Self-dual modules and self-dual codes for finite groups

Conchita Martínez-Pérez*
Departamento de Matemáticas
Universidad de Zaragoza,
50009 Zaragoza

Wolfgang Willems
Institut für Algebra und Geometrie
Fakultät für Mathematik
Otto-von-Guericke-Universität
39016 Magdeburg

1 Introduction

Self-dual codes are of special interest and many of them are acted on by a non-trivial group. So we may ask the question:

Under what conditions on a finite field K and a finite group G does there exist a KG-module V which carries a nondegenerate G-invariant K-bilinear form, say b, and has a self-dual G-invariant code, i.e. a KG-submodule C which satisfies $C = C^{\perp}$ with respect to b.

Note that a KG-module V carries a nondegenerate G-invariant bilinear form if and only if $V \cong V^* = \mathrm{Hom}_K(KG, K)$ as KG-modules where the action of G on V^* is given by

$$v(fg) = (vg^{-1})f \text{ for } v \in V,\ f \in V^*,\ g \in G.$$

The nondegenerate forms b and the isomorphisms $\alpha : V \to V^*$ are related by

$$b(v, v') = (v\alpha)v' \qquad (v, v' \in V)$$

*Most of this work was carried out while the author was visiting the Otto-von-Guericke University of Magdeburg in August 2002. She was supported by the Department of Mathematics and by BFM2001-1667-C03-01.

(see [5], VII, 8.10). Throughout the paper b will always be symmetric. So we do not have to distingish between the right and left orthogonal $C^\perp$ of C. Furthermore the ambient space V will always be endowed with an orthonormal basis with respect to b.

If $V = KG$ is a group-algebra the above question has been answered partially in [13], [4] and in full generality in [16] for the standard form b which is defined by $b(g,h) = \delta_{g,h}$ for $g, h \in G$. It was shown that a self-dual G-invariant code $C \leq KG$ exists if and only if K is of characteristic 2 and 2 divides $|G|$. The binary extended $[24, 12, 8]$ Golay-code may serve here as an example (see [2]). In order to find the ternary extended $[12, 6, 6]$ Golay-code one can choose a 3-block B for V in the group algebra $\mathbb{F}_3\mathrm{SL}_2(3)$ with the elements of the alternating group A_4 on four letters as a natural basis since B is isomorphic to a twisted group-algebra $\mathbb{F}_3^\alpha\mathrm{A}_4$ (see [2]).

Dealing with the general problem which we stated at the beginning we are faced with many questions in representation theory. So we first concentrate on self-duality in representation theory. On the way we prove the remarkable fact that a group of odd order has a non-trivial self-dual irreducible module in characteristic 2 if and only if it has an irreducible module of even dimension. Note that the only if part is Fong's lemma ([5], VII, 8.13). Exploiting representation theoretical methods which we develop in section 4 we get many new results in coding theory; for instance on the existence of self-dual extended group codes, in particular on quasi-cyclic codes. Results are also obtained for weights in such codes. So we prove that there is a binary self-dual extended group code if the length of the code is divisible by 8. Note that this is the converse of a well-known result of Gleason ([15], 6.3.8) provided the code is a group code. The powerful methods of representation theory are also used to give new proofs of known coding theoretical facts.

Throughout the paper all modules are assumed to be of finite dimension over the underlying field. For facts in group and representation theory we refer to [1] or chapter VII in [6], and for coding theoretical facts to [11].

2 Preliminaries

In this section we collect some known facts about modules over group algebras which we freely use in the sequel. By K and F we denote fields and by G a finite group.

Lemma 2.1 *Let $W = e \oplus_{i=1}^n V_i$ be a KG-module with irreducible pairwise non-isomorphic KG-modules V_i. Then, for n odd, $W \cong W^*$ implies $V_i \cong V_i^*$ for some i.*

Proof: By the Krull-Schmidt Theorem, the assumption $W \cong W^*$ implies $\{V_1, \dots, V_n\} = \{V_1^*, \dots, V_n^*\}$ up to isomorphisms. Now, if $V_i \ncong V_i^*$ for all i then n must be even.

Lemma 2.2 *Let F/K be a finite Galois extension with Galois group Γ. If W is an irreducible KG-module, then*

a) $W \otimes_K F \cong e \oplus_{\alpha \in U} V^\alpha$ with $e \in \mathbb{N}$, $U \leq \Gamma$ and V an irreducible FG-module. Furthermore, if $\operatorname{char} K > 0$ then $e = 1$.

b) $W \cong W^*$ if and only if $W \otimes_K F \cong (W \otimes_K F)^*$, and this happens if and only if $V^* \cong V^\alpha$ for some $\alpha \in U$. Moreover, if $|U|$ is odd then $W \cong W^*$ if and only if $V \cong V^*$. In particular, if $[F/K]$ is odd then there is a non-trivial irreducible self-dual G-module over F if and only if there is one over K.

c) If $[F/K]$ is odd and $\operatorname{char} K > 0$ then there is an irreducible FG-module of even dimension if and only if there is one for KG.

Proof: a) This is 1.18 and 1.15 in ([6], Chap. VII).
b) The first equivalence follows by Deuring-Noether's Theorem (see [6], Chap. VII, 1.22) as $W^* \otimes_K F \cong (W \otimes_K F)^*$. For the second assertion, note that $V^* \cong V^\alpha$ implies $V^\beta = (V^*)^{\alpha^{-1}})^\beta = (V^{\alpha^{-1}\beta})^*$ for all $\beta \in U$, hence $W \otimes_K F \cong (W \otimes_K F)^*$. On the other hand if $W \otimes_K F \cong (W \otimes_K F)^*$ then $V^* \cong V^\alpha$ by the Krull-Schmidt Theorem. Now, assume that $|U|$ is odd. If $W \cong W^*$ then $W \otimes_K F \cong (W \otimes_K F)^*$ and by Lemma 2.1, $(V^\alpha)^* \cong V^\alpha$ for some $\alpha \in U$. Thus we get

$$V^* \cong ((V^\alpha)^*)^{\alpha^{-1}} \cong (V^\alpha)^{\alpha^{-1}} \cong V.$$

The converse holds true since $V \cong V^*$ implies $V^\alpha \cong (V^\alpha)^*$ for all α.
c) By assumption, $\operatorname{char} K > 0$ and therefore $e = 1$ in a). Since $\dim_K W = |U| \dim_F V$ the assertion follows.

Lemma 2.3 *Let K be a finite field of characteristic p with $p \nmid |G|$.*

a) If $|G|$ is odd and $H \leq G$ then every irreducible KH-module occurs in $KG|_H$ with odd multiplicity.

b) If G is abelian all composition factors of KG have multiplicity one.

