On the annihilating ideal for trace forms

Martin Epkenhans


<http://www.numdam.org/item?id=JTNB_2003__15_1_115_0>
On the annihilating ideal for trace forms

par MARTIN EPKENHANS

Résumé. Nous donnons plusieurs exemples de familles de formes trace dont l'idéal annulateur dans \( \mathbb{Z}[X] \) est principal. Nous montrons aussi qu'en général, cet idéal n'est pas principal.

Abstract. We give several examples of classes of trace forms for which the ideal of annihilating polynomials is principal. We prove, that in general, the annihilating ideal is not a principal ideal.

1. Introduction

My talk given at the 20th Journées Arithmétiques at Limoges in 1997 concludes with a question on the injectivity of a certain map defined in the context of Burnside rings and trace forms. Now we are able to give an affirmative answer. Theorem 6 enables us to reduce questions on trace forms to corresponding questions of trace forms of 2-groups.

Let \( K \) be a field of characteristic different from 2. Since the Witt ring \( W(K) \) over \( K \) is an integral ring we may consider polynomials in \( \mathbb{Z}[X] \) evaluated at an element \( \phi \) of \( W(K) \). We say a polynomial \( p(X) \in \mathbb{Z}[X] \) annihilates \( \phi \) if \( p(\phi) = 0 \) in \( W(K) \).

Definition 1. Let \( M \) be any class of quadratic forms. Then the annihilating ideal \( I_M \) of \( M \) is defined to be

\[
I_M := \{ f(X) \in \mathbb{Z}[X] \mid f(\phi) = 0 \in W(K) \text{ for all } \phi \in M \}.
\]

During the last 15 years several examples of annihilating polynomials of quadratic forms have appeared in the literature. Let us first recall some of these results and present them in the context of annihilating ideals. D. Lewis [11] gives an annihilating polynomial for quadratic forms of dimension \( n \).

Theorem 1 (Lewis). Let \( Q_n \) be the class of all quadratic forms of dimension \( n \). Then \( I_{Q_n} \) is a principal ideal generated by the Lewis polynomial

\[
p_n(X) := \begin{cases} 
X(X^2 - 2^2)(X^2 - 4^2) \cdots (X^2 - n^2), & \text{if } n \equiv 0 \text{ mod } 2, \\
(X^2 - 1^2)(X^2 - 3^2) \cdots (X^2 - n^2), & \text{if } n \equiv 1 \text{ mod } 2.
\end{cases}
\]

Manuscrit reçu le 26 novembre 2001.
As usual, \((a) = aR\) denotes the principal ideal generated by the element \(a \in R\).

**Example 1.** Let \(P_n\) be the class of all \(n\)-fold Pfister forms. Then \(I_{P_n} = (X^2 - 2^n X)\).

Now let us recall the definition of the trace form. Let \(A\) be a finite dimensional étale \(K\)-algebra. With it we associate the quadratic form

\[
<A/K>: A \to K : x \mapsto \text{trace}_{A/K}(x^2),
\]

which is called the trace form of \(A/K\). From some unpublished result of P. E. Conner [2] we get the following theorem.

**Theorem 2 (Conner).** Let \(T_n\) be the class of trace forms of all separable field extensions of degree \(n\) of fields of characteristic \(\neq 2\). Then \(I_{T_n} = (C_n(X))\), where \(C_n(X) = \prod_{k \geq 0, p_n(k) = 0} (X - k)\).

In a certain sense, the result of P.E. Conner has been improved first by P. Beaulieu and T. Palfrey [1] and later on by D. Lewis and S. McGarraghy [12]. Consider a separable field extension \(L/K\) of degree \(n\) and let \(N/K\) be a normal closure of \(L/K\). Let \(f(X) \in K[X]\) be the minimal polynomial of a primitive element \(\alpha\) of \(L/K\). Then Beaulieu and Palfrey introduced the notion of the Galois number of a polynomial \(f(X)\). This number is defined to be the smallest number \(g_f\) such that any \(g_f\) roots of \(f(X)\) generate a splitting field of \(f(X)\). In a group theoretical context the Galois number of a \(G\)-set is defined to be the smallest natural number \(g\) such that any group element \(\sigma \in G\) with \(g\) fixed points acts as the identity. This number is also called the minimal degree of a permutation representation. See [9] for the determination of Galois numbers of doubly transitive groups. Now the polynomial of Beaulieu and Palfrey is defined to be

\[
B_f(X) := (X - n) \cdot \prod_{k = 0}^{g-1} (X - k) \text{ mod } 2
\]

**Theorem 3 (Beaulieu-Palfrey).** The polynomial \(B_f(X)\) has the property that \(B_f(\phi) = 0 \in W(K)\), where \(\phi\) is isometric to the trace form of the field extension given by the separable and irreducible polynomial \(f(X) \in K[X]\).

