Orders generated by character values

Andreas Bächle* and Benjamin Sambale†

June 10, 2019

Abstract

Let $K := \mathbb{Q}(G)$ be the number field generated by the complex character values of a finite group G. Let $\mathbb{Z}_K$ be the ring of integers of K. In this paper we investigate the suborder $\mathbb{Z}[G]$ of $\mathbb{Z}_K$ generated by the character values of G. We prove that every prime divisor of the order of the finite abelian group $\mathbb{Z}_K/\mathbb{Z}[G]$ divides $|G|$. Moreover, if G is nilpotent, we show that the exponent of $\mathbb{Z}_K/\mathbb{Z}[G]$ is a proper divisor of $|G|$ unless $G = 1$. We conjecture that this holds for arbitrary finite groups G.

Keywords: finite groups, field of character values, orders, algebraic integers
AMS classification: 20C15, 11R04

1 Introduction

It is well-known that the complex character values of a finite group G are algebraic integers. We like to measure how "many" algebraic integers actually arise in this way. The field

$$K := \mathbb{Q}(G) := \mathbb{Q}(\chi(g) : \chi \in \mathrm{Irr}(G),\ g \in G) \subseteq \mathbb{C}$$

of character values of G is contained in $\mathbb{Q}_{\exp(G)}$ where $\exp(G)$ denotes the exponent of G and $\mathbb{Q}_n$ is the cyclotomic field generated by the complex n-th roots of unity. Let $\mathbb{Z}_K$ be the ring of integers of K. The character values of G also generate an order $\mathbb{Z}[G]$ contained in $\mathbb{Z}_K$ (here $\mathbb{Z}[G]$ is neither the group algebra nor the ring of generalized characters). The deviation of $\mathbb{Z}[G]$ from $\mathbb{Z}_K$ can be measured by the structure of the finite abelian group $\mathbb{Z}_K/\mathbb{Z}[G]$. If G is a rational group for instance, then $K = \mathbb{Q}$ and $\mathbb{Z}[G] = \mathbb{Z} = \mathbb{Z}_K$. If G is abelian, then $K = \mathbb{Q}_{\exp(G)}$ and $\mathbb{Z}_K = \mathbb{Z}[e^{2\pi\sqrt{-1}/\exp(G)}]$. In this case it is easy to see that $\mathbb{Z}[G] = \mathbb{Z}_K$ as well. On the other hand, we construct a group G of order 240 such that

$$\mathbb{Z}_K/\mathbb{Z}[G] \cong C_{120}^2 \times C_{60}^2 \times C_{12}^4 \times C_4^4 \times C_2^{14}$$

where C_n denotes a cyclic group of order n. Nevertheless, our main theorems show that the structure of $\mathbb{Z}_K/\mathbb{Z}[G]$ is restricted by the order of G.

Theorem A. *Let G be a finite group and $K := \mathbb{Q}(G)$. Then the prime divisors of $|\mathbb{Z}_K/\mathbb{Z}[G]|$ divide $|G|$.*

Theorem B. *Let $G \neq 1$ be a nilpotent group and $K := \mathbb{Q}(G)$. Then the exponent of $\mathbb{Z}_K/\mathbb{Z}[G]$ is a proper divisor of $|G|$. In particular, $|G|\mathbb{Z}_K \subseteq \mathbb{Z}[G]$.*

*Vakgroep Wiskunde, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium, andreas.bachle@vub.be
†Institut für Mathematik, Friedrich-Schiller-Universität Jena, 07737 Jena, Germany, benjamin.sambale@uni-jena.de

In the final section we exhibit many examples which indicate that Theorem B might be true without the nilpotency hypothesis.

Conjecture C. *Let $G \neq 1$ be a finite group and $K := \mathbb{Q}(G)$. Then the exponent of $\mathbb{Z}_K/\mathbb{Z}[G]$ is a proper divisor of $|G|$.*

2 Preliminaries

In addition to the notation introduced above, we define

$$\begin{aligned}
\mathbb{Q}(g) &:= \mathbb{Q}(\chi(g) : \chi \in \mathrm{Irr}(G)) && (g \in G),\\
\mathbb{Z}[g] &:= \mathbb{Z}[\chi(g) : \chi \in \mathrm{Irr}(G)],\\
\mathbb{Q}(\chi) &:= \mathbb{Q}(\chi(g) : g \in G) && (\chi \in \mathrm{Irr}(G)),\\
\mathbb{Z}[\chi] &:= \mathbb{Z}[\chi(g) : g \in G].
\end{aligned}$$

For number fields $K \subseteq L$ we denote the relative discriminant of L with respect to K by $d_{L|K} \in \mathbb{Z}_K$. If $K = \mathbb{Q}$ we write $d_L := d_{L|\mathbb{Q}}$ as usual. We make use of the following tools from algebraic number theory.

Proposition 1. *The discriminant of any subfield of $\mathbb{Q}_n$ divides $n^{\varphi(n)}$.*

Proof. If $n = p^m$ is a power of a prime p, then by [9, Lemma I.10.1] the discriminant d_n of $\mathbb{Q}_n$ is $\pm p^{p^{m-1}(mp-m-1)}$, a divisor of $n^{\varphi(n)} = p^{mp^{m-1}(p-1)}$. For arbitrary n we obtain $d_n \mid n^n$ from [9, Proposition I.2.11]. Now if $K \subseteq \mathbb{Q}_n$ is any subfield, then by [9, Corollary III.2.10] even $d_K^{|\mathbb{Q}_n:K|}$ divides d_n. $\square$

Although we only need a weak version of the following result, it seems worth stating a strong form.

Proposition 2. *Let K and L be Galois number fields. Then*

$$\gcd(d_K, d_L)\mathbb{Z}_{KL} \subseteq \frac{\gcd(d_K, d_L)}{d_{K\cap L}^m}\mathbb{Z}_{KL} \subseteq \mathbb{Z}_K\mathbb{Z}_L$$

where $m := \min\{|KL : K|, |KL : L|\}$. In particular, $\mathbb{Z}_{KL} = \mathbb{Z}_K\mathbb{Z}_L$ if d_K and d_L are coprime.