Proof: This is well-known if we deal with splitting fields. For K, the statements then follow by 2.2 a).

In the sequel we often use Brauer's permutation Lemma which can be found in most books on representation theory. The way we use it here was proved in [7]. In order to state it we need the following notations. Let $\beta_1, \ldots, \beta_k$ denote the set of irreducible Brauer characters of G over an algebraically closed field of characteristic $p > 0$. By a result of Brauer, k is also the number of p-regular conjugacy classes of G (see [5], VII, 3.9). Let $g_1, \ldots, g_k$ denote representatives of these classes. Suppose there is a group, say H, which acts on the one hand on the set of irreducible Brauer characters of G by $\beta_i \to \beta_i^h$ and on the other hand on the set of p-regular classes of G by $g_i^G \to (g_i^G)^h$ for $h \in H$.

Lemma 2.4 (**Brauer's permutation Lemma)** *If the two permutation actions of H satisfy*

$$\beta_i^h(g_j) = \beta_i(g_j^h)$$

for all i, j and all $h \in H$ then we have:
For any $h \in H$ the number of cycles of a fixed length on $\{\beta_1, \ldots, \beta_k\}$ and $\{g_1, \ldots, g_k\}$ is the same. In particular, the number of fixed points of h on the set of irreducible Brauer characters is equal to the number of fixed points on the set of p-regular classes.

In applications the action of H is very often a Galois action. In order to describe this we fix a finite field F of characteristic p. Let K be a subfield of F and let $\Gamma = \mathrm{Gal}(F/K)$. If $|K| = p^a$ and $|F| = p^{ab}$ then to each $\alpha \in \Gamma$ corresponds a unique l with $1 \leq l \leq b$ such that

$$\alpha : f \longrightarrow f^{p^{al}}$$

for $f \in F$. (Remember that α is a power of the Frobenius map.) Now we define the action of Γ on G by

$$\alpha : g \longrightarrow g^{p^{al}}.$$

Let $g, h \in G$ be p-regular elements and suppose that $g^\alpha = (h^\alpha)^x$ for some $x \in G$. Then we obtain

$$g^{p^{al}} = g^\alpha = (h^\alpha)^x = (h^{p^{al}})^x = (h^x)^{p^{al}}.$$

Since g and h are p-regular we have

$$\langle g \rangle = \langle g^{p^{al}} \rangle = \langle (h^x)^{p^{al}} \rangle = \langle h^x \rangle.$$

Thus g and h^x commute and we get

$$(g^{-1}h^x)^{p^{al}} = 1,$$

hence $g = h^x$. This shows that the action of Γ on the p-regular conjugacy classes of G is injective, hence a permutation. Now suppose that F is a splitting field for G. If $\mathrm{IBr}_p(G) = \{\beta_1, \ldots, \beta_k\}$ is the set of irreducible Brauer characters in characteristic p and $\{g_1, \ldots, g_k\}$ a set of representatives for the p-regular conjugacy classes of G then

$$\beta_i^\alpha(g_j) = \beta_i(g_j)^\alpha = \beta_i(g_j)^{p^{al}} = \beta_i(g_j^{p^{al}}) = \beta_i(g_j^\alpha)$$

for all i, j and all $\alpha \in \Gamma$. Thus Brauer's permutation Lemma applies.

In order to deal with the main question which we asked in the Introduction we must know about the existence (or non-existence) of non-trivial irreducible self-dual modules. It turns out that this depends on the size of the underlying field.

3 Splitting fields of prime characteristic

Notations 3.1 For any prime t and any positive integer n with $t \nmid n$ let $s_t(n)$ denote the smallest positive integer such that

$$n \mid t^{s_t(n)} - 1.$$

Obviously, $t^{s_t(n)}$ is the size of a minimal field of characteristic t containing a primitive n-th root of unity and $s_t(n)$ is the order of t in the group $\mathbb{Z}_n^*$ of units in $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Thus $s_t(n) \mid \phi(n)$ where ϕ denotes the Euler function. In particular, if p is a prime then $s_t(p) \mid p-1$. Moreover, if m is any positive integer, then $n \mid t^m - 1$ if and only if $s_t(n) \mid m$. Furthermore, for a finite group G we put

$$s_t(G) = \mathrm{lcm}\,\{s_t(p) | \;\; p \mid |G|,\; p \text{ a prime and } p \neq t\}.$$

Finally, for $s, n \in \mathbb{N}$ we may factorize s into $s = s_n s_{n'}$ where $\gcd(s_{n'}, n) = 1$ and s_n contains only primes which divide n. The factor s_n is called the n-part of s.

Remark 3.2 For a finite group G let K_G denote the finite field of size t^k where

$$k = \mathrm{lcm}\,\{s_t(p^a) \mid \;\; p^a \mid |G|,\; p \text{ a prime},\; a \in \mathbb{N} \text{ and } p \neq t\}.$$

For $g \in G$ let $\mathrm{ord}(g)$ denote the order of g and $\mathrm{ord}_n(g)$ its n-part ($n \in \mathbb{N}$). Thus for any prime $p \neq t$ we have

$$\mathrm{ord}_p(g) \mid t^{s_t(\mathrm{ord}_p(g))} - 1 \mid t^k - 1.$$

In particular, $\mathrm{ord}_{t'}(g) \mid t^k - 1$. Thus, by ([6], Chap VII, 2.6), the field K_G is a splitting field of characteristic t for G and all its subgroups.

Lemma 3.3 *For a prime $p \neq t$ and $a \in \mathbb{N}$ we have*

$$s_t(p^a) = p^j s_t(p) \quad \textit{for some} \quad j \in \{0, 1, \ldots, a-1\}.$$

Proof: We proceed by induction on a. The case $a = 1$ is trivial. So we may assume $a > 1$ and $s_t(p^{a-1}) = p^j s_t(p)$ for some j with $0 \leq j \leq a-2$. Let F resp. K be minimal fields of characteristic t containing a primitive p^a-th root of unity, say β, resp. a primitive p^{a-1}-th root of unity, say α. We may assume that $K \subseteq F$ and $\beta^p = \alpha$. By minimality of F, we have $F = K[\beta]$. If $\beta \notin K$ then $x^p - \alpha \in K[x]$ is irreducible and therefore $\dim_K F = |F : K| = p$. Otherwise we have $F = K$. As $|K| = t^{s_t(p^{a-1})}$ we obtain $t^{p s_t(p^{a-1})} = |K|^p = |F| = t^{s_t(p^a)}$ in the first case, and $s_t(p^{a-1}) = s_t(p^a)$ in the second. Thus the claim follows.

