Two Sided and Abelian Group Ring Codes

By

Artur Schäfer

Masters Thesis

Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Mathematics
in the Faculty of Mathematics, Computer Science
and Natural Science
at RWTH Aachen University, October 2012
Supervisor: Prof. Dr. G. Nebe

Aachen, Germany

In the hallway of the university Wittgenstein asked a colleague: “I’ve always wondered why for so long people thought that the sun revolved around the earth.”

“Why?” said his surprised interlocutor, “well, I suppose it just looks that way.”

“Hmm”, retorted Wittgenstein, “and what would it look like if the earth revolved around the sun?”

This puzzled the interlocutor.

Contents

1 Introduction

In 1948, Claude Shannon's paper "A Mathematical Theory of Communiction" gave rise to the disciplines of *information theory* and *coding theory*. Both are aiming for the improvement of communication regarding convenience, reliability and efficiency. This means, the transfer of information should be as fast as possible, considering the amount of data, and as reliable as necessary. Since these two goals are conflicting, our job is to find a satisfying balance.

Coding theory is the attempt to tackle this task with algebraic means. In other words, there are two essential aspects to coding theory, namely data compression and error correction. Two main sections in coding theory are working on this major problem. The first is on *linear block codes*, the second on *convolutional codes*. Both analyse three essential properties of codes called *parameter*. These are the word length, the total number of valid code words and the minimum distance between two valid code words. Here we will focus on linear block codes and call them *linear codes*.

Algebraic codes are a comparatively good example for the fact that the more algebraic structure one adds to a system, the better one is able to describe the system. For instance, going from codes to linear codes, one can easily calculate the minimum distance of the code by calculating only the minimum weight of the code. Then using *cyclic codes* instead of linear codes one obtains an even more fruitful description.

With the release of the paper "Error detecting and error correcting codes" by R. W. Hamming in 1950 [14], linear codes received more and more attention. A linear code is a subspace of a vector space over a finite field. In its early stages, the subject of *binary codes* were focussed on, whereas nowadays there is also a theoretical interest in codes over a finite field with odd characteristic, because the error correcting properties are better.

The most important linear codes are cyclic codes. As aforementioned, these have a richer structure and thus have good error correcting properties. A cyclic code can be considered as an ideal of the ring $F[x]/(x^n - 1)$, where F is a finite field and n a positive integer. This structure gives rise to fast-decoding algorithms [10, Chapter 3], which is now a considerable aspect regarding the conditions on communication. One important class of cyclic codes is the class of BCH-codes including the Reed-Solomon-codes. The latter ones play a pivotal role in practical

terms.

Later F. J. MacWilliams [11] was the first person considering cyclic codes as ideals of the group ring $FC_n \cong F[x]/(x^n - 1)$. From that moment the new concept of *group ring codes* arose [13] and arbitrary group rings $\mathbb{F}G$ were studied using ring- and character-theoretical results. The left- or two-sided ideals were identified as left group codes or group codes respectively.

More recently, it is desirable to generalise the concept of cyclic codes. Therefore, *abelian codes*, which are group codes for an abelian group, were developed. One of the questions about this new class of codes was whether or not the class of group codes is equal to the class of abelian codes.

A. d. Rio [1] proved that there are more left-group codes than abelian codes. In the same paper he introduced the concept of an *abelian decomposition* for an arbitrary group G, and also the result that if G has an abelian decomposition then every G-code is an abelian code. Later A. A. Nechaev et al [3] showed that the symmetric group S_4 over the Galois field $\mathbb{F}_5$ contains a group code which is non abelian.

However, the answer to this problem on group codes where the group is nilpotent is still open. Especially, assuming the group is a p-group, for some prime p, the solution is not clear, either. Thus, the purpose of this master thesis is to construct examples of two-sided p-group codes that are non abelian. Moreover, we will discuss an application to abelian codes using extra-special groups.

In chapter 2 we are going to introduce necessary mathematical tools and results on the theory of algebras and character theory [7, 8]. The most important results will be the Wedderburntheorem on semisimple algebras and the computation of the central primitive idempotents of the semisimple group algebra FG. Furthermore, we will describe tensor products in order to discuss group rings of nilpotent groups.

Next, we will present in chapter 3 the basic concepts and definitions of classical coding theory. In order to introduce the concept of coding theory to the reader, we will also give some results on two interesting kinds of cyclic codes, i.e., Reed-Solomon codes and binary Hamming codes.

Afterwards, we will present the essential theory on group codes in chapter 4. Not only will we give an explicit example that $\mathbb{F}_5 S_4$ has a non abelian code, but also we are going to investigate this issue using p-groups. Another highlight is the generalization of A. d. Rio's theorem [1, Theorem 1.2] to monomial equivalences of codes given in theorem (4.1.13).

In chapter 5 we apply some results of the preceding chapter to group codes of extra-special groups. Before we get to this in chapter 5 we will provide in the first section results on two topics from a basic algebra course. The first topic

is on symplectic vector spaces and the second one on finite p-groups. We will apply these results in the following section to determine the structure of extra-special groups. Thus, we recommend the advanced reader to skip this chapter and go on. Later, we are going to have a look on abelian codes coming from extra-special groups. In [9] the authors H. G. Aun and D. W. C. Keong discussed the properties of codes using extra-special groups. Here, we will present a more basic description of these codes by using ring- and character theory and provide the proof that these codes are orthogonal sums of cyclic codes.

Finally, in chapter 6 we are going to review, give a conclusion and suggest what new work is now appropriate.

2 Algebras, Modules and minimal Ideals

The goal of this chapter is to give basic results on the theory of semisimple algebras and character theory. In order to use these tools, firstly, we will develop a basic theory on algebras. An important result is given by Wedderburn (2.1.13) which says that any semisimple algebra is a direct product of several matrix rings. This result will be necessary to divide the finite dimensional group algebra FG into minimal ideals and to study FG in detail. Afterwards, we will introduce ordinary character theory, i.e., we will study the group algebra $\mathbb{C}G$ over the complex numbers. The results given in this section are on characters and representations and will be used to describe the primitive central idempotents of the group algebra FG. Although not all the results presented are true for a field with positive characteristic, there are some which are of major importance for the next chapters. Finally, we are going to present some results on tensor products of group algebras and the connection to the direct product of two groups.

In this section we are going to introduce basic results given in the first ten lectures on elementary representation theory. Consequently, the advanced reader should use this section only as a reference. Most of the results given in this chapter can be found in books on elementary representation theory, for instance in [7, 8].

2.1 Algebras and Modules

As previously mentioned we are going to describe the structure of semisimple algebras using Wedderburn's theorem. Firstly, we will introduce the concept of minimal ideals which are the blocks for this framework. Later we will see that we will obtain some useful consequences due to this approach. For instance, the number of conjugacy classes of a group G will be equal to the number of isomorphism classes of irreducible FG-modules.

Before we start giving the precise definition we will show what an algebra is.

(2.1.1) Example

1. *A field extension $E|F$ over the field F is an algebra.*
2. *$F^{n\times n}$ is the algebra of $n \times n$ matrices over the field F.*
3. *For a finite group $G = \{g_1, ..., g_n\}$ and a field F the **group ring** or **group algebra** $FG := F[G] := \{\sum_{i=1}^{n} a_i g_i \mid a_i \in F, \text{ for } i = 1, ..., n\}$ is an algebra.* ◇

(2.1.2) Definition

Let F be a field.

1. *An **algebra** A is an F-vector space which is also a ring with 1, such that*

$$(ax)y = a(xy) = x(ay), \quad \text{for all } a \in F, \text{ and all } x, y \in A.$$

2. *A **division algebra** is an algebra which has a multiplicative identity element, say $1 \neq 0$, and every non zero element has a multiplicative inverse.*
3. *Let A be an F-algebra and V an F-vector space. V is an A**-(left)-module** if for all $x, y \in A$, $v, w \in V$ and $a \in F$ holds*

$$\begin{aligned} &1) && x(v+w) = xv + xw \\ &2) && (x+y)v = xv + yv \\ &3) && y(xv) = (yx)v \\ &4) && x(cv) = c(xv) = (cx)v \\ &5) && 1v = v. \end{aligned}$$

4. *A° denotes the **regular module**.*
5. *A^{op} is called the **opposite ring**, where A^{op}=$(A,+,*)$ and $a * b = b \cdot a$.* ◇

The preceding definition tells us how an algebra acts on a vector space. Now, we want to investigate this action to some extent. Similar to finite groups which act on orbits, we would like to see if there is some minimal invariant submodule.

(2.1.3) Definition

1. *An A-module $V \neq 0$ is called **irreducible** if 0 and V are the only submodules of V.*
2. *An A-module V is called **completely reducible** if for every submodule $W \leq V$ there exists a submodule $U \leq V$ with $V = U \oplus W$.*
3. *An algebra A is called **semisimple** if its regular module A° is completely reducible.* ◇

In view of this concept the following two results are a simple consequence.

(2.1.4) Theorem (Schur, see [7], Lemma 1.5)
Let $V \neq 0 \neq W$ be irreducible A-modules. Then $0 \neq \phi \in Hom_A(V,W)$ has an inverse. ◇

(2.1.5) Corollary (See [7], Corollary 1.6)

1. *If V is an irreducible A-module then $End_A(V)$ is a division algebra.*
2. *Suppose that F is an algebraically closed field (so every Endomorphism has an eigenvalue), A an F-algebra and V an irreducible A-module. Then $End_A(V) = F \cdot 1$.* ◇

Our next target is the description of completely reducible A-modules.

(2.1.6) Theorem (See [7], Theorems 1.10/1.11)
Let V be an A-module. Then the following is equivalent:

1. *V is completely reducible.*
2. *V is a sum of irreducible submodules.*
3. *V is a direct sum of irreducible submodules.* ◇

(2.1.7) Example
The vector space $\mathbb{R}^n$ is a completely reducible $\mathbb{R}$-module. It holds

$$\mathbb{R}^n = \bigoplus^n \mathbb{R}.$$

Similarly, $(\mathbb{R}^{n\times n})^\circ$ can be written as

$$\mathbb{R}^{n\times n} = \bigoplus^n \mathbb{R}^{n\times 1}.$$ ◇

By the preceding result these are the direct sum of irreducible submodules. This will stimulate the purpose of collecting some of the irreducible submodules which are similar. We will explain this in the next definition.

(2.1.8) Definition
Let V be a completely reducible A-module and let M be an irreducible A-module. We will denote the sum of all irreducible submodules of V which are isomorphic to M by $M(V)$.◇

Although there are more results concerning $M(V)$, we will present only the next one and focus on further prerequisites for Wedderburn's theorem. With this intention we will show afterwards that in order to describe all irreducible A-modules, it is sufficient to study the set of homomorphic images of A°.

(2.1.9) Lemma (See [7], Lemma 1.13)
Let $V = \sum W_i$ be a direct sum of irreducible A-modules and M be any irreducible A-module. Then $M(V) = \sum_{W_i \cong M} W_i$. ◇

(2.1.10) Lemma (See [7], Lemma 1.14)
Let A be an F-algebra. Then every irreducible A-module is isomorphic to a factor module of A°. Furthermore, if A is semisimple then every irreducible A-module is isomorphic to a submodule of A°. ◇

(2.1.11) Corollary
The number of isomorphism classes of irreducible A-modules is finite. In particular, this number is equal to $\dim(Z(A))$ *[7, Corollary 1.17].* ◇

In order to describe the structure of a semisimple algebra we introduced the notion of the A-module A°. As a consequence of our results above we are able to write A° as

$$A^\circ = \sum_{M \in S} M(A^\circ), \tag{2.1}$$

where S is the finite set of isomorphism classes of irreducible A-modules.

The following theorem is the basis for Wedderburn's theorem and says that $M(A^\circ)$ is a minimal ideal for every $M \in S$. Thus these ideals are the blocks for the structure of a semisimple algebra. Due to notational issues we will identify A° by A.

(2.1.12) Theorem
Let A be a semisimple algebra and let M be an irreducible A-module. Then,

1. *$M(A)$ is a minimal ideal of A.*
2. *if W is an irreducible submodule of A, not isomorphic to M, then $M(A)$ annihilates W.*
3. *A is the direct sum of irreducible minimal ideals.* ◇

Eventually, our final result of this section is a consequence of the previous theorem and the reason for our effort.

(2.1.13) Corollary (Wedderburn, see [8], Theorem 26.4)
Let F be an algebraically closed field and A a semisimple F-algebra. Also, let $M_1, ..., M_n$ be the system of representatives of isomorphism classes of irreducible A-modules, $D_i^{op} = End_A(M_i)$ and $A^\circ \cong \bigoplus_{i=1}^n \bigoplus^{k_i} M_i$. Then

$$A \cong \bigoplus_{i=1}^{n} D_i^{k_i \times k_i}. \tag{2.2}$$

◇

(2.1.14) Example
Suppose $A := \mathbb{Q}[x]/\langle x^3 - 1\rangle$. Clearly,

$$A \cong \mathbb{Q} \oplus \mathbb{Q}[x]/\langle x^2 + x + 1\rangle.$$

Now, if we take an algebraically closed field we can apply the previous result:

$$\mathbb{C}[x]/\langle x^3 - 1\rangle \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}.$$ ◇

2.2 An Introduction to Representation Theory

On the account of the previous theory on semisimple algebras we will develop the theory of representation over the complex numbers $\mathbb{C}$. As in lectures on elementary representation theory, we are going to show that the concept of representations and characters of the finite group G is the same over $\mathbb{C}$. Furthermore, we will present the orthogonality relations and the relationship of characters of G to normal subgroups of G. Also, we want to highlight the results on the center $Z(G)$ and other results related to these.

2.2.1 Representations and Characters over $\mathbb{C}$

(2.2.1) Definition

1. *Let F be a field and A an F-algebra. A **representation** of the algebra A of **degree** n is an algebra homomorphism $X : A \to F^{n\times n}$.*
2. *Two representations X and D of degree n are called **similar** if there exists $P \in GL(n, F)$ such that $X(a) = P^{-1}D(a)P$ for all $a \in A$.* ◇

(2.2.2) Example

Let $G := \langle (1,3), (1,2,3,4)\rangle$ be the dihedral group of order 8. Then we will give a few possible representations of $\mathbb{Q}G$. It will turn out that these are all the irreducible representations of $\mathbb{Q}G$.

$$
\begin{aligned}
X_1 &: (1,3) \mapsto 1, \quad (1,2,3,4) \mapsto 1.\\
X_2 &: (1,3) \mapsto 1, \quad (1,2,3,4) \mapsto -1.\\
X_3 &: (1,3) \mapsto -1, \quad (1,2,3,4) \mapsto 1.\\
X_4 &: (1,3) \mapsto -1, \quad (1,2,3,4) \mapsto -1.\\
X_5 &: (1,3) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (1,2,3,4) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.
\end{aligned}
$$

(2.2.3) Theorem (Maschke, see [7], Theorem 1.9)

Let G be a finite group and F a field whose characteristic does not divide $|G|$. Then every FG-module is completely reducible. ◇

This theorem helps us to study the group algebra FG, considered as an FG-module, using all the previous theory. We will see that some results are a simple consequence derived by results about semisimple algebras.

First, we will give some remarks about representations in general, and define the term *character* of a group.

(2.2.4) Remark
If X is a representation of the group algebra FG then X is a homomorphism $X : FG \to F^{n\times n}$. X induces a homomorphism $X_0 : G \to GL(n, F)$.