Proof. Most textbooks only deal with the last claim. To prove the general case we follow [9, Proposition I.2.11]:

We consider the compositum KL as an extension over $M := K \cap L$. Note that $\mathbb{Z}_{KL}$ ($\mathbb{Z}_K$, $\mathbb{Z}_L$ respectively) is the integral closure of $\mathbb{Z}_M$ in KL (K, L respectively). Let $b_1, \ldots, b_n$ be a $\mathbb{Z}_M$-basis of $\mathbb{Z}_K$ and let $c_1, \ldots, c_m$ be a $\mathbb{Z}_M$-basis of $\mathbb{Z}_L$. Then $\{b_ic_j : i = 1, \ldots, n, j = 1, \ldots, m\}$ is an M-basis of KL as is well-known. Let $\alpha \in \mathbb{Z}_{KL}$ be arbitrary and write

$$\alpha = \sum_{i,j} a_{ij}b_ic_j$$

with $a_{ij} \in M$ for all i, j. Since KL is a Galois extension over $\mathbb{Q}$, it is also a Galois extension over K and over L. Thus, we may write $\mathrm{Gal}(KL|K) = \{\sigma_1, \ldots, \sigma_m\}$ and $\mathrm{Gal}(KL|L) = \{\tau_1, \ldots, \tau_n\}$. Then

$$\mathrm{Gal}(KL|M) = \{\sigma_i\tau_j : i = 1, \ldots, m, j = 1, \ldots, n\}$$

and restriction yields isomorphisms $\mathrm{Gal}(KL|K) \to \mathrm{Gal}(L|M)$ and $\mathrm{Gal}(KL|L) \to \mathrm{Gal}(K|M)$. Let

$$D = (\tau_i(b_j))_{i,j=1}^n \in \mathbb{Z}_K^{n\times n}, \qquad a = (\tau_1(\alpha), \ldots, \tau_n(\alpha)) \in \mathbb{Z}_M^n, \qquad b := \Big(\sum_{j=1}^m a_{ij}c_j\Big)_{i=1}^n \in L^n.$$

Then

$$\det(D)^2 = \det(D^{\mathrm{t}}D) = \det((\mathrm{Tr}_{K|M}(b_ib_j)_{i,j})) = d_{K|M}$$

(here D^{t} denotes the transpose of D and $\mathrm{Tr}_{K|M}$ is the trace map of K with respect to M). Moreover, $Db = a$. Denoting the adjoint matrix of D by $D^* \in \mathbb{Z}_K^{n\times n}$ we obtain $\det(D)b = D^*Db = D^*a$. The right hand side is an integral vector and so must be the left hand side. It follows that

$$d_{K|M}a_{ij} = \det(D)^2 a_{ij} \in \mathbb{Z}_M \subseteq \mathbb{Z}_K$$

for all i,j. Now by [9, Corollary III.2.10], we have

$$d_K = d_M^{|K:M|}\mathrm{N}_M(d_{K|M})$$

where N_M denotes the norm map of M with respect to $\mathbb{Q}$. Since M is a Galois extension, the norm of $d_{K|M}$ is the product of all Galois conjugates of $d_{K|M}$ in M. In particular, $d_{K|M}$ divides $\mathrm{N}_M(d_{K|M}) = d_K/d_M^{|K:M|}$ in $\mathbb{Z}_M$. Hence, $\frac{d_K}{d_M^{|K:M|}}a_{ij} \in \mathbb{Z}_M$ for all i,j. By a symmetric argument, $\frac{d_L}{d_M^{|L:M|}}a_{ij} \in \mathbb{Z}_M$ and therefore $\frac{\gcd(d_K,d_L)}{d_M^m}a_{ij} \in \mathbb{Z}_M$. Hence, we derive

$$\frac{\gcd(d_K,d_L)}{d_M^m}\alpha \in \mathbb{Z}_K\mathbb{Z}_L$$

as desired. □

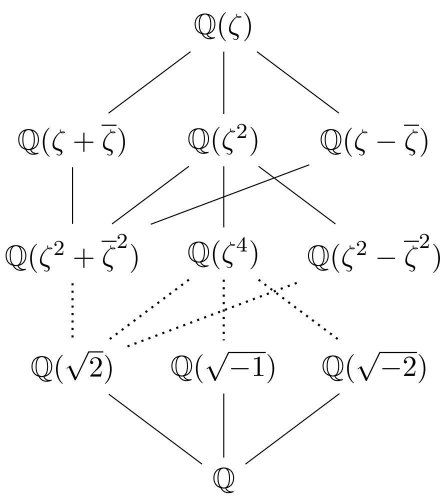
It is well-known that $\mathbb{Z}_{\mathbb{Q}_n} = \mathbb{Z}[\zeta]$ for every primitive n-th root of unity ζ. We also need the following refinements.

Proposition 3 (Leopoldt, see [12, Proposition 6.1])**.** *Let K be a number field contained in $\mathbb{Q}_n$. Then $\mathbb{Z}_K$ is generated as abelian group by the traces*

$$\sum_{\sigma\in\mathrm{Gal}(K(\zeta)|K)} \sigma(\zeta)$$

of n-th roots of unity ζ.

Lemma 4. *Every subfield of $\mathbb{Q}_{2^n}$ has the form $K = \mathbb{Q}(\xi)$ where $\xi \in \{\zeta, \zeta \pm \overline{\zeta}\}$ and ζ is a 2^n-th root of unity. The inclusion of subfields is given as follows*



If $\xi = \zeta \pm \overline{\zeta}$, then the elements 1 *and* $\zeta^k + (\pm\overline{\zeta})^k$ *with* $k = 1, \ldots, 2^{n-2} - 1$ *generate* $\mathbb{Z}_K$ *as abelian group.*

Proof. If $n \leq 2$, then $K \in \{\mathbb{Q}, \mathbb{Q}_4\}$ and the claim holds with $\xi = \zeta \in \{1, \sqrt{-1}\}$. Hence, let $n \geq 3$. By induction on n, we may assume that $K \nsubseteq \mathbb{Q}_{2^{n-1}}$ and ζ is a primitive 2^n-th root of unity. The subfields of $\mathbb{Q}_{2^n}$ correspond via Galois theory to the subgroups of the Galois group

$$\mathcal{G} := \mathrm{Gal}(\mathbb{Q}_{2^n}|\mathbb{Q}) \cong (\mathbb{Z}/2^n\mathbb{Z})^\times \cong C_2 \times C_{2^{n-2}}.$$

The involutions of $\mathcal{G}$ are $\alpha : \zeta \mapsto \zeta^{-1} = \overline{\zeta}$, $\beta : \zeta \mapsto \zeta^{-1+2^{n-1}} = -\overline{\zeta}$ and $\gamma : \zeta \mapsto \zeta^{1+2^{n-1}} = -\zeta$. Since $K \nsubseteq \mathbb{Q}_{2^{n-1}} = \mathbb{Q}_{2^n}^{\gamma}$, we must have $\mathrm{Gal}(\mathbb{Q}_{2^n}|K) \in \{\langle\alpha\rangle, \langle\beta\rangle\}$, i. e. $K = \mathbb{Q}(\zeta \pm \overline{\zeta})$.