Denote the Galois group of \(N/K\) by \(G(N/K)\). Then the action of \(G(N/K)\) on the left cosets of \(G(N/K)/G(N/L)\) defines a \(G\)-set. For any \(G\)-set \(S\) of cardinality \(n\) and any subgroup \(U < G\) let \(\text{inv}_U(S) := \#\{s \in S \mid s^\sigma = s \text{ for all } \sigma \in U\}\) be the number of fixed points of the restricted action. Set \(\text{inv}(S) := \{\text{inv}_U(S) \mid U < G\}\). The definition of the following polynomial is due to Lewis and McGarraghy (see [12, corollary 3.5]). For
any $G$-set $S$ set

$$\varphi(S) := \{ \text{inv}_U(S) \mid U < G, \text{inv}_U(S) \equiv \text{u} \mod 2 \}. $$

Now set

$$p_{G,S} := \prod_{k \in \varphi(S)} (X - k).$$

**Theorem 4** (Lewis-McGarraghy). Let $L/K$ be a finite and separable field extension and let $p_{G,S}(X)$ be defined as above. Then $p_{G,S}(X)$ annihilates the trace form of $L/K$.

Note, that the result above can be generalized to trace forms of étale algebras. Using Springer's theorem on the lifting of quadratic forms according to odd degree extensions, we get annihilating polynomials of lower degree (see [8, Theorem 2.10]).

Now we come to the definition of the class of quadratic forms we like to discuss in this paper.

**Definition 2.** Let $G$ be a finite group and let $H < G$ be a subgroup with $\cap_{\sigma \in G} H\sigma^{-1} = 1$. Then the class $M(G, H)$ consists of those quadratic forms $\phi$ such that

1. there exists an irreducible and separable polynomial $f(X) \in K[X]$ with Galois group $\text{Gal}(f)$ isomorphic to $G$;
2. the action of $\text{Gal}(f)$ on the roots of $f(X)$ and the action of $G$ on the left cosets $G/H$ are equivalent;
3. $\phi$ and the trace form $<(K[X]/(f(X)))/K>$ are isometric.

Note, that the condition on $H$ guarantees, that $G$ acts faithfully on $G/H$. The work of Lewis [11] and Conner [2] give annihilating polynomials for quadratic forms, resp. trace forms of dimension $n$. To finish the determination of the annihilating ideal, we have to consider signatures. The zeros of $p_n(X)$, resp. $C_n(X)$ are exactly those integers, which occur as signature values of quadratic forms in $Q_n$, resp. $T_n$.

**Definition 3.** Let $M$ be a class of quadratic forms. Then the set of signatures of $M$ is denoted

$$\text{sign}(M) := \{ s \in \mathbb{Z} \mid s = \text{sign } \phi \text{ for some } \phi \in M \}. $$

If $\text{sign}(M)$ is finite, the signature polynomial of $M$ is given by

$$\text{Sign}_M(X) := \prod_{k \in \text{sign}(M)} (X - k).$$

Since the signature is a ring homomorphism we get
Proposition 1. Let $M$ be a class of quadratic forms. If $\text{sign}(M)$ is a finite set, then

$$I_M \subset (\text{Sign}_M(X)).$$

Otherwise, we get $I_M = (0)$.

The signature of a trace form $<L/K>$ equals the number of real embeddings of $L$ into $\mathbb{R}$, which is the number of real roots of a polynomial $f(X)$ with $L \cong K[X]/(f(X))$ (see [13]). This observation gives rise to the definition of a signature in a group theoretical setting.

Definition 4. Let $S$ be a finite $G$-set and $\sigma \in G$ with $\sigma^2 = 1$. Then

$$\text{sign}_\sigma(S) := \#\{s \in S \mid \sigma^2 = s\}$$

is called the signature of $S$ according to $\sigma$.

$$\text{sign}(S) := \{\text{sign}_\sigma(S) \mid \sigma \in G, \sigma^2 = 1\}$$

is the set of signatures of $S$.