Corollary 3.4

a) $s_t(p^a)_q = s_t(p)_q$ *for all primes* $q \neq p$.

b) $(\log_t |K_G|)_q = s_t(G)_q$ *if q is a prime and $q \nmid |G|$.*

Proof: Assertion a) follows immediately by 3.3. To get b) we have to look only at $s_t(p)$ for primes p with $p \mid |G|$ and $p \nmid t$. By assumption, such primes p satisfy $p \neq q$ and the assertion follows by part a).

Theorem 3.5 *Let G be a finite group and let F be a minimal splitting field for G in characteristic t. If $|F| = t^s$ then for any prime q with $q \nmid |G|$ we have*

$$s_q = s_t(G)_q.$$

In particular, $s_{|G|'}$ can easily be computed.

Proof: We fix a prime q with $q \nmid |G|$. Note that K_G is a splitting field for G, by 3.2. As F is a minimal splitting field we get $F \subseteq K_G$. Now, if $k_t(G) = \log_t |K_G|$ then $s_q \mid k_t(G)_q = s_t(G)_q$, by 3.4.

To prove $s_t(G)_q \mid s_q$ we put $q^a = s_t(G)_q$ and choose a field $K \subseteq K_G$ with $|K_G : K| = q^a$. Note that

$$q^a = s_t(G)_q = \operatorname{lcm}\{s_t(p)_q \mid \ p \mid |G|, \ p \text{ a prime and } p \neq t\}.$$

Clearly, we may assume that $a > 0$. Thus there exists a prime $p \neq t$ for which $s_t(p)_q = q^a$ and an element $x \in G$ of order p. Next, we consider the Galois action of $\Gamma = \mathrm{Gal}(K_G/K)$ on $\langle x \rangle$. If $\Gamma = \langle \alpha \rangle$ then $x^\alpha = x^{t^{k_t(G)/q^a}}$ by the above definition. We claim that the elements

$$x, x^\alpha, x^{\alpha^2}, \ldots, x^{\alpha^{q^a - 1}}$$

are pairwise not G-conjugated. In particular, they are pairwise different. By contradiction, assume that for some $g \in G$ we have $x^g = x^{\alpha^m}$ with $0 \leq m < q^a$. Then $g \in N_G(\langle x \rangle)$ and $x^{g^{q^a}} = x^{\alpha^{q^a m}} = x$ as α is of order q^a. This implies that $g^{q^a} \in C_G(\langle x \rangle)$. Recall that $C_G(\langle x \rangle) \trianglelefteq N_G(\langle x \rangle)$ and $q \nmid |N_G(\langle x \rangle)/C_G(\langle x \rangle)|$ as $q \nmid |G|$ by assumption. So we get $g \in C_G(\langle x \rangle)$ and therefore

$$x = x^{\alpha^m} = x^{t^{mk_t(G)/q^a}}.$$

As x is of order p we deduce that $p \mid t^{mk_t(G)/q^a} - 1$. Thus $s_t(p) \mid mk_t(G)/q^a$ and

$$q^a = s_t(G)_q \mid (mk_t(G)/q^a)_q = m_q,$$

which contradicts $m < q^a$. So far we have proved that $\mathrm{Gal}(K_G/K)$ has an orbit of lenght q^a on the set of t-regular conjugacy classes of G. Since KF is a splitting field for G the group $\mathrm{Gal}(K_G/KF)$ acts trivially on these classes by Brauer's permutation lemma. Thus

$$\mathrm{Gal}(K_G/K)/\mathrm{Gal}(K_G/KF)$$

has an orbit of length q^a on the set of t-regular conjugacy classes of G. Since $\mathrm{Gal}(F/L) \cong \mathrm{Gal}(K_G/K)/\mathrm{Gal}(K_G/KF)$ where $L = F \cap K$ we obtain

$$q^a \mid \ |\mathrm{Gal}(F/L)| = |F : L|.$$

Therefore

$$s_t(G)_q = q^a \mid \ |F : L| \ \mid \ s_q$$

and the first part of the proof is complete.

For the latter assertion note that

$$s_{|G|'} = \prod_{q \nmid |G|} s_t(G)_q.$$

Remark 3.6 For nilpotent groups, in particular, abelian groups an easier argument works as follows: Let G be nilpotent and let q be a prime with $q \nmid |G|$. As before we have $s_q \mid s_t(G)_q$. In our special situation there is a normal subgroup N of G such that

$$G/N \cong \prod_{p \text{ a prime}, \, p \,|\, |G|} C_p$$

where C_p denotes a cyclic group of order p. Thus any splitting field of G must also be a splitting field of C_p for any prime p dividing $|G|$. So it must contain primitive p-th roots of unity. This forces $s_t(p) \mid s$ for $p \mid |G|$, and therefore

$$s_t(G)_q = \max\{s_t(p)_q \mid \; p \mid |G|, \, p \text{ a prime}\} \mid s_q,$$

as required.

4 Irreducible self-dual modules

In this section all fields are assumed to be of characteristic 2. To avoid complications we furthermore assume that they are finite. This fits in with the applications in coding theory which we have in mind. If F is a splitting field for G and G has odd order then all irreducible FG-modules have odd dimension. In particular, by Fong's Theorem ([6], Chap. VII, 8.13), there is no non-trivial self-dual irreducible FG-module. If F is not a splitting field this may not be true. So we may look for conditions on fields K which guarantee the existence of a non-trivial irreducible self-dual KG-module. To be brief we put $s(n) = s_2(n)$ and $s(G) = s_2(G)$.

Proposition 4.1 *Let G be a finite group of odd order. Then there exists an irreducible KG-module W with $K \not\cong W \cong W^*$ if and only if the following equivalent conditions hold true:*

a) For a (any) splitting field F of G there is a non-trivial irreducible FG-module V such that V^* is isomorphic to some module in the orbit $V^{\mathrm{Gal}(F/F\cap K)}$.

b) For a (any) splitting field F of G there is an $x \in G$ with $x \neq 1$ such that x^{-1} is G-conjugated to some element in the orbit $x^{\mathrm{Gal}(F/F\cap K)}$.