As remarked above, $1, \zeta, \ldots, \zeta^{2^{n-1}-1}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_{\mathbb{Q}_{2^n}}$. Hence, every $x \in \mathbb{Z}_K$ can be written in the form

$$x = \sum_{k=0}^{2^{n-1}-1} a_k \zeta^k$$

with $a_0, \ldots, a_{2^{n-1}-1} \in \mathbb{Z}$. Since x is invariant under α or β, we obtain $a_k = -(\pm 1)^k a_{2^{n-1}-k}$ for $k = 1, \ldots, 2^{n-1} - 1$. Hence,

$$x = a_0 + \sum_{k=1}^{2^{n-2}-1} a_k(\zeta^k + (\pm\overline{\zeta})^k)$$

and the second claim follows. □

Proposition 5 ([8, Theorem 3.11])**.** *Let G be a finite group and $g \in G$. Then the natural map*

$$\mathrm{N}_G(\langle g\rangle)/\mathrm{C}_G(g) \to \mathrm{Gal}(\mathbb{Q}_{|\langle g\rangle|}|\mathbb{Q}(g))$$

is an isomorphism.

3 General results

We start our investigation with the "column fields" $\mathbb{Q}(g)$. Since products of characters are characters, we have $\mathbb{Z}[g] = \sum_{\chi \in \mathrm{Irr}(G)} \mathbb{Z}\chi(g)$.

Proposition 6. *For every finite group G and $g \in G$ we have*

$$|\mathrm{N}_G(\langle g\rangle)/\langle g\rangle|\mathbb{Z}_{\mathbb{Q}(g)} \subseteq \mathbb{Z}[g].$$

Proof. Let $n := |\langle g\rangle|$ and $K := \mathbb{Q}(g) \subseteq \mathbb{Q}_n$. By Proposition 3, $\mathbb{Z}_K$ is generated by the traces

$$\xi := \sum_{\sigma \in \mathrm{Gal}(K(\zeta)|K)} \sigma(\zeta)$$

of n-th roots of unity ζ. Let ψ be a character of $\langle g\rangle$ such that $\psi(g) = \xi \in K$. Then by Proposition 5 it follows that

$$\mathbb{Z}[g] \ni (\psi^G)(g) = \frac{1}{|\langle g\rangle|} \sum_{x \in \mathrm{N}_G(\langle g\rangle)} \psi(g^x) = |\mathrm{N}_G(\langle g\rangle)/\langle g\rangle|\xi.$$

This implies $|\mathrm{N}_G(\langle g\rangle)/\langle g\rangle|\mathbb{Z}_K \subseteq \mathbb{Z}[g]$. □

The following consequence implies Theorem A.

Corollary 7. *For every finite group G there exists $e \in \mathbb{N}$ such that*

$$|G|^e \mathbb{Z}_{\mathbb{Q}(G)} \subseteq \mathbb{Z}[G].$$

Proof. Clearly, $\mathbb{Q}(G) = \prod_{g \in G} \mathbb{Q}(g)$. By Proposition 1, the discriminants of the fields $\mathbb{Q}(g)$ for $g \in G$ divide $|G|^{|G|}$. Hence, Proposition 2 and Proposition 6 imply

$$|G|^e \mathbb{Z}_{\mathbb{Q}(G)} \subseteq |G|^{|G|} \prod_{g \in G} \mathbb{Z}_{\mathbb{Q}(g)} \subseteq \prod_{g \in G} \mathbb{Z}[g] \subseteq \mathbb{Z}[G]$$

for some (large) $e \in \mathbb{N}$. $\square$

For specific groups one can estimate the exponent e in Corollary 7 by using the full strength of Propositions 1 and 2. For nilpotent groups G we will prove next that e can be taken to be 1.

4 Nilpotent groups

Lemma 8. *Let G and H be finite groups of coprime order. Let $K := \mathbb{Q}(G)$ and $L := \mathbb{Q}(H)$. Then $\mathbb{Q}(G \times H) = KL$, $\mathbb{Z}_{KL} = \mathbb{Z}_K \mathbb{Z}_L$ and $\mathbb{Z}[G \times H] = \mathbb{Z}[G]\mathbb{Z}[H]$.*

Proof. Since $\mathrm{Irr}(G \times H) = \mathrm{Irr}(G) \times \mathrm{Irr}(H)$, it is clear that $\mathbb{Q}(G \times H) = KL$ and

$$\mathbb{Z}[G \times H] = \Big\{ \sum_{i=1}^{n} x_i y_i : n \in \mathbb{N}, x_1, \ldots, x_n \in \mathbb{Z}[G], y_1, \ldots, y_n \in \mathbb{Z}[H] \Big\} = \mathbb{Z}[G]\mathbb{Z}[H].$$

Since $K \subseteq \mathbb{Q}_{|G|}$ and $L \subseteq \mathbb{Q}_{|H|}$, the discriminants d_K and d_L are coprime according to Proposition 1. By Proposition 2, we obtain $\mathbb{Z}_{KL} = \mathbb{Z}_K \mathbb{Z}_L$ $\square$

In the situation of Lemma 8 it is easy to determine $\mathbb{Z}_{KL}/\mathbb{Z}[G \times H]$ from the elementary divisors of $\mathbb{Z}_K/\mathbb{Z}[G]$ and $\mathbb{Z}_L/\mathbb{Z}[H]$. For instance, if $\mathbb{Z}_K/\mathbb{Z}[G]$ has elementary divisors $1, 2, 4$ (in particular, $\mathbb{Z}_K$ has rank 3) and $\mathbb{Z}_L/\mathbb{Z}[L]$ has elementary divisors $1, 3$, then

$$\mathbb{Z}_{KL}/\mathbb{Z}[G \times H] \cong C_2 \times C_4 \times C_3 \times C_6 \times C_{12} \cong C_2 \times C_6 \times C_{12}^2.$$

The following is a special case of Theorem B.