On the other hand if X_0 is a homomorphism from G to $GL(n, F)$ then we will obtain a representation $X : FG \to F^{n\times n}$ using

$$X\left(\sum a_g g\right) := \sum a_g X_0(g). \tag{2.3}$$

So X and X_0 correspond to each other, so we will not distinguish them in the future. ◇

(2.2.5) Remark
Let $N \trianglelefteq G$ and X a representation of G with $N \subseteq ker(X)$. Then we obtain a representation $\overline{X}$ of G/N using $\overline{X}(gN) := X(g)$.
On the other hand if $\overline{X}$ is a representation of G/N then we can obviously obtain a representation X by $X(g) := \overline{X}(gN)$ which suffices the condition $N \subseteq ker(X)$. Again, we will not distinguish between X and $\overline{X}$. ◇

(2.2.6) Definition

1. *Let X be a representation of G. Then $\chi : G \to F$, $\chi(g) := tr(X(g))$ is called a **character** of G afforded by the representation X.*
2. *Let χ be a character of G with respect to the representation X. Then $\chi(1) = tr(X(I))$ is the **degree** of the representation.*
3. *Characters of degree one are called **linear characters**. All others are non linear characters. The character $1_G : G \to F^\times, g \mapsto 1$ is called the **principal character**.*
4. *A character χ is called **irreducible** if the representation affording χ is irreducible. The set of all irreducible characters is denoted by $Irr(G)$.* ◇

In other words a character is a function from a group G into a field F and the value of a character on a group element is the trace of some matrix. In fact these few values will be able to describe properties of a group. Thus the concept of characters is quite impressive. However, we will present some properties of characters below:

(2.2.7) Remark

1. *A character is not necessarily a homomorphism.*
2. *Let $\lambda : G \to F^\times$ be a homomorphism. Then $X(g) := \lambda(g)$ is a representation of G affording the character λ.*
3. *Similar representations afford similar characters.*
4. *Characters are constant on conjugacy classes.* ◇

From this point on we need a restriction on the group algebra to obtain further important results. To put it in another way, we will study the special case where

the group algebra is $\mathbb{C}G$. Nevertheless, some of the results presented here are true for arbitrary fields, as long as the group algebra is semisimple. These results are useful for group rings over finite fields and therefore for the coding theory which we introduce in the next chapters.

The group ring over the complex numbers gives us the possibility to describe the conjugacy classes of the group G using the central algebra $Z(\mathbb{C}G)$.

(2.2.8) Theorem
Let $K_1, ..., K_r$ be the conjugacy classes of G. Set $k_i := \sum_{x \in K_i} x \in \mathbb{C}G$. Then the $\{k_i\}_{i=1}^r$ form a basis for $Z(\mathbb{C}G)$ and if $k_i k_j = \sum a_{ijl} k_l$ then then a_{ijl} are positive integers. ◇

Proof (See [7], Theorem 2.4)
Clearly, $k_i \in Z(\mathbb{C}[G])$. The k_i are linearly independent, since they are the sum of distinct elements of G. Our task now is to show that $\{k_i\}_{i=1}^r$ is a generating set. Put $z = \sum a_g g \in Z(\mathbb{C}[G])$ it follows that $z = h^{-1}zh = \sum a_{h^{-1}gh} g$. By comparing the coefficients we obtain $a_g = a_{h^{-1}gh}\ \forall h \in G$. Hence, all the coefficients are constant on the conjugacy classes of G, so $z = \sum a_i k_i$. Pick a $g \in K_l$ then the coefficient of g in $k_i k_j$ is an integer. ■

Before we present a consequence of this result we want to introduce the idea of generating idempotents.

(2.2.9) Remark
By Wedderburn's theorem (2.1.13) we can write the group ring as

$$\mathbb{C}G = \bigoplus_{i=1}^{r} M_i,$$

*for minimal twosided ideals M_i of $\mathbb{C}G$. Consequently, we can write $1 = \sum_{i=1}^{r} e_i$, for some elements $e_i \in M_i$. The elements e_i are called **central primitive idempotents**. Furthermore, each of them generates a minimal ideal M_i, for $i = 1, ..., r$, i.e.,*

$$M_i = e_i \mathbb{C}G = \mathbb{C}G e_i.$$ ◇

The next corollary is a consequence from both the previous theorem and our theoretical results on algebras from the preceding section.

(2.2.10) Corollary (See [7], Corollary ff. 2.5)

1. *The number of conjugacy classes of G is equal to the number of irreducible characters of G and equals the number of isomorphism classes of irreducible $\mathbb{C}G$-modules.*
2. $|G| = \sum_{\chi \in Irr(G)} (\chi(1))^2$.
3. *G is abelian if and only if every irreducible character is linear.* ◇

(2.2.11) Definition
*Let $Irr(G) = \{\chi_1, ..., \chi_n\}$ and $a_1, ..., a_r$ be representatives of the conjugacy classes of the group G. We define the **character table** to be the matrix $(\chi_i(a_j))_{i=1,...,n,\ j=1,...,r}$.* ◇

(2.2.12) Example
From our example (2.2.2) on the dihedral group of order 8 we obtain the following character table:

a_i:	1	$(1,3)(2,4)$	$(1,3)$	$(1,2,3,4)$	$(1,2)(3,4)$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

◇

(2.2.13) Definition
*A **class function** on a group is a function $\phi : G \to \mathbb{C}$ which is constant on the conjugacy classes.* ◇

Although class functions are of minor importance to this thesis, we will motivate this term by the following result. Also, we will use class functions as a motivation for characters of direct products of groups.

The next theorem says that characters of a group G are a basis for the $\mathbb{C}$-space of all class functions. Moreover, the second part is a useful equivalence.

(2.2.14) Theorem (See [7], Theorem 2.8)
Every class function is uniquely determined by $\phi = \sum_{\chi \in Irr(G)} a_\chi \chi$, for $a_\chi \in \mathbb{C}$. In particular, a class function ϕ is a character if and only if all a_χ are positive integers and $\phi \neq 0$. ◇

(2.2.15) Corollary (See [7], Corollary 2.9)
Let X and D be representations of G. X and D are similar if and only if they afford the same characters. ◇

In order to describe the minimal ideals of a group ring we want to determine the idempotents e_i from our previous discussion in (2.2.9). On this account we have to calculate the coefficients a_g of the e_i, where $e_i = \sum_{g \in G} a_g g \in \mathbb{C}G$. First we define the **regular character** ρ to be the character afforded by a representation corresponding to the regular module $\mathbb{C}[G]^\circ$. This character will be our tool for the next major result.

(2.2.16) Lemma
For the regular character holds $\rho(1) = |G|$ and $\rho(g) = 0\ \forall g \neq 1$. ◇

Proof (See [7], Lemma 2.10)
Choose the basis G of $\mathbb{C}[G]^\circ$ and choose $x \in G$. Consider the endomorphism $\phi : \mathbb{C}[G]^\circ \to \mathbb{C}[G]^\circ$, $g \mapsto gx$. Since the equation $gx = g$ holds if and only if x is the identity, the representation afforded by ϕ has trace equal to n if $x = 1$ and otherwise trace equal to 0. ■

(2.2.17) Lemma (See [7], Lemma 2.11)
It holds $\rho = \sum_{i=1}^{k} \chi_i(1)\chi_i$. ◇

Since all minimal ideals are generated by a single idempotent e_i, for $i = 1, ..., |Irr(G)|$, the next theorem is the basis of our investigation of ideals of group rings. Note that the next result holds also for finite fields satisfying Maschke's theorem (2.2.3).

(2.2.18) Theorem (See [7], Theorem 2.12)
Let $Irr(G) = \{\chi_1, ..., \chi_n\}$. *Then the idempotent* e_i *is determined by*

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g, \quad \text{for } i = 1, ..., n. \tag{2.4}$$

◇

The next step is to obtain the orthogonality relations. These are a precious tool in determining irreducible characters of groups.

(2.2.19) Theorem (Orthogonality general, see [7], Theorem 2.13)
It holds

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(gh)\chi_j(g^{-1}) = \delta_{ij} \frac{\chi_i(h)}{\chi_i(1)}, \quad \forall h \in G.$$ ◇

Now that we have the general orthogonality formula we want to derive more special cases. The first derived formula is the orthogonality relation for the rows of the character table. The second one gives the orthogonality relation for the columns.

(2.2.20) Corollary (1st orthogonality relation, see [7], Theorem 2.14)
Put k=1 then

$$\frac{1}{|G|} \sum_{g} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}.$$ ◇

(2.2.21) Corollary (2nd orthogonality relation, see [7], Theorem 2.18)
Let $g, h \in G$, *then*

$$\sum_{\chi \in Irr(G)} \chi(g)\overline{\chi(h)}$$

is equal to $|C_G(g)|$ *if* g *is conjugated to* h *and otherwise it is equal to* 0. ◇

Since we consider $\mathbb{C}$-characters, we can simplify a few formulae and get some significant properties. In particular we want to emphasise the importance of the first result in the following Lemma.

(2.2.22) Lemma (See [7], Lemma 2.15)
Let X be a $\mathbb{C}$-representation of G affording the character χ. Let $g \in G$ be an element of order n. Then

1. *$X(g)$ is similar to a diagonal matrix diag(ϵ_1,...,$\epsilon_{\chi(1)}$), where $\epsilon_1, ..., \epsilon_{\chi(1)}$ are nth roots of unity.*
2. *$\chi(g) = \sum_i \epsilon_i$ and $|\chi(g)| \leq \chi(1)$, for all $g \in G$.*
3. *$\chi(g^{-1}) = \overline{\chi(g)}$, for all $g \in G$.* ◇

Thanks to the previous Lemma, the orthogonality relation becomes simply to calculate in $\mathbb{C}$. This stimulates a new definition.

(2.2.23) Definition
Let ϕ and θ be $\mathbb{C}$-class functions of G. Then we define a bilinear form by

$$[\phi, \theta] = \frac{1}{|G|} \sum_g \phi(g)\overline{\theta(g)}. \tag{2.5}$$

◇

It is clear that this bilinear form is an inner product [7, p. 20 f.]. Furthermore, it establishes a particular connection between an arbitrary class function ϕ and the irreducible characters in $Irr(G)$, namely $\phi = \sum_i c_i\chi_i$, where $c_i = [\phi, \chi_i]$. Some convenient properties of this inner product are given by the following remark.

(2.2.24) Remark

1. *$[\cdot, \cdot]$ is symmetric.*
2. *$[\phi, \phi] = 1$ if and only if ϕ is irreducible.* ◇

(2.2.25) Example
We have calculated the characters for the dihedral group of order 8 in example (2.2.12). With the formula above we can easily check that the given characters are irreducible. ◇

2.2.2 Normal Subgroups from Character Tables

(2.2.26) Lemma (See [7], Lemma 2.19)
Let X be a $\mathbb{C}$-representation. Let χ be afforded by X. Then $g \in G$ is in the kernel of X if and only if $\chi(g) = \chi(1)$. ◇

(2.2.27) Definition
*We define $ker(\chi)$ to be the set $\{g \in G |\ \chi(g) = \chi(1)\}$. If $ker(\chi) = 1$ then the character χ is called **faithful**.* ◇

(2.2.28) Remark
Let χ be a character.

1. *If $\chi = \sum_{\chi_i \in Irr(G)} n_i\chi_i$ then $ker(\chi) = \bigcap_{n_i>0} ker(\chi_i)$.*

2. *Furthermore,* $\bigcap_{\chi_i \in Irr(G)} ker(\chi_i) = 1$.
3. $ker(\chi_i)$ *are subgroups of* G*, for all* $\chi_i \in Irr(G)$. ◇

Every normal subgroup is the intersection of some $ker(\chi_i)$. Suppose N is normal in G and let X be the regular representation of G/N. Then $ker(X) = N/N$. Now, consider X as a representation of G with kernel N and let X afford the character χ. Then

$$N = ker(X) = ker(\chi) = \bigcap_{[\chi,\chi_i] \neq 0} ker(\chi_i). \tag{2.6}$$

Recall that in the previous section we discussed representations of factor groups G/N, where N is normal in G. Next, we want to derive similar results on characters from this discussion.

(2.2.29) Lemma
Let N *be a normal subgroup of* G.

1. *Let* χ *be a character of* G*, then* $\overline{\chi}(gN) := \chi(g)$ *is a character of* G/N.
2. *Let* $\overline{\chi}$ *be a character of* G/N*, then* $\chi(g) := \overline{\chi}(gN)$ *is a character of* G.
3. *It holds:* $\chi \in Irr(G)$ *if and only if* $\overline{\chi} \in Irr(G/N)$. ◇

One possible problem is that at the transfer from G to G/N some conjugacy classes could have the same image in G/N. However, we can distinguish the conjugacy classes in G/N using characters.

(2.2.30) Lemma
Let $g, h \in G/N$*, then* g *is conjugate to* h *if and only if* $\chi(g) = \chi(h)$ *for all* $\chi \in Irr(G/N)$. ◇

Proof
The *if* part is clear by definition. The trick is to use the second orthogonality relation (2.2.21). Suppose $\chi(g) = \chi(h)$ holds for all $\chi \in Irr(G/N)$. After an application of this orthogonality relation we obtain

$$\sum_{\chi} \chi(g)\overline{\chi(h)} = \sum_{\chi} |\chi(g)|^2 = |C_{G/N}(g)|.$$

Therefore, g and h are conjugate. ■

By calculating the character table of G/N we can determine whether or not G/N is abelian. This can be used to show that $G' \subseteq N$.

(2.2.31) Proposition (See [7], Theorem 2.23)
$|G : G'|$ *is equal to the number of irreducible linear characters of* G. ◇

(2.2.32) Example
Now we will compute all normal subgroups of the dihedral group of order 8 (here G) using the previous results from example (2.2.12). Therefore, we only need the kernel of each character:

$$\begin{aligned} ker(\chi_1) &= G \\ ker(\chi_2) &= \{1\} \cup \{(1,3)(2,4)\} \cup \{(1,3),(2,4)\}. \\ ker(\chi_3) &= \{1\} \cup \{(1,3)(2,4)\} \cup \{(1,2,3,4),(1,4,3,2)\}. \\ ker(\chi_4) &= \{1\} \cup \{(1,3)(2,4)\} \cup \{(1,2)(3,4),(1,4)(2,3)\}. \\ ker(\chi_5) &= \{1\} \cup \{(1,3)(2,4)\}. \end{aligned}$$

Moreover, we want to calculate the character table of G/Z, where $Z = \{1,(1,3)(2,4)\}$ is the center of G:

	$1Z$	$(1,3)Z$	$(1,2,3,4)Z$	$(1,2)(3,4)Z$
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

As a result we see that G/Z is abelian. Actually it holds $G/Z \cong C_2 \times C_2$. Consequently, $G' \subseteq Z$. On the other hand, as G is not abelian G' is not trivial either. Hence $G' = Z$. These kind of groups are called extra-special groups (see chapter 5). ◇

2.2.3 Characters and the Center of a Group

As we have seen in the previous example, the center of a group can have some interesting properties. Where this is the case, we will study a subgroup related to the center, but in a more general sense. We will define this group using characters. Thus, it will be easy to identify this group by looking at the character table. On the other hand, if we have information about this group we can calculate the character table of an unknown group.

(2.2.33) Definition
Let χ be a $\mathbb{C}$-character of G. Then define $Z(\chi)$ to be the set $\{g \in G \mid \chi(1) = |\chi(g)|\}$. ◇

Since we are aiming for two theorems which give information about the index of $Z(\chi)$ in G, we will only present the next several results. For further reading we refer to [7, Chapter 2].

The following results provide a couple of valuable properties of $Z(\chi)$.