Proof: Let F be a (finite) splitting field for G. If $K \not\cong W \cong W^*$ for some irreducible KG-module W then, by 2.2, we have $K \not\cong U \cong U^*$ for some irreducible $(K \cap F)G$-module U. Again by 2.2, there exists a non-trivial irreducible FG-module V such that $V^* \cong V^\alpha$ for some $\alpha \in \mathrm{Gal}(F/F \cap K)$. Conversely, if such a module exists we may assume that V is an irreducible (KF)G-module (F is a splitting field for G) and that $\alpha \in \mathrm{Gal}(KF/K)$ since the restriction map

$$\mathrm{res}_{KF \to F} : \mathrm{Gal}(KF/K) \to \mathrm{Gal}(F/F \cap K)$$

is surjective. Applying again 2.2, we get a non-trivial irreducible self-dual KG-module W. So far we have proved the equivalence of the existence of W and the assertion in a).
Part b) of the Theorem follows immediately by Brauer's permutation Lemma. Note that the assumptions of 2.4 are satisfied. For the group H acting on the set of irreducible characters and the set of p-regular conjugacy classes of G we may take $H = \mathrm{Gal}(F/F \cap K) \times \langle h \rangle$ where h is of order 2 acting on G by $g \to g^h = g^{-1}$ and on $\mathrm{IBr}_2(G)$ by $\beta \to \beta^\alpha = \overline{\beta}$.

The next result is a special case of Theorem 4.3 which we apply in its proof. We will state it slightly more general than we need in 4.3. In addition, we give a direct proof avoiding the use of Brauer's permutation lemma.

Proposition 4.2 *Let $G = C_n$ be a cyclic of odd order n. If $(\log_2 |K|)_2 < s(G)_2$ then there exists an irreducible KG-module V with $K \not\cong V \cong V^*$.*

Proof: Let F be a field of size $2^{s(n)}$. Note that F is a minimal splitting field for G and thus, by 3.5 (or 3.6), we have $s(n)_2 = s(G)_2$. Furthermore, by assumption,

$$1 \leq (\log_2 |K|)_2 < s(G)_2 = s(n)_2.$$

Thus $s(n)$ is even and there exists a subfield, say L, of F with $|F : L| = 2$. Let $\mathrm{Gal}(F/L) = < \alpha >$. Since

$$n \mid 2^{s(n)} - 1 = (2^{s(n)/2} - 1)(2^{s(n)/2} + 1)$$

we may write $n = ab$ with $a \mid 2^{s(n)/2} - 1$ and $b \mid 2^{s(n)/2} + 1$. Clearly, $b \neq 1$, by definition of $s(n)$. If ξ is a primitive n-th root of unity in F then the irreducible FG-modules are given by ξ^i for $i = 1, \ldots, n$. Note that

$$(\xi^a)^\alpha = \xi^{a 2^{s(n)/2}} = \xi^{-a}$$

since $n \mid a(2^{s(n)/2}+1)$. Thus $V^\alpha \cong V^*$ if V denotes the module corresponding to ξ^a. Furthermore, $n \nmid a$ as $b \neq 1$. Hence $V \not\cong F$ and the assertion of the Proposition follows by 2.2 b).

We are now prepared to prove

Theorem 4.3 *If G is a group of odd order then the following conditions are equivalent:*

a) There exists an irreducible KG-module W with $K \ncong W \cong W^*$.

b) There exists an irreducible KG-module of even dimension.

c) $(\log_2 |K|)_2 < s(G)_2$.

Proof: Let $|K| = 2^k$. By Fong's Lemma, a) implies b). Next assume that b) holds true but $k_2 \geq s(G)_2$. Let F denote a minimal splitting field for G of characteristic 2. If $|F| = 2^s$ then $s_2 = s(G)_2$, by 3.5. Thus $k_2 \geq s_2$ and therefore $2 \nmid |KF : K|$. Since KF is a splitting field for G all irreducible $(KF)G$-modules are of odd dimension. Thus, by 2.2 c), all irreducibe KG-modules are of odd dimension which contradicts b). To finish the proof we assume that $k_2 < s(G)_2$. By definition we have

$$s(G)_2 = \max \{s(p)_2 \mid p \text{ a prime, } p \mid |G|\} = s(p)_2$$

for a suitable prime p dividing $|G|$. In particular, there exists an element $x \in G$ of order p such that $k_2 < s(p)_2 = s(\langle x \rangle)_2$. Thus, by 4.2, there is an irreducible $K\langle x \rangle$-module, say V, with $K \ncong V \cong V^*$. By 4.1, we get $x^{-1} \in x^{\mathrm{Gal}(KK_G/K)}$ where K_G is the field defined in 3.2. In particular x^{-1} is G-conjugated to an element in $x^{\mathrm{Gal}(KK_G/K)}$. Applying 4.1 again we obtain an irreducible KG-module W which satisfies $K \ncong W \cong W^*$. Thus a) holds true.

Remarks 4.4 a) Theorem 4.3 tells us that KG has an irreducible KG-module of even dimension if and only if KG has a non-trivial irreducible self-dual module. Clearly, each non-trivial irreducible self-dual module in characteristic 2 is of even dimension by Fong's Lemma. But the converse does not hold true in general. Take for example $G = C_{21} = C_7 \times C_3$ and K a field with 8 elements. Note that K is not a splitting field for G. A minimal splitting field has 64 elements. One easily checks that KG has 14 irreducible modules where 7 of them are of dimension 1 and the other 7 of dimension 2, but only one of the 2-dimensional modules is self-dual.
b) By part c) of Theorem 4.3, we can prove the existence of an irreducible non-trivial self-dual KG-module just by number theoretical computations. From the group G we only need to know the primes dividing $|G|$.

In the sequel let $^- : KG \to KG$ denote the anti-algebraautomorphism defined by $g \to g^{-1}$.

Proposition 4.5 *If G is of odd order then the following conditions are equivalent.*

a) The trivial module is the only self-dual irreducible KG-module.

b) There is a decomposition

$$1 = e_0 + e + \bar{e} \in KG$$

with centrally orthogonal idempotents $e_0 = \sum_{g \in G} g$, e and $\bar{e}$.

Proof: a) $\Rightarrow$ b) Since the trivial module is the only self-dual irreducible KG-module Maschke's Theorem implies

$$KG = e_0 K \oplus (W_1 \oplus \ldots \oplus W_t) \oplus (W_1^* \oplus \ldots \oplus W_t^*)$$

with non-trivial irreducible pairwise non-isomorphic KG-modules W_i and $e_0 = \sum_{g \in G} g$. This leads to a decomposition $1 = e_0 + e + e^*$ with centrally orthogonal idempotents e_0, e, e^* and $eKG = W_1 \oplus \ldots \oplus W_t$, resp. $e^*KG = W_1^* \oplus \ldots \oplus W_t^*$. By a result of Okuyama and Tsushima [12], we have $e^*KG \cong (eKG)^* \cong \bar{e}KG$. Thus, by ([8], 3.12), e^* and $\bar{e}$ are conjugate in the unit group of KG. Since $\bar{e}$ is central we obtain $e^* = \bar{e}$, hence $1 = e_0 + e + \bar{e}$.
b) $\Rightarrow$ a) Clearly, $KG = e_0KG \oplus eKG \oplus \bar{e}KG$ and $\bar{e}KG \cong (eKG)^*$, by the result of Okuyama and Tsushima. Since $e\bar{e} = 0$ an irreducible KG-module W is not self-dual unless $W \cong K$.