Proposition 9. *Let G be a nilpotent group of odd order and let $p_1, \ldots, p_n$ be the prime divisors of $|G|$. Then*

$$|G|\mathbb{Z}_{\mathbb{Q}(G)} \subseteq q\mathbb{Z}[G]$$

where $q := \prod_{i=1}^{n} \min\{p_i^3, |G|_{p_i}\}$.

Proof. We may write $G = P_1 \times \ldots \times P_n$ with Sylow subgroups $P_1, \ldots, P_n$. By Lemma 8, it follows that

$$|G|\mathbb{Z}_{\mathbb{Q}(G)} = |P_1|\mathbb{Z}_{\mathbb{Q}(P_1)} \ldots |P_n|\mathbb{Z}_{\mathbb{Q}(P_n)}.$$

Thus, we may assume that G is a non-abelian p-group for some odd prime p. In particular, $|G| \geq p^3$. The Galois group of $\mathbb{Q}_{|G|}$ (and therefore of every subfield) is cyclic. By Proposition 5, $\mathrm{Gal}(\mathbb{Q}_{|\langle g \rangle|}|\mathbb{Q}(g))$ is a cyclic p-group for every $g \in G$. Hence, the fields $\mathbb{Q}(g)$ are all cyclotomic and therefore they are totally ordered. In particular, there exists $g \in G$ such that $K := \mathbb{Q}(G) = \mathbb{Q}(g)$. By Proposition 6, it follows that $N\mathbb{Z}_K \subseteq \mathbb{Z}[G]$ where $N := |\mathrm{N}_G(\langle g\rangle)/\langle g\rangle|$. If $N \le |G|/p^3$, then we are done. So we may assume that $N \ge |G|/p^2$. If $\mathbb{Q}(G) = \mathbb{Q}_p$, then $\mathbb{Z}_K = \mathbb{Z}[\lambda] \subseteq \mathbb{Z}[G]$ for any non-trivial linear character $\lambda \in \mathrm{Irr}(G)$. Therefore, we may assume that $|G| \ge p^4$, $|\langle g\rangle| = p^2$ and $\mathrm{N}_G(\langle g\rangle) = \mathrm{C}_G(g) = G$. By Proposition 5, $\mathbb{Q}(g) = \mathbb{Q}_{|\langle g\rangle|} = \mathbb{Q}(\zeta)$ for some root of unity ζ. Since the regular character of G is faithful, there exists $\chi \in \mathrm{Irr}(G)$ such that the restriction $\chi_{\langle g\rangle}$ is faithful. Since $g \in \mathrm{Z}(\chi)$, we have $\chi(g) = \chi(1)\zeta^k$ for some integer k coprime to p. Then for every $l \ge 0$ we also have $\chi(g^{p^l}) = \chi(1)\zeta^{kp^l}$. This implies $\chi(1)\mathbb{Z}_K \subseteq \mathbb{Z}[G]$. Since $|G| \ge p^4$ and $\chi(1)^2 < |G|$, we obtain $|G|\mathbb{Z}_K \subseteq p^3\mathbb{Z}[G]$. □

The analysis of 2-groups G is more delicate, since it may happen that $\mathbb{Q}(G) \ne \mathbb{Q}(g)$ for all $g \in G$.

Lemma 10. *Let G be a 2-group and $g \in G$ such that $\mathbb{Q}(g)$ is not a cyclotomic field. Then for every subfield K of $\mathbb{Q}(g)$ there exists $\chi \in \mathrm{Irr}(G)$ such that $K = \mathbb{Q}(\chi(g))$.*

Proof. We argue by induction on $|G|$. We may assume that $|\mathbb{Q}(g) : \mathbb{Q}| > 2$. In particular, $G \ne 1$. By Lemma 4, the subfields of $\mathbb{Q}(g)$ are totally ordered. In particular, there exists $\chi \in \mathrm{Irr}(G)$ such that $\mathbb{Q}(\chi(g)) = \mathbb{Q}(g)$. Let Z be a central subgroup of G of order 2. Then χ^2 is a character of G/Z and $|\mathbb{Q}(\chi(g)) : \mathbb{Q}(\chi(g)^2)| \le 2$. Since

$$\mathbb{Q}(gZ) = \mathbb{Q}(\psi(gZ) : \psi \in \mathrm{Irr}(G/Z)) \subseteq \mathbb{Q}(g),$$

we obtain $|\mathbb{Q}(g) : \mathbb{Q}(gZ)| \le 2$. Since $|\mathbb{Q}(g) : \mathbb{Q}| > 2$, also $\mathbb{Q}(gZ)$ is not a cyclotomic field. By induction, every proper subfield of $\mathbb{Q}(g)$ has the form $\mathbb{Q}(\psi(g))$ for some $\psi \in \mathrm{Irr}(G/Z)$. □

The cyclic group $G = \langle g\rangle \cong C_8$ shows the assumption on $\mathbb{Q}(g)$ in Lemma 10 is necessary.

Lemma 11. *Let G be a 2-group and $g \in G$ such that $K := \mathbb{Q}(g)$ is not a cyclotomic field. Then*

$$M\mathbb{Z}_K \subseteq 2\mathbb{Z}[G]$$

where $M := \max\{\chi(1) : \chi \in \mathrm{Irr}(G)\}$.

Proof. By Lemma 4, there exists a primitive 2^n-th root of unity ζ such that $K = \mathbb{Q}(\zeta \pm \overline{\zeta})$. Moreover, $\mathbb{Z}_K$ is generated by the elements 1 and $\xi_k := \zeta^k + (\pm\overline{\zeta})^k$ with $k = 1, \ldots, 2^{n-2} - 1$. For every such k there exists $\chi \in \mathrm{Irr}(G)$ such that $\mathbb{Q}(\chi(g)) = \mathbb{Q}(\xi_k)$ by Lemma 10. It suffices to show that $\chi(1)\xi_k$ is an integral linear combination of the Galois conjugates of $2\chi(g)$. To this end, we may assume that $k = 1$ and $\xi := \xi_1$.