Observe, that $\text{sign}_\sigma(S) = \text{inv}_{<\sigma>}(S)$. From proposition 3 in [6] we conclude

Proposition 2. Let $G$ be a finite group and let $H$ be a subgroup of $G$ with $\cap_{\sigma \in G} \sigma H \sigma^{-1} = 1$. Then

$$\text{Sign}(M(G,H)) = \text{Sign}(G/H).$$

2. Burnside rings

The proofs of Conner, Beaulieu-Palfrey and Lewis-McGarraghy are based on certain identities in the Burnside ring $B(G)$ of $G$ and translated into identities in the Witt ring by applying a homomorphism given by Dress [5] (see also [7, proposition 3]).

Let $B(G)$ denote the Burnside ring of $G$-sets (for more details see [4, chapter 11 §80]). Let $\chi_H^G$ denote the $G$-set given by the action of $G$ on the set of left cosets $G/H$. Let $S = S(G)$ be a full set of nonconjugate subgroups of $G$. By corollary 80.6 in [4]

$$B(G) = \oplus_{H \in S} \mathbb{Z} \cdot \chi_H^G.$$

For any $\sigma \in G, \sigma^2 = 1$, the definition of signatures given in definition 4 gives rise to a signature homomorphism

$$\text{sign}_\sigma : B(G) \to \mathbb{Z}.$$

Let $L(G) := \cap_{\sigma \in G, \sigma^2 = 1} \ker(\text{sign}_\sigma)$ be the kernel of the total signature homomorphism. For any Galois extension $N/K$ with Galois group $G(N/K)$ isomorphic to $G$ there is a ring homomorphism $h_{N/K} : G \to W(K)$. Let $T(G) := \cap \ker(h_{N/K})$ denote the trace ideal of $G$ (see [6],[7],[8] for more details). Here $N/K$ runs over all Galois extensions of fields of characteristic
\( \not= 2 \) with Galois group \( G(N/K) \simeq G \). Then \( T(G) \subset L(G) \). Theorem 16 in [7] states

**Theorem 5.** Let \( G \) be a finite group. Then \( L(G)/T(G) \) is a finite 2-group.

\[
(B(G)/T(G))_{\text{tor}} = L(G)/T(G)
\]

and the only torsions in \( B(G)/T(G) \) are 2-torsions.

Together with proposition 1 we conclude

**Corollary 1.** Let \( G \) be a finite group and let \( H \) be a subgroup with

\[
\bigcap_{\sigma \in G} \sigma H \sigma^{-1} = 1.
\]

Then there is an integer \( l \in \mathbb{N}_0 \) such that

\[
(2^l \cdot \text{Sign}_{M(G,H)}(X)) \subset I_{M(G,H)} \subset (\text{Sign}_{M(G,H)}(X)).
\]

We can choose \( 2^l \) to be the exponent of the finite abelian 2-group \( L(G)/T(G) \).

Let \( (a : b) := \{ x \in R \mid xb \subset a \} \) be the ideal quotient of the ideals \( a, b \) in the ring \( R \). Then

\[
I_{M(G,H)} = (I_{M(G,H)} : (\text{Sign}_{M(G,H)}(X))) \cdot (\text{Sign}_{M(G,H)}(X)).
\]

Since \( I_{M(G,H)} \) contains monic polynomials, we get

**Corollary 2.** \( I_{M(G,H)} \) is a principal ideal if and only if

\[
I_{M(G,H)} = (\text{Sign}_{M(G,H)}(X)).
\]

We introduce some more notation. For any subgroup \( H \) of \( G \) let \( \text{res}_H^G : B(G) \longrightarrow B(H) \) denote the restriction homomorphism (see [7]). Let \( < a_1, \ldots, a_n > \) denote the diagonal matrix with diagonal entries \( a_1, \ldots, a_n \).

For \( n \in \mathbb{N} \) and a matrix \( A \) denote the \( n \)-fold orthogonal sum by \( n \times A := \bigoplus_{i=1}^n A \).

**Proposition 3.** Let \( e(G) \) denote the exponent of \( L(G)/T(G) \). If any subgroup of a 2-Sylow subgroup \( G_2 \) of \( G \) is a normal subgroup in \( G_2 \), then

\[
(e(G)/2) \cdot \text{Sign}_{M(G,H)}(X) \in I_{M(G,H)}.
\]

**Proof.** The proof of proposition 4.3 in [8] implies \( \text{res}_{G_2}^G(\text{Sign}_{M(G,H)}(X_G^G)) \in 2 \cdot B(G) \). Since \( \text{Sign}_{M(G,H)}(X_H^G) \in L(G) \) we are done by corollary 1.