Proposition 4.6 *Suppose the statements of* 4.5 *hold true. Then*

a) $1 \in \mathrm{supp}(e)$ *if and only if* $|G| \equiv -1 \bmod 4$.

b) $eKG \subseteq (eKG)^{\perp}$.

c) (Square root bound) *If* $\mathrm{d} = \mathrm{d}((1+e)KG) < \mathrm{d}(eKG)$ *then* $d^2 - d + 1 \geq |G|$.

d) If $|K| = 2$ *and* $|G| \equiv -1 \bmod 8$ *then all weights in eKG are divisible by* 4.

e) If $|K| = 2$ *then*

$$\begin{aligned} \mathrm{supp}(e) \cup \mathrm{supp}(\bar{e}) &\supseteq G \setminus \{1\} \\ \mathrm{supp}(e) \cap \mathrm{supp}(\bar{e}) &\subseteq \{1\}. \end{aligned}$$

Proof: a) Let ρ denote the regular character on KG. If $e = \sum_{g\in G} k_g g$ then $\rho(e) = k_1|G| = k_1$ since $|G|$ is odd and K of characteristic 2. On the other hand $KG = e_0K \oplus eKG \oplus \bar{e}KG$ (see 4.5) implies

$$\begin{array}{rcll} \rho(e) & = & \dim eKG & \mod 2 \\ & = & \frac{|G|-1}{2} & \mod 2. \end{array}$$

Thus $1 \in \mathrm{supp}(e)$, i.e., $k_1 \neq 0$ (indeed $k_1 = 1$) if and only if $|G| \equiv -1 \mod 4$.
b) If b denotes the canonical bilinear form on KG then

$$b(eKG, eKG) = b(KG, \bar{e}eKG) = 0$$

since $\bar{e}e \in eKG \cap \bar{e}KG = 0$.
c) Let $(1+e)a$ with $a \in KG$ be an element of minimal weight in $(1+e)KG$. By the assumption we have $(1+e)a \notin \bar{e}KG$ since $\mathrm{d}(eKG) = \mathrm{d}(\bar{e}KG)$. Furthermore

$$(1+e)a = (e_0 + \bar{e})a = ke_0 + \bar{e}a.$$

Hence $k \neq 0$. Now consider

$$(1+e)a(1+\bar{e})\bar{a} = k(e_0 + \bar{e}a)k(e_0 + e\bar{a}) = k^2 e_0 \in (1+e)KG.$$

The left hand side of this equation has at most $d^2 - d + 1$ terms different from 0. Thus we get $d^2 - d + 1 \geq |G|$.
d) By a), we have $1 \in \mathrm{supp}(e)$ and therefore

$$\mathrm{wt}(e) = 1 + \frac{|G|-1}{2} = \frac{|G|+1}{2}$$

which is divisible by 4 as $|G| \equiv -1 \mod 8$. Since $\{eg \mid g \in G\}$ is a K-linear generating system for eKG we find a basis of eKG whose elements all have weigths divisible by 4. Thus eKG has a basis consisting of elements whose weigths are all divisible by 4, and by 3.1.7 a) of [15], the code eKG is doubly even.
e) This is obvious.

Note that in case of a cyclic group G and $|K| = 2$ the space eKG is a duadic code with respect to the splitting μ_{-1} (see [10]).

5 Self-dual (H,G)-group codes

If there is an G-invariant nondegenerate form on a KG-module V then, as in 4.6, two different kinds of duality come into play. On the one hand we are concerned with self-dual modules, i.e. modules V which satisfy $V \cong V^*$, on the other hand with self-dual G-invariant codes, i.e. G-invariant codes V which satisfy $V = V^\perp$ with respect to a given form. Both modules are related as 5.1 shows. This is the key point for most what follows. Although part a) can already be found in ([5], VII, 8.3) we give a proof for reader's convenience.

Proposition 5.1 *Let K be any field and let G be a finite group. Suppose that V is a KG-module carrying a nondegenerate G-invariant K-bilinear form b.*

a) If C is a submodule of V then $V/C^\perp \cong C^*$ as KG-modules.

b) Let H be a subgroup of G. $V|_H$ has an irreducible self-dual KH-composition factor with odd multiplicity then V does not contain a self-dual G-invariant code.

Proof: a) Let C be a submodule of V. We consider the K-linear map $\alpha : V \to C^*$ defined by $c(v\alpha) = b(c, v)$ for $c \in C$ and $v \in V$. Since

$$c((vg)\alpha) = b(c, vg) = b(cg^{-1}, v) = (cg^{-1})(v\alpha) = c((v\alpha)g)$$

for all $v \in V, c \in C$ and $g \in G$ the map α is KG-linear. Obviously, $\operatorname{Ker}\alpha = C^\perp$. Thus there is a KG-monomorphism from $V/C^\perp$ into C^*. On the other hand, $\beta : C \to (V/C^\perp)^*$ given by $(v + C^\perp)(c\beta) = b(c, v)$ for $c \in C$ and $v \in V$ is well defined and a KG-monomorphism. It follows that

$$\dim C \leq \dim(V/C^\perp)^* = \dim V/C^\perp \leq \dim C^* = \dim C.$$

This shows that $V/C^\perp \cong C^*$ as KG-modules.
b) Suppose that $C = C^\perp$ is a self-dual G-invariant code in V. Now, if W is a KH-composition factor of $C = C^\perp$ with multiplicity m then W^* is a composition factor of $C^* \cong V/C^\perp$ with the same multiplicity m. Thus a self-dual irreducible composition factor of V occurs with even multiplicity.

Definition 5.2 Let G be a finite group and let $H \leq G$.

a) By an (H, G)-group code we denote an H-invariant K-linear subspace of KG. For brevity a (G, G)-group code is simply called a group code for G.

b) An extended (H, G)-group code is an H-invariant K-linear subspace of $K \oplus KG$ where G, in particular H, acts trivially on the additional component K (which may be used as a parity check component).

Note that for cyclic groups a group code is nothing else than a cyclic code in the usual sense. A $(1, G)$-group code simply denotes a linear code of length $|G|$.

Theorem 5.3 *If K is a finite field of characteristic 2 and G a finite group of odd order with subgroup H then the following conditions are equivalent.*

a) There exists a self-dual extended (H, G)-group code.

b) The trivial module is the only irreducible self-dual KH-module.

a) $(\log_2 |K|)_2 \geq s_2(H)_2$.