Let $d := \chi(1)$ and note that $d > 1$ since $\mathbb{Q}(\chi(g)) = \mathbb{Q}(\xi) = K$ is not a cyclotomic field. There exist integers $a_0, \ldots, a_{2^{n-1}-1}$ such that

$$\chi(g) = \sum_{i=0}^{2^{n-1}-1} a_i\zeta^i = a_0 + \sum_{i=1}^{2^{n-2}-1} a_i\xi_i.$$

Since $\chi(g)$ is a sum of d roots of unity, $|a_0| + \ldots + |a_{2^{n-1}-1}| \le d$ (it may happen that other roots, even of higher order than 2^n, cancel each other out). The Galois group $\mathcal{G}$ of $\mathbb{Q}_{2^n}$ acts on K and on $\{\psi(g) : \psi \in \mathrm{Irr}(G)\}$. Let $\sigma \in \mathcal{G}$ such that $\sigma(\zeta) = \zeta^{1+2^{n-1}} = -\zeta$. Then

$$\omega := \sum_{i=0}^{s-1} b_i\xi_{2i+1} = \chi(g) - \sigma(\chi(g)) \in \mathbb{Z}[G]$$

where $s := 2^{n-3}$ and $b_i := 2a_{2i+1}$ for $i = 0, \ldots, s-1$. Let $\tau \in \mathcal{G}$ such that $\tau(\zeta) = \zeta^5$. Note that $\tau^s(\xi) = \sigma(\xi) = -\xi$. We may relabel the elements b_i in a suitable order such that

$$\omega = \sum_{i=0}^{s-1} b_i \tau^i(\xi).$$

Next we consider

$$\gamma := \sum_{i=0}^{s-1} b_i \zeta^{4i} \in \mathbb{Z}_{\mathbb{Q}_{2s}}.$$

It is known that the prime 2 is fully ramified in $\mathbb{Q}_{2s}$. More precisely, $(2) = (\zeta^4 - 1)^s$ and $(\zeta^4 - 1)$ is a prime ideal (see [9, Lemma I.10.1]). Let e be the 2-part of $\gcd(b_0, \ldots, b_{s-1})$. Then $\frac{1}{e}\gamma$ is an algebraic integer, but $\frac{1}{2e}\gamma$ is not. Hence, $(\frac{1}{e}\gamma) = (\zeta^4 - 1)^t \mathfrak{p}$ where $t < s$ and $\mathfrak{p}$ is an ideal of $\mathbb{Z}_{\mathbb{Q}_{2s}}$ coprime to $(\zeta^4 - 1)$. This implies the existence of some $\delta \in \mathbb{Z}_{\mathbb{Q}_{2s}}$ such that $\gamma\delta = 2em$ where m is an odd integer. We write $\delta = \sum_{i=0}^{s-1} c_i \zeta^{4i}$ with $c_0, \ldots, c_{s-1} \in \mathbb{Z}$. Then

$$2em = \gamma\delta = \sum_{i,j=0}^{s-1} b_i c_j \zeta^{4(i+j)}.$$

Comparing coefficients yields

$$\sum_{i+j=t} b_i c_j - \sum_{i+j=s-t} b_i c_j = \begin{cases} 2em & \text{if } t = 0, \\ 0 & \text{if } 1 \le t \le s-1. \end{cases}$$

Finally we compute

$$\sum_{j=0}^{s-1} c_j \tau^j(\omega) = \sum_{i,j=0}^{s-1} b_i c_j \tau^{i+j}(\xi) = \sum_{t=0}^{s-1} \Big(\sum_{i+j=t} b_i c_j - \sum_{i+j=s-t} b_i c_j \Big) \tau^t(\xi) = 2em\xi.$$

Hence, $2em\xi \in \mathbb{Z}[G]$. By Proposition 6 we also have $|G|\xi \in |G|\mathbb{Z}_{\mathbb{Q}(g)} \subseteq \mathbb{Z}[G]$. Therefore,

$$2e\xi = \gcd(2em, |G|)\xi \in \mathbb{Z}[G].$$

Note that

$$e \le \sum_{i=0}^{s-1} |b_i| = \sum_{i=0}^{2^{n-2}-1} |a_{2i+1}| \le \sum_{i=0}^{2^{n-1}-1} |a_i| \le d. \tag{4.1}$$

Suppose that $d\xi \notin 2\mathbb{Z}[G]$. Then $d \le 2e$ (keep in mind that d and e are 2-powers). If the first inequality in (4.1) is strict, then $2e \le \sum_{i=0}^{s-1} |b_i|$ since the right hand side is divisible by e. Thus, in any case one of the inequalities in (4.1) is an equality. If $e = \sum_{i=0}^{s-1} |b_i|$, then $e = |b_i|$ and $\omega = b_i \tau^i(\xi)$ for some $i \in \{0, \ldots, s-1\}$. Then we obtain $e\xi \in \mathbb{Z}[G]$. If, on the other hand, $\sum_{i=0}^{2^{n-2}-1} |a_{2i+1}| = \sum_{i=0}^{2^{n-1}-1} |a_i|$, then $\omega = 2\chi(g)$ and $e\xi \in \mathbb{Z}[G]$ by the computation above. Hence in any case we deduce that $d = e$. But now $\chi(g) = a_{2i+1}\tau^i(\xi)$ and $d = 2|a_{2i+1}|$. This implies $d\xi \in 2\mathbb{Z}[G]$ as desired. □

The next result is a restatement of Theorem B.