The following theorem gives an affirmative answer to a question asked in [7]. With it we are able to translate certain problems on annihilating polynomials to the corresponding problems over 2-groups.
Theorem 6. Let $G$ be a finite group with 2-Sylow subgroup $G_2$. Then for any element $\chi \in B(G)$ we get

$$\chi \in T(G) \iff \text{res}_{G_2}^G(\chi) \in T(G_2).$$

Hence the restriction homomorphism induces an injection

$$L(G)/T(G) \hookrightarrow L(G_2)/T(G_2).$$

Proof. From lemma 4.2a in [6] we know $\text{res}_{G_2}^G(\chi) \in T(G_2)$ implies $\chi \in T(G)$. Let $n := \text{ord}(G)$ and let $N/K$ be a Galois extension with Galois group $G(N/K) \simeq G_2$. Set $L := K(X_1, \ldots, X_n)$, where $X_1, \ldots, X_n$ are algebraically independent indeterminates. The regular representation of $G$ defines a monomorphism $G \to \mathfrak{S}(\{X_1, \ldots, X_n\})$, where $\mathfrak{S}(\{X_1, \ldots, X_n\})$ denotes the symmetric group of the set $\{X_1, \ldots, X_n\}$. Hence $G$ is a subgroup of the group of automorphisms $\text{Aut}_K(L)$. Set $F := L^G$ and $F_2 := L^{G_2}$.

Since $G$ acts transitively on $\{X_1, \ldots, X_n\}$, the polynomial

$$f(X) := (X - X_1) \cdots (X - X_n)$$

is irreducible over $F$. Hence $X_1$ is a primitive element of $L/F$ and of $L/F_2$. Assume, that $X_1, \ldots, X_m, m := \text{ord}(G_2)$ are the conjugates of $X_1$ over $F_2$. For any $H < G_2$ we can choose a primitive element $\alpha_H$ of $L^H/F_2$ of the form $\sum_{i=0}^{m-1} g_i X_i^t$ with $g_i \in L[X_1, \ldots, X_n] \cap F_2 := R$.

Let $\chi \in T(G)$. Then $h_{L/F}(\chi) = 0$ implies $\text{res}_{G_2}^G(\chi) = \sum_{H \in S} m_H \chi_H \in \ker(h_{L/F_2})$, where $H$ runs over a full set $S$ of nonconjugate subgroups of $G_2$. For any $H \in S$ calculate a matrix $M_H$ of $\langle N^H/F_2 \rangle$ with respect to the $F_2$-basis $1, \alpha_H, \ldots, \alpha_H^{[G_2:H]-1}$. Hence $M_H \in \text{Gl}(n_H, R)$ with $n_H := [G_2 : H]$. Since $h_{L/F_2}(\text{res}_{G_2}^G(\chi)) = 0 \in W(F_2)$, there is a matrix $A \in \text{Gl}(t, R)$ and a non-zero polynomial $g \in R$ with

$$A \cdot (\oplus_{H \in S} m_H M_H) \cdot A^T = g^2 \cdot (t/2x < 1, -1 >).$$

Let $\alpha \in N$ be a primitive element of $N/K$ and let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_m$ be the conjugates of $\alpha$ over $N^{G_2}$. Label these elements according to the action of $G_2$ on $\{X_1, \ldots, X_m\}$.