Proof: a) $\Rightarrow$ b) Suppose there exists a non-trivial irreducible self-dual KH-module W. As $|G|$ is odd the multiplicity of W in $KG|_H$ is odd (see 2.3). This contradicts 5.1.
b) $\Rightarrow$ a) Let $x_1, x_2, \ldots, x_l$ denote a left transversal of H in G. Thus we may write

$$KG|_H = x_1 KH \oplus \ldots \oplus x_l KH.$$

We now consider $V = K \oplus KG$ as a KH right module. Observe that V carries a symmetric nondegenerate G-invariant bilinear form b defined by

$$b(k + \sum_{g \in G} k_g \, g, k' + \sum_{g \in G} k'_g \, g) = kk' + \sum_{g \in G} k_g k'_g.$$

With this form we clearly have

$$KG|_H = x_1 KH \perp \ldots \perp x_l KH$$

and, by 4.5, we obtain

$$V = K \oplus KG = K \perp x_1(e_0 K \oplus eKH \oplus \bar{e}KH) \perp \ldots \perp x_l(e_0 K \oplus eKH \oplus \bar{e}KH)$$

with centrally orthogonal idempotents $e_0, e, \bar{e}$ of KH. Next we put

$$v = 1_K + \sum_{i=1}^{l} x_i e_0 = 1_K + \sum_{g \in G} g$$

and claim that

$$C = vK + \sum_{i=1}^{l} x_i eKH$$

is a self-dual H-invariant code in V.
Clearly, C is H-invariant by construction, and $b(v,v) = 0$ since 2 divides $1+|G|$. Furthermore,

$$b(x_i eKH, x_i eKH) = b(1, KG\bar{e}\bar{x}_i x_i eKG) = 0$$

as $\bar{e}e = 0$, and

$$b(v, x_i eKG) = b(\sum_{g\in G} g, x_i eKG) = b(1, \sum_{g\in G} geKG) = b(1, \sum_{i=1}^{l} x_i e_0 eKG) = 0.$$

The equivalence of b) and c) is already contained in 4.3

Let $G = \langle g \rangle$ be a cyclic group of order n and let $l \in \mathbb{N}$. We define an l-quasi-cyclic code of length n over the field K as an g^l-invariant K-subspace of KG. In other words, it is a K-subspace of K^n which is invariant under l cyclic shifts. For brevity, such codes are called l-qc codes. Obviously, the 1-qc codes are the cyclic codes.

For $l \mid n$ an l-qc code C is an H-invariant subspace of

$$KG|_H \cong \underbrace{KH \oplus \ldots \oplus KH}_{l}$$

where H is a subgroup of G of order $e = \frac{n}{l}$. For G cyclic of odd order, Theorem 5.3 completely characterizes the situations in which self-dual extended l-qc codes exist.

Corollary 5.4 *Let l be a positive integer with $l \mid n = 2m-1$ ($m \in \mathbb{N}$) and let K be a finite field of characteristic 2. Then there is a self-dual extended l-qc code of length $2m$ over K if and only if*

$$(*) \quad \log_2(|K|)_2 \geq \max\{s_2(p)_2 \mid \ p \textit{ a prime}, \ p \mid \frac{n}{l}\}.$$

Examples 5.5 a) Suppose that $m \in \mathbb{N}$ is odd. Then for all primes p with $p \mid n = 2^m - 1$ we get $s(p)$ odd as $s(p) \mid m$. Thus, by 5.4, there exists a self-dual extended cyclic code of length 2^m over any finite field of characteristic 2.
b) Now let $m \in \mathbb{N}$ be even. Then $3 \mid n = 2^m - 1$ and $s(3)_2 = 2$. Thus, by 5.4, there is no binary extended cyclic self-dual code of length 2^m. This is also Corollary 1 of [3].

If we specialize $m = 6$ then for $l = 9$

$$1 = (\log_2 |K|)_2 = \max \{s_2(p)_2 \mid \ p \text{ a prime}, \ p \mid \frac{63}{9} = 7\}$$

and there exists a binary self-dual 9-qc code of length 64.

In order to check $(*)$ in 5.4 for $|K| = 2$ only primes $p \equiv 1 \bmod 8$ with $p \mid \frac{n}{l}$ have to be considered as the next lemma shows.

Lemma 5.6 *Let p be an odd prime.*

a) If $p \equiv -1 \bmod 8$ then $s_2(p)$ is odd.

b) If $p \equiv \pm 3 \bmod 8$ then $s_2(p)$ is even.

Proof: a) If $p \equiv -1 \bmod 8$ then 2 is a square in $\mathbb{Z}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ (see for instance 2.4.4 in [15]) and $\frac{p-1}{2}$ is odd. Thus there exists an integer x with $x^2 = 2 \bmod p$ and we get $1 = (x^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}}$.
b) If $p \equiv \pm 3 \bmod 8$ then 2 is not a square mod p (see again 2.4.4 in [15]). In particular $s_2(p)$ must be even.

6 Weigths in self-dual group codes

It is well known that a binary self-dual cyclic code C is not doubly even, i.e., not all weigths are divisible by 4. This fact is an immediate consequence of 6.1 which is due to Sloane and Thompson (see [14]). We give here a representation theoretical proof which also shows that codewords of weight $2 \bmod 4$ are contained in eC where e is the central idempotent generating the principal 2-block of KG.

Theorem 6.1 (Sloane, Thompson, [14]) *Let K be a field of characteristic 2 and let G be a finite group which has a cyclic Sylow 2-subgroup. If there exists a self-dual G-invariant code in KG then C contains a codeword of weight $2 \bmod 4$.*

Proof: Let $T = \langle t \rangle$ be a Sylow 2-subgroup of G with $|T| = 2^m$. Since T is cyclic there exists a normal subgroup $H \trianglelefteq G$ of odd order such that $G/H \cong T$ (see [5], Kap. IV, 2.8). If we put $e = \frac{1}{|H|} \sum_{h \in H} h$ then $eKG = eKT$ is the principal 2-block of $KG = eKG \oplus (1-e)KG$. Since $\bar{e}(1-e) = e(1-e) = 0$ we even have $KG = eKG \perp (1-e)KG$. Furthermore, $C^\perp = C = eC \perp (1-e)C$ where eC is a self-dual ideal in $eKG = eKT$. Let J denote the Jacobson radical of KT. Since $eKT \cong KT$ as KT-modules and KT is uniserial with KT-submodules J^i $(i = 0, \ldots, 2^m)$ we get $eC = eJ^{2^{m-1}}$. Clearly,

$$c = e(1-t)^{2^{m-1}} \in eJ^{2^{m-1}} = eC \subseteq C$$

and $c = e(1-t)^{2^{m-1}} = e(1-t^{2^{m-1}})$. Furthermore, $t^{2^{m-1}} \neq 1$. Thus the weight of c is congruent $2\,|H|$ which is 2 mod 4 as $|H|$ is odd.