Theorem 12. *For every nilpotent group $G \neq 1$ the exponent of $\mathbb{Z}_{\mathbb{Q}(G)}/\mathbb{Z}[G]$ is a proper divisor of $|G|$.*

Proof. By Proposition 9 and its proof, we may assume that G is a 2-group. By Lemma 4, $\mathbb{Q}(G) = \mathbb{Q}(\xi)$ where $\xi \in \{\zeta, \zeta \pm \overline{\zeta}\}$ and ζ is a primitive 2^n-th root of unity. If there exists $g \in G$ such that $\mathbb{Q}(G) = \mathbb{Q}(g)$, then we obtain $|G|\mathbb{Z}_{\mathbb{Q}(G)} \subseteq \mathbb{Z}[G]$ from Proposition 6. Otherwise we have $n \geq 3$, $\mathbb{Q}(G) = \mathbb{Q}(\zeta)$ and there exists $g \in G$ such that $K := \mathbb{Q}(g) = \mathbb{Q}(\zeta \pm \overline{\zeta})$. Moreover, there exist $h \in G$ and $\psi \in \mathrm{Irr}(G)$ such that

$$\psi(h) = \sum_{i=0}^{2^{n-1}-1} a_i \zeta^i \notin K$$

where $a_0, \ldots, a_{2^{n-1}-1} \in \mathbb{Z}$. Lemma 11 shows that $M\mathbb{Z}_K \subseteq 2\mathbb{Z}[G]$ where $M := \max\{\chi(1) : \chi \in \mathrm{Irr}(G)\}$. It suffices to prove $|G|\zeta^k \in 2\mathbb{Z}[G]$ for every $k \in \mathbb{Z}$.

Let σ be the Galois automorphism of $\mathbb{Q}(\zeta)$ such that $\sigma(\zeta) = \pm\overline{\zeta}$. Since $\psi(h) \notin K$, we have $\psi(h) \neq \sigma(\psi(h))$. We consider

$$\omega := \psi(h) - \sigma(\psi(h)) = \sum_{i=1}^{2^{n-1}-1} b_i \zeta^i \in \mathbb{Z}[G]$$

where $b_i := a_i \pm a_{2^{n-1}-i}$ if i is odd and $b_i := a_i + a_{2^{n-1}-i}$ otherwise. Let e be the 2-part of $\gcd(b_0, \ldots, b_{2^{n-1}-1})$. As in the proof of Lemma 11 there exists an odd integer m such that $2em\omega^{-1}$ is an algebraic integer. Hence for every $k \in \mathbb{Z}$,

$$2em\frac{\zeta^k - \sigma(\zeta)^k}{\omega} \in \mathbb{Z}_{\mathbb{Q}(\zeta)} \cap \mathbb{Q}(\zeta)^\sigma = \mathbb{Z}_K.$$

We conclude that

$$2emM\zeta^k = emM(\zeta^k + \sigma(\zeta)^k) + emM\frac{\zeta^k - \sigma(\zeta)^k}{\omega}\omega \in \mathbb{Z}[G].$$

By Corollary 7, there exists $s \in \mathbb{N}$ such that $|G|^s\zeta^k \in \mathbb{Z}[G]$. Hence,

$$2eM\mathbb{Z}_{\mathbb{Q}(G)} \subseteq \gcd(2emM, |G|^s)\mathbb{Z}[\zeta] \subseteq \mathbb{Z}[G].$$

If $b_i \neq 0$ for some $i \neq 2^{n-2}$, then $e \leq |b_i| \leq |a_i| + |a_{2^{n-1}-1}| \leq \psi(1)$. Otherwise, $\omega = 2a_{2^{n-2}}\sqrt{-1}$. If, in this case, there exists some $a_i \neq 0$ with $i \neq 2^{n-2}$, then $e \leq |b_{2^{n-2}}| < 2|a_{2^{n-2}}| + |a_i| \leq 2\psi(1)$. Since e and $\psi(1)$ are 2-powers, we still have $e \leq \psi(1)$. Finally, let $\psi(h) = a_{2^{n-2}}\sqrt{-1} = \omega/2$. Then we may repeat the calculation above with $\psi(h)$ instead of ω in order to obtain $eM\mathbb{Z}_{\mathbb{Q}(G)} \subseteq \mathbb{Z}[G]$ where $e \leq 2\psi(1)$. In summary,

$$2M\psi(1)\mathbb{Z}_{\mathbb{Q}(G)} \subseteq \mathbb{Z}[G]$$

in every case. Since $|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2$, we have $2M\psi(1) \leq 2M^2 \leq |G|$. If $2M\psi(1) = |G|$, then $\psi(1) = M$ and ψ is the only irreducible character of degree M. But then ψ is rational and we derive the contradiction $\psi(h) \in K$. Therefore, $2M\psi(1) < |G|$ and the claim follows. □

5 Examples

We show first that Proposition 9 is sharp in the following sense.

Proposition 13. *For every prime p and every integer $n \geq 1$ there exists a group P of order p^{2n+2} and exponent p^2 such that $K := \mathbb{Q}(P) = \mathbb{Q}_{p^2}$ and $\mathbb{Z}_K/\mathbb{Z}[P] \cong C_{p^n}^{(p-1)^2}$.*

Proof. Let P be the central product of an extraspecial group E of order p^{2n+1} (it does not matter which one) and a cyclic group $C = \langle c \rangle$ of order p^2. The irreducible characters of P are those of $E \times C$ which agree on $\mathrm{Z}(E) = \langle z \rangle$ and $\langle c^p \rangle$. It is well-known that $\mathrm{Irr}(E)$ consists of p^{2n} linear character and $p-1$ faithful characters $\chi_1, \ldots, \chi_{p-1}$ of degree p^n (see [6, Example 7.6(b)] for instance). Since E/E' is elementary abelian, the linear character values of E and also of P generate $\mathbb{Q}_p$. Let ζ be a primitive p^2-th root of unity. After relabeling, we may assume that $\chi_i(z) = p^n \zeta^{ip}$ and $\chi_i(g) = 0$ for $g \in E \setminus \mathrm{Z}(E)$ and $i = 1, \ldots, p-1$. Hence, the non-linear character of P take the values 0 and $p^n \zeta^i$ for $i \in \mathbb{Z}$. This shows $K = \mathbb{Q}_{p^2}$ and

$$\mathbb{Z}[G] = \mathbb{Z}[\zeta^p, p^n \zeta^i : \gcd(i, p) = 1].$$

Since the elements $1, \zeta, \zeta^2, \ldots, \zeta^{p(p-1)-1}$ form a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, the claim follows easily. $\square$