Now we choose algebraically independent indeterminates $Y_1, \ldots, Y_m$ and set $Z_1 := Y_1 + \alpha_1 Y_2 + \alpha_1^2 Y_3 + \ldots + \alpha_1^{m-1} Y_m, \ldots, Z_m := Y_1 + \alpha_1 Y_2 + \alpha_2 Y_3 + \ldots + \alpha_m^{m-1} Y_m$. By looking at the Vandermonde determinant we see that $Z_1, \ldots, Z_m$ are algebraically independent. Replace $X_1, \ldots, X_m$ by $Z_1, \ldots, Z_m$. Denote the new polynomials resp. matrices by $\bar{g}$, resp. $\bar{M}_H$. Hence $\bar{A} \cdot (\oplus_{H \in S} m_H \bar{M}_H) \cdot \bar{A}^T = \bar{g}^2 \cdot (t/2x < 1, -1 >)$, and $\bar{g} \neq 0$. Since the set of primitive elements of a separable field extension is a non-empty Zariski-open subset, there is an $n$-tuple $a = (a_1, \ldots, a_n) \in K^n$, such
that $\bar{\sigma}(a_1, \ldots, a_n) \neq 0$ and for any $H \in S$ the element $\sum_{i=0}^{m-1} \bar{\sigma}_i(a)\alpha_i^i$ is a primitive element of $N^H/K$. We get
\[ \bar{A}(a) \cdot [\Phi_{H \in S} m_H \bar{M}_H(a)] \cdot \bar{A}(a)^T = \bar{\sigma}(a)^2 \cdot (t/2 < 1, -1 >), \]
and $\bar{\sigma}(a) \in K, \bar{A}(a) \in M(t, K), \bar{M}_H(a) \in M(n_H, K)$. Hence $h_{N/K}(\text{res}^{G_2}_G(\chi)) = 0 \in W(K)$.

3. Groups with quaternion 2-Sylow subgroups

This section contains a class of examples, where $I_{M(G,H)}$ is not a principal ideal.

**Proposition 4.** Let $G$ be a finite group with 2-Sylow subgroup a quaternion group of order 8. Let $H \leq G$ be a subgroup of $G$ with $\langle H \rangle = 1$.

Then
\[ (a) \text{ord}(H) \equiv 1 \mod 2, \]
\[ (b) \text{ord}(H) \equiv 2 \mod 4, \]
\[ (c) \text{ord}(H) \equiv 0 \mod 4 \text{ and the permutation representation of } G \text{ on } G/H \text{ contains only even permutations.} \]

(2) Let $\text{ord}(H) \equiv 0 \mod 4$ and suppose, that the permutation representation of $G$ on $G/H$ contains an odd permutation.

(a) Then $G$ is a semidirect product of $G_2$ and a normal subgroup $A$ of odd order. The conjugation of $G_2$ on $A$ induces a monomorphism $\Phi : G_2 \to \text{Aut}(A)$.

(b) Let $n := [G : H]$ and $s := \text{sign}_G \chi_H$ with $\sigma \in G_2$ the unique involution of $G_2$. Then
\[ I_{M(G,H)} = \begin{cases} (X, 2) \cdot ((X - n)(X - s)), & \text{if } n \equiv 4 \mod 8, \\ (X - 1, 2) \cdot ((X - n)(X - s)), & \text{if } n \equiv 0 \mod 8. \end{cases} \]

**Proof.** 1) see proposition 5.2 in [8]. 2(a) follows from lemma 5.2 in [8].

2(b): We use the notation of §5 in [8]. By proposition 3, theorem 6 and [6, proposition 7] we get $2(X - n)(X - s) \in I_{M(G,H)}$.

Assertion. $X(X - n)(X - s) \in I_{M(G,H)}$ if $8 \nmid n$.

By proposition 7 in [6] we have to determine the coefficients $m_i$ of $\chi_H$ in $\text{res}^{G_2}_{G_2}(\chi_H^c(\chi_H^c - n\chi_H^c)(\chi_H^c - s\chi_H^c))$. Since $\alpha = 0$ we get $m_i = a'b_i + 2b_i^2(2b_i - n - s)$. Observe, that $a' = ns \equiv 0 \mod 4$ and $n + s \equiv 2a \equiv 0 \mod 4$. Hence $m_i \equiv 0 \mod 4$. We conclude $(2, X) \subset (I_{M(G,H)} : (\text{Sign}_{M(G,H)}(X)))$. By the preceding theorem and by proposition 5.5 in [8] $\text{Sign}_{M(G,H)}(X) \notin I_{M(G,H)}$. Since $(2, X)$ is a maximal ideal in $\mathbb{Z}[X]$, we are done.

The case $8 \mid n$ is left to the reader. □

The smallest example is as follows. The automorphism group of $A = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a double cover of $\mathfrak{S}_4$, which contains $Q_8$ as a subgroup.
Set $G := A \times Q_8$ and let $H$ be a subgroup of order 4 in $G$. Then $I_{M(G,H)} = (X, 2) \cdot ((X - 18)(X - 2))$ (see [8, Example 5.6]).