(2.2.34) Lemma (See [7], Theorem 2.27)
Let χ be a $\mathbb{C}$-character of G and X the corresponding representation. Then

1. $Z(\chi) = \{g \in G | X(g) = \epsilon \cdot I \text{ for some } \epsilon \in \mathbb{C}\}$
2. $Z(\chi)$ *is a subgroup of* G.
3. $\chi_{Z(\chi)} = \chi(1) \cdot \lambda$ *for some linear character* λ *of* $Z(\chi)$.
4. $Z(\chi)/ker(\chi)$ *is cyclic.*
5. $Z(\chi)/ker(\chi) \subseteq Z\left(G/ker(\chi)\right)$. *Specially, for an irreducible character holds equality.* ◇

(2.2.35) Corollary (See [7], Corollary 2.28)
It holds $Z(G) = \bigcap_{\chi \in Irr(G)} Z(\chi)$. ◇

By the previous corollary we can easily determine from the character table whether or not G is nilpotent. In order to give an answer we have to determine the upper central series. We calculate alternately the character table of G modulo the center and read out the center of the new group.

(2.2.36) Lemma
Let H be a subgroup of G and $\chi \in Irr(G)$. Then it holds $[\chi_H, \chi_H] \leq |G : H|[\chi, \chi]$ with equality if and only if $\chi(g) = 0$ for all $g \in G \setminus H$. ◇

Proof (See [7], Lemma 2.29)

$$|H|[\chi_H, \chi_H] = \sum_{h \in H} |\chi(h)|^2 \leq \sum_{g \in G} |\chi(g)|^2 = |G|[\chi, \chi]. \tag{2.7}$$

■

(2.2.37) Corollary (See [7], Corollary 2.30)
If χ is an irreducible character then it holds $\chi(1)^2 \leq |G : Z(\chi)|$. In particular, equality holds if and only if $\chi(g) = 0$ for all $g \in G \setminus Z(\chi)$. ◇

The corollary above is a powerful tool for the calculation of the character table. We already know, that $\chi(1)^2 \leq |G|$, for $\chi \in Irr(G)$. Now, we have $\chi(1)^2 \leq |G : Z(G)|$ and if equality holds then $Z(\chi) = Z(G)$ and χ vanishes on $G \setminus Z(G)$. This will be a useful tool to determine characters of extra-special groups; specially, the following two results will simplify our effort.

(2.2.38) Theorem (See [7], Theorem 2.31)
Let $\chi \in Irr(G)$ and $G/Z(\chi)$ be abelian. Then equality holds in the corollary above, i.e., $|G : Z(\chi)| = \chi(1)^2$. ◇

(2.2.39) Corollary
Let $|G'| = p$ be a prime, $G' \subseteq Z(G)$ and $\chi \in Irr(G)$ a non linear character. Then $\chi(1)^2 = |G : Z(G)|$. ◇

Proof
The idea is to show that $Z(G) = Z(\chi)$ and to apply the preceding result. First, we show that a non linear character χ satisfies the conditions from the previous result (2.2.38).

Since $G' \subseteq Z(G) \subseteq Z(\chi)$, the factor group $G/Z(\chi)$ is abelian and thus, by theorem (2.2.38), it holds $|G : Z(\chi)| = \chi(1)^2$. Note that $\chi(1)^2 > 1$ holds, since χ is non linear. Now for the harder part. It remains to show that $Z(G) = Z(\chi)$.

By corollary (2.2.35) $Z(G)$ is the intersection of all $Z(\chi)$, for $\chi \in Irr(G)$. Thus, $Z(G)$ is a subset of $Z(\chi)$. Conversely, take an element $g \in Z(\chi)$. Suppose there exists an element $x \in G$ with non trivial commutator $1 \neq [g, x] =: h$. Since G' has prime order, the element h generates G'. Furthermore, let X be the representation affording χ, then

$$X(h) = X(g)^{-1}X(x)^{-1}X(g)X(x) = \alpha^{-1}IX(x)^{-1}\alpha IX(x) = I.$$

Hence, G' is in the kernel $ker(X) = ker(\chi)$. Now, the factor group $G/ker(\chi)$ is abelian. It follows by theorem (2.2.34) that $Z/ker(\chi) = Z(G/ker(\chi)) = G/ker(\chi)$ and thus $|G : Z(\chi)| = 1$. A contradiction. ■

(2.2.40) Example
Recall that we computed the character table of the dihedral group of order 8 by calculating the traces of the representations given in example (2.2.2). On the other hand, if the character values are unknown, one can use some of the results above to determine these. For instance, we will calculate the values of the single non trivial character.

Suppose we know that $Z(G) = G'$ has order 2. By the preceding corollary (2.2.39) the non trivial character has degree 2 and vanishes on $G \setminus Z(G)$. By the first orthogonality relation (2.2.20) the other value of χ on the center has to be -2. Hence, we obtain

a_i:	1	$(1,3)(2,4)$	$(1,3)$	$(1,2,3,4)$	$(1,2)(3,4)$
χ_5	2	-2	0	0	0

◇

The next few results are of a different kind then the ones on the center of G. However, we want to mention them here, since they are about the values of characters. In particular, we determine what properties the degree of the characters need to have. Another more intuitive result, but somewhat harder to proof, is the result from Burnside which says that if a character is non linear then it has 0 as a value.

(2.2.41) Lemma (See [7], Theorem 3.11)
Let χ be an irreducible character then $\chi(1)$ divides $|G|$. ◇

The next result improves the one above.

(2.2.42) Theorem (See [7], Theorem 3.12)
Let χ be an irreducible character then $\chi(1)$ divides $|G : Z(\chi)|$. ◇

Now comes an intuitive but important result from Burnside.

(2.2.43) Theorem (See [7], Theorem 3.15)
Let χ be an irreducible non linear character then $\chi(g) = 0$ for some $g \in G$. ◇

2.3 Tensor Products and Products of Characters

In this last section we will investigate the problem; what happens if one multiplies two characters To be more precise, we know that for two characters χ and ϕ the product $(\chi\phi)(g) = \chi(g)\phi(g)$ is a class function. The question now is more subtle; is $\chi\phi$ a character Indeed the answer is yes. In particular, the characters of direct products of groups are given by this construction. Afterwards, we are going to study the relationship between the rings $F[G \times H]$ and its building blocks $F[G]$ and $F[H]$.

To discuss this issue we need to introduce the tensor product of two vector spaces and an action of G on it.

(2.3.1) Definition
Let V and W be F-vector spaces. Then a tensor product (T, ϕ) of V and W over F is an F-vector space T and a bilinear map $\phi : V \times W \to T$, such that for any bilinear map $\psi : V \times W \to U$ into the F-space U there exists a unique linear map $\alpha : T \to U$ with $\psi = \alpha\phi$. We will write $V \otimes W$ instead of T. ◇

(2.3.2) Lemma (See [15], Part 1, Chapter 1, Lemma 3.2)
Let V and W be F-spaces with basis (v_i) and (w_j). Then $(v_i \otimes w_j)$ is a basis for $V \otimes W$. Furthermore, every element $x \in V \otimes W$ can be written uniquely as the finite sum

$$x = \sum_i v_i \otimes x_i, \quad \text{for } x_i \in W \tag{2.8}$$

or as

$$x = \sum_j x'_i \otimes w_j, \quad \text{for } x'_i \in V. \tag{2.9}$$

◇

Now, we can make use of some more structure and see what happens to the tensor product.

(2.3.3) Lemma (See [15], Part 1, Chapter 1, Lemma 3.3)
Let V and W be F-algebras. Then $V \otimes W$ is an F-algebra with multiplication given by

$$(v_1 \otimes w_1)(v_2 \otimes w_2) = (v_1 v_2) \otimes (w_1 w_2), \quad \text{for all } v_1, v_2 \in V, w_1, w_2 \in W. \tag{2.10}$$

◇

At this place we have enough information to describe characters of tensor products. However, let us determine the action of FG on the tensor product first. Suppose V and W are FG-modules. The group G acts on $V \otimes W$ by

$$g(v_i \otimes w_j) := gv_i \otimes gw_j. \tag{2.11}$$

We extend this action to an action of FG by

$$x\left(\sum a_g g\right) := \sum a_g(xg), \tag{2.12}$$

where $x \in V \otimes W$ and $\sum a_g g \in FG$.

Again, we will present the next few result using the complex numbers $\mathbb{C}$. This way the reader gets more insight into the situation on how characters of direct products of groups are generated. Afterwards, we will give a more general result.

(2.3.4) Theorem (See [7], Theorem 4.1)
Let V and W be $\mathbb{C}[G]$-modules which afford the characters χ and ϕ. Then $V \otimes W$ affords $\chi\phi$ and this construction is independent of the choice of basis. ◇

(2.3.5) Corollary
Products of characters are characters. ◇

The next result is significant for the calculation of character tables of direct products of groups. Firstly, we introduce some notation.

(2.3.6) Definition
Let $G = H \times K$ be the direct product of the groups H and K and let θ and ϕ be class functions on H and K, respectively. Define $\chi = \theta \times \phi$ by

$$\chi(hk) = \theta(h)\phi(k), \quad \text{for } h \in H \text{ and } k \in K. \tag{2.13}$$

◇

(2.3.7) Lemma
If θ and ϕ are characters then $\chi = \theta \times \phi$ is a character as well. ◇

Proof (See [7], p. 59)
Since H is isomorphic to the factor group G/K, the character θ corresponds to $\overline{\theta}(hk) = \theta(h)$ with $K \subseteq ker(\theta)$. Similarly, since K is isomorphic to G/H, the character ϕ corresponds to $\overline{\phi}(hk) = \phi(k)$ with $H \subseteq ker(\phi)$. Therefore, the class function $\chi(hk) = (\theta \times \phi)(hk) = \theta(h)\phi(k) = \overline{\theta}(h)\overline{\phi}(k)$ is a character. ■

(2.3.8) Theorem
Let $G = H \times K$ be the direct sum of the groups H and K. Then the characters in

$$\{\theta \times \phi \mid \theta \in Irr(H),\ \phi \in Irr(K)\}$$

are exactly the irreducible characters of G. ◇

Proof (See [7], Theorem 4.21)
Let $\theta, \theta_1 \in Irr(H)$ and $\phi, \phi_1 \in Irr(K)$. Suppose $\chi = \theta \times \phi$ and $\chi_1 = \theta_1 \times \phi_1$. Then it holds $[\chi, \chi_1] = [\theta, \theta_1][\phi, \phi_1]$. Hence, the characters $\theta \times \phi$ are distinct and irreducible. Moreover,

$$\sum_{\theta \in Irr(H); \phi \in Irr(K)} (\theta \times \phi)(1)^2 = |H||K| = |G|. \tag{2.14}$$

Thus all the elements of $Irr(G)$ are given by the construction $\theta \times \phi$. ■

(2.3.9) Example
The easiest direct product is $C_2 \times C_2$. Suppose this group is generated by $\langle a \rangle \times \langle b \rangle$. The character table of C_2 is given by

$$\begin{array}{c|cc} & 1 & a \\ \hline \chi_1 & 1 & 1 \\ \chi_2 & 1 & -1 \end{array} \tag{2.15}$$

Let M be the character table of C_2, namely $M := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. By the previous theorem the character table of $C_2 \times C_2$ is given by the tensor product (use the Kronecker product for matrices)

$$M \otimes M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{2.16}$$

After permuting rows and columns this table is equal to the character table of $C_2 \times C_2$ given in example (2.2.32). ◇

As mentioned before we will now give the more general result. On one hand it implies the previous one and on the other hand it determines the structure of $F[G \times H]$, for groups G and H.

(2.3.10) Theorem
Let $G \times H$ be a direct product of two finite groups and F a field. Then

$$F[G \times H] \cong F[G] \otimes_F F[H]. \tag{2.17}$$

◇

Proof (See [15], Part 1, Chapter 1, Lemma 3.4)
It is easy to check that $\phi : F[G \times H] \to F[G] \otimes F[H], \quad \sum a_{gh}(g,h) \mapsto \sum a_{gh} g \otimes h$ is an isomorphism. ■

3 Classical Coding Theory

The subject on classical coding theory was born in the 1950s. It deals with arrays of length n over some alphabet A. Owing to the linearity property to compute the *minimum distance* between two codewords, the former setting developed into the idea to consider vectors in vector spaces over a finite field. A *linear code* is a subspace of this finite vector space. The minimum distance and the dimension of this subspace give information about the quality of a code. Thus, in this chapter we will introduce this concept. We want to highlight two ideas. First, we want to emphasize the idea of equivalences of codes. Since we will use *permutation* and *monomial* equivalences later, we recommend the reader to begin thinking in this manner. Second, we want to highlight the section on cyclic codes, which are the most important codes, since there are good decoding algorithms for practical use.

3.1 The Main Problem in Coding Theory

Coding theory is a very young mathematical topic. It started on the basis of transferring information from one place to another. For instance, suppose we are using electronic devices to transfer information (telephone, television, etc.). Here, information is converted into bits of 1's and 0's and sent through a channel, for example a cable or via satellite. Afterwards, the 1's and 0's are reconverted into information again. Due to technical problems, one can assume that while the bits are sent through the channel, there is a positive probability p that single bits are being changed. Thus the received bits could be wrong. The idea of coding theory is to give a method of how to convert the information into bits, such that there are no mistakes in the received information, or such that at least some of them are corrected. On this account, encoding and decoding algorithms are used to convert and reconvert these bits properly. Some examples of these algorithms are given in [10].

3.2 Linear Codes and Other Basic Definitions

(3.2.1) Definition
*Let F be a finite field and n a non negative integer. A **linear code** C of length n is a subspace of F^n. A **generator matrix** G of C is a matrix such that the rows form a basis of C. A **parity check matrix** H is a matrix which satisfies $HG^T = 0$.* ◇

We will agree that if we talk about codes in this dissertation then we always mean linear codes. Also, we want to remark that we introduced linear codes as column vectors. Nevertheless, we are going to use the row vector form as well and hope not to confuse the reader.

In order to define a code, it is common to give either a generator matrix of this code or equivalently a parity check matrix. By the formula $HG^T = 0$ we can calculate one matrix from the other and vice versa.

(3.2.2) Example
We define the code $C \leq \mathbb{F}_2^7$ to be given by the parity check matrix H. Equivalently, we will present the generator matrix G.

$$H := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad G := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

This code is called Hamming code and we will define these kind of codes later in this chapter. This code has length 7 and dimension 4. ◇

Next we will define the *minimum distance* of a code.

(3.2.3) Definition
Let $C \leq F^n$ be a code.

1. *Let $c, c' \in C$. The number $d(c, c') = |\{i \in \{1, ..., n\} \mid c_i \neq c'_i\}$ is called the **Hamming distance** of c and c'; moreover, $d = d(C) = \min\{d(c, c') \mid c, c' \in C\}$ is the **minimum distance** of the code C.*
2. *The number $wt(c) = d(c, 0) = |\{i \in \{1, ..., n\} \mid c_i \neq 0\}$ is the **Hamming weight** of c.* ◇

(3.2.4) Remark
For a linear code C holds $d(c, c') = wt(c - c')$, for $c, c' \in C$. Therefore, $d = wt(C) = \min\{wt(c) \mid c \in C\}$. The parameter d tells us that the number of flaws which can be corrected is $\lfloor \frac{d-1}{2} \rfloor$. ◇

Finally, we have introduced all the usual parameters of a code, and thus we will introduce a new notation.