Proposition 13 already shows that neither $|\langle g \rangle| \mathbb{Z}_{\mathbb{Q}(g)} \subseteq \mathbb{Z}[G]$ nor $\exp(G)\mathbb{Z}_{\mathbb{Q}(G)} \subseteq \mathbb{Z}[G]$ is true in general. Also the dual statements, motivated by Lemma 11, $\chi(1)\mathbb{Z}_{\mathbb{Q}(\chi)} \subseteq \mathbb{Z}[G]$ and

$$\mathrm{lcm}\{\chi(1) : \chi \in \mathrm{Irr}(G)\}\mathbb{Z}_{\mathbb{Q}(G)} \subseteq \mathbb{Z}[G]$$

do not always hold. Using GAP [5] and MAGMA [1] we computed the following example: The group

$$G = \texttt{SmallGroup}(48, 3) \cong C_4^2 \rtimes C_3$$

gives $K := \mathbb{Q}(G) = \mathbb{Q}_{12}$ and $\mathbb{Z}[G] = \mathbb{Z}[2\sqrt{-1}, \zeta]$ where ζ is a primitive third root of unity. Hence, $\mathbb{Z}_K/\mathbb{Z}[G] \cong C_2^2$, but $\mathrm{lcm}\{\chi(1) : \chi \in \mathrm{Irr}(G)\} = 3$.

For a single entry $\omega = \chi(g)$ of the character table of G the group $\mathbb{Z}_{\mathbb{Q}(\omega)}/\mathbb{Z}[\omega]$ usually has nothing to do with G. For instance, $G = D_{26} \times C_3$ has a character value ω such that $\mathbb{Z}_{\mathbb{Q}(\omega)}/\mathbb{Z}[\omega]$ is cyclic of order $5^2 \cdot 157 \cdot 547$. It is not hard to show that every algebraic integer of an abelian number field occurs in the character table of some finite group (see proof of [4, Theorem 6]).

For 2-groups the gap between G and $\mathbb{Z}_K/\mathbb{Z}[G]$ can get even bigger than in Proposition 13: The exponent and the largest character degree of $G = \texttt{SmallGroup}(2^9, 6480850)$ is 8, but

$$\mathbb{Z}_K/\mathbb{Z}[G] \cong C_{64} \times C_8 \times C_4.$$

Similarly, the group $G = \texttt{SmallGroup}(2^9, 60860)$ yields $|\mathbb{Z}_K/\mathbb{Z}[G]| = 2^{33}$.

For non-nilpotent groups, the arguments from the last section drastically fail as our next example shows. Let

$$G = \texttt{SmallGroup}(240, 13) \cong C_{15} \rtimes D_{16}$$

where the dihedral group D_{16} acts with kernel D_{16}' (commutator subgroup) on C_{15}. Then $K = \mathbb{Q}_{120}$ and $2\mathbb{Z}_{\mathbb{Q}(g)} \subseteq \mathbb{Z}[G]$ for all $g \in G$, but

$$\mathbb{Z}_K/\mathbb{Z}[G] \cong C_{120}^2 \times C_{60}^2 \times C_{12}^4 \times C_4^4 \times C_2^{14}.$$

Now we consider some simple groups which support Conjecture C.

Proposition 14.

(i) Let $G = \mathrm{PSL}(2, q)$ for some prime power $q \neq 1$. Then $\mathbb{Z}_{\mathbb{Q}(G)} = \mathbb{Z}[G]$.

(ii) Let $G = \mathrm{Sz}(q)$ for $q \geq 8$ an odd power of 2. Then $\mathbb{Z}_{\mathbb{Q}(G)}/\mathbb{Z}[G] \cong C_2^a$ where $a = \varphi((q^2+1)(q-1))/32$.

Proof.

(i) Assume first that $q \geq 5$ is odd. Then G has two irreducible characters taking only rational values and three families χ_i, θ_j, η_k taking (potentially) irrational values (see [3, Theorem 38.1] for instance). Let ζ_n be a primitive n-th root of unity and let $\epsilon := (-1)^{(q-1)/2}$. Set $r := (q-1)/2$ and $s := (q+1)/2$. Then the values of the χ_i lie in $K := \mathbb{Q}(\zeta_r + \overline{\zeta_r})$ and they contain the integral basis from Lemma 4. Similarly the values of the θ_j generate the ring of integers of $L := \mathbb{Q}(\zeta_s + \overline{\zeta_s})$. Finally, the values of the η_k generate the ring of integers of $M := \mathbb{Q}(\sqrt{\epsilon q})$. The discriminants of K, L and M are pairwise coprime by Proposition 1. Hence, by Proposition 2 we have

$$\mathbb{Z}[G] = \mathbb{Z}_K \mathbb{Z}_L \mathbb{Z}_M = \mathbb{Z}_{KLM} = \mathbb{Z}_{\mathbb{Q}(G)}.$$

For q a power of 2, the result follows for $\mathrm{PSL}(2, q) = \mathrm{SL}(2, q)$ with a similar argument from [3, Theorem 38.2].

(ii) The character table of the group $G = \mathrm{Sz}(q)$ was determined by Suzuki in [11, Theorem 13]. We use the names of characters in that theorem. Set $r := q-1$, $s := q+\sqrt{2q}+1$ and $t := q-\sqrt{2q}+1$ and note that these odd numbers are pairwise coprime. Observe that $\mathbb{Q}(G) = KLMN$, the composita of the fields $K = \mathbb{Q}(X_1) = \mathbb{Q}(\zeta_r + \bar{\zeta_r})$, $L = \mathbb{Q}(Y_1) = \mathbb{Q}(\zeta_s + \zeta_s^q + \zeta_s^{q^2} + \zeta_s^{q^3})$, $M = \mathbb{Q}(Z_1) = \mathbb{Q}(\zeta_t + \zeta_t^q + \zeta_t^{q^2} + \zeta_t^{q^3})$ and $N = \mathbb{Q}(W_1) = \mathbb{Q}(\sqrt{-1})$, which have pairwise coprime discriminant by Proposition 1. Now $\mathbb{Z}_K = \mathbb{Z}[\zeta_r + \bar{\zeta_r}] = \mathbb{Z}[X_1]$ and $\mathbb{Z}_L = \mathbb{Z}[\zeta_s + \zeta_s^q + \zeta_s^{q^2} + \zeta_s^{q^3}] = \mathbb{Z}[Y_1]$ and similarly for Z_1. Further $\mathbb{Z}[W_1] = \mathbb{Z}[W_2] = \mathbb{Z}[2\sqrt{-1}]$, hence $\mathbb{Z}_N/\mathbb{Z}[W_1]$ has elementary divisors 1 and 2. Similar to the remark following Lemma 8, we can conclude that $\mathbb{Z}_{KLMN}/\mathbb{Z}[G]$ has elementary divisors 1 and 2 each with multiplicity

$$[KLM : \mathbb{Q}] = \frac{\varphi(r)}{2}\frac{\varphi(s)}{4}\frac{\varphi(t)}{4} = \frac{\varphi((q^2+1)(q-1))}{32}. \qquad \square$$

