristic p has been fixed a priori. In this sense we will identify the eigenvalues of Θ_{2m} and the summands in χ_{2m}.

Since units of prime order in $\mathrm{V}(\mathbb{Z}G)$ are rationally conjugate to elements of G by Proposition 2.3.1.(2), we deduce that the kernel of Θ_2 on $\langle u \rangle$ is trivial and hence $\Theta_2(u)$ has order n. As the values of χ_2 on p-regular elements of G are real, by Proposition 2.3.1.(1) and Theorem 1.3.1, the set of eigenvalues of $\Theta_2(u)$ is closed under taking inverses (counting multiplicities). Therefore, $\Theta_2(u)$ is conjugate to $\operatorname{diag}(1, \zeta, \zeta^{-1})$ for a suitable primitive n-th root of unity ζ. Hence by Proposition 2.3.1 there exists an element $g_0 \in G$ of order n such that $\Theta_2(g_0)$ and $\Theta_2(u)$ are conjugate. From now on we abuse the notation and consider ζ both as a primitive n-root of unity in a field of characteristic p and as a complex primitive n-root of unity. Then for any positive integer m we have

$$\Theta_{2m}(g_0) \text{ is conjugate to } \operatorname{diag}\left(1, \zeta, \zeta^{-1}, \zeta^2, \zeta^{-2}, \dots, \zeta^m, \zeta^{-m}\right),$$

and for every integer i we have

$$\chi_{2m}(g_0^i) = \sum_{j=-m}^{m} \zeta^{ij} = 1 + \sum_{j=1}^{m} \alpha_{ij}. \tag{3.14}$$

The element $g_0 \in G$ and the primitive n-th root of unity ζ will be fixed throughout.

By Proposition 2.3.1.(1), $x \mapsto (g_0^x)^G$ defines a bijection from Γ_n to the set of conjugacy classes of G formed by elements of order dividing n. For an integer x (or $x \in \Gamma_n$) we set

$$\varepsilon_x = \varepsilon_{g_0^x}(u) \quad \text{and} \quad \lambda_x = \sum_{i \in \Gamma_n} \varepsilon_i \alpha_{ix}.$$

By Theorem 1.2.4, u is rationally conjugate to an element of G if and only if $\varepsilon_x \geq 0$ for every $x \in \Gamma_n$.

Lemma 3.3.3. *u is rationally conjugate to g_0 if and only if*

$$\lambda_i = \alpha_i, \text{ for any positive integer } i. \tag{3.15}$$

Proof. If u is rationally conjugate to g_0, then $\varepsilon_1 = 1$ and $\varepsilon_x = 0$ for any $x \in \Gamma_n \setminus \{1\}$. Therefore (3.15) holds. Conversely, assume that (3.15) holds. For $v \in \mathrm{V}(\mathbb{Z}G)$ of order dividing n let $\lambda_i'(v) = \sum_{x \in \Gamma_n} \varepsilon_{g_0^x}(v)\alpha_{xi}$. Then $\lambda_i = \lambda_i'(u) = \sum_{j=0}^{n-1} \varepsilon_{g_0^j}(u)\zeta_n^{ij}$ and $\alpha_i = \sum_{j=0}^{n-1} \varepsilon_{g_0^j}(g_0)\zeta_n^{ij}$. As the Vandermonde matrix $(\zeta_n^{ij})_{1 \leq i,j \leq n}$ is invertible we deduce that $\varepsilon_{g_0^j}(u) = \varepsilon_{g_0^j}(g_0)$ for every $j \in \Gamma_n$. So $\varepsilon_j = \varepsilon_{g_0^j}(u) = \varepsilon_{g_0^j}(g_0) = 0$ for every $j \in \Gamma_n \setminus \{1\}$ and $\varepsilon_1 = 1$. As we are assuming that if d is a divisor of n different from 1 then u^d is rationally conjugate to an element of G, we also have $\varepsilon_g(u^d) \geq 0$ for every $g \in G$. Thus u is rationally conjugate to an element of $g \in G$ by Theorem 1.2.6. Then $\varepsilon_{g_0}(g) = \varepsilon_{g_0}(u) = 1$ and therefore g is conjugate to g_0 in G. We conclude that u and g_0 are rationally conjugate. □

By Lemma 3.3.3, in order to achieve our goal it is enough to prove (3.15). We argue by contradiction, so suppose that $\lambda_d \neq \alpha_d$ for some positive integer d which we assume to be minimal with this property. Observe that if $\lambda_i = \alpha_i$ and j is an integer such that $\gcd(i, n) = \gcd(j, n)$, then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ such that $\sigma(\alpha_i) = \alpha_j$ and applying σ to the equation $\lambda_i = \alpha_i$ we obtain $\lambda_j = \alpha_j$. This implies that d divides n. Note that $\alpha_1 = \lambda_1$ by our choice of g_0 and hence $d \neq 1$. Moreover, $d \neq n$ because $\lambda_n = 2\sum_{x\in\Gamma_n} \varepsilon_x = 2 = \alpha_n$ as the augmentation of u is 1.

We claim that

$$\lambda_d = \alpha_d + d\tau \text{ for some } \tau \in \mathbb{Z}[\alpha_1]. \tag{3.16}$$

Indeed, for any $x \in \Gamma_n$ let $B_x = \varepsilon_x - 1$ if $x \sim_n 1$ and $B_x = \varepsilon_x$ otherwise. Then for any integer i we have $\lambda_i - \alpha_i = \sum_{x\in\Gamma_n} B_x \operatorname{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha_1)}(\zeta^{ix})$. Therefore, applying Corollary 2.2.3 for $F = \mathbb{Q}(\alpha_1)$, $R = \mathbb{Z}[\alpha_1]$ and $\omega_i = \lambda_i - \alpha_i$, the claim follows.

By (3.14) we have, using Theorem 1.3.1, that

$$\chi_{2d}(g_0) = 1 + \sum_{i=1}^{d} \alpha_i \tag{3.17}$$

and that

$$\chi_{2d}(u) = \sum_{x\in\Gamma_n} \varepsilon_x \chi_{2d}(g_0^x) = \sum_{x\in\Gamma_n} \varepsilon_x \left(1 + \sum_{i=1}^{d} \alpha_{ix}\right) = 1 + \sum_{i=1}^{d} \lambda_i. \tag{3.18}$$

Combining this with (3.16) and the minimality of d, we obtain $\chi_{2d}(u) = \chi_{2d}(g_0) + d\tau$. Furthermore, $\tau \neq 0$, as $\lambda_d \neq \alpha_d$. Therefore

$$C_b(\chi_{2d}(u) - 1) \equiv C_b(\chi_{2d}(g_0) - 1) \bmod d \quad \text{for every } b \in \mathbb{B} \tag{3.19}$$

and

$$d \leq |C_{b_0}(\chi_{2d}(u) - 1) - C_{b_0}(\chi_{2d}(g_0) - 1)| \quad \text{for some } b_0 \in \mathbb{B}. \tag{3.20}$$

The bulk of our argument relies on an analysis of the eigenvalues of $\Theta_{2d}(u)$ and the induction hypothesis on n and d. More precisely, we will use (3.19) and (3.20) to obtain a contradiction by comparing the eigenvalues of $\Theta_{2d}(g_0)$ and $\Theta_{2d}(u)$. Of course we do not know the eigenvalues of the latter but we know the eigenvalues of each $\Theta_{2d}(g_0^i)$. Moreover, if c is a divisor of n with $c \neq 1$ then u^c is rationally conjugate to an element g of G. Then $\Theta_2(g)$, $\Theta_2(u^c)$ and $\Theta_2(g_0^c)$ are conjugate in $M_3(F)$, for a suitable field F, and as Θ_2 is injective on $\langle g_0 \rangle$ and g is conjugate to an element of $\langle g_0 \rangle$ we conclude that u^c is conjugate to g_0^c. Thus we know the eigenvalues of $\Theta_{2d}(u^c)$. This has consequences for the eigenvalues of $\Theta_{2d}(u)$.

To be more precise we fix $\nu_1, \dots, \nu_d \in \Gamma_n$ (with repetitions if needed) such that the eigenvalues of $\Theta_{2d}(u)$ with multiplicities are $1, \zeta^{\pm\nu_1}, \dots, \zeta^{\pm\nu_d}$. This is possible by the last statement of Proposition 2.3.1.(1) and (1.1) (see Section 2.3). By the above paragraph, if $c \mid n$ with $c \neq 1$ then the lists $(c\nu_i)_{1\leq i\leq d}$ and $(ci)_{1\leq i\leq d}$ represent the same elements in Γ_n, up to ordering, and hence $(\nu_i)_{1\leq i\leq d}$ and $(i)_{1\leq i\leq d}$ represent the same elements of $\Gamma_{\frac{n}{c}}$, up to ordering. We express this by writing

$$(\nu_i) \sim_{\frac{n}{c}} (i) \qquad \text{for every } c \mid n \text{ with } c \neq 1.$$

This provides restrictions on d, n and the ν_i.

Moreover, $C_b(\chi_{2d}(u) - 1)$ and $C_b(\chi_{2d}(g_0) - 1)$ are the coefficients of α_b in the expression in the basis $\mathcal{B}$ of $\alpha_{\nu_1} + \cdots + \alpha_{\nu_d}$ and $\alpha_1 + \cdots + \alpha_d$, respectively. By (3.17), (3.18) and Proposition 2.2.5 we obtain for every $b \in \mathbb{B}$ that

$$C_b(\chi_{2d}(g_0) - 1) = \sum_{i=1}^{d} \mu(\gamma(i)) \cdot \delta_{b,i}^{(n/\gamma(i))} \tag{3.21}$$

and that

$$C_b(\chi_{2d}(u) - 1) = \sum_{i=1}^{d} \kappa_{\nu_i} \cdot \mu(\gamma(\nu_i)) \cdot \delta_{b,\nu_i}^{(n/\gamma(\nu_i))}. \tag{3.22}$$

Therefore

$$C_b(\chi_{2d}(u) - 1) - C_b(\chi_{2d}(g_0) - 1) = \sum_{i=1}^{d} \left(\kappa_{\nu_i}\mu(\gamma(\nu_i))\delta_{b,\nu_i}^{(n/\gamma(\nu_i))} - \mu(\gamma(i))\delta_{b,i}^{(n/\gamma(i))} \right). \tag{3.23}$$

Lemma 3.3.4. *1. If $\kappa_{\nu_i} \neq 1$ for some $1 \leq i \leq d$ then $\frac{n}{d}$ is the smallest prime dividing n and $\kappa_{\nu_j} = 1$ for every $1 \leq j \leq d$ with $j \neq i$.*

2. If $d > 3$ then n is not divisible by any prime greater than d.

Proof. Let p denote the smallest prime dividing n.

(1) Suppose that $\kappa_{\nu_i} \neq 1$. Then $\nu_i \equiv 0 \bmod n$. As $(i) \sim_{\frac{n}{p}} (\nu_i)$ we deduce that $k \equiv 0 \bmod \frac{n}{p}$ for some $1 \leq k \leq d$. Therefore $d = k = \frac{n}{p}$ and for every $1 \leq j \leq d$ with $j \neq i$ we have $\nu_j \not\equiv 0 \bmod \frac{n}{p}$. Hence $\kappa_{\nu_j} = 1$.

(2) Suppose that q is a prime divisor of n with $d < q$. Then $\frac{n}{d} \neq p$ and therefore, by (1), $\kappa_{\nu_i} = 1$ for every $1 \leq i \leq d$. Thus, by (3.20) and (3.23) and ignoring the signs provided by the $\mu(\gamma(i))$ and $\mu(\gamma(\nu_i))$, it is enough to show that $\delta_{b,i}^{(n/\gamma(i))} \neq 0$ for at most two i's and $\delta_{b,\nu_i}^{(n/\gamma(\nu_i))} \neq 0$ for at most two i's, since by assumption $d > 3$, i.e. $d \geq 5$. Observe that if $1 \leq i \leq d$ then $q \nmid i$ and hence $\frac{n}{\gamma(i)}$ is multiple of q. Moreover, if $1 \leq i, j \leq d$ with $i \neq j$ then $-q < i - j < i + j < 2q$. Therefore $i \not\sim_q j$ unless $j = q - i$. As $(i) \sim_{n/p} (\nu_i)$ and $q \mid \frac{n}{p}$ we have $(i) \sim_q (\nu_i)$, the lemma follows. □

We obtain an upper bound for $|C_b(\chi_{2d}(u) - 1) - C_b(\chi_{2d}(g_0) - 1)|$ in terms of $P(d)$. Recall that $P(d)$ denotes the number of prime divisors of d.

Lemma 3.3.5. *For every $b \in \mathbb{B}$ we have*

$$|C_b(\chi_{2d}(u) - 1) - C_b(\chi_{2d}(g_0) - 1)| \leq 1 + 2^{P(d)+2}.$$

Moreover if $\kappa_{\nu_i} = 1$ for every $1 \leq i \leq d$ then

$$|C_b(\chi_{2d}(u) - 1) - C_b(\chi_{2d}(g_0) - 1)| \leq 2^{P(d)+2}.$$

Proof. Using (3.23), and ignoring the sings given by $\mu(\gamma(i))$ and $\mu(\gamma(\nu_i))$, it is enough to prove that

$$\sum_{i=1}^{d} \delta_{b,i}^{(n/\gamma(i))} \leq 2^{P(d)+1} \quad \text{and} \quad \sum_{i=1}^{d} \kappa_{\nu_i} \delta_{b,\nu_i}^{(n/\gamma(\nu_i))} \leq 1 + 2^{P(d)+1}.$$

Observe that $\kappa_{\nu_i} = 2$ for at most one i by Lemma 3.3.4.(1). Recall that $d' = \prod_{p|d} p$. Thus the lemma is a consequence of the following inequalities for every e dividing d':

$$\left|\left\{1 \leq i \leq d : \gcd(d, \gamma(i)) = e, \delta_{b,i}^{(n/\gamma(i))} = 1\right\}\right| \leq 2 \quad \text{and}$$

$$\left|\left\{1 \leq i \leq d : \gcd(d, \gamma(\nu_i)) = e, \delta_{b,\nu_i}^{(n/\gamma(\nu_i))} = 1\right\}\right| \leq 2,$$

since the number of divisors of d' is $2^{P(d)}$ and if $\kappa_{\nu_i} = 2$ for some ν_i this provides an additional 1. We prove the second inequality, only using that $(\nu_i) \sim_d (i)$. This implies the first inequality by applying the second one to $u = g_0$.

For a fixed e dividing d' let

$$Y_e = \left\{1 \le i \le d : \gcd(d, \gamma(\nu_i)) = e, \delta_{b,\nu_i}^{(n/\gamma(\nu_i))} = 1\right\}.$$

By changing the sign of some ν_i's, we may assume without loss of generality that if $\delta_{b,\nu_i}^{(n/\gamma(\nu_i))} = 1$ then $b \equiv \nu_i \mod \frac{n}{\gamma(\nu_i)}$. Thus, if $i \in Y_e$ then $b \equiv \nu_i \mod \frac{n}{\gamma(\nu_i)}$. We claim that if $i, j \in Y_e$ then $\nu_i \equiv \nu_j \mod d$. Indeed, let p be prime divisor of d. If $n_p \neq d_p$ then $d_p \le \left(\frac{n}{\gamma(\nu_i)}\right)_p$, so $\nu_i \equiv \nu_j \mod d_p$. If $p \nmid e$ then $n_p = \left(\frac{n}{\gamma(\nu_i)}\right)_p$ and so also $\nu_i \equiv \nu_j \mod d_p$. Otherwise, i.e. if $n_p = d_p$ and $p \mid e$, then p divides both $\gamma(\nu_i)$ and $\gamma(\nu_j)$ and $\nu_i \equiv \nu_j \mod \frac{d_p}{p}$. Therefore $\nu_i \equiv \nu_j \mod n_p$, by Lemma 2.2.4.(2). As $(\nu_i) \sim_d (i)$ and there are at most two i's with $1 \le i \le d$ representing the same class in Γ_d, we deduce that $|Y_e| \le 2$, as desired. □

We are ready to finish the proof of Theorem 3.3.1. Recall that we are arguing by contradiction and n, and hence also d, is odd.

By (3.20) and Lemma 3.3.5 we have $d \le 1 + 2^{P(d)+2}$ and this has strong consequences on the possible values of d. Indeed if $P(d) \ge 3$ then

$$1 + 2^{P(d)+2} \ge d \ge 3 \cdot 5 \cdot 7 \cdot 2^{P(d)-3} > (105 - 2^5) + 2^{P(d)+2} = 73 + 2^{P(d)+2},$$

a contradiction. Thus, if $P(d) = 2$ then $d = 15$ and if $P(d) = 1$ then $d \in \{3, 5, 7, 9\}$.

However, if $d = 9$ then we have that $|C_{b_0}(\chi_{18}(u) - 1) - C_{b_0}(\chi 18(g_0) - 1)| = 9$ by Lemma 3.3.5 and hence $\kappa_{\nu_i} = 2$ for one $1 \le i \le d$. This implies, by Lemma 3.3.4.(1), that $n = 27$ contradicting the assumptions that n is not a prime power. Therefore $d \in \{3, 5, 7, 15\}$. We deal with these cases separately using (3.21), (3.22) and (3.23). Observe that if p is a prime integer bigger than d then $p \mid \frac{n}{\gamma(i)}$ for every $1 \le i \le d$ and so also $p \mid \frac{n}{\gamma(\nu_i)}$, since $(i) \sim_p (\nu_i)$.

Assume that $d = 3$. Combining Lemma 3.3.4.(1) with the assumptions that n is not a prime power, we deduce that $\kappa_{\nu_i} = 1$ for every $1 \le i \le 3$. Suppose that there is a prime $p \mid n$ with $p \ge 7$. Then $p \mid \frac{n}{\gamma(i)}$ and $p \mid \frac{n}{\gamma(\nu_i)}$ for every $1 \le i \le 3$. Therefore

$$\left|\left\{1 \le i \le 3 : \delta_{b,i}^{(n/\gamma(i))} = 1\right\}\right| \le 1 \text{ for every } b \in \mathbb{B}$$

and

$$\left|\left\{1 \le i \le 3 : \delta_{b,\nu_i}^{(n/\gamma(\nu_i))} = 1\right\}\right| \le 1 \text{ for every } b \in \mathbb{B}$$

which implies $|C_{b_0}(\chi_6(u)-1) - C_{b_0}(\chi_6(g_0)-1)| \le 2$, contradicting (3.20). So $n' = 15$.

Moreover, $n_3 = 3$ because otherwise $3 \mid \frac{n}{\gamma(i)}$ and $3 \mid \frac{n}{\gamma(\nu_i)}$ and so $15 \mid \frac{n}{\gamma(i)}$ and $15 \mid \frac{n}{\gamma(\nu_i)}$ for every $1 \le i \le 3$. Hence $|C_{b_0}(\chi_6(u)-1)|$ and $|C_{b_0}(\chi_6(u)-1)|$ are both at most 1, in contradiction with (3.20). If $5^3 \mid n$, then $25 \mid \frac{n}{\gamma(\nu_i)}$ and $25 \mid \frac{n}{\gamma(i)}$ for every $1 \le i \le 3$, which implies $|C_{b_0}(\chi_6(g_0)-1)| \le 1$ and $|C_{b_0}(\chi_6(u)-1)| \le 1$, again a contradiction. Therefore $n \in \{15, 75\}$. Since $(i) \sim_3 (\nu_i)$, we may assume that $3 \mid \nu_3$ and $3 \nmid \nu_i$ for $i = 1, 2$.