(3.2.5) Definition
Let $C \leq F^n$ be a code of length n, dimension k, and minimum distance d. Then we call C a $[n,k,d]$-code. ◇

In order to describe the weights of the codewords in a code, we introduce the weight enumerator and the complete weight enumerator:

(3.2.6) Definition
Let $\mathbb{C}[x,y]$ be the polynomial ring in x and y over the complex numbers $\mathbb{C}$ and let $C \leq F^n$ be a code over the finite field F. Then:

1. *The polynomial*

$$h(C)(x,y) = \sum_{c \in C} x^{n-wt(c)} y^{wt(c)} \in \mathbb{C}[x,y] \tag{3.1}$$

   *is called **(Hamming-) weight enumerator**.*

2. *Let $c \in C$ and $a \in F$. Furthermore, let $\#_a(c)$ the denote the number $|\{i \mid c_i = a\}|$. Then, the polynomial*

$$p(C) = \sum_{c \in C} \prod_{a \in \mathbb{F}} x_a^{\#_a(c)} \in \mathbb{C}[x_a | a \in \mathbb{F}] \tag{3.2}$$

   *is called **complete weight enumerator**.* ◇

Many more things can be said at this place about general linear codes than we say here. For instance, the first and basic decoding method is using *syndromes*, or in other words cosets of a linear code. In this method, the parity check matrix decodes the received words. Other aspects include investigating the error probability of received words or how a code can be extended to longer code. However, we will leave these topics to the reader and refer to [12, Chapter 1].

— Dual Codes —

The next section deals with bilinear forms and duality. We will shortly present an important result by MacWilliams on the weight enumerator. The concept of dual codes has been widely studied and the best codes are, indeed, self-dual codes. For detailed results we refer to [17]. Although we introduce more general bilinear forms, we will merely use the standard scalar product in this dissertation.

(3.2.7) Definition
*Let $C \leq F^n$ be a code and $\beta : F^n \times F^n \to F$ a non-degenerate bilinear or Hermitian form. Then the **dual** of a code C is*

$$C^\perp = \{x \in F^n \mid \beta(x,y) = 0 \text{ for all } y \in C\}. \tag{3.3}$$

*A code C is **self-dual** if $C = C^\perp$.* ◇

(3.2.8) Theorem (MacWilliam's Identity, see [12], Chapter 5 §6.)
Suppose $q = p^m$ is a prime power, $F = \mathbb{F}_q$ and $C \leq F^n$ is a code with weight enumerators $h(C)$ and $p(C)$. Then for the dual code $C^\perp$ holds:

$$h(C^\perp)(x,y) = \frac{1}{|C|} h(C)(x + (q-1)y, x - y) \tag{3.4}$$

and

$$p(C^\perp)(x_0, ..., x_{p-1}) = \frac{1}{|C|} p(C)(y_0, ..., y_{p-1}), \tag{3.5}$$

where $y_i = \sum_{j=0}^{p-1} \zeta_p^{ij} x_j$ and ζ_p is a pth root of unity in $\mathbb{C}$. ◇

(3.2.9) Example
Let $C = \langle 110, 011 \rangle$ be a binary code. The dual $C^\perp$ is $\langle 111 \rangle$. Thus the weight enumerators are $h(C) = x^3 + 3xy^2$ and $h(C^\perp) = x^3 + y^3$. ◇

— Equivalence of Codes —

(3.2.10) Definition
Let $F = \mathbb{F}_{p^m}$ be a finite field and n a positive integer. Then

1. *$P(F^n)$ consists of all permutation matrices of $GL(n, F)$.*
2. *$M(F^n)$ consists of all monomial matrices of $GL(n, F)$.*
3. *$A(F^n)$ consists of all products of elements $\alpha \circ \beta$, where $\alpha \in M(F^n)$ and $\beta \in Gal(F|\mathbb{F}_p)$.* ◇

(3.2.11) Remark
Matrices act on F^n as usual and $Gal(F|\mathbb{F}_p)$ acts on F^n by acting on the coordinates. ◇

(3.2.12) Definition
Let C and D be codes over F of length n. We say that C and D are

1. ***permutation equivalent** if there exists an element $x \in P(F^n)$ such that $xC = D$.*
2. ***monomial equivalent** if there exists an element $x \in M(F^n)$ such that $xC = D$.*
3. ***equivalent** if there exists an element $x \in A(F^n)$ such that $xC = D$.*

*Furthermore, $PAut(C) = \{x \in P(F^n) \mid xC = C\}$ is called the **permutation automorphism group** of C ($MAut(C)$ and $Aut(C)$ respectively).* ◇

(3.2.13) Example
Suppose C, D and E are codes over $\mathbb{F}_5$ given by $C := \langle (1,0,1,0), (0,1,0,1) \rangle$, $D := \langle (1,1,0,0), (0,0,1,1) \rangle$ and $E := \langle (1,2,0,0), (0,0,1,3) \rangle$. Then C and D are permutation equivalent and E is monomial equivalent to both C and D. ◇

(3.2.14) Remark

1. *Obviously we can identify $P(F^n)$ with the symmetric group S_n.*
2. *The group $M(F^n)$ is more tricky, since for an element $x \in M(F^n)$ and $v = (v_1, ..., v_n)^T \in F^n$ the action is given by*

$$xv = \begin{pmatrix} \lambda_1 v_{\pi(1)} & \lambda_2 v_{\pi(2)} & \cdots \lambda_n v_{\pi(n)} \end{pmatrix}^T,$$

for $\pi \in S_n$ and $\lambda_i \in F^\times$, for $i = 1, ..., n$. Thus, $M(F^n)$ is isomorphic to the semidirect product $(F^\times)^n \rtimes S_n$. ◇

— Bounds on Linear Codes —

Now, we will present some restrictions on the parameters of a linear code. These restrictions can be useful for determining missing parameters.

(3.2.15) Definition
We define $A_q(n, d)$ to be the maximal number such that there exists a code over the Galois field $\mathbb{F}_q$ of length n and minimum distance at least d with precisely $A_q(n, d)$ elements exists. ◇

Note that for linear codes it has to be $A_q(n, d) = q^k$ for some k. Therefore, $A_q(n, d)$ is the maximal number such that there exists a $[n, k, d]$-code.

(3.2.16) Example
Suppose $n = d$. Then $C := \langle (1 \cdots 1) \rangle \leq \mathbb{F}_q^n$ is the only code satisfying the condition above. Thus $A_q(n, n) = |C| = q$ ◇

(3.2.17) Proposition (Singleton bound)
Let C be a $[n, k, d]$-code. Then it holds $k \leq n - d + 1$. ◇

Proof (See [10], Satz 4.1.4)
Delete the last $d - 1$ symbols of each codeword. This new elements form another code of length $n - d + 1$, dimension k and minimum distance at least 1. ■

(3.2.18) Example
Suppose C is the binary $[3, 2, 2]$-code given by $\langle (1, 1, 0), (0, 1, 1) \rangle$. Then, clearly, $A_2(3, 2) \geq |C| = 4$. Using the Singleton bound we obtain that $A_2(3, 2) \leq |C| = 4$. Thus, there is no $[3, 2, 2]$-code with a bigger dimension. ◇

(3.2.19) Proposition (Hamming bound)
Let C be a code of length n and minimum distance $2d + 1$ over $\mathbb{F}_q$. Then it holds

$$|C| \leq \frac{q^n}{\sum_{i=0}^{d} (q-1)^i \binom{n}{i}}.$$ ◇

Proof
First note that we can put a sphere of radius d on each codeword in C such that all the spheres are disjoint (otherwise the code would not be d-error-correcting). Thus the number of elements of $\mathbb{F}_q^n$ which are inside a sphere is

$$|C| \cdot \left(\sum_{i=0}^{d} (q-1)^i \binom{n}{i} \right). \qquad \blacksquare$$

The next bound we will only give as a reference [10, Satz 5.2.4].

(3.2.20) Proposition (Plotkin bound)
For $t = \frac{q-1}{q}$ and two positive integers n and d with $tn < d \leq n$ holds

$$A_q(n,d) \leq \frac{d}{d-tn}. \qquad \diamond$$

3.3 Cyclic Codes

The cyclic codes are the most important kind of codes. In fact almost all codes used for practical issues are cyclic codes. This is due to the existence of fast encoding and decoding algorithms. Two examples of these algorithms are presented in [10, Sections 3.4 and 3.5]. Before we give an example, we determine what cyclic codes are and give their properties.

(3.3.1) Definition
*Let C be a code of length n over the finite field F. A **cyclic** code is a code with the property, if $(c_0, ..., c_{n-2}, c_{n-1}) \in C$ then $(c_{n-1}, c_1, ..., c_{n-2}) \in C$.* $\diamond$

Obviously, we can identify a cyclic code as a subspace of $F[x]/(x^n - 1)$, using $(c_0, ..., c_{n-1}) \mapsto \sum_{i=0}^{n-1} c_i x^i$. Furthermore, by this correspondence it holds that a linear code is cyclic if and only if it is an ideal in $F[x]/(x^n - 1)$.

(3.3.2) Remark
*Since $F[x]/(x^n - 1)$ is a principal domain, any ideal in R is a principal ideal, i.e., it is generated by a single polynomial, say g. Therefore, we will call g **generator polynomial**.* $\diamond$

(3.3.3) Example
Assume C is the code given by $\langle (1,0,1,0), (0,1,0,1) \rangle \leq \mathbb{F}_5$ in example (3.2.13). Clearly, C is cyclic and corresponds to the ideal generated by $\left(1 + x^2, x + x^3\right) \trianglelefteq \mathbb{F}_5[x]/(x^4 - 1)$. We can immediately see that $g(x) = x^2 + 1$ is the generator polynomial of the code C. $\diamond$

Let q and n be coprime. Assume $f(x) \in F[x]$ is a normed polynomial of degree n which factorizes into irreducible polynomials, say $f(x) = f_1(x) \cdots f_r(x)$. By the Chinese Remainder Theorem [10, Satz 3.2.1] each $R_i := F[x]/(f_i(x))$, for $i = 1, ..., r$, corresponds to a minimal ideal of $R := F[x]/(f(x))$ and it holds

$$R \cong \bigoplus_{i=1}^{r} R_i. \tag{3.6}$$

Consequently, we obtain:

(3.3.4) Corollary

1. *Every cyclic code is a direct sum of minimal cyclic codes.*
2. *There exist 2^r cyclic codes.*

Also, by equation (3.6), we can write the element $1 \in R$ as a sum $1 = \sum_{i=1}^{r} e_i$, for $e_i \in R_i$. It is a simple fact that each e_i is a primitive idempotent and generates the minimal ideal R_i. It follows:

(3.3.5) Corollary

If C is a cyclic code then there exists an idempotent in $F[x]/(x^n - 1)$ which generates C. ◇

The next result given tells us something about the relationship between the generating polynomial and the generating idempotent. For the proof see [10, Lemma 3.2.7].

(3.3.6) Lemma

We obtain the generating polynomial g from the idempotent e via

$$g = gcd(e, x^n - 1).$$ ◇

(3.3.7) Example

We will go on with the example (3.3.3). The code C has the generating polynomial $g(x) = x^2 + 1$. By the previous lemma we can calculate the idempotent. We obtain

$$e(x) = (x^2 + 1) \cdot (x - 1) = x^3 + 4x^2 + x + 4,$$

and clearly $g(x) = e(x) \cdot (x^3 + x^2 + x + 1)$. Thus, both generate the code C. ◇

3.3.1 Some Examples of Cyclic Codes

— **Reed-Solomon Codes** —

Reed-Solomon codes are of major importance for practical use. These codes are used to correct errors on several types of data media. For instance, they are used to read the data on compact discs and to decode them properly. Thus we will present this code to the reader. For a more detailed approach we refer to [12].

(3.3.8) Definition
Let $F = \mathbb{F}_q$ be a finite field, for $q = p^m$, and $F^\times = \langle \alpha \rangle$. Furthermore, set $n = q - 1$ and $1 \leq k \leq n - 1$. The code

$$C := \{\Big(f(\alpha^0), f(\alpha^1), ..., f(\alpha^{n-1})\Big) \in F^n \mid f \in F[z],\ \deg(f) \leq k\} \tag{3.7}$$

*is called **Reed-Solomon code**.* ◇

(3.3.9) Remark
C is a cyclic code. ◇

Proof
Assume $x \in C$ with $x_i = f(\alpha^{i-1})$, for $1 \leq i \leq n$, and a polynomial f. We define the polynomial g by $g(z) = f(\alpha z)$. Both have the same degree and it holds $g(\alpha^{i-1}) = f(\alpha^i) = x_{i+1}$, for all $1 \leq i \leq n$. ■

(3.3.10) Proposition (See [10], Satz 4.1.3)
The code C has the generator polynomial $g(z) = (z - \alpha^{k+1}) \cdots (z - \alpha^{n-1})$. ◇

(3.3.11) Example
Let C be the code over $\mathbb{F}_4$, where $\mathbb{F}_4^\times = \langle \alpha \rangle$, with generator matrix $\begin{pmatrix} 1 & 0 & \alpha^2 \\ 0 & 1 & \alpha \end{pmatrix}$. We obtain the code C from the definition using $k = 1$; moreover, by the preceding proposition, the generator polynomial of C is $g(z) = z + \alpha^2$.

Another good property of this code is that we are able to determine the minimum distance easily. Moreover, equality holds for the Singleton bound. This bound gives us the minimum distance.

(3.3.12) Theorem (See [10], Satz 4.1.6)
If C a Reed-Solomon code then C satisfies the Singleton bound, i.e., $d = n - k + 1$. ◇

— **Binary Hamming codes** —

The class of Hamming codes is another class of important cyclic codes. The Hamming codes are easily encoded and decoded. In this section we will consider binary Hamming codes only.

(3.3.13) Definition
*The **Hamming code** H_r is a code of length r whose parity check matrix has columns consisting of all non zero vectors of $\mathbb{F}_2^r$.* ◇

(3.3.14) Example
The $[7, 4, 3]$-code from example (3.2.2) is a Hamming code. ◇

(3.3.15) Lemma
A Hamming code has length $2^r - 1$, dimension $2^r - 1 - r$ and minimum distance 3. ◇

Proof
The length and dimension of a Hamming code are clear. We will show that the minimum distance is $d = 3$. Let H be the parity check matrix of this code. Since H has no zero column, it can not be $d = 1$. Assume $d = 2$ and let v be the vector with Hamming distance 2. Assume $v_i = v_j = 1$, for $1 \leq i < j \leq r$. Now let b be given by $Hv^T = b^T$. Then $b = h_i + h_j$, where h_l are the columns of H, for $1 \leq l \leq 2^r - 1$. Since $i \neq j$, the sum $h_i + h_j$ is not the zero vector. Thus v is not in the code. ■

(3.3.16) Theorem
For the Hamming code C of length n, dimension k and minimum distance d holds $d = n - k + 1$. ◇

Proof
Since $d = 3$, we can put spheres of radius 1 around each codeword. Then each element in $\mathbb{F}_2^r$ is in exactly one sphere. ■

We can identify each column of the parity check matrix of a Hamming code with an element of the Galois field $\mathbb{F}_{2^r}$. If α is a primitive element in this field then we obtain by this identification the matrix

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2r-2} \end{pmatrix}.$$

The minimal polynomial of α is the generator polynomial of this code. We will just refer to the proof of this fact [12, Ch. 7. §3.] and summarize this result in the following theorem.

(3.3.17) Theorem
The Hamming code H_r *is a cyclic code.* ◇

4 A Description of Group Codes

In this chapter we are going to investigate the structure of group codes and give a criterion to decide if a linear code is a group code. Many classical linear codes have been shown to be group codes. It started when F. J. MacWilliams [12] identified cyclic codes which are ideals in $F[x]/(x^n - 1)$ with ideals in FC_n, where C_n is the cyclic group of order n. Over the years the idea of abelian codes was introduced to generalize cyclic codes. Abelian codes are ideals over the group ring FG, where G is an abelian group. At the moment there is still no satisfying description of abelian group codes. However, there is a promising property of groups, namely the abelian decomposition of a group, which implies that every group code is abelian. Recently, group properties, such as nilpotency, are investigated in order to find a sufficient condition for codes to be abelian. This is the point where this thesis contributes to the investigation.