A minimal simple group (i. e. a simple group with all proper subgroups solvable) is isomorphic to some $\mathrm{PSL}(2, q)$, to some $\mathrm{Sz}(2^{2f+1})$ or to $\mathrm{PSL}(3, 3)$. For the last group one can check easily that $\mathbb{Z}_{\mathbb{Q}(G)} = \mathbb{Z}[G]$. Hence, for minimal simple groups G, the exponent of $\mathbb{Z}_{\mathbb{Q}(G)}/\mathbb{Z}[G]$ is at most 2.

Finally we compute $\mathbb{Z}[G]$ for the alternating group $G = A_n$ of (small) degree n. Let $g \in G$ be non-rational. Then there exists a partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n into pairwise distinct odd parts such that

$$\mathbb{Z}[g] = \mathbb{Z}[(1 + \sqrt{d})/2]$$

where $d = (-1)^{(n-k)/2}\lambda_1 \ldots \lambda_k \equiv 1 \pmod 4$ (see [7, Theorem 2.5.13] for instance). We may write $\sqrt{d} = e\sqrt{d'}$ such that d' is squarefree. Let $K := \mathbb{Q}(g) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$. Then

$$\mathbb{Z}_K = \mathbb{Z}[(1 + \sqrt{d'})/2]$$

and we obtain $e\mathbb{Z}_K \subseteq \mathbb{Z}[g]$. Note that $e^2 \mid d \mid n! = 2|G|$. Since the discriminant of K is $d' \equiv 1 \pmod 2$, it follows that $|\mathbb{Z}_{\mathbb{Q}(G)}/\mathbb{Z}[G]|$ is odd by Proposition 2. It seems fairly difficult to determine the precise structure of $\mathbb{Z}_{\mathbb{Q}(G)}/\mathbb{Z}[G]$. For $n \geq 25$, a theorem by Robinson–Thompson [10] states that

$$\mathbb{Q}(G) = \mathbb{Q}(\sqrt{p^*} : p \text{ odd prime }, n-2 \neq p \leq n)$$

where $p^* := (-1)^{\frac{p-1}{2}} p$. By Proposition 2, $\mathbb{Z}_{\mathbb{Q}(G)}$ is generated as abelian group by all products of the elements $(1 + \sqrt{p^*})/2$ with p as above. The following table lists the (non-trivial) elementary divisors of $\mathbb{Z}_{\mathbb{Q}(G)}/\mathbb{Z}[G]$ for $n \leq 31$. In every case Conjecture C is fulfilled.

n	$\mathbb{Z}_{\mathbb{Q}(A_n)}/\mathbb{Z}[A_n]$
≤ 11	1
$12, 13, 14$	3^4
15	$3^4 \times 15^4 \times 45^4$
16	$3^4 \times 15^4$
17	$3^{12} \times 9^4 \times 45^4 \times 135^4$
18	$3^8 \times 15^8 \times 45^8$
19	$3^8 \times 15^8$
20	$3^{36} \times 9^{12} \times 45^{32} \times 10395^{28} \times 31185^4$
21	$3^{36} \times 105^4 \times 315^{12}$
22	$3^{52} \times 105^8 \times 315^{52} \times 945^4$
23	$3^{64} \times 4095^{32}$
24	1
25	$3^{32} \times 15^{32} \times 315^{32}$
26	$3^{38} \times 15^{40} \times 45^{40} \times 315^{56} \times 945^8$
27	$3^{112} \times 9^{112} \times 27^{16}$
28	$3^{96} \times 15^{80} \times 45^{48}$
29	$3^{224} \times 15^{128}$
30	$3^{128} \times 105^{128}$
31	3^{256}

Acknowledgment

The work on this paper started with a visit of the first author at the University of Jena in January 2019. He appreciates the hospitality received there. The authors also like to thank Thomas Breuer for making them aware of the CoReLG package [2] of GAP [5] which was used for computations with alternating groups. The first author is a postdoctoral researcher of the FWO (Research Foundation Flanders). The second author is supported by the German Research Foundation (SA 2864/1-1 and SA 2864/3-1).

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] H. Dietrich, P. Faccin and W. A. de Graaf, *CoReLG - a GAP package*, Version 1.20 (2014), `http://users.monash.edu/~heikod/corelg/`.

[3] L. Dornhoff, *Group representation theory. Part A: Ordinary representation theory*, Pure and Applied Mathematics, Vol. 7, Marcel Dekker, Inc., New York, 1971.

[4] B. Fein and B. Gordon, *Fields generated by characters of finite groups*, J. London Math. Soc. (2) **4** (1972), 735–740.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.0*; 2018, (`http://www.gap-system.org`).

[6] B. Huppert, *Character theory of finite groups*, De Gruyter Expositions in Mathematics, Vol. 25, Walter de Gruyter & Co., Berlin, 1998.

[7] G. James and A. Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its Applications, Vol. 16, Addison-Wesley Publishing Co., Reading, Mass., 1981.

[8] G. Navarro, *Character theory and the McKay conjecture*, Cambridge Studies in Advanced Mathematics, Vol. 175, Cambridge University Press, Cambridge, 2018.

[9] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, Vol. 322, Springer-Verlag, Berlin, 1999.

[10] G. R. Robinson and J. G. Thompson, *Sums of squares and the fields* $\mathbb{Q}_{A_n}$, J. Algebra **174** (1995), 225–228.

[11] M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. (2) **75** (1962), 105–145.

[12] X. Wang and A. Weiss, *Permutation summands over* $\boldsymbol{Z}$, J. Number Theory **47** (1994), 413–434.