Suppose that $n = 15$. Then, as $(i) \sim_5 (\nu_i)$, we have $\gamma(1) = \gamma(2) = \gamma(\nu_1) = \gamma(\nu_2) = 1$ and $\gamma(3) = \gamma(\nu_3) = 3$. So $C_b(\chi_6(g_0)-1) = \delta_{b,1}^{15} + \delta_{b,2}^{15} - \delta_{b,3}^{5}$ and $C_b(\chi_6(u)-1) = \delta_{b,\nu_1}^{15} + \delta_{b,\nu_2}^{15} - \delta_{b,\nu_3}^{5}$ for every $b \in \mathbb{B}$, implying

$$C_b(\chi_6(u)-1) - C_b(\chi_6(g_0)-1) = \delta_{b,\nu_1}^{15} + \delta_{b,\nu_2}^{15} - \delta_{b,\nu_3}^{5} - \delta_{b,1}^{15} - \delta_{b,2}^{15} + \delta_{b,3}^{5}.$$

Since $1 \nsim_{15} 2$, we must have $C_{b_0}(\chi_6(u)-1) - C_{b_0}(\chi_6(g_0)-1) = 3$ and $\nu_3 \sim_5 1$ while $\nu_1 \sim_5 \nu_2 \sim_5 2$. Then $C_1(\chi_6(u)-1) - C_1(\chi_6(g_0)-1) = -2$, contradicting (3.19).

Suppose that $n = 75$. Then $\gamma(1) = \gamma(2) = 5$, $\gamma(3) = 3$ and

$$C_b(\chi_6(g_0)-1) = -\delta_{b,1}^{15} - \delta_{b,2}^{15} - \delta_{b,3}^{25} \text{ for every } b \in \mathbb{B}.$$

Suppose $\nu_3 \sim_{25} 3$. Then

$$C_b(\chi_6(u)-1) = -\delta_{b,\nu_1}^{15} - \delta_{b,\nu_2}^{15} - \delta_{b,\nu_3}^{25} \text{ for every } b \in \mathbb{B}.$$

As $\delta_{b,\nu_3}^{25} = \delta_{b,3}^{25}$, we have $|C_{b_0}(\chi_6(u)-1) - C_{b_0}(\chi_6(g_0)-1)| \le 2$, contradicting (3.20). Thus $\nu_3 \not\sim_{25} 3$ and we may assume $\nu_1 \sim_{25} 3$. If $\nu_3 \sim_{25} 2$ then

$$C_b(\chi_6(u)-1) = \delta_{b,\nu_1}^{75} - \delta_{b,\nu_2}^{15} + \delta_{b,\nu_3}^{5} \text{ for every } b \in \mathbb{B}.$$

However $C_{13}(\chi_6(u)-1) - C_{13}(\chi_6(g_0)-1) = 2$, contradicting (3.19). So $\nu_3 \sim_{25} 1$ and arguing as above we obtain $C_{14}(\chi_6(u)-1) - C_{14}(\chi_6(g_0)-1) \in \{1, 2\}$, again a contradiction with (3.19).

<u>Assume that $d = 5$</u>. By Lemma 3.3.4.(2) and the assumptions on n, we obtain $n' = 15$. As $(i) \sim_5 (v_i)$, we may assume that $5 \mid \nu_5$ and $5 \nmid \nu_i$ for every $1 \leq i \leq 4$. Suppose that $n = 15$. In this case

$$C_b(\chi_{10}(g_0) - 1) = \delta^{15}_{b,1} + \delta^{15}_{b,2} - \delta^{5}_{b,3} + \delta^{15}_{b,4} - \delta^{3}_{b,5} \text{ for every } b \in \mathbb{B}.$$

If $3 \mid \nu_5$ and $3 \nmid \nu_i$ for every $1 \leq i \leq 4$, then

$$C_b(\chi_{10}(u) - 1) = \delta^{15}_{b,\nu_1} + \delta^{15}_{b,\nu_2} + \delta^{15}_{b,\nu_3} + \delta^{15}_{b,\nu_4} + 2 \text{ for every } b \in \mathbb{B}$$

and hence

$$C_1(\chi_{10}(u) - 1) - C_1(\chi_{10}(g_0) - 1) = 2 + \delta^{15}_{1,\nu_1} + \delta^{15}_{1,\nu_2} + \delta^{15}_{1,\nu_3} + \delta^{15}_{1,\nu_4} \leq 4,$$

contradicting (3.19). Therefore, as $(i) \sim_3 (\nu_i)$, we may assume that $3 \mid \nu_1$ and $3 \nmid \nu_i$ for every $2 \leq i \leq 5$. This implies

$$C_b(\chi_{10}(u) - 1) = -\delta^{5}_{b,\nu_1} + \delta^{15}_{b,\nu_2} + \delta^{15}_{b,\nu_3} + \delta^{15}_{b,\nu_4} - \delta^{3}_{b,\nu_5} \text{ for every } b \in \mathbb{B}.$$

As both $|C_{b_0}(\chi_{10}(u) - 1)|$ and $|C_{b_0}(\chi_{10}(g_0) - 1)|$ are at most 2, we obtain a contradiction with (3.20). Therefore $n \neq 15$ and $\kappa_{\nu_i} = 1$ for every $1 \leq i \leq 5$ by Lemma 3.3.4.(1).

If $25 \mid n$ or $27 \mid n$ then it is easy to see that $|C_{b_0}(\chi_{10}(u) - 1)| \leq 2$ and $|C_{b_0}(\chi_{10}(g_0) - 1)| \leq 2$, contradicting (3.20). Thus $n = 45$. In this case we have

$$C_b(\chi_{10}(g_0) - 1) = -\delta^{15}_{b,1} + \delta^{45}_{b,2} + \delta^{45}_{b,3} + \delta^{45}_{b,4} - \delta^{9}_{b,5} \text{ for every } b \in \mathbb{B}.$$

If $\nu_5 \sim_9 1$ then

$$C_b(\chi_{10}(u) - 1) = \delta^{45}_{b,\nu_1} + \delta^{45}_{b,\nu_2} + \delta^{45}_{b,\nu_3} + \delta^{45}_{b,\nu_4} + \delta^{3}_{b,\nu_5} \text{ for every } b \in \mathbb{B}.$$

As $(i) \sim_{15} (\nu_i)$, we obtain $|C_{b_0}(\chi_{10}(u) - 1)| \leq 2$ and $|C_{b_0}(\chi_{10}(g_0) - 1)| \leq 2$ contradicting (3.20). If $\nu_5 \not\sim_9 1$ then we may assume that $\nu_1 \sim_9 1$. Hence

$$C_b(\chi_{10}(u) - 1) = -\delta^{15}_{b,\nu_1} + \delta^{45}_{b,\nu_2} + \delta^{45}_{b,\nu_3} + \delta^{45}_{b,\nu_4} - \delta^{9}_{b,\nu_5} \text{ for every } b \in \mathbb{B}.$$

Again as $(i) \sim_{15} (\nu_i)$, we have both $|C_{b_0}(\chi_{10}(u)-1)|$ and $|C_{b_0}(\chi_{10}(g_0)-1)|$ at most 2, which yields a contradiction.

Assume that $d = 7$. As $(i) \sim_7 (\nu_i)$, we may assume that $7 \mid \nu_7$ and $7 \nmid \nu_i$ for every $1 \leq i \leq 6$. Thus $7 \mid \frac{n}{\gamma(i)}$ and $7 \mid \frac{n}{\gamma(\nu_i)}$ for every $1 \leq i \leq 6$. Hence $|C_{b_0}(\chi_{14}(g_0)-1)| \leq 3$. Moreover, if $\kappa_{\nu_7} \neq 2$ then we also have $|C_{b_0}(\chi_{14}(u)-1)| \leq 3$ yielding a contradiction with (3.20). Therefore $\kappa_{\nu_7} = 2$ (i.e. $n \mid \nu_7$) and by Lemma 3.3.4 and the assumptions on n we deduce that either $n = 21$ or $n = 35$.

Suppose that $n = 21$. As $(i) \sim_3 (\nu_i)$ we may assume that $3 \mid \nu_3$ and $3 \nmid \nu_i$ for every $i \in \{1,2,4,5,6\}$. This implies for every $b \in \mathbb{B}$ that

$$C_b(\chi_{14}(u)-1) = \delta^{21}_{b,\nu_1} + \delta^{21}_{b,\nu_2} - \delta^{7}_{b,\nu_3} + \delta^{21}_{b,\nu_4} + \delta^{21}_{b,\nu_5} + \delta^{21}_{b,\nu_6} + 2$$

and

$$C_b(\chi_{14}(g_0)-1) = \delta^{21}_{b,1} + \delta^{21}_{b,2} - \delta^{7}_{b,3} + \delta^{21}_{b,4} + \delta^{21}_{b,5} - \delta^{7}_{b,6} - \delta^{3}_{b,7}.$$

Hence, as $(i) \sim_7 (\nu_i)$, we obtain $|C_{b_0}(\chi_{14}(g_0)-1)| \leq 2$ and $|C_{b_0}(\chi_{14}(u)-1)| \leq 4$, contradicting (3.20).

Suppose that $n = 35$. As $(i) \sim_5 (\nu_i)$ and $(i) \sim_7 (\nu_i)$, we have for every $b \in \mathbb{B}$ that

$$C_b(\chi_{14}(u)-1) = \delta^{35}_{b,\nu_1} + \delta^{35}_{b,\nu_2} + \delta^{35}_{b,\nu_3} + \delta^{35}_{b,\nu_4} + \delta^{35}_{b,\nu_5} + \delta^{35}_{b,\nu_6} + 2$$

and

$$C_b(\chi_{14}(g_0)-1) = \delta^{35}_{b,1} + \delta^{35}_{b,2} + \delta^{35}_{b,3} + \delta^{35}_{b,4} - \delta^{7}_{b,5} + \delta^{35}_{b,6} - \delta^{5}_{b,7}.$$

Hence, again $|C_{b_0}(\chi_{14}(g_0)-1)| \leq 2$ and $|C_{b_0}(\chi_{14}(u)-1)| \leq 4$, yielding a contradiction with (3.20).

Finally assume that $d = 15$. Suppose that $n = 45$. In this case we have for every $b \in \mathbb{B}$ that

$$\begin{aligned} C_b(\chi_{30}(g_0)-1) \quad = \quad & -\delta^{15}_{b,1} + \delta^{45}_{b,2} + \delta^{45}_{b,3} + \delta^{45}_{b,4} - \delta^{9}_{b,5} + \delta^{45}_{b,6} + \delta^{45}_{b,7} - \delta^{15}_{b,8} \\ & -\delta^{15}_{b,9} + \delta^{3}_{b,10} + \delta^{45}_{b,11} + \delta^{45}_{b,12} + \delta^{45}_{b,13} + \delta^{45}_{b,14} - \delta^{9}_{b,15}, \end{aligned}$$

which implies that $|C_{b_0}(\chi_{30}(g_0)-1)| \leq 4$. Since $(i) \sim_5 (\nu_i)$, we deduce that $|C_{b_0}(\chi_{30}(u)-1)| \leq 10$, since at most ten of the $\mu(\gamma(\nu_i))$ are equal. This yields a contradiction with (3.20). Therefore $n \neq 45$ and $\kappa_{\nu_i} = 1$ for every $1 \leq i \leq 15$ by

Lemma 3.3.4.(1). If there is a prime $p \mid n$ with $p \geq 7$ then it is easy to see that $|C_{b_0}(\chi_{30}(g_0) - 1)| \leq 7$ and $|C_{b_0}(\chi_{30}(u) - 1)| \leq 7$, in contradiction with (3.20). Thus $n' = 15$. If $25 \mid n$ or $27 \mid n$ then $|C_{b_0}(\chi_{30}(g_0) - 1)| \leq 6$ and $|C_{b_0}(\chi_{30}(u) - 1)| \leq 6$, again a contradiction. As 15 is a proper divisor of n, this implies $n = 45$ yielding the final contradiction.

This finishes the proof of Theorem 3.3.1.

CHAPTER 4

On the Zassenhaus Conjecture for SL(2,q)

In this chapter we study (ZC1) for the special linear groups $\mathrm{SL}(2,q)$ with q a prime power. The results appeared in [dRS18].

Along this chapter

$$p \text{ is a prime integer}, \quad q = p^f \text{ for a positive integer f}, \quad G = \mathrm{SL}(2,q)$$

$$\overline{G} = \mathrm{PSL}(2,q) \quad \text{and} \quad \bar{\pi} : G \to \overline{G}.$$

The goal of this chapter is to prove Theorem 4.2.2, namely we prove that every torsion unit in $\mathrm{V}(\mathbb{Z}G)$ of order coprime with p is rationally conjugate to an element of G. As a consequence of this result we prove (ZC1) for the groups $\mathrm{SL}(2,p)$ and $\mathrm{SL}(2,p^2)$ with p a prime number (see Theorem 4.2.1). This is the first positive result on (ZC1) for an infinite series of non-solvable groups. Theorem 4.2.1 will follow as a consequence of Theorem 4.2.2 and known results on torsion units of $\mathrm{V}(\mathbb{Z}G)$ collected in Section 2.3.

The proof of Theorem 4.2.2 follows the structure of the proof of Theorem 3.3.1 with different calculations based on two facts. On the one hand, the order of the unit might be even which introduces some difficulties not encountered in the proof of Theorem 3.3.1. Observe that a similar result for $\overline{G}$ and units of even order is not possible using this method by Theorem 3.2.1. On the other hand, this result is valid for G and not for $\overline{G}$ because of the fact that the characters Ψ_m of G (see Lemma 2.3.3) with m even do not lift to characters on $\overline{G}$.

In Section 4.1 we deal with units of order a prime power. For that we simply apply the standard HeLP Method. Finally in Section 4.2 we complete the proof of Theorem 4.2.2.

Throughout this chapter we use Notation 2.3.4 without further mention.

4.1 Units of prime power order

In this section we prove a particular case of Theorem 4.2.2.

We first prove some consequences of Proposition 2.3.1. Recall that J denotes the unique element of order 2 in G. Let u be an element of order n in $\mathrm{V}(\mathbb{Z}G)$ with $\gcd(n,q)=1$.

Proposition 4.1.1. *1. If $4 \nmid n$ and $\overline{\pi}(u)$ is rationally conjugate to an element of $\overline{G}$ then u is rationally conjugate to an element of G.*

2. If $\gcd(n,q)=1$ and either $n=4$ or $4 \nmid n$ then u is rationally conjugate to an element of G.

3. If $f \leq 2$ and $p \mid n$ then u is rationally conjugate to an element of G.

Proof. (1) Suppose that n is not multiple of 4. If n is even then the order of Ju is odd, by Proposition 2.3.2.(1). Thus, we may assume without loss of generality that the order of u is odd. If $\varepsilon_g(u) \neq 0$ then $|g|$ is odd, by Proposition 2.3.2.(3), and hence $\varepsilon_g(u) = \varepsilon_{\overline{\pi}(g)}(\overline{\pi}(u)) \geq 0$, by Proposition 2.3.1.(4). Thus u is rationally conjugate to an element of G.

(2) Suppose that $p \nmid n$. By Proposition 2.3.1.(3), G has a unique conjugacy class C formed by elements of order 4 and a unique element of order 2. Thus, by Theorem 1.2.4.(1) and Proposition 2.3.2.(3), if $n=4$ then $\varepsilon_g(u)=0$ for every $g \notin C$, and hence u is rationally conjugate to an element of G, by Theorem 1.2.6.

If $4 \nmid n$ then $|\pi(u)|$ is coprime with $2q$, by Proposition 2.3.2.(2), and hence $\pi(u)$ is rationally conjugate to an element of $\overline{G}$, by Theorem 3.3.1. Then u is rationally conjugate to an element of G by (1).

(3) In this case $|\overline{\pi}(u)| = p$ by Proposition 2.3.2.(2) and [BM17a, Theorem A]. Then n is either p or $2p$, by Proposition 2.3.2.(2), and $\overline{\pi}(u)$ is rationally conjugate to an element of $\overline{G}$, by Proposition 2.3.1.(2). Thus u is rationally conjugate to an element of G, by (1). □

We introduce some p-Brauer characters of G. Let g be an element of G of order n with $p \nmid n$ and let ξ_n denote a primitive n-th root of unity in a field F of characteristic p. By Lemma 2.3.3, we deduce that for every positive integer m there is an F-representation θ_m of G of degree $1+m$ such that

$$\theta_m(g) = \begin{cases} \operatorname{diag}\left(1, \xi_n^2, \xi_n^{-2}, \dots, \xi_n^m, \xi_n^{-m}\right), & \text{if } 2 \mid m; \\ \operatorname{diag}\left(\xi_n, \xi_n^{-1}, \xi_n^3, \xi_n^{-3}, \dots, \xi_n^m, \xi_n^{-m}\right), & \text{if } 2 \nmid m. \end{cases} \tag{4.1}$$

In particular, the restriction to $\langle g \rangle$ of the p-Brauer character associated to θ_m is given by

$$\Psi_m(g^i) = \sum_{\substack{j=-m \\ j \equiv m \bmod 2}}^{m} \zeta_n^{ij}.$$

Proposition 4.1.2. *Let $G = \mathrm{SL}(2,q)$ with q an odd prime power and let u be a torsion element of $\mathrm{V}(\mathbb{Z}G)$. If the order of u is a prime power and it is coprime with q then u is rationally conjugate to an element of G.*

Proof. By Proposition 4.1.1.(2) we may assume that $|u| = 2^r$ with $r \geq 3$. We argue by induction on r. So we assume that units of order 2^k with $1 \leq k \leq r-1$ are rationally conjugate to an element of G. By Proposition 2.3.2.(3) and Proposition 2.3.1.(3), G has an element g_0 of order 2^r such that $\{g_0^k : k = 0, 1, 2, \dots, 2^{r-1}\}$ is a set of representatives of the conjugacy classes of G with order a divisor of 2^r. By Theorem 1.2.4.(3), the only possible non-zero partial augmentations of u are the integers $\varepsilon_k = \varepsilon_{g_0^k}(u)$, with $k = 1, \dots, 2^{r-1}-1$. By the induction hypothesis, if $2 \leq i \leq r$ then $\varepsilon_g(u^{2^i}) \geq 0$ for every $g \in G$ and, by Theorem 1.2.6, it suffices to prove that $\varepsilon_k = 0$ for all but one $k = 0, 1, \dots, 2^{r-1}$.

By Proposition 2.3.1.(2) and Proposition 2.3.2.(2), $\bar{\pi}(u)$ is rationally conjugate to an element of order 2^{r-1} in $\overline{G}$ and hence $\varepsilon_{2^{r-2}} = \varepsilon_{\bar{\pi}(g_0)^{2^{r-2}}}(\bar{\pi}(u)) = 0$, by Proposition 2.3.1.(4).

For a p-Brauer character Ψ of G and an integer ℓ define

$$A(\Psi, \ell) = \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \cdot \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\Psi(g_0^k) \cdot \zeta_{2^r}^{-\ell}\right)$$

and

$$B(\Psi,\ell)=\sum_{k=0}^{r-1}\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\Psi(g_0^{2^{r-k}})\cdot\zeta_{2^k}^{-\ell}\right).$$

Then, by (1.1), we have

$$\frac{1}{2^r}\left(A(\Psi,\ell)+B(\Psi,\ell)\right)\in\mathbb{Z}_{\geq 0}. \tag{4.2}$$

Observe that $B(\Psi,\ell+2^{r-1})=B(\Psi,\ell)$ and $A(\Psi,\ell+2^{r-1})=-A(\Psi,\ell)$. Therefore, from (4.2) it follows that

$$\text{if } B(\Psi,\ell)=0 \text{ then } A(\Psi,\ell)=0; \tag{4.3}$$

and that

$$\text{if } B(\Psi,\ell)=2^{r-1} \text{ then } A(\Psi,\ell)=\pm 2^{r-1}. \tag{4.4}$$

We will calculate $B(\Psi,\ell)$ and $A(\Psi,\ell)$ for several p-Brauer characters Ψ and several integers ℓ and for that we will use Lemma 2.2.6 without further mention. We start proving that

$$\text{if } 0\leq h\leq r-2 \text{ and } 2^{r-1}\mid\ell \text{ then } B(\Psi_{2^h},\ell)=\begin{cases}2^{r-1}, & \text{if } h\geq 1;\\ 0, & \text{if } h=0;\end{cases} \tag{4.5}$$

and that if $0\leq h\leq r-3$, $2^h\mid\ell$ and $2^{r-1}\nmid\ell$ then

$$B(\Psi_{2^h},\ell)=\begin{cases}2^{r-1}, & \text{if } \ell\equiv\pm 2^h \bmod 2^{r-1};\\ 0, & \text{otherwise.}\end{cases} \tag{4.6}$$

In both cases we argue by induction on h with the cases $h=0$ and $h=1$ being straightforward. Suppose that $1<h\leq r-2$, $2^{r-1}\mid\ell$ and $B(\Psi_{2^{h-1}},\ell)=2^{r-1}$. If j is even, then it easy to see that

$$\sum_{k=0}^{r-1}\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}}\left(\zeta_{2^k}^{2^{h-1}+j}+\zeta_{2^k}^{-2^{h-1}-j}\right)=0.$$

This implies that

$$B(\Psi_{2^h},\ell) = B(\Psi_{2^{h-1}},\ell) + \sum_{\substack{j=2 \\ 2|j}}^{2^{h-1}} \sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left(\zeta_{2^k}^{2^{h-1}+j} + \zeta_{2^k}^{-2^{h-1}-j}\right) = 2^{r-1}.$$

This finishes the proof of (4.5).