Initially we will define the term *group code* and present the criterion on groups given by A. d. Rio [1, Theorem 1.2]. Then we will generalize the concept of group codes which are permutation equivalent to group codes which are monomial equivalent (Theorem (4.1.13)). The next part of this chapter focuses on the investigation of abelian group codes and the abelian decomposition of groups. Finally, we will determine whether or not there are group codes, where the group is nilpotent, which are not abelian group codes. A counterexample using p-groups is given as a result (Theorem (4.3.5)).

4.1 Group Codes and a Criterion

(4.1.1) Remark

1. *Let S_n be the symmetric group on n points and F a finite field. Then S_n acts on F^n via*

$$\sigma(x_1, ..., x_n) = (x_{\sigma(1)}, ..., x_{\sigma(n)}), \quad \text{for } (x_1, ..., x_n) \in F^n, \sigma \in S_n.$$

   In the preceding chapter we called two codes $C_1, C_2 \leq F^n$ permutation equivalent if there is an element $\sigma \in S_n$ such that $\sigma(C_1) = C_2$.

2. *The action of the group $M(F^n)$ of monomial equivalences on the space F^n is given*

by

$$a(x_1, ..., x_n) = (\lambda_1 x_{\pi(1)}, ..., \lambda_n x_{\pi(n)})$$

for $(x_1, ..., x_n) \in F^n$, $a \in M(F^n)$, $\pi \in S_n$ *and* $\lambda_1, ..., \lambda_n \in F^\times$. *Therefore, we will identify* $M(F^n)$ *with the semidirect product*

$$\left(F^\times\right)^n \rtimes S_n = \{\lambda \cdot \pi \mid \lambda \in \left(F^\times\right)^n, \pi \in S_n\}.$$

3. *Let* $C \leq F^n$ *be a code. We set*

$$PAut(C) := \{\sigma \in S_n \mid \sigma(C) = C\}$$

and

$$MAut(C) := \{\lambda \cdot \pi \in M(F^n) \mid (\lambda \cdot \pi)(C) = C\}. \quad \diamond$$

(4.1.2) Definition
Let G *be a finite group and* F *a finite field. If we choose a basis* $\{g_1, ..., g_n\}$ *of* FG *then any (left/right) ideal* I *of* FG *defines a linear code* $C \leq F^n$ *by*

$$(a_1, a_2, ..., a_n) \in C \Leftrightarrow a_1 g_1 + a_2 g_2 + \cdots + a_n g_n \in I.$$

Any code which is permutation equivalent to C *for some (left/right) ideal* I *of* FG *is called a* ***(left/right)*** G***-code****.*

Similarly, any code which is monomial equivalent to C *for some (left/right) ideal* I *of* FG *is called a* ***(left/right)*** G***-mcode****.*

A (left/right) ***abelian group code*** *(respectively,* ***cyclic group code****,* ***solvable group code****, etc.) is a* G*-code for some abelian (respectively, cyclic, solvable, etc.) group* G *(respectively* ***abelian group mcode****, etc.).* $\diamond$

(4.1.3) Remark
Every G*-code is a* G*-mcode.* $\diamond$

(4.1.4) Example
The code $C = \langle (1,0,2,0), (0,1,0,3) \rangle \leq \mathbb{F}_5^4$ *is an* C_4*-mcode but not a* C_4*-code (see example (3.2.13)).* $\diamond$

Before we present a theorem by A. d. Rio on the description of G-codes, we need some prerequisites.

(4.1.5) Lemma (See [1], Lemma 1.1)
Let G *be a regular subgroup of* S_n *and fix* $i_0 \in \{1, ..., n\}$. *Let* $\psi : G \to \{1, ..., n\}$ *be a bijection given by* $\psi(g) = g(i_0)$, *for* $g \in G$. *Then there is an anti-isomorphism* $\sigma : G \to C_{S_n}(G)$, $g \mapsto \sigma_g$ *and it holds*

$$\sigma_g(i) = \psi^{-1}(i)(g(i_0)), \quad \text{for } i \in \{1, ..., n\}. \quad \diamond$$

(4.1.6) Remark
Let G be a regular subgroup of S_n and assume we are in the situation as in the lemma above. Then for $h \in G$ the action of σ_h on the set $\{1,...,n\}$ induces an action of σ_h on the basis $\{g_1,...,g_n\}$ of FG given by the identification $\psi(g_i) = i$, where $g_i(i_0) = i$ for $1 \leq i \leq n$, and the equation

$$\sigma_h(g_i) = g_{\sigma_h(i)} = g_{\psi^{-1}(i)h(i_0)} = \psi^{-1}((\psi^{-1}(i)h)i_0) = \psi^{-1}(i)h = g_ih$$

Thus σ_h acts by right multiplication with an element of G on FG. We will identify $\sigma(G)$ with this right multiplication of G. ◇

The next theorem gives an intrinsic description of G-codes. Later we will see that these results can be generalized to G-mcodes.

(4.1.7) Theorem
Let C be a linear code of length n over a field F and let G be a finite group of size n. Then, it holds:

1. *C is a left G-code if and only if G is isomorphic to a transitive subgroup of S_n which is contained in $PAut(C)$.*
2. *C is a G-code if and only if G is isomorphic to a transitive subgroup $H \leq S_n$ such that $H \cup C_{S_n}(H) \subseteq PAut(C)$.* ◇

Proof (See [1], Theorem 1.2)
Without loss of generality we may assume that G is a regular subgroup of S_n.

Assume C is permutation equivalent to the code D, where D is an left ideal of FG. Then, clearly, $G \subseteq PAut(D) = PAut(C)$. If D is a two sided ideal then, by the previous remark (4.1.6), $\sigma_g D = Dg = D$ and so it holds $C_{S_n}(G) \subseteq PAut(D) = PAut(C)$.

Conversely, assume $C \leq F^n$ is a code with $G \subseteq PAut(C)$. We can identify C with a subspace of the group ring FG. Since $gC = C$, for all $g \in G$, the subspace C is an ideal of FG. If, furthermore, $C_{S_n}(G) \subseteq PAut(C)$ then, again by the previous remark (4.1.6), $Cg = \sigma_g C = C$. Thus C is a two sided ideal of FG. ■

(4.1.8) Remark
Note that for $|G| = n$ the group S_n acts on the set of G-codes. Thus the set of G-codes is a union of isomorphism classes. Therefore, being a G-code is a property of the isomorphism class of a code. For instance the next example shows that all cyclic codes are C_n-codes, but not all C_n-codes are cyclic codes. Similarly, this is true for G-mcodes. ◇

(4.1.9) Example
Let C be the code given by $\langle(1,1,0,0),(0,0,1,1)\rangle \leq \mathbb{F}_5^4$ (see example (3.2.13)). Then, C is not a cyclic code but permutation equivalent to a cyclic code. Thus, C is a C_4-code. ◇

Before we give the generalization of the previous result we will describe the action of $MAut(C)$ on the code C.

(4.1.10) Remark
By the action of $M(F^n) = (F^\times)^n \rtimes S_n$ on F^n we obtain an homomorphism

$$\phi : M(F^n) \to S_n, \quad \lambda \cdot \pi \mapsto \pi. \qquad \diamond$$

Moreover, $PAut(C)$ is a subgroup of $\phi(MAut(C))$.

(4.1.11) Lemma
Suppose $H \leq M(F^n)$ such that $H \cong \phi(H)$, where $\phi(H)$ is a regular subgroup of S_n and ϕ the homomorphism given in the previous remark. Then H is conjugated to a subgroup of S_n, i.e., it exists an element $\lambda \in (F^\times)^n$ such that $\lambda^{-1}H\lambda$ can be identified with a subgroup of S_n. $\diamond$

Proof
Suppose $H = \{1, h_2, ..., h_n\}$ and let $E = \{e_1, ..., e_n\}$ be a basis of F^n. The group H acts regular on E. Furthermore, suppose $1e_1 = e_1$ and $h_i e_1 = \lambda_i e_i$, for $i = 2, ..., n$ and set $\lambda = \mathrm{diag}(1, \lambda_2, ..., \lambda_n) \in (F^\times)^n$. Then, by taking the transformed basis $\{e_1, h_2 e_1, ..., h_n e_1\}$, we obtain the equation

$$(\lambda^{-1} h_j \lambda) e_i = \lambda^{-1} h_j \lambda_i e_i = \lambda^{-1} h_k e_1 = e_k, \tag{4.1}$$

for all $1 \leq i, j \leq n$, where h_k is uniquely determined by $h_j h_i = h_k$. Since H is isomorphic to the regular group $\phi(H)$ we see that $\lambda^{-1}H\lambda$ permutes the basis E.■

Next, we will investigate the centralizer $C_{M(F^n)}(H)$.

(4.1.12) Lemma
Let $H \leq M(F^n)$ be the group from the preceding Lemma and assume $\lambda^{-1}H\lambda \leq S_n$. Then $C_{M(F^n)}(H) = \langle F^\times, C_{S_n}(\lambda^{-1}H\lambda)\rangle$. $\diamond$

Proof
Set $X := \langle F^\times, C_{S_n}(\lambda^{-1}H\lambda)\rangle$. Since we can assume that $H \leq S_n$ we obtain the inclusion $\supseteq$. Conversely, take an element $c \in C_{M(F^n)}(H)$. As in the previous proof the element c acts on the basis E. Without loss of generality we may assume that $ce_1 = e_1$ holds (otherwise we would multiply with an element of X). It is enough to show that c acts as the identity. This holds by the equation $ce_k = ch_k e_1 = h_k c e_1 = h_k e_1 = e_k$, where $1 \leq k \leq n$. ■

(4.1.13) Theorem
Let C be a linear code of length n over a field F and let G be a finite group of size n. Moreover, let ϕ be the homomorphism given in (4.1.10). Then, it holds:

1. *C is a left G-mcode if and only if G is isomorphic to a subgroup $H \leq MAut(C)$ such that $\phi(H)$ is a regular subgroup of S_n.*

2. *C is a G-mcode if and only if G is isomorphic to a subgroup $H \leq MAut(C)$ such that $H \cup C_{M(F^n)}(H) \subseteq MAut(C)$ and $\phi(H)$ is a regular subgroup of S_n.* ◇

Proof

1. Suppose C is a left G-mcode. Then C is monomial equivalent to a code D, where D is an left ideal of FG. Without loss of generality we may assume that G is a regular subgroup of S_n for some positive integer n. The group G permutes the code D, so G is a subgroup of $PAut(D)$. Moreover, it holds $PAut(D) \subseteq MAut(D)$. The result follows, since $MAut(D)$ equals $MAut(C)$. Conversely, suppose $G \leq MAut(C)$ for a code $C \leq F^n$ such that $\phi(G) \leq S_n$ is regular. Let $E := \{e_1, ..., e_n\}$ be a basis of F^n and let $\alpha : E \to G$, $e_{\phi(g)(1)} \mapsto g$ be a bijection which we will extend to a vector space isomorphism $\overline{\alpha} : F^n \to FG$. Suppose $\overline{\alpha}(C) = D$. The trick is to show that $gD = D$ for all $g \in G$.

   By the previous remark the group G acts regular on the set $\{1, ..., n\}$ via $g(i) = \phi(g)(i)$. Consequently, this induces an action of G on E. If $g, h \in G$ then it holds $g\alpha(e_{\phi(h)(1)}) = gh = \alpha(ge_{\phi(h)(1)})$ and since $\phi(G)$ is regular, it follows $g(\alpha(e_i)) = \alpha(g(e_i))$, for $i = 1, ..., n$. Therefore, $gD = g(\overline{\alpha}(C)) = \overline{\alpha}(gC) = \overline{\alpha}(C) = D$, since $g \in G \subseteq MAut(C)$.

2. Firstly, we note that together with the identification (4.1.6) we obtain from the conditions on H the relation $\phi(C_{MAut(C)}(H)) \leq C_{S_n}(\phi(H)) \cong \sigma(\phi(H))$. Furthermore, since the left group is regular it follows $\phi(C_{MAut(C)}(H)) \cong \sigma(\phi(H))$. Secondly, we go for the "if" part. We may suppose that $D := \psi(C)$ is a G-code, where $\psi \in M(F^n)$. Clearly, it holds $G \leq PAut(D) = MAut(D) \cap S_n$. Now, by the criterion (4.1.7) and identification (4.1.6), we obtain the relation $\sigma(G) \leq PAut(D)$. Conversely, we will assume that G equals H. Moreover, by Lemma (4.1.11) there exists an element $\lambda \in (F^\times)^n$ such that $\lambda^{-1}G\lambda \leq PAut(C) \leq S_n$. Thus, without loss of generality we may assume that $G \leq S_n$. Consequentely, we obtain $G \leq MAut(C) \cap S_n = PAut(C)$. The crucial point now is to show that $\sigma(G) \leq PAut(C)$. On this account we will consider the centralizer $C_{MAut(C)}(G)$. By the identification (4.1.6) and Lemma (4.1.12), we can identify the centralizer $C_{MAut(C)}(G)$ with $\langle F^\times, \sigma(G)\rangle$. Hence, it holds $\sigma(G) \leq MAut(C)$. Using the relation $\sigma(G) \cong \sigma(\phi(G)) \cong \phi(C_{MAut(C)}(G)) \leq S_n$ we obtain $\sigma(G) \leq MAut(C) \cap S_n = PAut(C)$. Thus, by the criterion (4.1.7), C is an G-code. ■

(4.1.14) Corollary

1. *A code C of length n is an abelian code if and only if there exists an abelian regular subgroup of S_n that is contained in $PAut(C)$.*

2. *A code C of length n is an abelian mcode if and only if there exists an abelian subgroup A of $MAut(C)$ such that $\phi(A)$ is regular.* ◇

Proof (See [2])

1. The "if" part holds by the equivalence of left G-codes (4.1.7). Conversely, if C is a left G-code for an abelian group G then C is clearly a two sided ideal of the commutative ring FG and thus an abelian code.
2. It is the same proof for G-mcodes as for G-codes. ■

4.2 Groups with an Abelian Decomposition

In the context of group codes several questions arise, for instance 'Are all left group codes abelian group codes?' or 'Are all group codes abelian group codes?'. In this section we will introduce a special class of groups which contains the class of abelian groups properly. This class is defined by the following property and we will show in the next section that for this class of groups, all group codes are abelian. This will give a partly answer to the second question.

(4.2.1) Definition
*We say that a group G has an **abelian decomposition** if there are two abelian subgroups $A, B \leq G$ such that*

$$G = AB = \{ab \mid a \in A, b \in B\}.$$ ◇

(4.2.2) Remark
Let AB be a group where A and B are two subgroups of a group G. Then AB satisfies

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

Thus, if both A and B are abelian and $|A|$ and $|B|$ are coprime then G has an abelian decomposition if and only if $|G| = |AB| = |A||B|$ holds. ◇

(4.2.3) Lemma
Assume that G has a normal abelian subgroup N with a cyclic quotient G/N. Then G has an abelian decomposition. ◇

Proof (See [2])
Say $G/N = \langle aN \rangle$. Then by the coset decomposition of G we see that $\langle a \rangle N$ generates G. ■

(4.2.4) Remark
In the previous Lemma it is not enough for the factor group G/N to be abelian. ◇

(4.2.5) Corollary
If G is a metacyclic group then it has an abelian decomposition. ◇

Proof
Follows by the previous result. ■

(4.2.6) Proposition
Any p-group of order p^3 and p^4 has an abelian decomposition. ◇

Proof (See [2])
Suppose G is non abelian. If G is of size p^3, then $G/Z(G)$ is abelian and it holds $|Z(G)| = p$. Consequently, there exists an element $xZ(G) \in G/Z(G)$ of order p; moreover, the group $\langle x, Z(G)\rangle$ is an abelian normal subgroup and the result follows by (4.2.3).