4. Some more 2-groups

**Lemma 1.** Let $G$ be a finite 2-group and let $H = \langle \tau \rangle$ be a subgroup of order 2 in $G$ with $\cap_{\sigma \in G} H \sigma^{-1} = 1$. Then
\[
\text{Sign}_{M(G,H)}(X) = X(X - \text{sign}_r \chi_H)(X - \text{ord}(G)/2); \\
\text{sign}_r \chi_H = \text{ord}(C_G(\tau))/2; \\
I_{M(G,H)} = (\text{Sign}_{M(G,H)}(X)).
\]

Here $C_G(\tau)$ denotes the centralizer of $\tau$ in $G$.

**Proof.** Set $n := [G : H] = \text{ord}(G)/2$. Since $\tau$ is not contained in the non-trivial center of $G$, we get $X \subseteq X$ by lemma 3.3(2) in [8]. Now proposition 10 and corollary 11 in [7] gives the result on $\text{Sign}_{M(G,H)}(X)$ and the signature value.

We easily calculate $\chi_H^2 = \text{sign}_r(\chi_H) \cdot \chi_H + \frac{n - \text{sign}_r \chi_H}{2} \cdot \chi_1$. Hence
\[
\text{Sign}_{M(G,H)}(\chi_H) = (\chi_H^2 - \text{sign}_r(\chi_H) \cdot \chi_H)(\chi_H - n \chi_G) \\
= \frac{n - \text{sign}_r \chi_H}{2} \cdot \chi_1 \cdot (\chi_H - n \chi_G) \\
= \frac{n - \text{sign}_r \chi_H}{2} \cdot (n \chi_1 - n \chi_1) = 0.
\]

\[
\square
\]

5. Examples

Finally, let us summarize some examples, where $I_{M(G,H)}$ is a principal ideal.

**Theorem 7.** In the following cases we get
\[
I_{M(G,H)} = (\text{Sign}_{M(G,H)}(X))
\]

1. $G$ has odd order. Then $I_{M(G,H)} = (X - n)$.
2. $G_2$ is elementary abelian or cyclic.
3. $G_2$ is a dihedral group of order $2^m \geq 8$.
5. $G$ is abelian.
6. $G$ is a Frobenius group.
7. $G$ is a Zassenhaus group $\neq PML(2,q)$.
8. $G = 2G_2(q), q = 3^{2m+1}, m \geq 1$ the Ree group in its doubly transitive permutation representation of degree $q^3 + 1$ and $H$ a one point stabilizer.
(9) $G$ a group of order $\leq 31$.
(10) $G = Q_{2l}, M(2^l), QD_{2l}$.

There exists four groups of order $2^{l+1} \geq 8$, which contain an element of order $2^l$. Beside the dihedral group $D_{2l}$ there are the generalized quaternion group $Q_{2l}$, the quasidihedral group $QD_{2l}$ and the group $M(2^l)$ (see [10][I. Satz 14.9]).

Proof. For (1) see [3] corollary 1.6.5, resp. proposition 17 in [7]. Use proposition 3 and [6, propositions 5 and 6] to prove (2). (3) follows from proposition 5.1 in [8].

4) If $H = 1$, then $\Sigma_{M(G,H)}(X) = B_{G,H}(X) = X - n$, resp. $= X(X - n)$.

5) The condition on $H$ implies $H = 1$.

(6), (7) and (8) follow from [8, propositions 6.1, 6.3 and 3.4].

9) By (1), (2), (3) and (5) it remains to consider non-abelian groups of order $n = 8, 16, 24$ and the case $n = 24, G_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

$n = 8$. Apply (3), resp. (5) in the case of the quaternion group.

$n = 16$. Any subgroup $H < G$ of order $\geq 4$ has a non-trivial intersection with the center of $G$ (see [14]). Now use lemma 1.

$n = 24$. The result for $G_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ follows from some unpublished determination of the exponent of $L(G)/T(G)$ for $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^l\mathbb{Z}$.

Since there is no injection $Q_8 \hookrightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z})$, we are done by proposition 4. (10) follows from lemma 1, since any subgroup $H$ of $G$ of order $\geq 4$ has a non-trivial intersection with the center of $G$.  \hfill $\Box$

References


Martin Epkenhans  
Fb Mathematik  
Universität Paderborn  
D-33095 Paderborn  
Deutschland  
E-mail: martine@uni-paderborn.de