Suppose that $1 < h \le r-3$, $2^h \mid \ell$ and $2^{r-1} \nmid \ell$. In this case the induction hypothesis implies $B(\Psi_{2^{h-1}},\ell) = 0$. Arguing as in the previous paragraph we get $B(\Psi_{2^h},\ell) = \sum_{j=2,2|j}^{2^{h-1}} \sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left(\left(\zeta_{2^k}^{2^{h-1}+j} + \zeta_{2^k}^{-(2^{h-1}+j)}\right)\zeta_{2^k}^{-\ell}\right)$. However, if j is even and smaller than 2^{h-1} then

$$\sum_{k=0}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left(\left(\zeta_{2^k}^{2^{h-1}+j} + \zeta_{2^k}^{-(2^{h-1}+j)}\right)\zeta_{2^k}^{-\ell}\right) = 0.$$

Therefore, having in mind that $\zeta_{2^{h+2}}^{2^h} + \zeta_{2^{h+2}}^{-2^h} = 0$ we have

$$\begin{aligned} B(\Psi_{2^h},\ell) &= \sum_{k=0}^{h} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left(\left(\zeta_{2^k}^{2^h} + \zeta_{2^k}^{-2^h}\right)\zeta_{2^k}^{-\ell}\right) + \epsilon 2^{h+1} \\ &\quad + \sum_{k=h+3}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left(\left(\zeta_{2^k}^{2^h} + \zeta_{2^k}^{-2^h}\right)\zeta_{2^k}^{-\ell}\right), \end{aligned}$$

where $\epsilon = 1$ if $2^{h+1} \nmid \ell$ and $\epsilon = -1$ otherwise. Then the claim follows using the following equalities that can be proved by straightforward calculations:

$$\sum_{k=0}^{h} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left(\left(\zeta_{2^k}^{2^h} + \zeta_{2^k}^{-2^h}\right)\zeta_{2^k}^{-\ell}\right) = 2^{h+1}$$

and

$$\sum_{k=h+3}^{r-1} \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}} \left(\zeta_{2^k}^{2^h-\ell} + \zeta_{2^k}^{-2^h-\ell}\right) = \begin{cases} 0, & \text{if } 2^{h+1} \mid \ell; \\ 2^{r-1} - 2^{h+2}, & \text{if } 2^{h+1} \nmid \ell, \ell \equiv \pm 2^h \bmod 2^{r-1}; \\ -2^{h+2}, & \text{if } 2^{h+1} \nmid \ell, \ell \not\equiv \pm 2^h \bmod 2^{r-1}. \end{cases}$$

This finishes the proof of (4.6).

We now prove, by induction on h, that the following two statements hold for any integer $0 \le h \le r-3$ and $X_h = \{i \in \{1, \dots, 2^{r-2}\} : i \equiv \pm 1 \bmod 2^{r-h}\}$:

$$\sum_{k \in X_h} (\varepsilon_k - \varepsilon_{k+2^{r-h-1}}) = \pm 1; \tag{4.7}$$

$$\text{if } i \equiv \pm j \bmod 2^{r-h-1} \text{ and } i \not\equiv 0, \pm 1 \bmod 2^{r-h-1} \text{ then } \varepsilon_i = \varepsilon_j; \tag{4.8}$$

and that the next one holds for every $0 \le h \le r-2$:

$$\text{if } i \equiv 0 \bmod 2^{r-h-1} \text{ then } \varepsilon_i = 0. \tag{4.9}$$

Observe that $X_0 = \{1\}$. Fix an integer i. Then for every integer k we have

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} \left(\left(\zeta_{2^r}^k + \zeta_{2^r}^{-k} \right) \zeta_{2^r}^{-i} \right) = \begin{cases} 2^{r-1}, & \text{if } k \equiv i \bmod 2^r; \\ -2^{r-1}, & \text{if } k \equiv 2^{r-1} - i \bmod 2^r; \\ 0, & \text{otherwise.} \end{cases}$$

Thus $A(\Psi_1, i) = 2^{r-1} (\varepsilon_i - \varepsilon_{i+2^{r-1}})$ and hence for $h = 0$, (4.7) and (4.8) follows at once from (4.3), (4.4) and (4.6). Moreover, for $h = 0$, (4.9) is clear because $\varepsilon_{2^{r-1}} = 0$.

Suppose $0 < h \le r-3$ and (4.7), (4.8) and (4.9) hold for h replaced by $h-1$. Suppose also that $i \not\equiv 0 \bmod 2^{r-h-1}$. To prove (4.7) and (4.8) we first compute $A(\Psi_{2^h}, 2^h i)$ which we split in three summands:

$$\begin{aligned} A(\Psi_{2^h}, 2^h i) \quad = \quad & \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \, \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} (\zeta_{2^r}^{-2^h i}) \\ & + \sum_{\substack{j=2 \\ 2|j}}^{2^h-2} \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \, \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} \left(\left(\zeta_{2^r}^{kj} + \zeta_{2^r}^{-kj} \right) \zeta_{2^r}^{-2^h i} \right) \\ & + \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \, \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} \left(\zeta_{2^r}^{2^h (k-i)} + \zeta_{2^r}^{-2^h (k+i)} \right). \end{aligned}$$

We now prove that the first two summands are 0. This is clear for the first one because $2^{r-1} \nmid 2^h i$. To prove that the second summand is 0, let $2 \le j \le 2^h - 2$

and $2 \mid j$. Observe that $2^h \nmid j$. Thus, if k is odd then the order of $\zeta_{2^r}^{\pm kj-2^h i}$ is multiple of 2^{r-h-1} and, as $h \leq r-3$, we deduce that $\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{kj-2^h i}\right) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{-kj-2^h i}\right) = 0$. Thus we only have to consider the summands with k even. Actually we can exclude also the summands with $2^{r-h} \mid k$ because, by the induction hypothesis on (4.9), for such k we have $\varepsilon_k = 0$. For the remaining values of k (i.e. k even and not multiple of 2^{r-h}) we have $\varepsilon_k = \varepsilon_l$ if $k \equiv l \bmod 2^{r-h-1}$, by the induction hypothesis on (4.8). So, we can rewrite

$$\sum_{k=1}^{2^{r-1}-1} \varepsilon_k \,\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\left(\zeta_{2^r}^{kj} + \zeta_{2^r}^{-kj}\right)\zeta_{2^r}^{-2^h i}\right)$$

as

$$\sum_{l \in \mathbb{Z}/2^{r-h-1}\mathbb{Z}} \varepsilon_l \,\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{l-2^h i}\left(\sum_{a=0}^{2^h-1}(\zeta_{2^r}^{2^{r-h-1}j})^a\right) + \zeta_{2^r}^{-l-2^h i}\left(\sum_{a=0}^{2^h-1}(\zeta_{2^r}^{-2^{r-h-1}j})^a\right)\right),$$

which is 0 because $\zeta_{2^r}^{2^{r-h-1}j}$ is a root of unity different from 1 and of order dividing 2^h, as j is even but not multiple of 2^h. This finishes the proof that the first two summands are 0. To finish the calculation of $A(\Psi_{2^h}, 2^h i)$ we compute

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}\left(\zeta_{2^r}^{2^h(k-i)} + \zeta_{2^r}^{-2^h(k+i)}\right) = \begin{cases} 2^{r-1}, & \text{if } k \in X_{h,i}; \\ -2^{r-1}, & \text{if } k - 2^{r-1} \in X_{h,i}; \\ 0, & \text{otherwise,} \end{cases}$$

where $X_{h,i} = \{k \in \{1, \dots, 2^{r-2}\} : k \equiv \pm i \bmod 2^{r-h}\}$. So we have proved the following:

$$A(\Psi_{2^h}, 2^h i) = 2^{r-1} \sum_{k \in X_{h,i}} (\varepsilon_k - \varepsilon_{k+2^{r-h-1}}).$$

Then (4.7) follows from (4.4), (4.6) and the previous formula. Using (4.3) we also obtain that $\sum_{k \in X_{h,i}} \varepsilon_k = \sum_{k \in X_{h,i}} \varepsilon_{k+2^{r-h-1}}$ if $i \not\equiv \pm 1 \bmod 2^{r-h-1}$. However, in this case the induction hypothesis for (4.8) means that the ε_k with $k \in X_{h,i}$ are all equal and the $\varepsilon_{k+2^{r-h-1}}$ with $k \in X_{h,i}$ are all equal. Hence (4.8) follows.

In order to deal with (4.9), assume that $0 < h \leq r-2$. By induction hypothesis on (4.9) we have $\varepsilon_k = 0$ if $2^{r-h} \mid k$, and by the induction hypothesis on (4.8), we have that ε_k is constant on the set X formed by integers $1 \le k \le 2^{r-1}$ such that $k \equiv 2^{r-h-1} \mod 2^{r-h}$. We will use these two facts without specific mention. Arguing as before we have

$$\begin{aligned} A(\Psi_{2^h}, 0) &= \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \operatorname{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} \left(1 + \zeta_{2^r}^{2^h k} + \zeta_{2^r}^{-2^h k}\right) \\ &\quad + \sum_{k=1}^{2^{r-1}-1} \varepsilon_k \operatorname{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} \left(\sum_{j=1}^{2^{h-1}-1} \zeta_{2^r}^{2jk} + \zeta_{2^r}^{-2jk} \right); \end{aligned}$$

and hence

$$A(\Psi_{2^h}, 0) = \sum_{k=1, 2^{r-h} \nmid k}^{2^{r-1}-1} \varepsilon_k \operatorname{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} \left(1 + \zeta_{2^r}^{2^h k} + \zeta_{2^r}^{-2^h k}\right).$$

As

$$\operatorname{Tr}_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}} \left(1 + \zeta_{2^r}^{2^h k} + \zeta_{2^r}^{-2^h k}\right) = \begin{cases} 2^{r-1}, & \text{if } 2^{r-h-1} \nmid k; \\ -2^{r-1}, & \text{if } 2^{r-h-1} \mid k \text{ and } 2^{r-h} \nmid k; \end{cases}$$

we obtain

$$\begin{aligned} A(\Psi_{2^h}, 0) &= 2^{r-1} \left(\sum_{2^{r-h-1} \nmid k} \varepsilon_k - \sum_{2^{r-h-1} \mid k} \varepsilon_k \right) \\ &= 2^{r-1} \left(1 - 2 \sum_{k \in X} \varepsilon_k \right) = 2^{r-1} \left(1 - 2|X| \varepsilon_k\right). \end{aligned}$$

From (4.4) and (4.5) we deduce that if $k \in X$ then $1 - 2|X|\varepsilon_k = \pm 1$ and hence $\varepsilon_k = 0$, since $|X| = 2^{r-h-1} \ge 2$, as $h \le r-2$. This finishes the proof of (4.9).

To finish the proof of the proposition it is enough to show that $\varepsilon_i \neq 0$ for exactly one $i \in \{1, \ldots, 2^{r-1}-1\}$. If i is even then $\varepsilon_i = 0$, by (4.9) with $h = r-2$.

We claim that if $\varepsilon_i \neq 0$ then $i \equiv \pm 1 \mod 2^{r-1}$. Otherwise, there are integers $2 \le v \le r-2$ and $2 < i < 2^{r-1}-1$ satisfying $i \not\equiv \pm 1 \mod 2^{v+1}$ and $\varepsilon_i \neq 0$. We choose v minimum with this property for some i. Then (1) $\varepsilon_k = 0$ for every

$k \not\equiv \pm 1 \bmod 2^v$ and (2) $i \equiv \pm(k+2^v) \bmod 2^{v+1}$ for every $k \in X_{r-v-1}$. (1) implies that $\sum_{k\in X_{r-v-1}}(\varepsilon_k+\varepsilon_{k+2^v}) = 1$. On the other hand $1 \le r-v-1 \le r-3$ and hence applying (4.7) and (4.8) with $h = r-v-1$ we deduce from (2) that $\varepsilon_i = \varepsilon_{k+2^v}$ for every $k \in X_{r-v-1}$ and $\sum_{k\in X_{r-v-1}}(\varepsilon_k - \varepsilon_{k+2^v}) = \pm 1$. Using $|X_{r-v-1}| = 2^{r-v-1}$ and $\varepsilon_i \ne 0$ we deduce that $2^{r-v}\varepsilon_i = 2\sum_{k\in X_{r-v-1}} \varepsilon_{k+2^{r-v}} = 2$, in contradiction with $2 \le r-v$. This finishes the proof of the claim.

Then the only possible non-zero partial augmentations of u are ε_1 and $\varepsilon_{2^{r-1}-1}$. Hence $\varepsilon_1 + \varepsilon_{2^{r-1}-1} = 1$ and, by applying (4.7) with $h = 0$ we deduce that $\varepsilon_1 - \varepsilon_{2^{r-1}-1} = \pm 1$. Therefore, either $\varepsilon_1 = 0$ or $\varepsilon_{2^{r-1}-1} = 0$, i.e. $\varepsilon_i \ne 0$ for exactly one $i \in \{1,\dots,2^{r-1}-1\}$, as desired. □

4.2 (ZC1) holds for units of order coprime to q in SL(2,q)

In this section we prove the following theorems.

Theorem 4.2.1. *(ZC1) holds for* $\mathrm{SL}(2,p^f)$ *with* p *a prime number and* $f \le 2$.

Theorem 4.2.2. *Let* $G = \mathrm{SL}(2,q)$ *with* q *an odd prime power and let* u *be a torsion element of* $\mathrm{V}(\mathbb{Z}G)$ *of order coprime with* q*. Then* u *is rationally conjugate to an element of* G*.*

Observe that for q odd, Theorem 4.2.1 follows at once from Theorem 4.2.2 and Proposition 4.1.1.(3). On the other hand $\mathrm{SL}(2,2) \cong S_3$ and $\mathrm{SL}(2,4) \cong A_5$ for which (ZC1) holds. So in the remainder of the section we concentrate on proving Theorem 4.2.2.

Let u be an element of order n in $\mathrm{V}(\mathbb{Z}G)$ with $\gcd(n,q) = 1$. We have to show that u is rationally conjugate to an element of G. By Proposition 4.1.1.(2), we may assume that n is multiple of 4 and by Proposition 4.1.2 that n is not a prime power. Moreover, we may also assume that $n \ne 12$ because this case follows easily from known results and the HeLP Method. Indeed, if $n = 12$ then $\bar{\pi}(u)$ has order 6, by Proposition 2.3.2.(2) and hence $\bar{\pi}(u)$ is rationally conjugate to an element of $\overline{G}$, by Proposition 2.3.1.(2). Using this and the fact that G has a unique conjugacy class for each of the orders 3, 4 or 6 and two conjugacy classes of elements of order 12, and applying (1.1) with $\chi = \Psi_1$ and $\ell = 1, 5$ it easily follows that all the partial augmentations of u are non-negative.

In the remainder we follow the strategy of the proof of Theorem 3.3.1. The difference with the arguments of this result is twofold: On the one hand, now n is even (actually multiple of 4) and this introduces some difficulties not appearing in the proof of Theorem 3.3.1 where n was odd. On the other hand, for G we have more Brauer characters than for $\overline{G}$ and this will help to reduce some cases.

As we did in Section 3.3, we have simplified the notation of Section 2.2 by setting

$$\gamma = \gamma_n, \quad \bar{\gamma} = \bar{\gamma}_n, \quad \alpha_x = \alpha_x^{(n)}, \quad \kappa_x = \kappa_x^{(n)}, \quad \beta_{b,x} = \beta_{b,x}^{(n)}, \quad \mathbb{B} = \mathbb{B}_n, \quad \mathcal{B} = \mathcal{B}_n.$$

We argue by induction on n. So we also assume that u^d is rationally conjugate to an element of G for every divisor d of n with $d \neq 1$.

We will use the representations θ_m of G and p-Brauer characters Ψ_m of G introduced in (4.1). Observe that the kernel of θ_m is trivial if m is odd, and otherwise it is the center of G. Using this and the induction hypothesis on n it easily follows that the order of $\theta_m(u)$ is $\frac{n}{2}$ if m is even, while, if m is odd then the order of $\theta_m(u)$ is n. Combining this with Proposition 2.3.2.(4) we deduce that $\theta_1(u)$ is conjugate to $\mathrm{diag}(\zeta, \zeta^{-1})$ for a suitable primitive n-th root of unity ζ. Hence there exists an element $g_0 \in G$ of order n such that $\theta_1(g_0)$ and $\theta_1(u)$ are conjugate. The element $g_0 \in G$ and the primitive n-th root of unity ζ will be fixed throughout and from now on we abuse the notation and consider ζ both as a primitive n-th root of unity in a field of characteristic p and as a complex primitive n-th root of unity. Then

$$\theta_m(g_0) \text{ is conjugate to } \begin{cases} \mathrm{diag}\left(1, \zeta^2, \zeta^{-2}, \dots, \zeta^m, \zeta^{-m}\right), & \text{if } 2 \mid m; \\ \mathrm{diag}\left(\zeta, \zeta^{-1}, \zeta^3, \zeta^{-3}, \dots, \zeta^m, \zeta^{-m}\right), & \text{if } 2 \nmid m; \end{cases}$$

and

$$\Psi_m(g_0^i) = \sum_{\substack{j=-m \\ j \equiv m \bmod 2}}^{m} \zeta^{ij} = \begin{cases} 1 + \alpha_{2i} + \alpha_{4i} + \cdots + \alpha_{mi}, & \text{if } 2 \mid m; \\ \alpha_i + \alpha_{3i} + \cdots + \alpha_{mi}, & \text{if } 2 \nmid m. \end{cases} \tag{4.10}$$

By the induction hypothesis on n, if c is a divisor of n with $c \neq 1$ then u^c is rationally conjugate to g_0^i for some i and hence $\zeta^c = \zeta^{\pm i}$. Therefore $c \sim_n i$ and hence u^c is conjugate to g_0^c.

Again as in Section 3.3, but now using Proposition 2.3.1.(3), we deduce that $x \mapsto (g_0^x)^G$ induces a bijection from Γ_n to the set of conjugacy classes of G formed by elements of order dividing n, and for ever integer x (or $x \in \Gamma_n$) we set

$$\varepsilon_x = \varepsilon_{g_0^x}(u) \quad \text{and} \quad \lambda_x = \sum_{i \in \Gamma_n} \varepsilon_i \alpha_{ix}.$$

The proof of the following lemma is exactly the same as the one of Lemma 3.3.3.