Now assume G is a non abelian group of order p^4. We consider two cases:

1. Suppose every normal abelian subgroup of G can be generated with at most two generators. Then, by [6, Kapitel III, Satz 12.4], G is either a metacylic group or it is the semidirect product of an abelian normal subgroup and a cyclic group. Hence the result follows by either corollary (4.2.5) or lemma (4.2.3).

2. Now suppose G has an abelian normal subgroup N generated by three elements. Then N is isomorphic to the group $C_p \times C_p \times C_p$ and the result follows by lemma (4.2.3). ■

For groups of small order we are able to use the computer algebra system GAP [4] to determine whether or not they have an abelian decomposition. This gives rise to the following proposition.

(4.2.7) Proposition
Let G be a group with $|G| = n$ and $n \leq 127$. If $n \notin \{24, 48, 54, 60, 64, 72, 96, 108, 120\}$ then G has an abelian decomposition. ◇

Proof
We will use GAP to calculate for G all possible combinations AB of abelian subgroups A and B and check whether or not AB is equal to G. In order to check the equality we will be using the formula given in (4.2.2) and check the orders instead. The function (7) in the appendix (.2) will compute these steps in GAP. ■

4.3 Applications to Group Codes

Let G be a group. In order to describe G-codes we want to set a few conditions on the group G such that the codes have some useful properties. One of the main questions we want to answer in this section is: Is any G-code an abelian code? The following two theorems give an answer to this question. The first one describes the situation when the corresponding group has an abelian decomposition, and the second one when the corresponding group has no abelian decomposition.

(4.3.1) Theorem
Suppose the group G has an abelian decomposition $G = AB$ and let C be a G-code . Then, C is an abelian group code for the group $A \times \sigma(B)/(\sigma(B) \cap A)$, where σ is the anti-isomorphism given in (4.1.5). ◇

Proof
In [1, Theorem 3.1] it is shown that C is an abelian code for the abelian group $K = \langle A, \sigma(B) \rangle$. Since K is abelian, it obviously holds $K \cong A \times \sigma(B)/(\sigma(B) \cap A)$.■

(4.3.2) Theorem
Suppose $F = \mathbb{Z}/5\mathbb{Z}$ and $G = S_4$ and let e be a primitive central idempotent of G which corresponds to a non linear character. Then G has no abelian decomposition and the G-code generated by e is not permutation equivalent to an abelian code. Moreover, this code is not monomial equivalent to an abelian code. ◇

Proof
In this proof we will give a counterexample using Magma. Therefore, we will refer to the Magma-code given in the appendix (.1).

First of all we compute the central primitive idempotents of FS_4 and call them $e_1, .., e_5$ (function (1)). Both codes $B_4 := e_4FS_4$ and $B_5 := e_5FS_4$ have dimension bigger than 1 (function (2)). Next, we will calculate the permutation automorphisms of each code and check whether or not any of them has a transitive abelian subgroup (function (3)). Since the 'Subgroups' function gives no output, there is no transitive abelian subroup which satisfies theorem (4.1.14) and, thus, the code is not permutation equivalent to an abelian code.

Now, we will check whether or not this code is monomial equivalent to an abelian code. On this account we will be using function (4). First, we calculate the monomial automorphism group. Note that in Magma this group acts on 96 points and, so, it is a subgroup of S_{96}. In order to obtain the action of this group on 24 points we will consider the action of the monomial automorphism group on the blocks of length 4. By the command 'Subgroups' the image of this action does not contain a subgroup which is abelian and transitive, so the monomial automorphism group does not contain a subgroup which satisfies (4.1.14). ■

Assume G has no abelian decomposition. The next step is to find a suitable sufficient condition for a group G such that all G-codes are abelian. Angel del Rio [1] asked if this is true for nilpotent groups. Owing to his question, the rest of this section focuses on the investigation of this question. As a result we will introduce an appropriate counterexample. The following question summarizes our next direction.

Question: Let G be a nilpotent group. Is any G-code an abelian code?

4.3.1 G-codes using nilpotent Groups

Let G be a nilpotent finite group and F a field with $\mathrm{char}(F)$ not dividing $|G|$. By the nilpotency property it holds

$$G = P_1 \times \cdots \times P_n, \quad \text{for Sylow}p_i\text{-subgroups } P_i \text{ and distinct primes } p_i.$$

Then, by (2.3.10), we obtain a decomposition

$$FG \cong FP_1 \otimes \cdots \otimes FP_n = \bigotimes^{n} FP_i. \tag{4.2}$$

But what about ideals of FG? How does the image of an ideal look like under the isomorphism from above? In other words, if $I \trianglelefteq FG$ and if $\widetilde{I}$ is the image, can we say anything about the structure of $\widetilde{I}$? The next Lemma gives an answer to that.

(4.3.3) Lemma
Let $\widetilde{I}$ be an ideal in $FP_1 \otimes \cdots \otimes FP_n$ and I_j an ideal in FP_j, for $j = 1, ..., n$. Then

$$\widetilde{I} \cong I_1 \otimes \cdots \otimes I_n. \qquad \diamond$$

Proof
Let $\phi : FG \to \bigotimes FP_i$ be the algebra isomorphism given in (4.2). Then ϕ maps an ideal to an ideal by mapping a basis to a basis. Thus, if $(e_i)_{i=1}^{r}$ is a basis of $I \trianglelefteq F[P_1 \times \cdots \times P_n]$ then

$$\phi(e_i) = \phi(\sum c \cdot (x_{i_1}, ..., x_{i_n})) = \sum c \cdot (x_{i_1} \otimes \cdots \otimes x_{i_n}). \tag{4.3}$$

Then $\widetilde{I} = \phi(I)$ has the basis $(x_{i_1} \otimes \cdots \otimes x_{i_n})_{i=1}^{r}$. By Lemma (2.3.2), we can identify $(x_{i_j})_{i=1}^{r}$ as a basis for an ideal $I_j \trianglelefteq FP_j$. Consequently, the result follows by the uniqueness (up to isomorphy) of an tensor product. ■

Before we continue, we want to discuss one aspect of the permutation group of such an tensor product. Assume $C \trianglelefteq \bigotimes^n FP_i$ is a code with $C \cong \bigotimes^n C_i$.

First assume $n = 2$, i.e., $C \cong C_1 \otimes C_2$. Say l_1 is the length of C_1 and l_2 the length of C_2. We can identify an element $c_1 \otimes c_2 \in C_1 \otimes C_2$ with an element of $F^{l_1 l_2}$ by

$$c := (c_{1_1} \cdot c_2, c_{1_2} \cdot c_2, ..., c_{1_{l_1}} \cdot c_2) \leq F^{l_1 l_2}.$$

The element $\pi_2 \in \mathrm{PAut}(C_2) \leq S_{l_2}$ acts on c via

$$\pi_2(c)_i = \pi_2(c_{1_i} \cdot c_2) = c_{1_i} \cdot \pi_2(c_2)$$

and $\pi_1 \in \mathrm{PAut}(C_1) \leq S_{l_1}$ via

$$\pi_1(c)_i = \pi_1(c_{1_i} \cdot c_2) = c_{\pi_1(1_i)} \cdot c_2.$$

This induces an action of $\mathrm{PAut}(C_1) \times \mathrm{PAut}(C_2)$ on C. Thus we obtain $\mathrm{PAut}(C_1) \times \mathrm{PAut}(C_2) \subseteq \mathrm{PAut}(C_1 \otimes C_2) = \mathrm{PAut}(C)$.

We can generalise this result to

$$\mathrm{PAut}(C_1) \times \mathrm{PAut}(C_2) \times \cdots \times \mathrm{PAut}(C_n) \subseteq \mathrm{PAut}(C_1 \otimes C_2 \otimes \cdots \otimes C_n). \quad (4.4)$$

The purpose of this section is to answer the following question: Is every G-code abelian if G is a nilpotent group Since p-groups are the simplest nilpotent groups, it is enough to consider these groups.

(4.3.4) Remark
We have seen in proposition (4.2.7) that $64 = 2^6$ is the smallest number such that there is a nilpotent group which has no abelian decomposition. Thus, it would be appropriate to think that groups with these properties are rare. However, this group gives rise to a large amount of other groups with these properties, for instance $G \times C_3$ or $G \times C_5$. ◇

The next theorem answers our previous question on nilpotent groups. In fact, the answer is no. There are non abelian codes which arise from nilpotent groups.

(4.3.5) Theorem
Let G be a group of size 64 given by

$$\begin{aligned} \langle x_1, ..., x_6 \quad | \quad & x_1^2 = \cdots = x_6^2 = 1, \\ & [x_4, x_1] = [x_5, x_1] = [x_6, x_1] = 1, \\ & [x_4, x_2] = [x_5, x_2] = [x_6, x_2] = 1, \\ & [x_4, x_3] = [x_5, x_3] = [x_6, x_3] = 1, \\ & [x_5, x_4] = [x_6, x_4] = [x_5, x_6] = 1, \\ & [x_2, x_1] = x_4, [x_3, x_1] = x_5, [x_3, x_2] = x_6 \rangle \end{aligned}$$

(This group is given in the GAP/Magma ([4]/[5]) library by SmallGroup(64,73)). Furthermore, let $\chi_1, .., \chi_{22}$ be the irreducible characters of G given in GAP/Magma and $e_1, ..., e_{22}$ be the corresponding central primitive idempotent. Set $e = e_2 + e_5 + e_7 + e_9 + e_{11} + e_{13} + e_{15} + e_{17} + e_{19}$.

Then the code corresponding to the ideal $e\mathbb{F}_3G$ is not monomial equivalent to an abelian code. ◇

Proof
The idea for the proof is to pick an ideal of FG such that the code contains a lot of non zero components. Hence, we have taken a sum of central primitive idempotents whose character values are non zero for most of the conjugacy classes. This gives fewer possibilities for permutation automorphisms. We use Magma to calculate the result:

As previously, we will generate a code using the functions (1) and (2) given in the appendix (.1). A good choice for an ideal appeared to be the ideal generated by the idempotents with the numbers (in Magma) $2, 5, 7, 9, 11, 13, 15, 17$ and 19. This code has a small permutation automorphism group, namely of order 1024. This gives us the possibility to use the 'Subgroups' command in Magma (see function (5)).

Again, since the 'Subgroups' command gives no output, there is no regular abelian subroup which satisfies (4.1.14) and, thus, the code is not permutation equivalent to an abelian code.

Now, we will check if this code is monomial equivalent to an abelian code using function (6). First, we calculate the monomial automorphism group. In Magma this group is given as a subgroup of the symmetric group on 128 points. On this account we will investigate the image of the action of the monomial automorphism group on the blocks of length 2. With the command 'Subgroups' we check if the image contains a subgroup which is abelian and transitive. Since there is no such group, this code is not monomial equivalent to an abelian code, by (4.1.14).■

(4.3.6) Remark
Since we have found a nilpotent group which contains a non abelian code, we can say that it is not enough for a group to be nilpotent in order to have abelian codes only. ◇

5 Abelian Codes using Extra-Special Groups

In this chapter we are going to investigate group codes using extra-special groups. We will see that these codes are semicyclic codes. Especially, they are abelian codes and thus this chapter is an application of the more general theory given in the preceding chapter.

Our focus will be on the paper "Group Codes Defined Using Extra-Special p-Groups of Order p^3" by H. G. Aun and D. W. C. Keong [9]. The authors provided useful information about the parameters of two types of codes using extra-special groups. More precisely, they investigated the minimal two sided ideals of the semisimple group algebra FG which decomposes into a direct sum $\bigoplus_i FGe_i$, where the e_i are central primitive idempotents. The first type of code is constructed using linear idempotents and the second type using non linear idempotents.

However, we are going to generalise the results of Aun and Keong using basic principles of character and group ring theory. Not only we are going to use extra-special groups of any order for the codes, we will also give generator matrices to all codes considered here. It turns out that all the codes investigated here are orthogonal sums of cyclic codes. In particular, the results of Aun and Keong can be considered as special cases of the results given in this chapter.

5.1 On a few Topics in Algebra

The intention of this section is to present prerequisites for the next section. In other words, this section will play a considerable role in describing extra-special groups. The results given here are basic results in algebra, i.e., on symplectic spaces and on the theory of p-groups. In case where the reader is not familiar with these topics we recommend to continue.

On the one hand we will show how symplectic vector spaces are made up and what their dimension is. On the other hand we will describe several properties of p-groups and give a correspondence of an $\mathbb{F}_p$-space to a factor group denoted by $G/\Phi(G)$.

5.1.1 Basic Results on Symplectic Spaces

(5.1.1) Definition
*Let F be a field and V be an F-space. Assume there is a non-degenerate alternating bilinear form $\beta : V \times V \to F$ on V. Then we will call V a **symplectic vector space**.* ◇

(5.1.2) Definition
*Let V be a symplectic F-space. We will say that V is the **orthogonal sum** of its subspaces V_i, for i=1,...,m, given by*

$$V = V_1 \perp V_2 \perp \cdots \perp V_n, \tag{5.1}$$

if $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$ is the direct sum of this spaces and for $i \neq j$ and all $v \in V_i$ and $w \in V_j$ holds $\beta(v, w) = 0$. ◇

(5.1.3) Example

1. *Clearly, there is no non-degenerate symplectic vector space of dimension 0.*
2. *Also, there is no such space of dimension 1. Suppose $V = \langle v \rangle$, then $v \in V^{\perp}$. This is a contradiction to $V \cap V^{\perp} = 0$.* ◇

(5.1.4) Theorem
Let V be a non-degenerate symplectic vector space. Then V is an orthogonal sum of two dimensional subspaces, i.e.,

$$V = V_1 \perp V_2 \perp \cdots \perp V_n, \tag{5.2}$$

where $V_i = \langle e_i, f_i \rangle$ for linear independent elements $e_1, ..., e_n, f_1, ..., f_n$.

In particular, $\dim(V) = 2n$. ◇

In order to proof this theorem we will use the next result without proof.

(5.1.5) Lemma (See, [6], Kapitel II, Hilfssatz 9.4)
Let U be a subspace of the non-degenerate symplectic space V. If U is non-degenerate then we can write V as an orthogonal sum $V = U \perp U^{\perp}$, for a non-degenerate subspace $U^{\perp}$, which satisfies $\beta(u, v) = 0$, for all $u \in U$ and $v \in U^{\perp}$. ◇

Proof (of (5.1.4))
Since V is non-degenerate, there are two linear independent elements v_1 and v_2 such that $\beta(v_1, v_2) = 1$. The previous Lemma and induction on the dimension of V gives the result. Note we gave the beginning of the induction in the example above. ■

5.1.2 Some Theory on p-Groups

Here, we will introduce a few group theoretical tools which we will use to describe the extra-special groups. In order the reader is not familiar with these results we recommend to read the published lecture notes on finite p-groups of Susan McKay [16].

(5.1.6) Remark
Let G be a group.

1. *We define the normal subgroup G^p of G by $\langle x^p \mid x \in G \rangle$.*
2. *The **Frattini subgroup** $\Phi(G)$ is the intersection of all proper maximal subgroups of G.*
3. *The group $\Phi(G)$ is normal in G and whenever $G = \langle X \cup \Phi(G) \rangle$, for some set $X \subseteq G$ then it holds $G = \langle X \rangle$.* ◇

By the time Sylow's theorems on finite groups were published, one property of these groups seemed to be interesting, namely that for every prime p dividing $|G|$ there exists exactly one Sylow p-subgroup of G, which is a direct summand of G. In other words, G can be written as a direct sum of Sylow p-subgroups for distinct primes p dividing $|G|$. Groups with this property were called **nilpotent**. Moreover, p-groups are a special case of nilpotent groups. Thus to study p-groups we want to present some properties which are equivalent to nilpotency.