By a well-known result of Gleason (see for instance [15], 6.3.8), a binary self-dual doubly even weight code has a length which is divisible by 8. For extended group codes the converse holds true, i.e.,

Theorem 6.2 *All binary self-dual extended group codes which have a length* $n \equiv 0 \bmod 8$ *are doubly even.*

Proof: Let $C = C^\perp \leq K \oplus KG$ where K denotes the prime field of size 2. By 5.3, the trivial module is the only self-dual irreducible KG-module. By **??** and 4.5, C contains a component of the form eKG and a 1-dimensional subspace of $K \oplus e_0 K$. Since, up to scalars, $v = 1_K + e_0$ is the only non-trivial isotropic vector in $K \oplus e_0 K$ we have $C = vK \oplus eKG$. Clearly, $8 \mid n = \mathrm{wt}(v)$. By 4.6 d), all weights in eKG are divisible by 4. Thus C has a basis consisting of vectors whose weigths are all divisible by 4. This implies that C is doubly even.

Examples 6.3 a) A binary self-dual extended QR-code is doubly even if the defining prime p satisfies $p = -1 \bmod 8$, but only even if $p \equiv 1 \bmod 8$ (see also [15], 6.3.8).
b) A binary self-dual Reed-Muller code of length 2^m with $m \geq 3$ is doubly even since it is an extended cyclic code for a group of order $2^m - 1$ with m odd. (The group involved here is the Singer cycle in $\mathrm{GL}(m, 2)$, and only for m odd self-dual Reed-Muller codes exist.)

7 Self-dual codes in group algebra components

As already mentioned in the introduction the group algebra KG has a G-invariant self-dual code if and only if $|K|$ is a power of 2 and 2 divides $|G|$. Particularly with regard to the question which we posed at the beginning we may ask for conditions under which a component i.e. a direct summand of KG has a G-invariant self-dual code. From viewpoint of coding theory such a component should have a natural basis. A canonical object here is the projective cover $P_G(K)$ of the trivial module K provided G is p-solvable. Then in case $\mathrm{char}\, K = p$ we have

$$P_G(K) = eKG = eKT$$

with $e = \frac{1}{|H|}\sum_{h\in H} h$ for a p-complement H of G and a Sylow p-subgroup T. A natural basis is given by $\{et \mid t \in T\}$ and the form b by $b(et, et') = |H|\delta_{t,t'}$ for $t, t' \in T$. In order to prove the existence of G-invariant self-dual codes in $P_G(K)$ we may identify eKT with KT endowed with a permutation action of H on T and the form $b(t, t') = \delta_{t,t'}$. Note that for $T \trianglelefteq G$ the permutation action of H on T (as a set) is just the conjugation action $t \to t^h$ for $t \in T$ and $h \in H$.
Obviously the existence of G-invariant self-dual codes in $P_G(K)$ forces $2 \mid |G|$ and $|K|$ a power of 2. So we shall assume these conditions in the following.

Lemma 7.1 *Let $G = TH$ be a finite group with $1 \neq T \trianglelefteq G$ an elementary abelian Sylow 2-subgroup and H a 2-complement. Then $P_G(K)$ contains a self-dual G-invariant code if*

(i) $\log_2 |T|$ *is odd or*

(ii) $(\log_2 |K|)_2 \geq s_2(H)_2$.

Proof: Let J denote the Jacobson radical of KT. Since the action of H on T is the conjugation J and all its powers are invariant under H. If $|T| = 2^m$ then by Jennings Theorem $J^m \neq 0$ and $J^{m+1} = 0$ (see [15], 7.2.2). We distinguish now two cases. First suppose that m is odd. In this case we take $C = J^{\frac{m+1}{2}}$. Then, by ([15], 7.2.10), we have

$$C^\perp = (J^{\frac{m+1}{2}})^\perp = J^{m+1-\frac{m+1}{2}} = J^{\frac{m+1}{2}} = C$$

and we are done if (i) is satisfied. Now let (ii) be true. We may assume that m is even. Thus we have

$$W = J^{\frac{m}{2}+1} \subseteq J^{\frac{m}{2}} = (J^{\frac{m}{2}+1})^\perp = V.$$

The form b defined on KG induces a G-invariant nondegenerate form b' on V/W by

$$b'(v + W, v' + W) = b(v, v') \text{ for } v, v' \in V = W^\perp.$$

Thus V/W is a self-dual KG-module. As H is of odd order V/W is a semisimple KH-module. So, by 4.3, we may write

$$V/W = lK \oplus U \oplus U^* \quad (l \in \mathbb{N})$$

where U does not contain any self-dual submodule of V/W. Clearly, $V/W = lK \perp (U \oplus U^*)$ since there is no nontrivial homomorphism from lK into $U \oplus U^*$. Moreover, $b'|_U \equiv 0$ as U does not contain with any submodule also its dual. Next we claim that lK contains a self-dual code. First observe that $2 \mid l$ as $2^m = 2\dim W + 2\dim U + l$ and $m \geq 1$. Let u and u' be linearily independent in lK and suppose that $b'(u,u) = a \neq 0$ and $b'(u',u') = a' \neq 0$. For $x \in K$ we get

$$b'(u+ku', u+ku') = b'(u,u) + 2kb'(u,u') + k^2 b'(u',u') = a + k^2 a'.$$

Since $K = K^2$ we may choose $k \in K$ such that $a + k^2 a' = 0$. Thus lK contains a non-trivial isotropic vector, say u_1. As b' is nondegenerate on the component lK there exists $u_1' \in lK$ with $b'(u_1, u_1') \neq 0$. It follows

$$lK = \langle u_1, u_1' \rangle \perp \langle u_1, u_1' \rangle^{\perp}$$

and by induction

$$lK = \langle u_1, u_1' \rangle \perp \ldots \perp \langle u_{\frac{l}{2}}, u'_{\frac{l}{2}} \rangle.$$

Thus $B = \langle u_1, \ldots, u_{\frac{l}{2}} \rangle$ is totally isotropic with respect to b'. Furthermore H acts trivially on B. Now let C be the KH-submodule of KT defined by $C/W = B \oplus U$. By construction $C = C^{\perp}$ and the proof is complete.