Lemma 4.2.3. *u is rationally conjugate to g_0 if and only if $\lambda_i = \alpha_i$ for any positive integer i.*

So we have to prove that $\lambda_i = \alpha_i$ for every positive integer i. We argue by contradiction, so we assume that $\lambda_d \neq \alpha_d$ for some positive integer d which we assume to be minimal with this property. As in the proof of Theorem 3.3.1, d is a proper divisor of n with $d \neq 1$, and $\lambda_d = \alpha_d + d\tau$ for some $\tau \in \mathbb{Z}[\alpha_1]$. By (4.10) we have

$$\Psi_d(g_0) = \sum_{\substack{i=0 \\ i \equiv d \bmod 2}}^{d} \alpha_i \quad \text{and} \quad \Psi_d(u) = \sum_{\substack{i=0 \\ i \equiv d \bmod 2}}^{d} \lambda_i.$$

Therefore we deduce that $\Psi_d(u) = \Psi_d(g_0) + d\tau$. Furthermore, $\tau \neq 0$, as $\lambda_d \neq \alpha_d$. Thus

$$C_b(\Psi_d(u)) \equiv C_b(\Psi_d(g_0)) \bmod d \quad \text{for every } b \in \mathbb{B} \tag{4.11}$$

and

$$d \leq |C_{b_0}(\Psi_d(u)) - C_{b_0}(\Psi_d(g_0))| \quad \text{for some } b_0 \in \mathbb{B}. \tag{4.12}$$

We will use (4.11) and (4.12) to obtain a contradiction by comparing the eigenvalues of $\theta_d(g_0)$ and $\theta_d(u)$, as we did in Section 3.3. Recall that if ξ is an eigenvalue of $\theta_d(u)$ then ξ and ξ^{-1} have the same multiplicity as eigenvalues of $\theta_d(u)$. Therefore, if $3 \leq h$ then the sum of the multiplicities of the eigenvalues of $\theta_d(u)$ of order h is even. Moreover, for every p-regular element g of G, the multiplicity of 1 as eigenvalue of $\theta_d(g)$ is congruent modulo 2 with the degree $d+1$ of Ψ_d. As n is not a prime power there is an odd prime r dividing n. By the induction hypothesis $\theta_d(u^r)$ is rationally conjugate to $\theta_d(g_0^r)$. Thus the multiplicity of -1 as eigenvalue of $\theta_d(u^r)$ is even. As the latter is the sum of the multiplicities as eigenvalues of $\theta_d(u)$ of -1 and the elements of order $2r$, we deduce that the multiplicity of -1 as eigenvalue of $\theta_d(u)$ is even. Using this we can see that $\theta_d(u)$ is conjugate to $\operatorname{diag}(\zeta^{\nu_{-d}}, \zeta^{\nu_{2-d}}, \dots, \zeta^{\nu_{d-2}}, \zeta^{\nu_d})$ for integers $\nu_{-d}, \nu_{-d+2}, \dots, \nu_{d-2}, \nu_d$ such that $\nu_{-i} = -\nu_i$ for every i. Let $X_d = \{i : 1 \le i \le d, i \equiv d \bmod 2\}$. Then, by Proposition 2.2.5, we have for every $b \in \mathbb{B}$ that

$$\begin{aligned} C_b(\Psi_d(u)) - C_b(\Psi_d(g_0)) &= \sum_{i \in X_d} (C_b(\alpha_{\nu_i}) - C_b(\alpha_i)) \\ &= \sum_{i \in X_d} \left(\kappa_{\nu_i} \beta_{b,\nu_i} \mu(\gamma(\nu_i)) \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} - \kappa_i \beta_{b,i} \mu(\gamma(i)) \delta_{b,i}^{(n/\bar{\gamma}(i))} \right). \qquad (4.13) \end{aligned}$$

We now express by writing $(\nu(X_d)) \sim_{\frac{n}{c}} (X_d)$ with $c \mid n$ and $c \neq 1$ that the lists $(\nu_i)_{i \in X_d}$ and $(i)_{i \in X_d}$ represent the same elements of $\Gamma_{\frac{n}{c}}$, up to ordering. This provides restrictions on d, n and the ν_i.

The following two lemmas are variants of Lemma 3.3.4 and Lemma 3.3.5. Their proofs need some substantials variations with respect to the proofs of the ones in Section 3.3. We include them for completeness.

Lemma 4.2.4. *1. Let $i \in X_d$. If $\kappa_i \neq 1$ then $n = 2d$ and $i = d$. If $\kappa_{\nu_i} \neq 1$ then $\frac{n}{d}$ is the smallest prime dividing n and $\kappa_{\nu_j} = 1$ for every $j \in X_d \setminus \{i\}$.*

2. If $d > 2$ then n is not divisible by any prime greater than d. In particular if d is prime then $\kappa_{\nu_i} = 1$ for every $i \in X_d$.

Proof. Let r denote the smallest prime dividing n.

(1) The first statement is clear. Suppose that $\kappa_{\nu_i} \neq 1$. Then either $r = 2$ and $\nu_i \equiv 0 \bmod \frac{n}{2}$ or $\nu_i \equiv 0 \bmod n$. As $(X_d) \sim_{\frac{n}{r}} (\nu(X_d))$ we deduce that $k \equiv 0 \bmod \frac{n}{r}$ for some $k \in X_d$. Therefore $d = k = \frac{n}{r}$ and for every $j \in X_d \setminus \{i\}$ we have $\nu_j \not\equiv 0 \bmod \frac{n}{r}$. Thus $\kappa_{\nu_j} = 1$.

(2) Suppose that t is a prime divisor of n with $d < t$. Then $\frac{n}{d} \neq r$ and therefore, by (1), $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_d$. Thus, by (4.12) and (4.13), it is enough to show that $\delta_{b,i}^{(n/\bar{\gamma}(i))} \neq 0$ for at most one $i \in X_d$ and $\delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} \neq 0$ for at most one $i \in X_d$. Observe that if $i \in X_d$ then $t \nmid i$ and hence $\frac{n}{\bar{\gamma}(i)}$ is multiple of t. Moreover, if i and j are different elements of X_d then i and j have the same parity and $-t < i - j < i + j < 2t$. Therefore $i \not\sim_t j$. Thus either $\delta_{b,i}^{\frac{n}{\bar{\gamma}(i)}} = 0$ or $\delta_{b,j}^{\frac{n}{\bar{\gamma}(j)}} = 0$. As $(X_d) \sim_t (\nu(X_d))$, this also proves that $\delta_{b,\nu_i}^{\frac{n}{\bar{\gamma}(\nu_i)}} = 0$ or $\delta_{b,\nu_j}^{\frac{n}{\bar{\gamma}(\nu_j)}} = 0$. □

We obtain an upper bound for $|C_b(\Psi_d(u)) - C_b(\Psi_d(g_0))|$ in terms of the number of prime divisors $P(d)$ of d.

Lemma 4.2.5. *For every $b \in \mathbb{B}$ we have*

$$|C_b(\Psi_d(u)) - C_b(\Psi_d(g_0))| \leq 2 + 2^{P(d)+1}.$$

Proof. Using (4.13) it is enough to prove that $\sum_{i\in X_d} \kappa_i \delta_{b,i}^{(n/\bar{\gamma}(i))} \leq 1 + 2^{P(d)}$ and that $\sum_{i\in X_d} \kappa_{\nu_i} \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} \leq 1 + 2^{P(d)}$. This is a consequence of Lemma 4.2.4.(1) and the following inequalities for every e dividing d':

$$\left|\left\{i \in X_d : \gcd(d, \bar{\gamma}(i)) = e, \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 1$$

and

$$\left|\left\{i \in X_d : \gcd(d, \bar{\gamma}(\nu_i)) = e, \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}\right| \leq 1.$$

We prove the second inequality, only using that $(\nu(X_d)) \sim_d (X_d)$. This implies the first inequality by applying the second one to $u = g_0$.

Let $Y_e = \left\{i \in X_d : \gcd(d, \bar{\gamma}(\nu_i)) = e, \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}$. By changing the sign of some ν_i's, we may assume without loss of generality that if $\delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1$ then $b \equiv \nu_i \bmod \frac{n}{\bar{\gamma}(\nu_i)}$. Thus, if $i \in Y_e$ then $b \equiv \nu_i \bmod \frac{n}{\bar{\gamma}(\nu_i)}$. We claim that if $i, j \in Y_e$ then $\nu_i \equiv \nu_j \bmod d$. Indeed, let r be prime divisor of d. If $n_r \neq d_r$ or $r \nmid e$ then clearly $\nu_i \equiv \nu_j \bmod d_r$. Otherwise, i.e. $n_r = d_r$ and $r \mid e$, then r divides both $\bar{\gamma}(\nu_i)$ and $\bar{\gamma}(\nu_j)$ and $\nu_i \equiv \nu_j \bmod \frac{d_r}{r}$. Therefore, by Lemma 2.2.4.(2), $\nu_i \equiv \nu_j \bmod n_r$, as desired. As $(\nu(X_d)) \sim_d (X_d)$ and the elements of X_d represent different classes in Γ_d we deduce that $|Y_e| \leq 1$. This finishes the proof of the lemma. □

We are ready to finish the proof of Theorem 4.2.2. Recall that we are arguing by contradiction.

By (4.12) and Lemma 4.2.5 we have $d \leq 2 + 2^{P(d)+1}$ and, using this, it is easy to show that $d \leq 6$ or $d = 10$. Indeed, if $P(d) \geq 3$ then

$$2 + 2^{P(d)+1} \geq d \geq 2 \cdot 3 \cdot 5 \cdot 2^{P(d)-3} > 14 + 2^{P(d)+1},$$

a contradiction. Thus $P(d) = 2$ and $d \leq 10$ or $P(d) = 1$ and $d \leq 5$. Hence d is either $2, 3, 4, 5, 6$ or 10. We deal with these cases separately.

Suppose that $d = 2$. Then $\nu_2 \sim_{n_p} 2$ for every prime p. By the assumptions on n and Lemma 4.2.4.(1), this implies that $\kappa_2 = \kappa_{\nu_2} = 1$, $\gamma(2) = \gamma(\nu_2)$ and $\beta_{b_0,2} = \beta_{b_0,\nu_2}$. Therefore

$$|C_{b_0}(\Psi_2(u)) - C_{b_0}(\Psi_2(g_0))| = \left|\mu(\gamma(2))\left(\delta_{b_0,2}^{(n/\bar{\gamma}(2))} - \delta_{b_0,\nu_2}^{(n/\bar{\gamma}(\nu_2))}\right)\right| \leq 1$$

contradicting (4.12).

Suppose that $d = 3$. By Lemma 4.2.4 and the assumptions on n, we have $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_3$ and $n' = 6$. If $2^4 \mid n$ or $3^2 \mid n$ then we have that

$$\left|\left\{i = 1, 3 : \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 1 \quad \text{and} \quad \left|\left\{i = 1, 3 : \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}\right| \leq 1,$$

which implies $|C_{b_0}(\Psi_3(u)) - C_{b_0}(\Psi_3(g_0))| \leq 2$, contradicting (4.12). Thus $n = 24$, since n is neither 12 nor a prime power and it is multiple of 4. In this case we have $\bar{\gamma}(1) = \gamma(1) = 2$, $\bar{\gamma}(3) = \gamma(3) = 3$, $\beta_{b,1} = \beta_{b,3} = 1$ and $C_b(\Psi_3(g_0)) = -\delta_{b,1}^{(12)} - \delta_{b,3}^{(8)}$ for every $b \in \mathbb{B}$. We may assume that $3 \mid \nu_3$ and $3 \nmid \nu_1$ because $(\nu(X_3)) \sim_3 (X_3)$. Suppose that $\nu_3 \sim_8 3$ and $\nu_1 \sim_8 1$. Then $\bar{\gamma}(\nu_1) = \gamma(\nu_1) = 2$, $\bar{\gamma}(\nu_3) = \gamma(\nu_3) = 3$, $\beta_{b_0,\nu_3} = 1$ and $\delta_{b_0,3}^{(8)} = \delta_{b_0,\nu_3}^{(8)}$, which implies $|C_{b_0}(\Psi_3(u)) - C_{b_0}(\Psi_3(g_0))| \leq 2$, contradicting (4.12). Suppose now that $\nu_3 \sim_8 1$ and $\nu_1 \sim_8 3$. This implies that $\nu_1 \equiv \pm 3 \bmod 8$ and $\nu_1 \equiv \pm 1 \bmod 3$ (because $3 \mid \nu_3$ but $3 \nmid \nu_1$). Thus either $\nu_1 \equiv \pm 11 \bmod 24$ or $\nu_1 \equiv \pm 5 \bmod 24$. As $(\nu(X_3)) \sim_{12} (X_3)$, we deduce that the only possibility is $\nu_1 \equiv \pm 11 \bmod 24$. In this case we have $\bar{\gamma}(\nu_1) = \gamma(\nu_1) = 1$ and $\bar{\gamma}(\nu_3) = \gamma(\nu_3) = 6$. Hence

$$C_{11}(\Psi_3(u)) - C_{11}(\Psi_3(g_0)) = \delta_{11,\nu_1}^{(24)} + \delta_{11,\nu_3}^{(4)} + \delta_{11,1}^{(12)} + \delta_{11,3}^{(8)} = 4,$$

contradicting (4.11).

Suppose that $d = 4$. By Lemma 4.2.4 and the assumptions on n, we have $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_4$ and $n' = 6$. If $3^3 \mid n$ or $2^3 \mid n$ then we have that

$$\left|\left\{i = 2, 4 : \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 1$$

which implies $|C_{b_0}(\Psi_4(u)) - C_{b_0}(\Psi_4(g_0))| \leq 3$, contradicting (4.12). Therefore $n = 36$. In this case we have $\gamma(2) = 1 = \beta_{b_0,2} = \beta_{b_0,4}$ and $\gamma(4) = 2$, which implies

$|C_{b_0}(\Psi_4(g_0))| \leq 1$ and hence $|C_{b_0}(\Psi_4(u)) - C_{b_0}(\Psi_4(g_0))| \leq 3$, contradicting (4.12).

Suppose that $d = 5$. Since $(\nu(X_5)) \sim_5 (X_5)$, there is exactly one ν_i which is divisible by 5, say ν_5. In particular, for $i \neq 5$ we have $5 \mid \frac{n}{\bar{\gamma}(\nu_i)}$ and $5 \mid \frac{n}{\bar{\gamma}(i)}$. Moreover, if j is an integer not multiple of 5 then $|\{i = 1, 3 : \nu_i \sim_5 j\}| \leq 1$. This implies that

$$\left|\left\{i = 1, 3 : \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 1 \quad \text{and} \quad \left|\left\{i = 1, 3 : \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}\right| \leq 1.$$

On the other hand, as $n \neq 10$, we deduce that $\kappa_i = 1$ for every $i \in X_5$, by Lemma 4.2.4.(1). Therefore, using (4.12) and (4.13), we deduce that $\kappa_{\nu_5} = 2$, in contradiction with Lemma 4.2.4.(1).

Suppose that $d = 6$. By Lemma 4.2.4, we have $n' \mid 30$ and $\kappa_i = \kappa_{\nu_i} = 1$ for every $i \in X_6$ because $n \neq 12$. If $25 \mid n$, or $9 \mid n$ or $8 \mid n$ then we have

$$\left|\left\{i = 2, 4, 6 : \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 2 \quad \text{and} \quad \left|\left\{i = 2, 4, 6 : \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}\right| \leq 2.$$

This implies that $|C_{b_0}(\Psi_6(u)) - C_{b_0}(\Psi_6(g_0))| \leq 4$, yielding a contradiction with (4.12). Therefore $n = 60$ and hence $\beta_{b,2} = \beta_{b,4} = \beta_{b,6} = 1$, $\bar{\gamma}(2) = 1$, $\bar{\gamma}(4) = \gamma(4) = 2$ and $\bar{\gamma}(6) = \gamma(6) = 3$. This implies that $|C_{b_0}(\Psi_6(g_0))| \leq 2$ and hence we obtain that $|C_{b_0}(\Psi_6(u)) - C_{b_0}(\Psi_6(g_0))| \leq 5$, yielding a contradiction with (4.12).

Suppose that $d = 10$. If $5 \nmid \frac{n}{\bar{\gamma}(i)}$ for some $i \in X_{10}$ then $n_5 = (\bar{\gamma}(i))_5 = 5$ and hence $5 \mid i$. The same also holds for ν_i. Therefore, if $5 \nmid i$ then $5 \mid \frac{n}{\bar{\gamma}(i)}$ and if $5 \nmid \nu_i$ then $5 \mid \frac{n}{\bar{\gamma}(\nu_i)}$. Thus

$$\left|\left\{i \in X_{10} : 5 \nmid i, \delta_{b,i}^{(n/\bar{\gamma}(i))} = 1\right\}\right| \leq 2 \quad \text{and} \quad \left|\left\{i \in X_{10} : 5 \nmid \nu_i, \delta_{b,\nu_i}^{(n/\bar{\gamma}(\nu_i))} = 1\right\}\right| \leq 2.$$

This implies $|C_{b_0}(\Psi_{10}(u)) - C_{b_0}(\Psi_{10}(g_0))| \leq 8$, contradicting (4.12).

This finishes the proof of Theorem 4.2.2.

CHAPTER 5

On the Zassenhaus Conjecture and direct products

In this chapter and the following one we explain our contribution to the study of the behavior of (ZC1) and (KP) under direct products. All the results of both chapters appeared in [BKS18].

Let G and H be finite groups and assume that (ZC1) holds for G and H. Then, as mention in the introduction, very little is known about whether (ZC1) holds for $G \times H$. If H is an elementary abelian 2-group this was answered affirmatively by Höfert and Kimmerle [HK06]. Moreover, Hertweck proved that (ZC1) holds for $G \times H$ provided H is nilpotent and G is an arbitrary finite group for which (ZC1) holds and whose order is coprime to $|H|$ [Her08a, Proposition 8.1].

In Section 5.1 we show that if G is a direct product of Sylow-by-abelian groups then (ZC1) holds for G provided the normal Sylow subgroups form a Hall subgroup of G (see Theorem 5.1.2). Section 5.2 deals with Frobenius and Camina groups. Among other we show that (ZC1) holds for a direct product of a Frobenius group with metacyclic complements and a finite abelian group (see Corollary 5.2.6).

Furthermore, in Section 5.1 we give a positive answer to (KP) in case G has a normal nilpotent Hall subgroup with abelian complement. Here G is embedded into a suitable direct product of Sylow-by-abelian groups for which (ZC1) is valid (see Corollary 5.1.3). Moreover we show in Section 5.1 that (KP) holds when G is a Sylow tower group. In particular, it holds for supersolvable groups.

On the other hand, it is not known whether (ZC1) behaves well with respect to quotient groups (for subgroups and extensions see Remark 5.1.4 below). The only easy observations one can make are the following ones:

Remark 5.0.1. *If H is a direct factor of a finite group G and (ZC1) holds for G then it also holds for H.*

Proof. Denote by $f\colon \mathbb{Q}H \to \mathbb{Q}G$ and $h\colon \mathbb{Q}G \to \mathbb{Q}H$ the ring homomorphisms induced by the inclusion of H into G and the projection of G onto H (i.e. $h \circ f = 1_{\mathbb{Q}G}$). Assume that u is a torsion element of $\mathrm{V}(\mathbb{Z}H)$. Then also $f(u)$ is a torsion element of $\mathrm{V}(\mathbb{Z}G)$ and by assumption $f(u)$ is conjugate to an element $g \in G$ by a unit $x \in \mathbb{Q}G$. This implies that $u = h(f(u))$ is conjugate by the unit $h(x) \in \mathbb{Q}H$ to $h(g) \in H$, as desired. □

Remark 5.0.2. *If the finite group H is contained in a finite group for which (ZC1) holds then (KP) has a positive answer for H.*

Proof. As H can be embedded into a finite group G for which (ZC1) holds, we have that each torsion element $u \in \mathrm{V}(\mathbb{Z}H)$ is conjugate within $\mathbb{Q}G$ to an element $g \in G$. This means $\varepsilon_g(u) \neq 0$. As necessarily $g^G \cap H \neq \emptyset$, u is also conjugate within $\mathbb{Q}G$ to an element of H. □

5.1 Nilpotent-by-abelian groups

The following lemma is a slight generalization of [Her08b, Lemma 5.5]. Recall that we use the notation $g \sim_G h$, for g and h elements of a group G, to express that g and h are conjugate in G. In case the group G is clear from the context we will write just $g \sim h$.

Lemma 5.1.1. *Let G be a finite group and π be a set of primes. Suppose that N is a normal nilpotent Hall π-subgroup of G with abelian complement K. Let x be a π-element of N and let $k \in K$. Then the set*

$$C = \{g \in G \ : \ g_\pi \sim x \text{ and } g = nk \text{ for some } n \in N\}$$

is a conjugacy class of G.