(5.1.7) Theorem (See, [6], Kapitel III, Hauptsatz 2.3)
Let G be a group. Then equivalent are:

1. *G is a direct sum of its Sylow subgroups.*
2. *For any subgroup $U \leq G$ it holds $U < N_G(U)$.*
3. *Any maximal subgroup of G is normal.* ◇

(5.1.8) Lemma
Let G be a p-group. Then any maximal subgroup of G is normal and of index p. ◇

Proof
Since p-groups are nilpotent, the maximal subgroups are normal by the previous theorem. Suppose the index of U in G is bigger than p. The p-group G/U has an element xU of order p. Therefore, there is an element of order p in $G \setminus U$ such that $U < \langle x, U \rangle < G$. This contradicts the maximality of U. ■

Next we want to introduce a method of how to create a vector space out of a p-group. Let G be a p-group and consider the factor group $G/(G'G^p)$. This group can also be considered as a vector space using the following rules:

$$(xG'G^p + yG'G^p) := (xy)G'G^p, \quad \text{for all } x, y \in G \tag{5.3}$$

and

$$n(xG'G^p) := x^n G'G^p, \quad \text{for } n \in \mathbb{F}_p \text{ and } x \in G. \tag{5.4}$$

Obviously, with this construction we can identify $G/(G'G^p)$ as an $\mathbb{F}_p$-space. Therefore, every subgroup corresponds to a subspace and vice versa. Also, we will use it in the next proof.

(5.1.9) Theorem
For p-groups holds $\Phi(G) = G'G^p$. ◇

Proof
Let N be a maximal subgroup of the p-group G. By our previous result, the group G/N has size p, so it is abelian. Thus, N contains G'. Also, every element x in G/N has order dividing p. Therefore, x^p is in N and so G^p is contained in N. This proves the first inclusion. Conversly, we already showed that every subgroup of $G/(G'G^p)$ corresponds one-to-one to an $\mathbb{F}_p$-subspace. Assume there is a subspace $xG'G^p$ with $x \notin G'G^p$ and dimension 1. Then, the factor space modulo this 1-dimensional space corresponds to a maximal subgroup not containing x. Hence, $\Phi(G)$ does not contain x. ■

5.2 Properties of Extra-Special Groups

5.2.1 The Structure of Extra-Special Groups

Before we start investigating group codes we want to make use of the extraordinary structure of extra-special groups. Therefore, we want to introduce basic results on extra-special groups both from a group theoretical and a character theoretical point of view.

(5.2.1) Definition
Let G be a p-group, for some prime p. G is called ***extra-special*** *if* $\Phi(G) = Z(G) = G'$ *and* $|\Phi(G)| = |Z(G)| = |G'| = p$. ◇

Although there is a variety of interesting results on extra-special groups, we only will give theorems which are of major importance for our purpose. Especially, the next two results reveal the true structure of these groups.

(5.2.2) Theorem
Let G be an extra-special group. Then, $G/Z(G)$ *is elementary abelian. In particular,* $G/Z(G)$ *is an* $\mathbb{F}_p$*-space.* ◇

Proof
By definition it holds $Z(G) = \Phi(G)$, so the result follows by theorem (5.1.9) and the remarks on the correspondence of an $\mathbb{F}_p$-space. ■

(5.2.3) Theorem (See [6], Chapter III, Theorem 13.7)
Let G be an extra-special group. Then, $|G| = p^{2n+1}$, for some positive integer n. ◇

Proof
Assume $Z(G) = G' = \langle g \rangle$, for an element $g \in G$ of order p. By the previous result we consider $V := G/Z(G)$ as an $\mathbb{F}_p$-space. Then we will show that the map,

$$\beta : V \times V \to \mathbb{F}_p, \quad (aZ(G), bZ(G)) \mapsto m, \tag{5.5}$$

where $[a,b] = a^{-1}b^{-1}ab = g^m$ holds for some $m \in F_p$, is a non-degenerate bilinear form.

Firstly, for $u, w \in Z(G)$ holds $[au, bw] = [a,b]$. Thus β is well-defined. Secondly, $[a,a] = g^0$, $\beta(a,b) = -\beta(b,a)$ and since $Z(G) = G'$, it also holds $[ab,c] = [a,c][b,c]$ and $[a,bc] = [a,b][a,c]$. Hence, β is an alternating bilinear form. Thirdly, suppose for $a \in G$ holds $\beta(a,b) = 0$ for all $b \in G$. In other words $[a,b] = g^0$ for all $b \in G$. This is only possible if $a \in Z(G)$. Therefore, β is non-degenerate.

That property of β makes V a non-degenerate symplectic vector space. By theorem (5.1.4) it holds $|G/Z(G)| = p^{2n}$, for some positive integer n. Therefore, G has order p^{2n+1}. ■

The property of extra-special groups presented in the theorem above makes these groups really interesting. This extra structure gives us the possibility to derive more results about these groups.

(5.2.4) Proposition
Let G be an extra-special group of order p^{2n+1}. Then it holds:

1. *Every maximal abelian normal subgroup has order p^{n+1}.*
2. *For every maximal abelian normal subgroup N_1 there exists another maximal abelian normal subgroup N_2 with*

$$G = N_1 N_2, \quad \textit{and} \quad N_1 \cap N_2 = Z(G). \tag{5.6}$$

◇

Proof

1. Assume, N is a maximal abelian normal subgroup in G. Then $Z(G)$ is a subgroup of N, since otherwise N would not be maximal, and $N/Z(G)$ is a maximal abelian normal subgroup of $G/Z(G)$. This gives us the opportunity to consider $U := N/Z(G)$ as a subspace of $V := G/Z(G)$. Since N is abelian, the commutator $[x,y]$, for all $x, y \in N$, is trivial. Thus, $\beta(xZ(G), yZ(G)) = 0$ for all $xZ(G), yZ(G) \in N/Z(G)$. By theorem (5.1.4) the space U needs to have the form

$$U = U_1 \perp U_2 \perp \cdots \perp U_n, \tag{5.7}$$

where U_i is a 1-dimensional subspace of V_i given in theorem (5.1.4), for $i = 1, ..., n$. Hence $N/Z(G)$ has order p^n and N has order p^{n+1}.

2. From 1. we can see that an arbitrary maximal abelian normal subgroup N has the form given in equation (5.7). Now, by setting $W := \langle x_1, ..., x_n \rangle$, where $x_i \in V_i \setminus U_i$, it is obvious that $V = W + U$ and that

$$W = \langle x_1 \rangle \perp \langle x_2 \rangle \perp \cdots \perp \langle x_n \rangle. \tag{5.8}$$

Thus, W corresponds to some subgroup of $G/Z(G)$ and so it corresponds to a maximal abelian normal subgroup of G, which satisfies the requirements. ■

5.2.2 Characters and Idempotents

In the next part of this section we are going to investigate the character theory of an extra-special group G over the complex numbers $\mathbb{C}$. We can use these results for group codes over finite fields, where the corresponding group ring is semisimple.

(5.2.5) Theorem
Let G be an extra-special group of order p^{2n+1}. Then

1. *G has $p-1$ non linear irreducible characters of degree p^n and p^{2n} irreducible linear characters.*
2. *G has $p^{2n}+p-1$ conjugacy classes; p have size 1 and $p^{2n}-1$ have size p.*
3. *$|Irr(G)| = p^{2n}+p-1$.*
4. *Let χ be a non linear irreducible character of G. Then χ is faithful and it holds $Z(G) = Z(\chi)$.* ◇

Proof

1. By theorem (2.2.31) the number of linear characters is $|G : G'| = p^{2n}$. Now, theorem (2.2.39) says that for every non linear character χ it holds $\chi(1)^2 = |G : Z(G)| = p^{2n}$. In order to satisfy the equation $|G| = \sum_{\chi \in Irr(G)} \chi(1)^2$ the only possible number of non linear characters is $p-1$.
2. By (5.2.2) the conjugacy classes which are not in $Z(G)$ have size $|Z(G)| = p$. Their number is $p^{2n}-1$. In addition, each element of $Z(G)$ has a conjugacy class consisting of one element.
3. A consequence of (1).
4. Let χ be an irreducible non linear character. From (2.2.35) we obtain $G' = Z(G) \subseteq Z(\chi)$. Hence, the factor group $G/Z(\chi)$ is abelian and so $p^{2n} = \chi(1)^2 = |G : Z(\chi)|$ holds by (2.2.38). Hence, $|Z(\chi)| = p$ and $Z(\chi) = Z(G) = G'$. Since $Z(\chi)/ker(\chi)$ is cyclic, there are two

choices, namely $ker(\chi) = 1$ or $ker(\chi) = Z(\chi) = G'$. Suppose the second case. Then, $G/ker(\chi)$ is abelian of size p^2. However, this contradicts $1 = |Z(\chi)/ker(\chi)| = |Z(G/ker(\chi))| = p^2$. ■

From now on, we are going to use the coset decomposition of G by G', namely

$$G = \biguplus_{i=0}^{p^{2n}} t_i G',$$

where $T = \{t_1 = 1, ..., t_{p^{2n}}\}$ is the transversal of G by $G' = Z(G)$. Furthermore, assume the cyclic group G' is generated by g.

Next, we want to enumerate the elements of G. Using the decomposition above we can write the elements of G like this:

$$G = \{1, g, ..., g^{p-1}, t_2, t_2 g, ..., t_2 g^{p-1}, ..., t_{p^{2n}}, t_{p^{2n}} g, ..., t_{p^{2n}} g^{p-1}\}. \tag{5.9}$$

This will be useful for the next paragraph.

Recall, that for a field F, with $char(F) \neq p$, the group ring FG is semisimple. In other words the group ring can be written as a direct sum of minimal ideals, say

$$FG = \bigoplus_{i=1}^{p^{2n+1}} e_i FG. \tag{5.10}$$

The central primitive idempotents e_i can be computed using character values and the formula

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g, \quad \text{for } \chi_i \in Irr(G) \text{ and } i = 1, ..., p^{2n} + p - 1.$$

With respect to the linear/non linear characters we will call the e_i linear/non linear idempotents.

There is one idempotent we want to put some emphasis on, since it is the generator of an ideal which we will call *trivial*:

$$\tilde{e} := \frac{1}{p} \sum_{i=0}^{p-1} g^i \in \mathbb{C}G. \tag{5.11}$$

Clearly, $\tilde{e}$ is a central idempotent. Moreover, this idempotent is the generator for a code only somewhat different from the repetition code. Surprisingly, it plays a considerable role in the original paper.

Before we present the next Lemma on the idempotent $\tilde{e}$, we will give a few of its properties using the structure of the elements of G:

1. $g\tilde{e} = \tilde{e}$ and

2. $t_j g^k \tilde{e} = t_j \tilde{e}$

First, we will compute the linear and non linear idempotents. By theorem (5.2.2) the value of a linear character on each conjugacy class of G is a pth root of unity. Moreover, each coset of G by G' is a conjugacy class. Thus, each linear idempotent is given by

$$e_i = \frac{1}{p^{2n+1}} \sum_{j=1}^{p^{2n}} \chi_i(t_j) \sum_{k=1}^{p} g^k t_j \tag{5.12}$$

$$= \frac{1}{p^{2n}} \sum_{j=1}^{p^{2n}} \chi_i(t_j) \tilde{e} t_j. \tag{5.13}$$

The structure of non linear characters of an extra-special group is also simple because, by (2.2.37) and (5.2.5), it holds $\chi_i(g) = 0$, for all $g \in G - Z(G)$, where χ_i is a non linear character. Thus, the corresponding idempotent e_i is identical to exactly one idempotent of the center $Z(G)$. Let ψ_k, for $k = 0, ..., p-1$, be the characters of $Z(G)$. Assume $\psi_0 = 1_{Z(G)}$. Then we obtain

$$f_k := \frac{1}{p} \sum_{i=0}^{p-1} \psi_k(g^{-i}) g^i, \quad \text{for } k = 1, ..., p-1$$

Therefore, for our purpose we will use the f_k instead of the non linear idempotents e_i. By permuting the ψ_k, we may assume that

$$f_k := \frac{1}{p} \sum_{i=0}^{p-1} \psi_k(g^i) g^i = \frac{1}{p} \sum_{i=0}^{p-1} \zeta^{ki} g^i, \quad \text{for } k = 1, ..., p-1. \tag{5.14}$$

On this account we obtain two useful properties of $\tilde{e}$ with respect to the idempotents of G, namely

$$\begin{aligned} e_i \tilde{e} &= \left(\frac{1}{p^{2n}} \sum_{j=1}^{p^{2n}} \chi_i(t_j) \tilde{e} t_j \right) \tilde{e} \\ &= \frac{1}{p^{2n}} \sum_{j=1}^{p^{2n}} \chi_i(t_j) \tilde{e} t_j \\ &= e_i, \quad \text{for} \quad i = 1, ..., p^{2n} \end{aligned}$$

and

$$\begin{aligned} f_k \tilde{e} &= \left(\frac{1}{p} \sum_{i=0}^{p-1} \zeta^{ki} g^i \right) \tilde{e} \\ &= \left(\frac{1}{p} \sum_{i=0}^{p-1} \zeta^{ki} \right) \tilde{e} \\ &= 0, \quad \text{for} \quad k = 1, ..., p-1. \end{aligned}$$

Now we will use these properties to prove the following Lemma.

(5.2.6) Lemma
Let G be an extra-special group of order p^{2n+1} and $e_1, ..., e_{p^{2n}}$ the central primitive idempotents corresponding to the irreducible linear characters $\chi_1, ..., \chi_{p^{2n}} \in Irr(G)$. Then,

$$\sum_{i=1}^{p^{2n}} e_i = \tilde{e}. \qquad \diamond$$

Proof
By equation (5.10) we have $FG = \bigoplus_{i=1}^{p^{2n}} e_i FG \oplus \bigoplus_{k=0}^{p-1} f_k FG$. By the properties above it holds that $FG\tilde{e} = \bigoplus_{i=1}^{p^{2n}} e_i FG$. Thus, $\tilde{e} = \sum_{i=1}^{p^{2n}} e_i$. ■

5.3 Properties of Group Codes using Extra-Special Groups

Now, it is time to investigate the group codes we mentioned in the beginning. The group G is still an extra-special group of order p^{2n+1}. Let $Z(G) = \langle g \rangle \cong C_p$ be the center of G. Assume $\chi_1, ..., \chi_{p^{2n}+p-1}$ are the irreducible characters of G and let $e_1, ..., e_{p^{2n}+p-1}$ be the corresponding idempotents. Moreover, let F be a field with $\mathrm{char}(F) = q$ not dividing p, which contains a primitive pth root of unity. Suppose F has q^m elements. Then, we can write the group algebra as a direct sum

$$FG = e_1 FG \oplus \cdots \oplus e_{p^{2n}} FG \oplus e_{p^{2n}+1} FG \oplus \cdots \oplus e_{p^{2n+1}} FG. \tag{5.15}$$

We will call the minimal ideal $e_i FG$ linear/ non linear ideal, if the idempotent e_i is linear/ non linear.

Since we want to investigate codes, or in other words two sided ideals of FG, we note that an ideal I is made up of some $e_i FG$, i.e.

$$I = \bigoplus_i e_i FG, \quad \text{for some } 1 \leq i \leq p^{2n} + p - 1.$$

Also, these ideals are subspaces of FG. Therefore, by choosing a basis we can consider I as a subspace of $K^{\dim(FG)}$. Our goal is the calculate the parameters of the code I. Moreover, we will identify the ideal I with the corresponding G-code using the map

$$\sum_{g \in G} a_g g \mapsto \left(a_1, a_g, ...a_{g^{p-1}}, a_{t_2}, a_{t_2 g}, ..., a_{t_2 g^{p-1}}, ..., a_{t_{p^{2n}}}, a_{t_{p^{2n}} g}, ..., a_{t_{p^{2n}} g^{p-1}} \right).$$

We present the next theorem, in order to identify these codes as abelian codes and, thus, to point up the connection to the preceding chapter.