Example 7.2 Let $G = \mathrm{A}_4$ be the alternating group on four letters. We may write $G = TH$ with $T \trianglelefteq G$, T a Klein four group and $H = \langle h \rangle$ a 2-complement of order 3.
a) If $|K| = 2$ then there exists a self-dual irreducible KH-module V of dimension 2 and $KT = P_G(K)$ is uniserial with composition factors K, V, K. Thus no self-dual G-invariant code exists in $P_K(G)$.
b) If $|K| = 4$ then KH has three irreducible modules $K, V, V^* \not\cong V$, all of dimension 1. One easily checks that KT has lower Loewy structure (see ([5], VII, 10.10) for definition)

$$\begin{array}{ccc} & K & \\ V & & V^* \\ & K & \end{array}.$$

Furthermore, the submodule

$$V \quad K$$

is self-dual. It is a $[4,2,3]$ code over K, hence a quaternary self-dual A_4-invariant MDS-Code.

Theorem 7.3 *Let G be a finite solvable group with $2 \mid |G|$ and let H be a 2-complement. If $(\log_2 |K|)_2 \geq s_2(H)_2$ then $P_G(K)$ has a G-invariant self-dual code.*

Proof: Let T denote a Sylow 2-subgroup of G. If $e = \frac{1}{|H|}\sum_{h \in H} h$ then $P_G(K) \cong eKG = eKT$. Suppose that $O_{2'}(G) \neq 1$. Clearly, this group acts trivially on eKT and $(\log_2(|K|)_2 \geq s_2(H) \geq s_2(G/O_{2'}(G))$. So we are done by induction on $|H|$, since the induction basis is given by Corollary 1.3 of [16]. Consequently we may assume that $O_{2'}(G) = 1$. Since G is solvable there exists an elementary abelian normal subgroup $N \neq 1$. Thus, by 7.1, there is a self-dual NH-invariant code in $P_{NH}(K)$. Inducing this module up to G we get a self-dual G-invariant code in $P_G(K)$ (see [16], 2.5).

Theorem 7.4 *Let $G = TH$ be a finite group with $1 \neq T \trianglelefteq G$, T an elementary abelian Sylow 2-subgroup and H a 2-complement. If for every prime p dividing $|H|$ there exists a cyclic subgroup $L \leq H$ of order p acting fixed point freely on $T \setminus \{1\}$ then the following three conditions are equivalent.*

a) $(\log_2 |K|)_2 \geq s_2(H)_2$.

b) There is a G-invariant self-dual code in $P_G(K)$.

c) There is an H-invariant self-dual code in $P_G(K)$.

Proof: a) $\Rightarrow$ b) This is 7.1.
b) $\Rightarrow$ c) There is nothing to prove here.
c) $\Rightarrow$ a) Suppose there exists an H-invariant self-dual code in $P_G(K)$ but $(\log_2 |K|)_2 < s_2(H)_2$. Then there is a prime p dividing $|H|$ such that $(\log_2 |K|)_2 < s_2(p)_2$. This implies that there is a cyclic group $L \leq H$ of order p which has a non-trivial self-dual L-invariant code (see 4.3). We may suppose that L acts fixed point freely on $T \setminus \{1\}$. Thus we have

$$P_G(K)|_L \cong KT|_L \cong K \oplus \underbrace{KL \oplus \ldots \oplus KL}_{d}.$$

Since $|T|$ is even d must be odd. Furthermore note that all irreducible KL-modules have multiplicity one as composition factor of KL by 2.3 b). Thus all irreducible non-trivial KL-modules occur with odd multiplicity as composition factor in $KT|_L$, contradicting 5.1.

The above theorem applies in many situations; in particular, if H acts fixed point freely on $T \setminus \{1\}$. So one may choose for T an elementary abelian 2-group of rank m and for H a subgroup of the group generated by the Singer cycle of $\mathrm{GL}(m,2)$. Likewise a Frobenius group with an elementary abelian 2-group as Frobenius kernel satisfies the assumption of 7.4. We should mention here that, by 5.4, part a) of 7.4 is equivalent to the existence of a self-dual extended l-qc code (for suitable l) of length 2^m. By b), moreover such a code may be chosen invariant under the action of an elementary abelian 2-group of rank m.

One can not drop the assumtion on the fixed point free action in Theorem 7.4 as the following example shows.

Remark 7.5 If $G = \mathrm{A}_4 \times C_2$ then $|H| = |G|_{2'} = 3$ and $s_2(H)_2 = s_2(3)_2 = 2$. Thus a) in Theorem 7.4 fails to be true for $|K| = 2$. But by 7.1, the module $P_G(K)$ has a self-dual code for any finite field of characteristic 2.

References

[1] J.L. Alperin and R.B.Bell, Groups and representations. Graduate Text in Math., Springer, New York, Heidelberg 1995.

[2] F. Bernhardt, P. Landrock and O. Manz, The extended Golay codes considered as ideals. J. Comb. Theory, Series A 55, 235-246 (1990).

[3] P. Charpin and F.Levy-dit-Vehel, On self-dual affine-invariant codes. J. Comb. Theory Ser. A 67, 223-244 (1994).

[4] G. Hughes, Structure theorems for group ring codes with an application to self-dual codes. Designs, Codes and Cryptography 24, 5-14 (2001).

[5] B. Huppert, Endliche Gruppen, Springer, Berlin, Heidelberg, New York 1967.

[6] B. Huppert and N. Blackburn, Finite groups II, Springer, Berlin, Heidelberg, New York 1982.

[7] L.G. Kovacs, The permutation lemma of Richard Brauer. Bull. Lond. Math. Soc. 14, 127-128 (1982).

[8] P. Landrock, Finite group algebras and their modules. Lecture Note Series 84, Cambridge University Press, 1983.

[9] P. Landrock and O. Manz, Classical codes as ideals in group algebras. Designs, Codes and Cryptography 2, 273-285 (1992).

[10] J.S. Leon, J.M. Masley and V. Pless, Duadic codes. IEEE Trans. Inform. Theory 30, 709-714 (1984).

[11] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes. North-Holland, Amsterdam 1977.

[12] T. Okuyama and Y. Tsushima, On a conjecture of P. Landrock. J. Algebra 104, 203-208 (1986).

[13] B.S. Rajan and M.U. Siddiqi, A generalized DFT for abelian codes over $\mathbb{Z}_m$. IEEE Trans. Inform. Theory 40, 2082-2090 (1994).

[14] N.J.A. Sloane and J.G. Thompson, Cyclic self-dual codes. IEEE Trans. Inform. Theory 29, 364-366 (1983).

[15] W. Willems, Codierungstheorie, deGruyter, Berlin, New York 1999.

[16] W. Willems, A note on self-dual group codes. IEEE Trans. Inform. Theory. to appear Dec. 2002.