Proof. Let $f, g \in C$. As K is abelian, we may after conjugation assume that $f_\pi = g_\pi = x$, $f = x \cdot n_1 k$ and $g = x \cdot n_2 n_1 k$ with $n_1, n_2 \in N$. Let $H = \langle n_1 k, n_2 \rangle$. Having in mind that $n_1 k$ and $n_2 n_1 k$ are the π'-parts of f and g respectively, we get that $x \in C_G(H)$. Let $M = N \cap H$. Then M is a normal subgroup of H and $K_1 = \langle n_1 k \rangle$ and $K_2 = \langle n_2 n_1 k \rangle$ are complements to M in H. By Theorem 1.1.2 we get that $K_1^h = K_2$ for some $h \in H$. As $(n_1 k)^h \in Nk$ we get $(n_1 k)^h = n_2 n_1 k$. It follows that $f^h = x^h (n_1 k)^h = x n_2 n_1 k = g$, which establishes the lemma. □

Theorem 5.1.2. *Let $p_1, \dots, p_k$ be prime integers (non-necessarily different) and for every i let P_i be a p_i-group. Let $G = (P_1 \rtimes A_1) \times \cdots \times (P_k \rtimes A_k)$ where each A_j is a finite abelian group for every j and $P_1 \times \cdots \times P_k$ is a Hall subgroup of G. Then (ZC1) holds for G.*

Proof. We may assume without lose of generality that the p_i are pairwise different. Let u be a torsion element of $\mathrm{V}(\mathbb{Z}G)$. We will show that all partial augmentations of u but one vanish. Let bars denote reduction modulo $N = P_1 \times \cdots \times P_k$ and note that all torsion units of $\mathbb{Z}\bar{G}$ are trivial as $\bar{G}$ is abelian. Denote by π the set of prime divisors of the order of N.

Let $p = p_i$ and let $P = P_i$. Then u_p maps to 1 under the natural map $\mathbb{Z}G \to \mathbb{Z}G/P$ as G/P is a p'-group. Thus u_p is conjugate in the units of $\mathbb{Z}_pG$ to an element $x_p \in P$ by Theorem 1.4.2. Using Proposition 1.4.3 we deduce that $\varepsilon_g(u) = 0$ for every $g \in G$ whose p-part is not conjugate to x_p. Let $x = \prod_{i=1}^k x_{p_i}$. If $\varepsilon_g(u) \neq 0$ then g_{p_i} is conjugate to x_{p_i} for every i and hence there is $a_i \in P_i \rtimes A_i$ with $g_{p_i} = x_{p_i}^{a_i}$. Then $g_\pi = x^a$ with $a = a_1 \dots a_k$.

Take any $h \in G$. The partial augmentation $\varepsilon_{\bar{h}}(\bar{u})$ is the sum of all partial augmentations $\varepsilon_g(u)$ with $g \in G$ and $\bar{g} = \bar{h}$ in $\bar{G}$ (since $\bar{G}$ is abelian). By the previous paragraph, we need to sum only over conjugacy classes of elements $g \in G$ whose π-part is conjugate to x (and $\bar{g} = \bar{h}$ of course). By Lemma 5.1.1, this sum extends over a single conjugacy class (if any).

Thus, $\varepsilon_{\bar{g}}(\bar{u}) = \varepsilon_g(u)$ for all $g \in G$ whose π-part is conjugate to x. By Theorem 1.2.4.(1), $\varepsilon_k(\bar{u}) \neq 0$ for exactly one $k \in \bar{G}$. Applying Lemma 5.1.1 again, we see that there is only one partial augmentation of u different from 0, as desired. □

Corollary 5.1.3. *Assume that the finite group H has a normal nilpotent Hall subgroup N such that H/N is abelian. Then H can be embedded into a group G for which (ZC1) holds. In particular (KP) has an affirmative answer for H.*

Proof. Let $A \simeq H/N$ be a complement of N in H and $N = \prod_{j=1}^{k} P_j$ the decomposition of N as direct product of its Sylow subgroups. Set $G = \prod_{j=1}^{k} (P_j \rtimes A)$, with A acting on P_j as in H. Then

$$H = NA \hookrightarrow G = N \rtimes \left(\prod_{j=1}^{k} A\right) : na \mapsto (n, a, ..., a)$$

is an embedding of H into G. Note that (ZC1) holds for G by Theorem 5.1.2. Hence (KP) has a positive answer for H by Remark 5.0.2. □

Remark 5.1.4. *The groups constructed by Eisele and Margolis in [EM17] as counterexamples to (ZC1) have normal abelian Hall subgroup with abelian complement, so Corollary 5.1.3 shows that these groups can be embedded as normal subgroups in a group for which (ZC1) holds. This shows that the property (ZC1) is not closed under taking subgroups, not even under taking normal subgroups. In contrast to this, (KP) is clearly a subgroup closed property. As (ZC1) holds for abelian groups, (ZC1) can also not be an extension closed property.*

Proposition 5.1.5. *If G has a normal Hall subgroup N which is a Sylow tower group and (KP) has a positive answer for G/N then it also has a positive answer for G.*

Proof. Arguing by induction on the number of primes dividing N and using the Sylow Theorem, it is enough to prove that if the finite group G has a normal Sylow p-subgroup P and that (KP) has a positive answer for G/P, then (KP) has also a positive answer for G.

Let u be a torsion element of $\mathrm{V}(\mathbb{Z}G)$. We will prove that $\varepsilon_{G[m]}(u) = 0$ for every integer m different to the order of u. Then the result will follow by Theorem 1.2.7.

Assume $|u| = p^m \cdot a$ and p does not divide a. By Theorem 1.4.2, u_p is conjugate within $\mathbb{Z}_p G$ to $g_0 \in G$. Now, by Proposition 1.4.3 each partial augmentation $\varepsilon_h(u) = 0$ if the p-part h_p is not conjugate to g_0. Thus $\varepsilon_g(u) \neq 0$ implies that g has order $p^m \cdot b$ where b divides a. Let σ be the reduction map from G onto G/P and denote by $\bar{u}$ the image of u under the induced map from $\mathbb{Z}G$ onto $\mathbb{Z}(G/P)$. Clearly, for any $g \in G$ we have that $\sigma(g)$ has order b if and only if g has order $p^k \cdot b$

for some integer k. Thus

$$\varepsilon_{G[p^m \cdot b]}(u) = \varepsilon_{\bar{G}[b]}(\bar{u}).$$

By assumption, the right hand side is zero if and only if $b \neq a$. This finishes the proof. □

Theorem 5.1.6. *(KP) has a positive answer for finite groups with a Sylow tower. In particular it has a positive answer for supersolvable groups.*

Proof. Supersolvable groups are Sylow tower groups [Hup67, VI, Satz 9.1]. Thus the result follows from Proposition 5.1.5. □

Remark 5.1.7. *a) It follows from Proposition 5.1.5 that (KP) has a positive answer for G provided G has a normal nilpotent Hall subgroup with abelian complement. This also follows from Corollary 5.1.3. Note however that (ZC1) for the larger group do not need to hold if (KP) has a positive answer.*

b) Further examples of Sylow tower groups G are finite groups having a nilpotent normal subgroup N such that G/N is a p-group. Vice versa, groups G with a normal p-subgroup P and nilpotent quotient G/P are Sylow tower groups. From Burnside's Transfer Theorem [Hup67, IV, Satz 2.7] it follows that finite solvable groups all of whose Sylow subgroups are abelian with different invariants have a Sylow tower.

5.2 Frobenius and Camina groups

Let G be a finite group. Recall that G is called a *Camina group* if $G \neq G'$ and $gG' = g^G$ for all $g \in G \setminus G'$. Camina groups found a lot of attention since they were introduced by Camina in 1978. All Camina groups were described by Dark and Scoppola (the capstone can be found in [DS96, Lew14] and for the last gap that was closed see [IL15]). We collect this in the following proposition:

Proposition 5.2.1. *If G is a finite non-abelian Camina group which is not a p-group, then it is a Frobenius group whose complement is cyclic or isomorphic to Q_8.*

In order to study (ZC1) for the direct product of a Camina group and a finite abelian group, we first verify (ZC1) for Camina groups in Proposition 5.2.4. To do that, we are going to use the following results:

Theorem 5.2.2. *[DJ96, Corollary 2.3] Let G be a finite group and let N be a normal subgroup of G. Suppose that (ZC3) holds for the factor group G/N. Then any finite subgroup of $\mathrm{V}(\mathbb{Z}G)$ whose order is relatively prime to the order of N is rationally conjugate to a subgroup of G.*

Theorem 5.2.3. *[Seh93, Theorem (37.17)] Suppose that the finite group G is a split extension $A \rtimes X$ where A is nilpotent. Then any finite subgroup H of $\mathrm{V}(\mathbb{Z}G)$ with $\gcd(|H|, |A|) = 1$ is conjugate in $\mathcal{U}(\mathbb{Q}G)$ to a subgroup of $\mathrm{V}(\mathbb{Z}X)$.*

Proposition 5.2.4. *(ZC1) holds for finite Camina groups.*

Proof. Let G be a finite Camina group. Using Proposition 5.2.1 and the fact that (ZC1) holds for nilpotent groups, we may assume that G is a finite Frobenius group whose complement is cyclic or isomorphic to Q_8. Let u be an element of $\mathrm{V}(\mathbb{Z}G)$ of order k. By Theorem 1.4.6 we deduce that k divides either the order of the Frobenius kernel N of G or the order of the Frobenius complement of G. In the first case, u gets mapped to 1 under the natural ring homomorphism induced by modding out N and the result follows from Theorem 1.4.5. Otherwise, k is relatively prime to the order of N and the result follows from Theorem 5.2.2. □

We will use the following elementary observation. Let N be a normal subgroup of G and set $\bar{G} = G/N$. For a torsion unit u in $\mathbb{Z}G$, we shall extend the bar convention when writing $\bar{u}$ for the image of u under the natural map $\mathbb{Z}G \to \mathbb{Z}\bar{G}$. Since any conjugacy class of G maps onto a conjugacy class of $\bar{G}$, we have for any $x \in G$:

$$\varepsilon_{\bar{x}}(\bar{u}) = \sum_{g^G,\ \bar{g}\sim\bar{x}} \varepsilon_g(u). \tag{5.1}$$

Proposition 5.2.5. *Let A be any finite abelian group and F a finite Frobenius group with Frobenius complement C. If (ZC1) holds for $C \times A$ then it also holds for $F \times A$.*

Proof. Let N be the Frobenius kernel of G so that $F = N \rtimes C$. Using Remark 5.0.1 and that (ZC1) holds for $C \times A$, we deduce that it also holds for C. We claim that (ZC1) holds for the Frobenius group F. Indeed, by Theorem 1.4.6, the order of an element of $\mathrm{V}(\mathbb{Z}F)$ is either a divisor of the order of N or a divisor of the order of C. In the first case, the unit maps to the identity under the natural homomorphism $\mathbb{Z}F \to \mathbb{Z}F/N$ and hence it is rationally conjugate to an element of F by Theorem 1.4.5. In the second case, it is conjugate to a unit of $\mathbb{Z}C$ by a unit of $\mathbb{Q}F$ by Theorem 5.2.3 and hence eventually rationally conjugate to an element of C. This finishes the proof of the claim. We will use it without further mention.

Let $G = F \times A$ and let u be an torsion element of $\mathrm{V}(\mathbb{Z}G)$. We will prove that all partial augmentations of u are non-negative and after obtaining that, the result will follow by Theorem 1.2.6. We argue by induction on $|u|$ and on $|G|$. Note that the Frobenius kernel N is nilpotent by a famous result of Thompson, so it has a normal Sylow p-subgroup for each prime divisor p of $|N|$.

By induction on $|G|$, for every prime $p \mid |N|$, (ZC1) holds for G/N_p. Therefore, if there is a prime $p \mid |N|$ such that $p \nmid |u|$ we can use equation (5.1) with the normal subgroup N_p and Theorem 1.2.4.(3) to obtain for every $x \in G$ that $\varepsilon_{\bar{x}}(\bar{u}) = \sum_{g^G, \bar{g} \sim \bar{x}} \varepsilon_g(u) = \varepsilon_x(u) \geq 0$, as desired. Thus we may assume that every prime dividing $|N|$ also divides $|u|$. Moreover, for every prime $p \mid |N|$ we have that $p \nmid |C|$ because $N \rtimes C$ is Frobenius and using Theorem 1.4.2 with $N_p \times A_p$ we obtain that u_p is conjugate to $n_p a_p$ in the units of $\mathbb{Z}_p G$ for some $n_p \in N_p$ and some $a_p \in A_p$.

Suppose that $n_p = 1$ for some prime $p \mid |N|$. Then u_p is conjugate to a_p in the units of $\mathbb{Z}_p G$, and as a_p is central in G, we get $u_p = a_p \in A_p$. Let $v = u \cdot a_p^{-1}$ be a torsion element of $\mathrm{V}(\mathbb{Z}G)$. Thus $v_p = u_p a_p^{-1} = 1$ and $v_q = u_q$ for every prime $q \neq p$. This implies $|v| \mid |u|$ and $p \nmid |v|$. By induction on $|u|$, all partial augmentations of v are non-negative, and thus also all of u. Therefore we may assume that $n_p \neq 1$ for every prime $p \mid |N|$.

We claim that if $\varepsilon_g(u) \neq 0$ for some $g \in G$ then $g_q \in N \times A$ for every prime q. Using Proposition 1.4.3 we deduce for every prime $p \mid |N|$ that $g_p \sim_G n_p a_p$. This implies that $g_p \in N \times A$ for every prime $p \mid |N|$. Let q be a prime divisor of $|C \times A|$. If $q \nmid |C|$ then clearly $g_q \in N \times A$. Suppose now that $q \mid |C|$. Write $g_q = h_q a_q$ with $h_q \in F$ and $a_q \in A$. As $g_p \sim_G n_p a_p$ and a_p is central in G for any prime $p \mid |N|$, there is $f \in F$ such that $g_p = f^{-1}n_pfa_p$. Let $b_p = f^{-1}n_pf$. If $h_q \neq 1$ then $g_pg_q = b_pa_ph_qa_q = b_ph_qa_pa_q$ where $1 \neq b_ph_q \in F$ and $pq \mid |b_ph_q|$ because $b_ph_q = b_pa_ph_qa_qa_p^{-1}a_q^{-1} = g_pg_qa_p^{-1}a_q^{-1} = g_qg_pa_p^{-1}a_q^{-1} = h_qb_p$, contradicting the fact that F is Frobenius. Thus, if $q \mid |C|$ then $h_q = 1$ and hence $g_q = a_q \in A_q \subseteq N \times A$. This finishes the proof of the claim.

As a consequence of the claim we get that $\varepsilon_g(u) \neq 0$ implies $g_q \sim_G n_qa_q \in N \times A$ for every prime q. Fix a prime r dividing $|A|$. Write $G = ((N \rtimes C) \times A_{r'}) \times A_r$ and let $x \in (N \rtimes C) \times A_{r'}$. Observe that (ZC1) holds for G/A_r by induction on $|G|$. So using (5.1) with A_r we get

$$0 \leq \varepsilon_x(\bar{u}) = \sum_{b \in A_r} \varepsilon_{xb}(u) = \varepsilon_{xa_r}(u),$$

as desired. □

Corollary 5.2.6. *(ZC1) holds for the direct product $G \times A$ where A is any finite abelian group and G is either a Camina group or a Frobenius group whose complement has odd order.*

Proof. By [Hup67, V. Satz 8.18] (or by [Pas68, Theorem 18.1]) we know that odd order Frobenius complements are metacylic. Hence, having in mind that (ZC1) holds for nilpotent groups, metacyclic groups and cyclic-by-abelian groups, the result follows combining Proposition 5.2.1, Proposition 5.2.4 and Proposition 5.2.5. □

Now we look at Frobenius groups and (KP). The following results will be used in the proof of Proposition 5.2.8.

Proposition 5.2.7. *Let G be a finite group. Then (ZC1) holds for G in the following cases:*

1. *[HK06]* $G = \begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,3) \\ \hline \end{array}$.

2. *[BH08]* $G = \begin{array}{|c|}\hline \mathrm{SL}(2,5) \\ \hline \end{array}$.

3. *[DJMP97]* $G = \begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,5) \\ \hline \end{array}$.

Proposition 5.2.8. *(KP) has a positive answer for finite Frobenius complements.*

Proof. Let C be a finite Frobenius complement. It is enough to prove that C has a normal Hall subgroup N which is a Sylow tower subgroup and that (KP) has a positive answer for G/N, because in that case the result will follow by Proposition 5.1.5. For that we use the structure of Frobenius complements given by Theorem 1.1.4 and also the notation introduced in this theorem. Observe that all Sylow subgroups of the metacyclic Z-group M appearing in Theorem 1.1.4 are cyclic. Thus M has in each case a Sylow tower and hence (KP) holds for M by Theorem 5.1.6. It follows that either C is metabelian or that C has a normal Hall subgroup N with a Sylow tower for which C/N is of order coprime to $|N|$ and C/N is isomorphic to

$$\begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,3) \\ \hline\end{array}\,, \quad \text{or} \quad \boxed{\mathrm{SL}(2,5)}\,, \quad \text{or} \quad \begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,5) \\ \hline\end{array}\,,$$

or trivial. In the first case, i.e. if C is metabelian, then it is known that (KP) has a positive answer for C [DS94, Corollary 1.4] and the result will follow. For the second case, observe that C/N is isomorphic to either $\begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,3) \\ \hline\end{array}$, or $\boxed{\mathrm{SL}(2,5)}$, or $\begin{array}{|c|}\hline C_2 \\ \hline \mathrm{SL}(2,5) \\ \hline\end{array}$. Then (ZC1) holds for C/N by Proposition 5.2.7, and in particular (KP) has a positive answer for C/N, as desired. □

Corollary 5.2.9. *(KP) has a positive answer for finite Frobenius groups.*

Proof. Let G be a finite Frobenius group with Frobenius kernel N and with Frobenius complement C. By Thompson's famous result, N is a nilpotent Hall subgroup. Thus we may apply Proposition 5.1.5 and get that (KP) has a positive answer for G if and only if it has a positive answer for C. But this follows from Proposition 5.2.8. □

Remark 5.2.10. *It is unknown whether (ZC1) holds for all finite Frobenius groups. The arguments in the proofs used above show that for many of them this is indeed the case.*

Remark 5.2.11. *Let G be a finite Frobenius group with Frobenius kernel N, C a Frobenius complement of G, and H a finite group for which (KP) has an affirmative answer. The analogous question to Proposition 5.2.5 is whether (KP) has positive answer for $G \times H$.*

If H is nilpotent then we may write $H = H_1 \times H_2$ such that $\gcd(|H_1|, |C|) = 1$ and each prime dividing $|H_2|$ divides $|C|$. Then $N \times H_1$ is a normal nilpotent Hall subgroup of $G \times H$. From Proposition 5.1.5 and Proposition 5.2.8 we see that (KP) has a positive answer for $G \times H_1$. Moreover (KP) has a positive answer for $G \times H$ if it is the case for $C \times H_2$. The latter is true when $C \times H_2$ has a Sylow tower and this holds when C has a Sylow tower.

In the following chapter we will study this problem when H is abelian.

CHAPTER 6

The Extended HeLP Method

In this chapter we continue the study of the behavior of (ZC1) and (KP) under direct product. However, now we concentrate on the case when one of the factors is an abelian finite group.

In Section 6.1 we extend the HeLP Method explained in Section 1.4 to group rings $\mathcal{O}G$ where $\mathcal{O}$ is a ring of algebraic integers and G is a finite group. This is the method we have used to investigate (ZC1) and (KP) for the direct product $G \times A$ mentioned above. Surprisingly this leads for many groups of small order to a positive result (see Proposition 6.1.9). However, this method is not enough to decide whether a normalized unit of order 4 in $\mathbb{Z}[i]S_4$ is conjugate by a unit of KS_4 to an element of S_4. Here S_4 denotes the symmetric group on 4 symbols and K is the field of fractions of $\mathbb{Z}[i]$. In a certain $\mathbb{Z}$-order containing $\mathbb{Z}[i]S_4$ there are such units arising from units of $\mathbb{Z}[i, 1/2]S_4$ and we will give one such unit explicitly.

Section 6.2 is dedicated to the proof of several applications of the extended version of the HeLP Method introduced in Section 6.1. Among other we prove that (KP) has a positive answer for the direct product of an abelian finite group with either a finite Frobenius group or a group whose order is at most 95 (see Theorem 6.2.7 and Theorem 6.2.8, respectively).

6.1 Extending coefficients

We start this section quoting the following result which serves as a motivation of the extended version of the HeLP Method we will explain later.

Proposition 6.1.1. *[Her08a, Proposition 8.2] Let G be a finite group and let A be a finite abelian group of exponent m. Suppose that any torsion element of $\mathrm{V}(\mathbb{Z}[\zeta_m]G)$ is conjugate in the units of $\mathbb{Q}(\zeta_m)G$ to an element of G. Then (ZC1) holds for $G \times A$.*

Let G be a finite group. There is an obvious generalization of (ZC1) to group rings where the coefficients are allowed to come from rings of algebraic integers.

Problem 6.1.2. *Let $\mathcal{O}$ be the ring of algebraic integers in a number field K. Let u be a torsion element of $\mathrm{V}(\mathcal{O}G)$. Is u conjugate by a unit of KG to an element of G?*

This question is connected to certain instances of the classical (ZC1), where the coefficients come from $\mathbb{Z}$, as can be seen from Proposition 6.1.1 above. We say that (KP) has a positive answer for $\mathbb{Z}[\zeta_m]G$ if and only if for every torsion element u in $\mathrm{V}(\mathbb{Z}[\zeta_m]G)$ there is a finite group H containing G as subgroup such that u is conjugate within $\mathbb{Q}(\zeta_m)H$ to an element of G.

Many of the usual theorems on torsion units of integral group rings still hold in the case of coefficients coming from a G-adapted ring. Recall that a ring R is said to be a *G-adapted ring* if it is an integral domain of characteristic 0 and no prime divisor of the order of G is invertible in R.

Theorem 6.1.3. *Let R be a G-adapted ring and let u be an element of order n in $\mathrm{V}(RG)$. Let K be the field of fractions of R. Then the following statements hold:*

1. *[Her08b, Theorem 1.1] n divides the exponent of G.*
2. *[Her08b, Theorem 1.1] $\varepsilon_1(u) = 0$ if $u \neq 1$.*
3. *[Her07, Proposition 2.2]) If $g \in G$ then $\varepsilon_g(u) = 0$ whenever $|g| \nmid n$.*
4. *[Her07, Theorem 2.1]) u is conjugate by a unit of KG to an element of G if and only if for all divisors d of n, all partial augmentations of u^d but one vanish.*

Using Theorem 6.1.3.(4) we obtain, with the same proof as in [MdR17] for Theorem 1.2.7, the following result:

Theorem 6.1.4. *Let G be a finite group and let m be a positive integer. Then the following conditions are equivalent:*

1. *(KP) has a positive answer for $\mathbb{Z}[\zeta_m]G$.*

2. *For every torsion element u of $\mathrm{V}(\mathbb{Z}[\zeta_m]G)$ we have that $\varepsilon_{G[k]}(u) = 0$ for every integer k different to the order of u.*

Hertweck's proof of Proposition 6.1.1 actually proves part a) of the following proposition. It may be easily modified for (KP) which is stated as part b).

Proposition 6.1.5. *Let G be a finite group, let A be a finite abelian group of exponent m and let t be a divisor of the exponent of $G \times A$.*

a) Suppose that any element of $\mathrm{V}(\mathbb{Z}[\zeta_m]G)$ of order dividing t is conjugate in the units of $\mathbb{Q}(\zeta_m)G$ to an element of G. Then each element of order dividing t in $\mathrm{V}(\mathbb{Z}(G \times A))$ is rationally conjugate to an element of $G \times A$.

b) If (KP) has a positive answer for $\mathbb{Z}[\zeta_m]G$ then it also has a positive answer for $\mathbb{Z}(G \times A)$. More precisely, if for any element u of $\mathrm{V}(\mathbb{Z}[\zeta_m]G)$ with order dividing t we have that $\varepsilon_{G[k]}(u) \neq 0$ if and only if $k = |u|$, then for any element u of $\mathrm{V}(\mathbb{Z}(G \times A))$ with order dividing t we also have that $\varepsilon_{(G\times A)[k]}(u) \neq 0$ if and only if $k = |u|$.

In view of the last statement, it is desirable to have tools at hand that can be used to produce constraints on partial augmentations of torsion units of $\mathrm{V}(RG)$. In the case of coefficients coming from $\mathbb{Z}$ this can be achieved, for example, by the well-known HeLP Method (see Section 1.4). We present an extension of this method to rings of algebraic integers.

In the sequel we fix a finite group G, a ring of algebraic integers $\mathcal{O}$, an element u of order n in $\mathrm{V}(\mathcal{O}G)$ and a complex primitive n-th root of unity ζ. Observe that $\mathcal{O}$ is G-adapted. We can linearly extend each ordinary (p-Brauer) character χ of G to a character of $\mathrm{V}(\mathcal{O}G)$ (of the p-regular torsion elements of $\mathrm{V}(\mathcal{O}G)$). Let D be a representation of G affording χ. With exactly the same proof (cf. e.g. [Her07, § 4]) the formula for the multiplicity of roots of unity as eigenvalues of $D(u)$ remains valid. In other words,

$$\mu(\zeta^\ell, u, \chi) = \frac{1}{n} \sum_{d|n} \mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}} \left(\chi(u^d)\zeta^{-d\ell}\right).$$

Hence, this expression has to be a non-negative integer. Note that we have $\chi(u^d) \in \mathbb{Q}(\zeta^d)$, as this is the sum of all the eigenvalues of $D(u^d)$. Isolating the term for $d = 1$ we obtain

$$\frac{1}{n}\left(\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\chi(u)\zeta^{-\ell}\right) + \sum_{\substack{d|n \\ d\neq 1}} \mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}\left(\chi(u^d)\zeta^{-d\ell}\right)\right) = \mu(\zeta^\ell, u, \chi) \in \mathbb{Z}_{\geq 0}, \quad (6.1)$$

and assume by induction on $|u|$ that the latter sum is known (see the discussion at the end of Section 1.4). We have that $\chi(u) = \sum_{g^G} \varepsilon_g(u)\chi(g)$ by Theorem 1.3.1 and that Theorem 6.1.3.(3) guarantees $\varepsilon_g(u) = 0$ whenever $|g| \nmid n$. So all the character values at conjugacy classes which might have a non-zero partial augmentation are contained in $\mathbb{Q}(\zeta)$. That also the partial augmentations are contained in $\mathbb{Q}(\zeta)$, so that we can use the $\mathbb{Q}$-linearity of the trace to simplify further, is guaranteed by the following lemma.

Lemma 6.1.6. *Let $\mathcal{O}$ be a ring of algebraic integers and G be a finite group. If u is an element of order n in $\mathrm{V}(\mathcal{O}G)$ and ζ is a primitive n-th root of unity, then*

$$\varepsilon_g(u) \in \mathbb{Z}[\zeta] \cap \mathcal{O}$$

for every $g \in G$.

Proof. Let $\mathrm{Irr}(G) = \{\chi_1, ..., \chi_h\}$ be the set of irreducible characters of G and let $\{g_1, ..., g_h\}$ be a set of representatives of the conjugacy classes of G. Without loss of generality we may assume that $g_1, ..., g_d$ are the conjugacy classes whose elements have order a divisor of n.

By Theorem 6.1.3.(3), we have $\varepsilon_{g_j}(u) = 0$ for $j \in \{d+1, .., h\}$ and it remains to show that $\varepsilon_{g_j}(u) \in \mathbb{Z}[\zeta]$ for $j \in \{1,..,d\}$. We have

$$\begin{pmatrix} \chi_1(u) \\ \chi_2(u) \\ \chi_3(u) \\ \vdots \\ \chi_h(u) \end{pmatrix} = \begin{pmatrix} \chi_1(g_1) & \chi_1(g_2) & \chi_1(g_3) & \dots & \chi_1(g_h) \\ \chi_2(g_1) & \chi_2(g_2) & \chi_2(g_3) & \dots & \chi_2(g_h) \\ \vdots & \vdots & \ddots & \vdots & \\ \chi_h(g_1) & \chi_h(g_2) & \chi_h(g_3) & \dots & \chi_h(g_h) \end{pmatrix} \begin{pmatrix} \varepsilon_{g_1}(u) \\ \vdots \\ \varepsilon_{g_d}(u) \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

As u has order n, the column on the left hand side is an element of $\mathbb{Z}[\zeta]^h$. Denote the character table of G with the ordering above as $C = (c_{i,j})$. Let $J = \{1, ..., d\}$. As C is invertible, we can choose $I \subseteq \{1, ..., h\}$ with $|I| = d$ in such a way that the $d \times d$-submatrix $(c_{i,j})_{i \in I, j \in J}$ is invertible. Note that $(c_{i,j})_{i\in I,j\in J} \in \mathrm{GL}(d, \mathbb{Q}(\zeta))$, as the entries are character values of elements with an order a divisor of n. Hence

$$(\varepsilon_{g_j}(u))_{j\in\{1,..,d\}} = (c_{i,j})^{-1}_{i\in I,j\in J}(\chi_i(u))_{i\in I} \in \mathbb{Q}(\zeta)^d.$$

As these partial augmentations are algebraic integers, we deduce that $\varepsilon_g(u) \in \mathbb{Z}[\zeta] \cap \mathcal{O}$ for all $g \in G$. This completes the proof. □

Remark 6.1.7. *Although the partial augmentations of normalized units in $\mathcal{O}G$ of order n are contained in $\mathbb{Z}[\zeta_n]$, this is in general not true for the coefficients: Let $G = S_3$ and $\mathcal{O} = \mathbb{Z}[\zeta_9]$. Then*

$$\begin{aligned} u &= (1,2,3) + \zeta_9(1,2) + \zeta_9^4(2,3) + \zeta_9^7(1,3) \\ &= (1,2,3) + \zeta_9\left((1,2) + \zeta_3(2,3) + \zeta_3^2(1,3)\right) \end{aligned}$$

is an element of $\mathrm{V}(\mathcal{O}G)$ of order 3.

We can choose a basis B of $\mathbb{Z}[\zeta] \cap \mathcal{O}$ over $\mathbb{Z}$ and express $\varepsilon_g(u) = \sum_{b\in B} \alpha_{g,b} b$ with $\alpha_{g,b} \in \mathbb{Z}$. Then

$$\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\chi(u)\zeta^{-\ell}\right) = \sum_{g^G} \sum_{b\in B} \alpha_{g,b} \, \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\chi(g)\zeta^{-\ell} b\right).$$

So using (6.1), we get a system of linear inequalities over $\mathbb{Z}$:

$$\sum_{g^G}\sum_{b\in B}\alpha_{g,b}\,\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\chi(g)\zeta^{-\ell}b\right)+\sum_{\substack{d|n\\ d\neq 1}}\mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}\left(\chi(u^d)\zeta^{-d\ell}\right)\in n\mathbb{Z}_{\geq 0}. \qquad (6.2)$$

Note that compared to the plain HeLP Method, where $\mathcal{O}=\mathbb{Z}$, the number of variables grows by a factor $[K\cap\mathbb{Q}(\zeta):\mathbb{Q}]$, where K denotes the field of fractions of $\mathcal{O}$. Now we want to exploit Proposition 6.1.1 to verify (ZC1) for direct products $G\times A$, where A is an arbitrary finite abelian group.

For a given divisor n of the exponent of G and ζ an arbitrary complex root of unity, we will show that each element of order n of $\mathrm{V}(\mathbb{Z}[\zeta]G)$ (if it exists) is conjugate in the units of $\mathbb{Q}(\zeta)G$ to an element of G by showing that every solution of (6.2) is in accordance with the condition of Theorem 6.1.3.(4) or that there is no solution to (6.2) at all (in case there is no group element of order n). We can again employ Lemma 6.1.6 to see that it is enough to do this for ζ a primitive n-th root of unity. So for each group G we are left with the problem of finding the solutions to a finite number of systems of linear inequalities over the integers. We will usually choose $B=\{1,\zeta,...,\zeta^{\varphi(n)-1}\}$ as basis of $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$ (recall that φ denotes the Euler totient function).

Recall that a rational prime p is called *totally ramified* in an algebraic number field K (or rather in its ring of algebraic integers $\mathcal{O}$) if for each prime ideal $\mathfrak{p}$ containing the ideal $p\mathcal{O}$, the field $\mathcal{O}/\mathfrak{p}$ has cardinality p. For example, p is totally ramified in $\mathbb{Z}[\zeta_{p^a}]$ for $a\in\mathbb{Z}_{\geq 0}$ (see e.g. [Wei63, Proposition 7.4.1]).

Based on a result of Cohn-Livingstone [CL65], one can establish extra constraints for torsion units of $\mathbb{Z}G$, sometimes called the "Wagner test", cf. [BM15, Proposition 3.1]. With an adapted proof we get the following version for coefficients in rings of algebraic integers.

Proposition 6.1.8 ("Wagner test"). *Let G be a finite group, p a prime integer and $\mathcal{O}$ a ring of algebraic integers such that p is totally ramified in $\mathcal{O}$. Let u be an element of* $\mathrm{V}(\mathcal{O}G)$ *with $|u|=p^jm$ and $m\neq 1$. Then for $s\in G$ and $\mathfrak{p}$ a prime* *ideal containing $p\mathcal{O}$, we have*

$$\sum_{g^G,\ g^{p^j}\sim s} \varepsilon_g(u) \equiv \varepsilon_s(u^{p^j}) \mod \mathfrak{p}.$$

Proof. Let $u = \sum_{g\in G} u_g g \in \mathrm{V}(\mathcal{O}G)$, set $q = p^j$ and $v = u^q$. By definition

$$\varepsilon_s(v) = \sum_{\substack{(g_1,\dots,g_q)\in G^q\\ g_1\cdots g_q\sim s}} \prod_{j=1}^{q} u_{g_j}. \tag{6.3}$$

The set over which the sum is taken can be decomposed into the disjoint sets $\mathcal{M} = \{(g,...,g) \in G^q : g^q \sim s\}$ and

$$\mathcal{N} = \{(g_1,...,g_q) \in G^q : g_1...g_q \sim s \text{ and there are } r, r' \text{ with } g_r \neq g_{r'}\}.$$

The cyclic group $C_q = \langle t\rangle$ of order q acts on the set $\mathcal{N}$ by letting the generator t shift the entries of a tuple to the left, i.e., $(g_1, g_2, g_3, ..., g_q) \cdot t = (g_2, g_3, ..., g_q, g_1)$. Note that all orbits have length p^i with $i \geq 1$. For elements in the same orbit, the same integer is summed up in (6.3). Using that $\mathcal{O}/\mathfrak{p}$ has characteristic p and that $\mathcal{O}/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$ we get

$$\varepsilon_s(v) = \sum_{(g,...,g)\in\mathcal{M}} u_g^q + \sum_{(g_1,...,g_q)\in\mathcal{N}} \prod_{j=1}^{q} u_{g_j} \equiv \sum_{(g,...,g)\in\mathcal{M}} u_g^q \equiv \sum_{(g,...,g)\in\mathcal{M}} u_g \equiv \sum_{g^G,\ g^{p^j}\sim s} \varepsilon_g(u) \mod \mathfrak{p},$$

as desired. □

We refer to this new version of the HeLP Method as the *extended HeLP Method*, abbreviated as *HELP* Method. This has been implemented in the computer algebra system GAP [GAP16] and applied to some groups of small order. We will present here the results of the calculations with these groups of small order but we will not include the calculations themselves which were performed by the mentioned implementation of the HELP Method.

First we exclude the groups covered by known results. If G is nilpotent, a Camina group, a cyclic-by-abelian group or if it has a normal Sylow p-subgroup with abelian quotient, then (ZC1) is known for $G \times A$, for A a finite abelian group.

So Proposition 6.1.1 together with the above method will not provide us in these cases with anything new. If we filter all groups up to order 95 that are not covered by what is said before, we are left with 17 groups (up to order 100, there are 73 such groups). We will list in the first two columns of Table 6.1 their SmallGroup IDs together with their structure description. The third column contains the orders n of elements in $\mathrm{V}(\mathbb{Z}[\zeta_n]G)$, where the HELP Method (including the "Wagner test") does not provide a complete solution; in parentheses, up to conjugacy, the number of distributions of non-trivial partial augmentations that cannot be ruled out is indicated. In case there are only trivial partial augmentations left, a checkmark is included. The last column contains the orders where either the Wagner test or the so-called "Quotient Method" (a unit would map to a unit with an already eliminated distribution of partial augmentations in an integral group ring of a quotient group) can be used together with the number for such distributions where this applies; if the Quotient Method does not provide new information, the zero is omitted.

Table 6.1: Groups of order at most 95 investigated with the HELP Method.

SmallGroupID	Structure Description	Order	Wagner test / Quotient Method
`[24,12]`	S_4	4(4)	4(4)
`[48,28]`	$C_2.S_4 = \mathrm{SL}(2,3).C_2$	8(8)	
`[48,29]`	$\mathrm{GL}(2,3)$	8(4)	4(1), 8(4)
`[48,30]`	$A_4 \rtimes C_4$	4(8)	4(21 / 5)
`[48,48]`	$C_2 \times S_4$	4(16)	4(12)
`[60,5]`	A_5	6(2)	
`[72,15]`	$((C_2 \times C_2) \rtimes C_9) \rtimes C_2$	4(4)	4(4), 12(3)
`[72,22]`	$(C_6 \times S_3) \rtimes C_2$	✓	4(2)
`[72,23]`	$(C_6 \times S_3) \rtimes C_2$	✓	4(2)
`[72,24]`	$(C_3 \times C_3) \rtimes Q_8$	✓	
`[72,31]`	$(C_3 \times C_3) \rtimes Q_8$	✓	
`[72,33]`	$(C_{12} \times C_3) \rtimes C_2$	✓	
`[72,35]`	$(C_6 \times C_6) \rtimes C_2$	✓	4(2)
`[72,40]`	$(S_3 \times S_3) \rtimes C_2 = S_3 \wr C_2$	3(2), 6(4)	4(2)
`[72,42]`	$C_3 \times S_4$	4(4), 12(8)	4(4)
`[72,43]`	$(C_3 \times A_4) \rtimes C_2$	4(4)	4(4), 12(2)
`[72,44]`	$A_4 \times S_3$	✓	

Note that the HELP Method fails for groups which have S_4, A_5 or the wreath product $S_3 \wr C_2$ as quotients. We record more precisely the consequences of these calculations and Proposition 6.1.5.

Proposition 6.1.9. *Let G be a group of order at most 95 and A a finite abelian group. Then:*

1. *(ZC1) holds for $G \times A$ except if G maps onto S_4 or $G \simeq A_5$ or $G \simeq S_3 \wr C_2$.*
2. *If $G \simeq A_5$ or $G \simeq S_3 \wr C_2$, then (ZC1) holds for $G \times A$ if A is a $3'$-group.*
3. *If G maps onto S_4, then (ZC1) holds for $G \times A$ if 4 does not divide the exponent of A.*
4. *In the case that S_4 is an image of G, all elements of $\mathrm{V}(\mathbb{Z}(A \times G))$ whose order is not divisible by 4 are rationally conjugate to an element of $A \times G$.*

Note that there are problems with normalized units of order a power of 2 if and only if G maps onto S_4. In particular, those distributions of partial augmentations that cannot be excluded in these groups, always map on one of the distributions of partial augmentations in S_4 that cannot be excluded. So, in order to solve Problem 6.1.2 for all groups of order at most 95, one has only to deal with S_4, A_5 and the wreath product $S_3 \wr C_2$.

We now focus on one of the problematic partial augmentations for S_4 that could not be ruled out yet. Note that `CharacterTable("S4")` in GAP produces a permutation of the columns of `CharacterTable(SmallGroup(24,12))`. We will use the notation for conjugacy classes of the latter table, i.e. $2a$ contains the transpositions (••) and $2b$ the double transpositions (••)(••). The irreducible characters of S_4 will be denoted by $\chi_{1a} = 1$, $\chi_{1b} = \mathrm{sgn}$, χ_2 (this is the inflation of the irreducible non-linear character of S_3), χ_{3a} and $\chi_{3b} = \chi_{3a} \otimes \mathrm{sgn}$. The character table of S_4 we are using is thus as follows (dots indicate zeros):

class	1a	2a	3a	2b	4a
cycletype	()	(••)	(• • •)	(••)(••)	(• • • •)
χ_{1a}	1	1	1	1	1
χ_{1b}	1	-1	1	1	-1
χ_2	2	.	-1	2	.
χ_{3a}	3	-1	.	-1	1
χ_{3b}	3	1	.	-1	-1

For normalized units u of order 4 we always have $u^2 \sim 2b$ and we are left with the following four cases of distributions of partial augmentations that do not correspond to units that are conjugate in $\mathbb{Q}(i)S_4$ to an element of the group:

$$\begin{aligned}
&\underline{\text{Case 1}}: && \varepsilon_{2a}(u) = i,\ \varepsilon_{2b}(u) = 1,\ \varepsilon_{4a}(u) = -i;\\
&\underline{\text{Case 2}}: && \varepsilon_{2a}(u) = 1+i,\ \varepsilon_{2b}(u) = 0,\ \varepsilon_{4a}(u) = -i;\\
&\underline{\text{Case 3}}: && \varepsilon_{2a}(u) = -i,\ \varepsilon_{2b}(u) = 1,\ \varepsilon_{4a}(u) = i;\\
&\underline{\text{Case 4}}: && \varepsilon_{2a}(u) = 1-i,\ \varepsilon_{2b}(u) = 0,\ \varepsilon_{4a}(u) = i.
\end{aligned}$$

Of course, all partial augmentations not recorded are zero. Consider the ring homomorphism $\tau\colon \mathbb{Z}[i]S_4 \to \mathbb{Z}[i]S_4$ induced by complex conjugation on the coefficients. Then one can see that a unit as in case 1 exists if and only if a unit as in case 3 exists and similarly for case 2 and 4. So it suffices to consider the first two cases.

Assume we are in case 1, i.e. $u = \sum_{g\in G} u_g g \in \mathrm{V}(\mathbb{Z}[i]S_4)$ is of order 4, $u^2 \sim 2b = (\bullet\bullet)(\bullet\bullet)$, a double transposition, and $(\varepsilon_{2a}(u), \varepsilon_{2b}(u), \varepsilon_{4a}(u)) = (i, 1, -i)$. Clearly $\chi_{1a}(u) = 1$, $\chi_{1b}(u) = 1$, $\chi_2(u) = 2$, $\chi_{3a}(u) = -1-2i$ and $\chi_{3b}(u) = -1+2i$. Let D be the direct sum of the representations corresponding to χ_{1a}, χ_{1b}, χ_2, χ_{3a} and χ_{3b} (in this order). Then in a diagonalized form $D(u)$ looks as follows:

$$D(u) \text{ is conjugate to } \left(1, 1, \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right), \begin{pmatrix} -1 & & \\ & -i & \\ & & -i \end{pmatrix}, \begin{pmatrix} -1 & & \\ & i & \\ & & i \end{pmatrix}\right).$$

From this it immediately follows that u is in the kernel of the natural homomorphism $\mathrm{V}(\mathbb{Z}[i]S_4) \to \mathrm{V}(\mathbb{Z}[i]S_3)$.

In [LT91, Section 2], Luthar and Trama obtained certain congruences modulo $|G|$ from the integrability of the coefficients of the group rings elements. In their paper it turned out to be sufficient to exclude the existence of certain units of order 4 and 6 in $\mathrm{V}(\mathbb{Z}S_5)$ and they could conclude that (ZC1) holds for S_5. We can obtain similar restrictions (modulo the ideal $24\mathbb{Z}[i]$) that express that the coefficients of the units in question actually lie in $\mathbb{Z}[i]$. However in this case, these systems do not provide us with contradictions. There are even solutions modulo $6\mathbb{Z}[i]$ corresponding to matrices of order 4. These solutions correspond to normalized units of order 4 in $\mathbb{Z}[i, \frac{1}{2}]S_4$, which even lie in an order of $\mathbb{Q}(i)S_4$ containing $\mathbb{Z}[i]S_4$.

One such example is

$$\begin{aligned} u = \frac{1}{4}\Big(&(-1+i)(1,2) + (1+i)(1,3) + i(1,4) + i(2,3) - (2,4) + (3,4) \\ &+ (1,2,3) + (-1+i)(1,3,4) - (1+i)(1,4,2) + (2,4,3) \\ &+ (2-i)(1,2)(3,4) + (2+i)(1,3)(2,4) - (1,2,3,4) \\ &- i(1,2,4,3) - (1+i)(1,3,2,4) + (1,4,2,3) + (1-i)(1,4,3,2) - i(1,3,4,2)\Big), \end{aligned}$$

which is of order 4.

Note that a torsion unit u of $\mathbb{Z}[i]S_4$ in case 2 above is not in the kernel of the natural homomorphism $\mathrm{V}(\mathbb{Z}[i]S_4) \to \mathrm{V}(\mathbb{Z}[i]S_3)$, but rather maps to an involution. For this case, in a diagonalized form $D(u)$ looks as follows:

$$D(u) \text{ is conjugate to } \left(1, -1, \left(\begin{smallmatrix} 1 & \\ & -1 \end{smallmatrix}\right), \begin{pmatrix} -1 & & \\ & -i & \\ & & -i \end{pmatrix}, \begin{pmatrix} 1 & & \\ & i & \\ & & i \end{pmatrix}\right).$$

The other two groups of order at most 95 that cannot be handled and do not project onto S_4 are A_5 and $S_3 \wr C_2$. We also provide all remaining non-trivial distributions of partial augmentations for these groups. In the sequel denote by $\zeta = \zeta_3$ a primitive 3rd root of unity.

For the group A_5, units u with augmentation one and order 6 in $\mathbb{Z}[\zeta]A_5$ can not be proved to be conjugate within $\mathbb{Q}(\zeta)A_5$ to a group element using the HELP Method. Let $2a$ and $3a$ denote the unique A_5-conjugacy class of involutions and elements of order 3, respectively. In all cases that cannot be excluded, $u^3 \sim 2a$, $u^2 \sim 3a$ and

$$\begin{aligned} &\underline{\text{Case 1}}\text{:}\quad \varepsilon_{2a}(u) = -2\zeta,\ \varepsilon_{3a}(u) = 1 + 2\zeta; \\ &\underline{\text{Case 2}}\text{:}\quad \varepsilon_{2a}(u) = -2\zeta^2,\ \varepsilon_{3a}(u) = 1 + 2\zeta^2. \end{aligned}$$

Observe that a unit in case 1 exist if and only if it exists in case 2 by the automorphism of $\mathbb{Q}(\zeta)$ given by $\zeta \to \zeta^2$. These cases can also not be excluded by using Brauer characters (which might provide additional information in case of non-solvable groups) or the so-called Lattice Method [BM17b].

For $G = S_3 \wr C_2$, units of order 3 and 6 with non-trivial partial augmentations in $\mathbb{Z}[\zeta]G$ remain after the application of the HELP Method. For elements of order

3 the non-trivial distributions of partial augmentations are

$$(\varepsilon_{3a}(u), \varepsilon_{3b}(u)) \in \left\{\left(-\zeta, -\zeta^2\right), \left(-\zeta^2, -\zeta\right)\right\}.$$

As before, this would be simplified in just one case via the automorphism $\zeta \to \zeta^2$. For elements of order 6 with non-trivial partial augmentations that cannot be excluded with the HELP Method we always have $u^3 \sim 2c$ (the class of involutions in C_2) and

$$\begin{aligned}
&\underline{\text{Case 1}}: \quad u^2 \sim 3b,\ \varepsilon_{2b}(u) = 1,\ \varepsilon_{2c}(u) = 1,\ \varepsilon_{6b}(u) = -1;\\
&\underline{\text{Case 2}}: \quad u^2 \sim 3b,\ \varepsilon_{2b}(u) = -1,\ \varepsilon_{2c}(u) = 1,\ \varepsilon_{6b}(u) = 1;\\
&\underline{\text{Case 3}}: \quad u^2 \sim 3a,\ \varepsilon_{2a}(u) = 1,\ \varepsilon_{2c}(u) = 1,\ \varepsilon_{6a}(u) = -1;\\
&\underline{\text{Case 4}}: \quad u^2 \sim 3a,\ \varepsilon_{2a}(u) = -1,\ \varepsilon_{2c}(u) = 1,\ \varepsilon_{6a}(u) = 1.
\end{aligned}$$

Note that case 1 and 3 and case 2 and 4 lie in the same $\mathrm{Aut}(S_3 \wr C_2)$ orbit (interchanging the two factors isomorphic to S_3 in the base group).

Remark 6.1.10. *The HELP Method can successfully be applied to the unique perfect group of order* 120, $\mathrm{SL}(2,5)$. *This proves (ZC1) for* $\mathrm{SL}(2,5) \times A$, *$A$ a finite abelian group.*

Corollary 6.1.11. *(ZC1) holds for $G \times A$ where A is any finite abelian group and G is a Frobenius group whose complement C either has order at most* 95 *but is not isomorphic to $C_2.S_4$ or $C = \mathrm{SL}(2,5)$.*

Proof. By [Pas68, Theorem 18.1] we know that all Sylow p-subgroups of Frobenius complements are cyclic (in case p is odd) or cyclic or quaternion (for $p = 2$). However the groups of order at most 95 in Table 6.1 that cannot be handled have at least one Sylow subgroup which is not of that form except the case of $C_2.S_4$. The result now follows combining Proposition 5.2.5, Proposition 6.1.9 and Remark 6.1.10. □

Remark 6.1.12. *For S_5 the HELP Method can successfully be applied except for units of order* 4, 6 *and* 12. *In these cases the problematic partial augmentations are as follows. Let $2a$ be the conjugacy class of involutions contained in A_5. For* *partial augmentations of $u \in \mathrm{V}(\mathbb{Z}[i]S_5)$ of order 4 that cannot be excluded we have $u^2 \sim 2b$ and*

$$((\varepsilon_{2a}(u), \varepsilon_{2b}(u), \varepsilon_{4a}(u)) \in \{(0, 1-i, i), (1, -i, i), (0, -i, 1+i), (0, i, 1-i), (0, 1+i, -i), (1, i, -i)\}.$$

For elements u in $\mathrm{V}(\mathbb{Z}[\zeta_3]S_5)$ of order 6 the following remain (always $u^2 \sim 3a$):

$u^3 \sim 2b$ *and* $((\varepsilon_{2a}(u), \varepsilon_{2b}(u), \varepsilon_{3a}(u), \varepsilon_{6a}(u)) \in \{(1-2\zeta_6, 1, -1+2\zeta_6, 0), (-1+2\zeta_6, 1, 1-2\zeta_6, 0)\}$;

$u^3 \sim 2a$ *and* $((\varepsilon_{2a}(u), \varepsilon_{2b}(u), \varepsilon_{3a}(u), \varepsilon_{6a}(u)) \in \{(2\zeta_6, 0, 1-2\zeta_6, 0), (2-2\zeta_6, 0, -1+2\zeta_6, 0)\}$.

For elements u in $\mathrm{V}(\mathbb{Z}[\zeta_{12}]S_5)$ of order 12 the following remain (always $u^6 \sim 2a$, $u^4 \sim 3a$):

$\varepsilon_{2b}(u^3)$	$\varepsilon_{4a}(u^3)$	$\varepsilon_{2a}(u^2)$	$\varepsilon_{3a}(u^2)$	$\varepsilon_{2b}(u)$	$\varepsilon_{4a}(u)$	$\varepsilon_{6a}(u)$
$1-i$	i	$2\zeta_6$	$1-2\zeta_6$	0	$1+\zeta_{12}+\zeta_{12}^2$	$-\zeta_{12}-\zeta_{12}^2$
$-i$	$1+i$	$2\zeta_6$	$1-2\zeta_6$	1	$\zeta_{12}-\zeta_{12}^2$	$-\zeta_{12}+\zeta_{12}^2$
i	$1-i$	$2\zeta_6$	$1-2\zeta_6$	1	$-\zeta_{12}-\zeta_{12}^2$	$\zeta_{12}+\zeta_{12}^2$
$1+i$	$-i$	$2\zeta_6$	$1-2\zeta_6$	0	$1+\zeta_{12}-\zeta_{12}^2$	$\zeta_{12}-\zeta_{12}^2$
$1-i$	i	$2-2\zeta_6$	$-1+2\zeta_6$	0	$2-\zeta_{12}-\zeta_{12}^2+\zeta_{12}^3$	$-1+\zeta_{12}+\zeta_{12}^2-\zeta_{12}^3$
$-i$	$1+i$	$2-2\zeta_6$	$-1+2\zeta_6$	1	$-1-\zeta_{12}+\zeta_{12}^2+\zeta_{12}^3$	$1+\zeta_{12}-\zeta_{12}^2-\zeta_{12}^3$
i	$1-i$	$2-2\zeta_6$	$-1+2\zeta_6$	1	$-1+\zeta_{12}+\zeta_{12}^2-\zeta_{12}^3$	$1-\zeta_{12}-\zeta_{12}^2+\zeta_{12}^3$
$1+i$	$-i$	$2-2\zeta_6$	$-1+2\zeta_6$	0	$2+\zeta_{12}-\zeta_{12}^2-\zeta_{12}^3$	$-1+\zeta_{12}+\zeta_{12}^2+\zeta_{12}^3$

Thus (ZC1) holds for $S_5 \times A$, A a finite abelian group if neither 4 nor 3 divides the exponent of A. Moreover units of order 4 are conjugate in $\mathbb{Q}(\zeta)S_5$ if $i \notin \mathbb{Z}[\zeta]$. Hence, units in $\mathrm{V}(\mathbb{Z}(S_5 \times A))$ of order 4 are rationally conjugate of an element of $S_5 \times A$ if 4 does not divide the exponent of A.

Remark 6.1.13. *For $G = 2.S_5 = \mathrm{SL}(2,5).2$ the HELP Method leaves problems with elements of order 8. Here the problematic distributions of partial augmentations for elements u in $\mathrm{V}(\mathbb{Z}[i]G)$ of order 8 are as follows. Let $2a, 4a, 4b, 8a, 8b$ denote the conjugacy classes of order 2, 4 and 8 of G respectively as in the character table `CharacterTable("2.Sym(5)")` in GAP. Then $u^4 \sim 2a$, $u^2 \sim 4b$ and*

$$(\varepsilon_{4a}(u), \varepsilon_{4b}(u), \varepsilon_{8a}(u), \varepsilon_{8b}(u)) \in \{(1-i, 0, 0, i), (i, 1, 0, -i), (-i, 1, i, 0), (1-i, 0, i, 0), (1+i, 0, 0, -i), (i, 1, -i, 0), (-i, 1, 0, i), (1+i, 0, -i, 0)\}$$

All partial augmentations not stated are zero. Thus (ZC1) holds for $2.S_5 \times A$ with A an abelian finite group, if 4 does not divide the exponent of A.

6.2 Applications

In this section we prove some applications of the HELP Method in the study of (KP) for the direct product $G \times A$, where A is an abelian finite group and G is either a finite Frobenius group or a group of order at most 95.

We first prove some preliminary results. For that we will need the following result of Hertweck.

Proposition 6.2.1. *[Her08a, Proposition 2] Suppose that the finite group G has a normal p-subgroup N, and that u is a torsion element of $\mathrm{V}(\mathbb{Z}G)$ whose image under the natural map $\mathbb{Z}G \to \mathbb{Z}G/N$ has strictly smaller order than u. Then $\varepsilon_g(u) = 0$ for every element $g \in G$ whose p-part has order strictly smaller than the p-part of u.*

Proposition 6.2.2. *Let G and H be finite groups, p a prime integer and $D = H \times G$. Let u be a torsion element of $\mathrm{V}(\mathbb{Z}D)$. Let M be a normal p-subgroup of D and denote by $\bar{u}$ the image of u under $\mathbb{Z}D \to \mathbb{Z}D/M$. Assume that $|\bar{u}| < |u|$ and that $\varepsilon_{(D/M)[w]}(\bar{u}) \neq 0$ if and only if $w = |\bar{u}|$. Then*

$$\varepsilon_{D[j]}(u) = 0, \quad \text{if } j \neq |u|.$$

Proof. Write $|u| = p^m \cdot k$ with k coprime to p. As $|\bar{u}| < |u|$, we get by Proposition 6.2.1 that $\varepsilon_g(u) = 0$ for each $g \in D$ whose p-part has smaller order than the p-part of u. Moreover, by Theorem 1.2.4.(3), $\varepsilon_g(u) = 0$ provided $|g|$ does not divide $|u|$. So $\varepsilon_g(u) \neq 0$ implies that $|g| = p^m \cdot l$ and l divides k. Looking at the map from $\mathbb{Z}D$ onto $\mathbb{Z}D/M$ and using Theorem 1.2.4.(4), it follows that

$$\varepsilon_{D[p^m \cdot l]}(u) = \sum_i \varepsilon_{(D/M)[p^i \cdot l]}(\bar{u}).$$

By assumption $\varepsilon_{D/M[p^i \cdot l]}(\bar{u}) = 0$ if $p^i \cdot l \neq |\bar{u}|$. Thus $\varepsilon_{D[p^m \cdot l]}(u) = 0$ if $l \neq k$ and the result follows. □

Corollary 6.2.3. *Let A be a finite abelian group. Then the following statements hold:*

1. *If $D = A \times S_4$ and u is a torsion element of $\mathrm{V}(\mathbb{Z}D)$ then $\varepsilon_{D[m]}(u) = 0$ provided $m \neq |u|$.*

2. *If $D = A \times G$ where G is a group of order 48 mapping onto S_4 and u is a torsion element of $\mathrm{V}(\mathbb{Z}D)$ then $\varepsilon_{D[m]}(u) = 0$ provided $m \neq |u|$.*

3. *If $D = A \times 2.S_5$ and u is a torsion element of $\mathrm{V}(\mathbb{Z}D)$ with 8 dividing the order of u then $\varepsilon_{D[m]}(u) = 0$ provided $m \neq |u|$.*

Proof. (1) If 4 does not divide the order of u then the result follows from Proposition 6.1.9. Assume otherwise that 4 divides the order of u. Choose $M = \mathrm{O}_2(D) = A_2 \times V_4$, where A_2 is the Sylow 2-subgroup of A and $V_4 = \mathrm{O}_2(S_4)$ denotes the Klein 4-subgroup. Then $D/M \simeq A_{2'} \times S_3$. Clearly D/M has a Sylow tower. Thus (KP) has a positive answer for D/M by Proposition 5.1.5. Moreover 4 does not divide the exponent of $A_{2'} \times S_3$. So Proposition 6.2.2 completes this case.

(2) As in the previous case, we may assume that 4 divides the order of u (otherwise the result will follow by Proposition 6.1.9). Note that $|\,\mathrm{O}_2(G)| \geq 8$ and that $D/\,\mathrm{O}_2(D)$ is isomorphic to $A_{2'} \times S_3$. Thus we may argue as in the proof of (1).

(3) Choose $M = A_2 \times Z$, where $Z \simeq C_2$ denotes the center of $2.S_5$. Then D/M is a direct product of an abelian group of odd order and S_5. Clearly D/M has no elements of order 8. By Remark 6.1.12, units of order dividing 4 of $\mathrm{V}(\mathbb{Z}\,D/M)$ are rationally conjugate to elements of D/M. Thus for such units we have $\varepsilon_{D[m]}(u) = 0$ if $m \neq |u|$. Now again Proposition 6.2.2 completes this case. □

We will meet groups with all non-trivial elements of prime order in Proposition 6.2.6. First we quote a structure description of these groups.

Proposition 6.2.4. *[CDLS93] If G is a finite group such that every non-trivial element of G has prime order, then either G is a p-group of exponent p, or it is a Frobenius group of order $p^a \cdot q$ with p and q different primes, or it is isomorphic to A_5.*

Let G be a finite group such that every non-trivial element of G has prime order. We use Proposition 6.2.4. If G is a p-group or it is isomorphic to A_5 then (ZC1) clearly holds for G. Finally, if G is a Frobenius group of order $p^a \cdot q$ with p and q different primes, then (ZC1) holds for G by Theorem 1.4.4. This serves as a proof of the following remark:

Remark 6.2.5. *(ZC1) holds for finite groups having all non-trivial elements of prime order.*

Proposition 6.2.6. *Let $D = N \times G$, where N is a finite nilpotent group and G is a finite group. Assume that each non-trivial element of G is of prime order. Then (KP) has a positive answer for D.*

Proof. By Remark 6.2.5, (KP) has a positive answer for G. Let u be an element of $\mathrm{V}(\mathbb{Z}D)$ of prime order r. Then by Theorem 1.2.4.(3), $\varepsilon_{D[m]}(u) = 0$ if $m \neq r$. Therefore we may assume that the order of u is divisible by at least two primes.

Assume that N is a p-group. Suppose that u has order $p^k \cdot q$ with p and q different primes dividing $|G|$. By assumption G has no elements of mixed order. Thus it follows from Theorem 1.2.4.(4) that u maps under $\mathbb{Z}D \to \mathbb{Z}G$ onto an element of order q. We may apply Proposition 6.2.2 with $M = N$ and obtain that

$$\varepsilon_{D[m]}(u) = 0 \text{ if } m \neq p^k \cdot q. \tag{6.4}$$

We claim that if v is a torsion element of $\mathrm{V}(\mathbb{Z}D)$ whose order is not a prime power, then it has order $p^k \cdot q$ with p and q different primes dividing $|G|$. Indeed, assume otherwise that v has order $p^k \cdot q \cdot r$, with r a prime different from p and q. Then projecting v via the natural homomorphism $\mathbb{Z}D \to \mathbb{Z}G$ we get an element of $\mathrm{V}(\mathbb{Z}G)$ whose order is multiple of $q \cdot r$, in contradiction with the assumptions on G. This finishes the proof of the claim. Therefore, combining (6.4) with the claim we deduce that (KP) has a positive answer in this case.

We proceed by induction on the number of primes dividing $|N|$. Let P be the Sylow p-subgroup of N and let $N = P \times M$. If $p \nmid |u|$ then by Theorem 1.2.4.(3) we have $\varepsilon_{D[m]}(u) = \varepsilon_{(D/P)[m]}(\bar{u})$ for each m dividing $|D/P|$, where $\bar{u}$ is the image of u under the map $\mathbb{Z}D \to \mathbb{Z}D/P$. So by induction $\varepsilon_{D[m]}(u) = 0$ if and only if $m = |u|$.

Suppose now that $|u| = p^l \cdot k$ with $l \geq 1$. If $l \geq 2$ then by Proposition 6.2.2 we get

$$\varepsilon_{D[m]}(u) = 0 \quad \text{if } m \neq |u|.$$

Note that the arguments work for each prime dividing $|N|$. Thus it suffices to consider units of order $p \cdot q \cdot k$, where p and q are different primes and k is squarefree and coprime to $p \cdot q$. Let P and Q be the Sylow subgroups of N corresponding to p and q.

Denote the image of u in $\mathbb{Z}D/P$ by u_1, in $\mathbb{Z}D/Q$ by u_2 and that one in $\mathbb{Z}D/(P \cdot Q)$ by v. Suppose that u_1 and u_2 both have order divisible by $p \cdot q$. As v is the image of u_1 under $\mathbb{Z}D/P \to \mathbb{Z}D/(P \cdot Q)$ and torsion units mapping to 1 under this homomorphism are q-elements by Theorem 1.2.4.(4), v has order divisible by p. Similarly, looking at u_2, one gets that v has order divisible by q. But then we also get a torsion unit of order $p \cdot q$ in $\mathrm{V}(\mathbb{Z}G)$, for which (KP) has a positive answer by assumption. This contradiction shows that either u_1 or u_2 have order not divisible by $p \cdot q$.

Without lose of generality, we assume that $p \cdot q$ does not divide $|u_1|$. Thus we may apply Proposition 6.2.2 with $M = P$. Note that by induction (KP) has a positive answer for D/P. Consequently $\varepsilon_{D[m]}(u) = 0$ if $m \neq |u|$, as desired. □

Theorem 6.2.7. *Let G be a finite Frobenius group and let A be a finite abelian group. Then (KP) has a positive answer for $G \times A$.*

Proof. Let C be a Frobenius complement of G. Using Remark 5.2.11 and Remark 6.1.10 we deduce that (KP) has a positive answer for $G \times A$ provided this is the case for $C \times A$. If C is metabelian then $C \times A$ is metabelian and it is known that (KP) has a positive answer for metabelian groups (see [DS94, Corollary 1.4]), so the result will follow.

Suppose now that C is not metabelian. Then by Theorem 1.1.4, it follows that C has a Sylow tower if it does not map onto $\mathrm{SL}(2,3).2$ or $\mathrm{SL}(2,5).2$. If it is the case, i.e. if C has a Sylow tower then the result follows by Theorem 5.1.6.

Let u be an element of $\mathrm{V}(\mathbb{Z}(C \times A))$ of order n. We study the two remaining cases.

Suppose first that C maps onto $\mathrm{SL}(2,3).2$. If $4 \nmid |u|$ then, having in mind that $\mathrm{SL}(2,3).2 = C_2.S_4$, it follows that u is rationally conjugate to an element of $C \times A$

by Proposition 6.1.9. Otherwise, i.e. if $4 \mid |u|$ then, by Corollary 6.2.3.(2), we have that $\varepsilon_{(C\times A)[k]}(u) = 0$ if $k \neq n$. Thus (KP) has a positive answer fo $C \times A$ and the result will follow.

Suppose finally that C maps onto SL(2, 5).2. If $8 \nmid |u|$ then, by Remark 6.1.13, we have that u is rationally conjugate to an element of $C \times A$. Otherwise, i.e. if $8 \mid |u|$ then, by Corollary 6.2.3.(3), we have that $\varepsilon_{(C\times A)[k]}(u) = 0$ if $k \neq n$. Therefore, (KP) has a positive answer for $C \times A$, as desired. □

Theorem 6.2.8. *Let G be a group with $|G| \leq 95$ and let A be a finite abelian group. Then (KP) has a positive answer for $G \times A$.*

Proof. By Proposition 6.1.9 even (ZC1) holds for $G \times A$ provided G does not map onto S_4 or G does not coincide with $S_3 \wr C_2$ or A_5.

If $G = S_3 \wr C_2$ then G is a Sylow tower group and hence also $G \times A$ is a Sylow tower group. Thus the result follows from Theorem 5.1.6.

If $G = A_5$ then clearly (ZC1) holds for G. Therefore the result follows from Proposition 6.2.6.

Assume now that G maps onto S_4. Let u be an element of $\mathrm{V}(\mathbb{Z}(G \times A))$ of order n. By Proposition 6.1.9 we know that if $4 \nmid n$ then u is rationally conjugate to an element of $G \times A$ and the result will follow. Suppose otherwise that $4 \mid n$. Using Corollary 6.2.3.(1) and Corollary 6.2.3.(2), we deduce that $\varepsilon_{(G\times A)[k]}(u) = 0$ if $k \neq n$, provided that $G = S_4$ or G is a group of order 48 mapping onto S_4. Finally suppose that G is a group of order 72 with S_4 as image. Then G has a minimal normal subgroup M isomorphic to $C_2 \times C_2$. We have that (ZC1) holds for G/M and also G/M has no elements of order 4. Thus Proposition 6.2.2 completes the proof. □

References

[Alp86] J. L. Alperin. *Local representation theory*, volume 11 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Modular representations as an introduction to the local representation theory of finite groups.

[Ari07] Mini-Workshop: Arithmetik von Gruppenringen. *Oberwolfach Rep. 4 no. 4, 3209–3239, Abstracts from the mini-workshop held November 25–December 1, 2007, Organized by Eric Jespers, Zbigniew Marciniak, Gabriele Nebe and Wolfgang Kimmerle, Oberwolfach Reports.*, 2007. Vol. 4, no. 4. `https://www.mfo.de/occasion/0748c/www_view`.

[BC17] A. Bächle and M. Caicedo. On the prime graph question for almost simple groups with an alternating socle. *Internat. J. Algebra Comput.*, 27(3):333–347, 2017.

[BH08] V. Bovdi and M. Hertweck. Zassenhaus conjecture for central extensions of S5. *J. Group Theory*, 1:63–74, 2008.

[BHC62] A. Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math.*, 75(2):485–535, 1962.

[BHK04] V. Bovdi, C. Hofert, and W. Kimmerle. On the first Zassenhaus conjecture for integral group rings. *Publ. Math. Debrecen 65*, pages 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, pages 1–6, 2017. https://doi.org/10.1080/10586458.2017.1306814.

[BKL08] V. A. Bovdi, A. B. Konovalov, and S. Linton. Torsion units in integral group ring of the Mathieu simple group M_{22}. *LMS J. Comput. Math.*, 11:28–39, 2008.

[BKL11] V. A. Bovdi, A. B. Konovalov, and S. Linton. Torsion units in integral group rings of conway simple groups. *Internat. J. Algebra Comput.*, 21(4):615–634, 2011.

[BKM18] A. Bächle, W. Kimmerle, and L. Margolis. Algorithmic aspects of units in group rings. *to appear in Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory, G. Böckle, W. Decker, G. Malle (eds.), Springer Verlag*, 2018. https://arxiv.org/abs/1612.06171.

[BKS18] A. Bächle, W. Kimmerle, and M. Serrano. On the Zassenhaus conjecture and direct products. 2018. https://arxiv.org/abs/1801.09422.

[BM15] A. Bächle and L. Margolis. HeLP – A GAP-package for torsion units in integral group rings. 2015. https://arxiv.org/abs/1507.08174.

[BM17a] A. Bächle and L. Margolis. On the prime graph question for integral group rings of 4-primary groups I. *Internat. J. Algebra Comput.*, 27(6):731–767, 2017.

[BM17b] A. Bächle and L. Margolis. Rational conjugacy of torsion units in integral group rings of non-solvable groups. *Proc. Edinb. Math. Soc. (2)*, 60(4):813–830, 2017.

[BN41] R. Brauer and C. Nesbitt. On the modular characters of groups. *Ann. of Math. (2)*, 42:556–590, 1941.

[Bov87] A. A. Bovdi. The unit group of an integral group ring (russian). *Uzhgorod Univ. Uzhgorod*, 1987.

[Bov98] A. A. Bovdi. The group of units of a group algebra of characteristic p. *Publ. Math. Debrecen*, 52(1-2):193–244, 1998.

[Bur76] R. Burkhardt. Die Zerlegungsmatrizen der Gruppen $\mathrm{PSL}(2, p^f)$. *J. Algebra*, 40(1):75–96, 1976.

[Cala] C. K. Caldwell. Heuristics: Deriving the Wagstaff Mersenne Conjecture. http://primes.utm.edu/mersenne/heuristic.html. Visited April 2018.

[Calb] C. K. Caldwell. Mersenne primes: History, theorems and lists. http://primes.utm.edu/mersenne/. Visited April 2018.

[CDLS93] K. N. Cheng, M. Deaconescu, M. Lang, and W. J. Shi. Corrigendum and addendum to: Classification of finite groups with all elements of prime order. *Proc. Amer. Math. Soc.*, 117:1205–1207, 1993.

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

[CMdR13] 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] Ch. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons Inc., New York, 1981. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[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.

[DJMP97] M. A. Dokuchaev, S. O. Juriaans, and C. Milies Polcino. Integral group rings of Frobenius groups and the conjectures of H. J. Zassenhaus. *Comm. Algebra*, 25(7):2311–2325, 1997.

[Dor71] Larry Dornhoff. *Group representation theory. Part A: Ordinary representation theory.* Marcel Dekker, Inc., New York, 1971. Pure and Applied Mathematics, 7.

[dRS06] 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.

[dRS17] Á. del Río and M. Serrano. On the torsion units of the integral group ring of finite projective special linear groups. *Comm. Algebra*, 45(12):5073–5087, 2017.

[dRS18] Á. del Río and M. Serrano. Zassenhaus conjecture on torsion units holds for $\mathrm{SL}(2,p)$ and $\mathrm{SL}(2,p^2)$. 2018. `https://arxiv.org/abs/1803.05342`.

[DS94] M. A. Dokuchaev and S. K. Sehgal. Torsion units in integral group rings of solvable groups. *Comm. Algebra*, 22:5005–5020, 1994.

[DS96] R. Dark and C. M. Scoppola. On camina group of prime power order. *J. Algebra*, 181:787–802, 1996.

[EK11] B. Eick and A. Konovalov. The modular isomorphism problem for the groups of order 512. In *Groups St Andrews 2009 in Bath. Volume 2*, volume 388 of *London Math. Soc. Lecture Note Ser.*, pages 375–383. Cambridge Univ. Press, Cambridge, 2011.

[EM17] F. Eisele and L. Margolis. A counterexample to the first Zassenhaus conjecture. 2017. `https://arxiv.org/abs/1710.08780`.

[Fer87] N. A. Fernandes. Torsion units in the integral group ring of S_4. *Bol. Soc. Brasil. Mat. 18*, no. 1:1–10, 1987.

[GAP16] GAP. 2016. The GAP group, Groups, Algorithms, and Programming, Version 4.8.3, `http://www.gap-system.org`.

[Her01] M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001.

[Her02] M. Hertweck. Integral group ring automorphisms without zassenhaus factorization. *Illinois J. Math. 46*, no. 1:233–245, 2002.

[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. 2007. `https://arxiv.org/abs/math/0612429`, 16 pages.

[Her08a] M. Hertweck. The orders of torsion units in integral group rings of finite solvable groups. *Comm. Algebra*, 36(10):3585–3588, 2008.

[Her08b] M. Hertweck. Torsion units in integral group rings of certain metabelian groups. *Proc. Edinb. Math. Soc. (2)*, 51(2):363–385, 2008.

[Her08c] M. Hertweck. Zassenhaus conjecture for A_6. *Proc. Indian Acad. Sci. Math. Sci.*, 118(2):189–195, 2008.

[Her12] M. Hertweck. On torsion units in integral group rings of Frobenius groups. 2012. `https://arxiv.org/abs/1207.5256v1`.

[Her13] M. Hertweck. A criterion for p-adic conjugacy of p-torsion units in finite group rings. *manuscript*, 2013.

[Hig40] G. Higman. The units of group-rings. *Proc. London Math. Soc. (2)*, 46:231–248, 1940.

[HK06] C. Höfert and W. Kimmerle. On torsion units of integral group rings of groups of small order. *Groups, rings and group rings, Lect. Notes Pure Appl. Math.*, 248:243–252, 2006.

[HP72] I. Hughes and K. R. Pearson. The group of units of the integral group ring $\mathbb{Z}S_3$. *Canad. Math. Bull.*, 15:529–534, 1972.

[HP80] B. Hartley and P. F. Pickel. Free subgroups in the unit groups of integral group rings. *Canad. J. Math.*, 32(6):1342–1352, 1980.

[HS06] M. Hertweck and M. Soriano. On the modular isomorphism problem: groups of order 2^6. In *Groups, rings and algebras*, volume 420 of *Contemp. Math.*, pages 177–213. Amer. Math. Soc., Providence, RI, 2006.

[Hup67] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[IL15] I. M. Isaacs and M. Lewis. Camina p-groups that are generalized Frobenius complements. *Arch. Math. (Basel)*, 104(5):401–405, 2015.

[Isa76] I. M. Isaacs. *Character theory of finite groups.* Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, No. 69.

[JdR16] E. Jespers and Á. del Río. *Group ring groups. Vol. 1. Orders and generic constructions of units.* De Gruyter Graduate. De Gruyter, Berlin, 2016.

[Jes98] E. Jespers. Units in integral group rings: a survey. In *Methods in ring theory (Levico Terme, 1997)*, volume 198 of *Lecture Notes in Pure and Appl. Math.*, pages 141–169. Dekker, New York, 1998.

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

[Kim13] W. Kimmerle. Unit groups of integral group rings: old and new. *Jahresber. Dtsch. Math.-Ver.*, 115(2):101–112, 2013.

[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.

[Kle94] E. Kleinert. Units of classical orders: a survey. *Enseign. Math.*, 40(3-4)(2):205–248, 1994.

[Kli91] L. Klingler. Construction of a counterexample to a conjecture of Zassenhaus. *Comm. Algebra 19*, no. 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.

[Lew14] M. Lewis. Classifying Camina groups: a theorem of Dark and Scoppola. *Rocky Mountain J. Math.*, 44:591–597, 2014.

[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.

[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.

[Mar16] L. Margolis. A Sylow theorem for the integral group ring of $\mathrm{PSL}(2, q)$. *J. Algebra*, 445:295–306, 2016.

[Mar17] L. Margolis. A theorem of Hertweck on p-adic conjugacy of p-torsion units in group rings. *https://arxiv.org/abs/1706.02117v1*, 2017. 13 pages.

[MdR17] L. Margolis and Á. del Río. Partial augmentations property: A Zassenhaus conjecture related problem. *http://arxiv.org/abs/1706.04787v2*, page 13 pages, 2017.

[MdRS17] 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. 2017. https://arxiv.org/abs/1608.05797.

[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.

[NS17] G. Navarro and B. Sambale. On the blockwise modular isomorphism problem. 2017. `https://arxiv.org/abs/1706.03476,preprint`, to appear in Manuscripta Math.

[Pas65] D. S. Passman. The group algebras of groups of order p^4 over a modular field. *Michigan Math. J.*, 12:405–415, 1965.

[Pas68] D. Passman. *Permutation groups.* W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Pas79] I.B.S. Passi. *Group rings and their augmentation ideals.* volume 715 of Lecture Notes in Mathematics. Springer, Berlin, 1979.

[Pas85] D. S. Passman. *The algebraic structure of group rings.* Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.

[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.

[PMS02] C. Polcino Milies and S. K. Sehgal. *An introduction to group rings*, volume 1 of *Algebras and Applications.* Kluwer Academic Publishers, Dordrecht, 2002.

[Pom81] C. Pomerance. Recent developments in primality testing. *Math. Intelligencer*, 3(3):97–105, 1980/81.

[Rob82] D. J. S. Robinson. *A course in the theory of groups*, volume 80. Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.

[Rog91] K. W. Roggenkamp. Observations on a conjecture of Hans Zassenhaus. In *Groups-St. Andrews 1989, Vol. 2*, volume 160 of *London Math. Soc. Lecture Note Ser.*, pages 427–444. Cambridge Univ. Press, Cambridge, 1991.

[RS87] K. W. Roggenkamp and L. L. Scott. Isomorphisms of p-adic group rings. *Ann. of Math.*, 126(2):no. 3, 593–647, 1987.

[RT92] K. W. Roggenkamp and M. J. Taylor. *Group rings and class groups*, volume 18 of *DMV Seminar*. Birkhäuser Verlag, Basel, 1992.

[San85] R. Sandling. The isomorphism problem for group rings: a survey. In *Orders and their applications (Oberwolfach, 1984)*, volume 1142 of *Lecture Notes in Math.*, pages 256–288. Springer, Berlin, 1985.

[Sco92] L. L. Scott. On a conjecture of Zassenhaus, and beyond. *Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989) (Providence, RI), Contemp. Math. Amer. Math. Soc.*, 131:325–343, 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, 1993.

[Ser78] J. P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978.

[Sri64] B. Srinivasan. On the modular characters of the special linear group $SL(2, p^n)$. *Proc. London Math. Soc. (3)*, 14:101–114, 1964.

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

[Wag83] S. Wagstaff. Divisors of Mersenne numbers. *Math. Comp.*, 40(161):385–397, 1983.

[Wag95] R. Wagner. Zassenhausvermutung uber die gruppen PSL(2,p). *Diplomarbeit Universitat Stuttgart*, 1995.

[Wei63] E. Weiss. *Algebraic number theory.* McGraw-Hill Book Co., Inc., New York-San Francisco-Toronto-London, 1963.

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

Index of Notation

Index