(5.3.1) Theorem
Every extra-special group G has an abelian decomposition. Thus, every G-code is an abelian code. ◇

Proof
By proposition (5.2.4), G has an abelian decomposition. The result follows from (4.3.1). ■

Recall that for codes we have introduced a non-degenerate bilinear form in order to describe the dual of a code. In this chapter we will consider the standard scalar product:

$$\beta(x,y) :=< x,y >:= \sum x_i y_i. \tag{5.16}$$

This time we will use the orthogonal decomposition of a vector space, with respect to this bilinear form, to describe codes.

5.3.1 Two trivial Codes

In our previous discussions we have already introduced the idempotent $\tilde{e}$, see equation (5.11). Now, the following decomposition gives rise to two ideals of particular interest:

$$FG = \tilde{e}FG \oplus (1-\tilde{e})FG.$$

We will denote $\tilde{e}FG$ by I and $(1-\tilde{e})FG$ by $I^{\perp}$. Also, this notation reveals already the nature of both ideals.

(5.3.2) Remark
In the previous situation it holds:

1. $\dim(I) = p^{2n}$.
2. *By the direct sum decomposition from above we get* $(1-\tilde{e})FG \cong I^{\perp}$.
3. $\dim(I^{\perp}) = p^{2n}(p-1)$. ◇

(5.3.3) Proposition
The code I is an $[p^{2n+1}, p^{2n}, p]$-code isomorphic to the orthogonal sum of p^{2n} copies of $\langle(1\cdots1)\rangle$, namely $\perp_{i=1}^{p^{2n}} \langle(1\cdots1)\rangle$. In particular, it is an orthogonal sum of cyclic codes. ◇

Proof
Again we will make use of the properties of $\tilde{e}$:

$$\begin{aligned} g\tilde{e} &= \tilde{e}, \\ x\tilde{e} &= \tilde{e}x \quad \text{for all } x \in G, \quad \text{and} \\ t_j g^k \tilde{e} &= t_j \tilde{e} \quad \text{for all } j = 1,...,p^{2n}, k = 0,1,...,p-1. \end{aligned}$$

Hence, $I = \tilde{e}FG$ corresponds to the subspace generated by the rows of the matrix

$$\begin{pmatrix} \overbrace{1\cdots1}^{p\text{-times}} & 0\cdots0 & 0\cdots0 & \cdots & 0\cdots0 \\ 0\cdots0 & 1\cdots1 & 0\cdots0 & \cdots & 0\cdots0 \\ 0\cdots0 & 0\cdots0 & 1\cdots1 & \cdots & 0\cdots0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0\cdots0 & 0\cdots0 & 0\cdots0 & \cdots & 1\cdots1 \end{pmatrix} \in F^{p^{2n}\times p^{2n+1}} \tag{5.17}$$

■

(5.3.4) Corollary
The weight enumerator $h(I)$ and the complete weight enumerator p_I are given by

$$\begin{aligned} h(I) &= (x^p + (q^m-1)y^p)^{p^{2n}} \\ &= \sum_{i=0}^{p^{2n}} (q^m-1)^i \binom{p^{2n}}{i} x^{p^{2n+1}-pi} y^{pi} \\ p_I &= \left(\sum_{i=0}^{q^m-1} x_i^p\right)^{p^{2n}} \end{aligned}$$

Proof
The orthogonal structure of the codes helps us to determine these polynomials by counting all possible combinations. We can compute these polynomials by multiplying the polynomials of each component. In other words, $h(I) = \prod h_i$, where h_i is the weight enumerator of the ith component of the orthogonal decomposition of the code I (p_I respectively). Moreover, we get easily $h(\langle(1\cdots1)\rangle) = x^p + (q-1)y^p$ and $p_{\langle(1\cdots1)\rangle} = \sum_{i=0}^{q-1} x_i^p$. ■

Next, we want to study $I^\perp$. We have already seen that $I \cong \perp_{i=1}^{p^{2n}} \langle(1\cdots1)\rangle$. On this account, we easily obtain results about $I^\perp$.

(5.3.5) Corollary
The code $I^\perp$ is a $[p^{2n+1}, p^{2n}(p-1), 2]$-code. Also, $I^\perp$ is an orthogonal sum of a cyclic code. ◇

Proof

$$\begin{aligned} I^\perp &\cong \perp_{i=1}^{p^{2n}} \left(\langle(1\cdots1)\rangle^\perp\right) \\ &= \perp_{i=1}^{p^{2n}} \langle(1\,0\,\cdots0\,-1), (0\,1\,\cdots0\,-1), ..., (0\,0\,\cdots1\,-1)\rangle \end{aligned}$$

Hence, the minimum distance of $I^\perp$ is $d(I^\perp) = 2$. ■

5.3.2 The non linear Ideals

In this last part of this chapter we want to pay attention to an more interesting set of ideals. Since we know that the idempotent $(1-\tilde{e})$ is the sum of all non linear idempotents, we want to focus on its components. In particular, we are going to study the ideals $I_i := e_iFG$ for non linear idempotents. In previous discussions we mentioned that we will use the notation f_k instead of e_i, see equation (5.14). Thus $I_i := f_iFG$, for $1 \leq i \leq p-1$.

Since each idempotent f_k corresponds to one of the non trivial characters of the cyclic group C_p, it is enough to consider the structure of FC_p to get information about the ideal.

(5.3.6) Theorem
Let I be the sum of some non linear ideals, say $I = I_{i_1} + \cdots + I_{i_k}$, for $1 \leq k \leq p-1$. Then, I is a $[p^{2n+1}, kp^{2n}, p-k+1]$-code with

$$I \cong \perp_{i=1}^{p^{2n}} \langle v_{i_1}, ..., v_{i_k} \rangle,$$

where v_{i_j} corresponds to a non trivial row of the character table of C_p, for $1 \leq j \leq k$. Especially, I is the orthogonal sum of a cyclic code. ◇

Proof
Again, we note that the following properties hold:

$$\begin{aligned} gf_k &= f_kg = \zeta^{-k}f_k, \\ t_if_k &= f_kt_i \end{aligned}$$

The sum $f = \sum_k f_{i_k}$ is an idempotent in $FC_p \cong F\langle g \rangle = FZ(G)$. Thus fFC_p corresponds to a cyclic code K_f. However, an extra-special group G contains, by the enumeration of the elements (5.9), p^{2n} times the structure of an FC_p. Hence it contains p^{2n} times the structure of the code K_f. Moreover, it holds $I \cong \perp_{i=1}^{p^{2n}} K_f$.

Now, to study I we can focus on the code K_f. It holds that $\dim(K_f) = k$. If we take K_f to be a code over F, then the minimum distance of K_f is given by

$$d(K_f) = p-k+1.$$ ■

(5.3.7) Example
Let $p = 5, n = 1, F = \mathbb{F}_{3^4}$ and ζ be a 5th root of unity in F. Furthermore, let $G = 5^3_+$ and ψ_i, for $i = 1, 2$, be a character of C_p with values:

	1	g	g^2	g^3	g^4
ψ_1	1	ζ^4	ζ^3	ζ^2	ζ
ψ_2	1	ζ^2	ζ^4	ζ^1	ζ^3

Thus,

$$\begin{aligned} f_{\psi_1} &= \frac{1}{5}(1+\zeta g+\zeta^2 g^2+\zeta^3 g^3+\zeta^4 g^4) \\ f_{\psi_2} &= \frac{1}{5}(1+\zeta^3 g+\zeta g^2+\zeta^4 g^3+\zeta^2 g^4) \\ v_{\psi_1} &= (1,\zeta,\zeta^2,\zeta^3,\zeta^4) \\ v_{\psi_2} &= (1,\zeta^3,\zeta,\zeta^4,\zeta^2) \end{aligned}$$

Then, I has generator matrix

$$\begin{pmatrix} A & 0 & 0 & \cdots & 0 \\ 0 & A & 0 & \cdots & 0 \\ 0 & 0 & A & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A \end{pmatrix} \in F^{2\cdot 5^2 \times 5^3}, \tag{5.18}$$

where the rows of the matrix $A \in F^{2\times 5}$ are given by v_{ψ_1} and v_{ψ_2}. Obviously,

$$I \cong \perp_{i=1}^{5^2} \langle \psi_1, \psi_2 \rangle. \qquad \diamond$$

6 Conclusion

In this final chapter we are going to review shortly what has been done in this dissertation. Also, we will point out the limitations and give suggestions on what new investigations would be appropriate.

In chapter 4 we focused on group ring codes. Especially, we generalized A. d. Rio's theorem on G-codes (4.1.13). Moreover, we gave a counterexample (4.3.5) which proves that there are group ring codes over nilpotent groups which are not abelian. However, there are still open questions on this topic. For instance, we did not generalize this theorem to general equivalences given by the group $A(F^n)$. Also, we did not investigate whether or not there are other group properties like "having an abelian decomposition" which are sufficient to imply that all group codes are abelian. These appear to be interesting tasks left. Here, we give more interesting questions on this topic:

1. What properties of the code or the corresponding ideal are invariant under the permutation/monomial equivalence?
2. Are there group properties which are related to the property "having an abelian decomposition"?
3. Regarding the counterexample (4.3.5), it would be interesting if we were able to derive information from the permutation group of the counterexample to obtain information on why this example is a counterexample.

Finally, in chapter 5 we improved the results given by H. G. Aun and D. W. C. Keong [9] on abelian group ring codes over extra-special groups. We used group rings to describe these codes and their parameters and gave generator matrices. As a result we found out that all the codes considered are orthogonal sums of cyclic codes ((5.3.3),(5.3.6)). However, we did not consider the case where the code is generated by only some linear ideals, and where the code is generated by a mix of linear and non linear ideals. This will be the next step in order to describe these codes to a full extent. Other questions we did not work on are given here:

1. It is still unclear what weight enumerators the codes generated by non linear ideals have.
2. Also, one can compute the automorphism group for these codes.

Appendices

.1 Magma Code

Code (Function 1)

```
generateminimalideals:=function(g);
// Generates the central primitive idempotents and
// the minimal ideals of the group ring FG, where
// F is the cyclotomic field with |g|th root of unity.

A:=GroupAlgebra(CyclotomicField(#g),g);
d:=ClassFunctionSpace(g);b:=Basis(d);
// Generates all  complex characters.

e:=[];
// Generate the central primitive idempotents
// over the splitting field of the group g.

for i in [1..#b] do
a:=0;
for j in g do
s:=b[i](j^(-1))*A!j;
a:=a+s;
end for;
e[i]:=b[i](Id(g))/(#g)*a;
end for;

B:=[];
// Generate the minimal ideals corresponding to the
// central primitive idempotents.

for i in [1..#b] do
B[i]:=ideal<A|e[i]>;
end for;
return e,B;
// Returns the idempotents and the minimal ideals.

end function;
```

Code (Function 2)

```
generatecode:=function(B,F,g);
// Generates a linear code over the field F corresponding to
// the ideal B of the group ring Fg (see section 4.1).
```

```
m:=ZeroMatrix(F,Dimension(B),#g);
// Generate the generator matrix of the code by
// filling in the coefficients of the basis of B.

bb:=Basis(B);
for ii in [1..Dimension(B)] do
for jj in [1..#g] do
m[ii][jj]:=Coefficients(bb[ii])[jj];
end for;
end for;
return LinearCode(m);
// Returns the linear code generated by the matrix m.

end function;
```

Code (Function 3)

```
g:=Sym(4);
e,B:=generateminimalideals(g);
C1:=generatecode(B[4],GF(5),g);P1:=PermutationGroup(C1);
C2:=generatecode(B[5],GF(5),g);P2:=PermutationGroup(C2);
// Computes the permutation automorphism groups of
// the codes C1 and C2.

Subgroups(P1:IsAbelian:=true,IsTransitive:=true);
Subgroups(P2:IsAbelian:=true,IsTransitive:=true);
// Returns all subgroups of P1 and P2 which are
// abelian and transitive.
```

Code (Function 4)

```
M1:=MonomialGroup(C1);
M2:=MonomialGroup(C2);
phiofM1:=Image(BlocksAction(M1,{1,2,3,4}));
phiofM2:=Image(BlocksAction(M2,{1,2,3,4}));
// Computes the monomial groups and the image of
// the action homomorphism of the action of M1 (M2 respectively)
// on the blocks of length 4.

Subgroups(phiofM1:IsAbelian:=true,IsTransitive:=true);
Subgroups(phiofM2:IsAbelian:=true,IsTransitive:=true);
// Returns all subgroups of phiofM1 and phiofM2
// which are abelian and transitive.
```

Code (Function 5)

```
g:=SmallGroup(64,73);
e,B:=generateminimalideals(g);

I:=B[2]+B[5]+B[7]+B[9]+B[11]+B[13]+B[15]+B[17]+B[19];
// the ideal I is the sum of some minimal ideals B[i]

C:=generatecode(I,GF(3),g);
P:=PermutationGroup(C);#P;
// Computes the permutation automorphism group of the code C.
// The permutation group is relatively "small".

Subgroups(P:IsAbelian:=true,IsTransitive:=true);
// Returns all subgroups of P which are abelian and transitive.
```

Code (Function 6)

```
M:=MonomialGroup(C);
phiofM:=Image(BlocksAction(M,{1,2}));
// Computes the monomial group of the code and the image of
// the action homomorphism of the action of M
// on the blocks of length 2.

Subgroups(phiofM:IsAbelian:=true,IsTransitive:=true);
// Returns all subgroups of phiofM which are
// abelian and transitive.
```

.2 Gap Code

Code (Function 1, see [3])

```
HasAbelianDecomposition:=function(G)
# Calculates for a group G whether or not G has
# an abelian decomposition.

local lat, A, x, xx, y, z, n, flag;
n:=Size(G);
lat:=LatticeSubgroups(G);
# GAP computes the structure of all subgroups of G.

A:=Filtered(ConjugacyClassesSubgroups(lat),
```

```
x->IsAbelian(Representative(x)));
# A is the list all abelian subgroups of G.

for xx in A do
x:=Representative(xx);
# Checks whether or not for all abelian subgroups
# equation (4.1) holds.

for y in A do for z in AsList(y) do
if Size(x)*Size(z)/Size(Intersection(x,z))=n
then return true; fi;
od; od;
od;
return false;
# Returns true if equation (4.1) holds and so G has
# an abelian decomposition and returns false
# if it does not hold. If false is returned
# then G has no abelian decomposition.

end;
```

Bibliography

[1] J.J. Bernal, A del Rio, J.J. Simon, An intrinsical description of group codes, Designs, Codes and Cryptography, 51, no. 3, 289-300 (2009).

[2] C.G. Pillado, Santos Gonzalez, Victor Markov, Consuelo Martinez, Alexandr Nechaev, Non abelian group codes (submitted).

[3] C. Garcı´ a Pillado, S. Gonza´ lez, V. T. Markov, C. Martı´ nez, A. A. Nechaev, When are all group codes of a noncommutative group Abelian (a computational approach)?, (russian), Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 2, pp. 75—85.

[4] http://www.gap-system.org/.

[5] http://magma.maths.usyd.edu.au/magma/.

[6] B. Huppert, Endliche Gruppen I, Springer (1967)

[7] I. M. Isaacs, Character Theory of Finite Groups, Academic Press(1976)

[8] C. W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras

[9] H. G. Aun, D. W. C. Keong, Group Codes Defined Using Extra-Special p-Groups of Order p^3, Bull. Malays. Math. Sci. Soc (2) 27 (2004), 185-205

[10] W. Lütkebohmert, Codierungstheorie, Vieweg (2003)

[11] F. J. MacWilliams, Codes and ideals in group algebras, Combinatorial Mathematics and its Applications, University of North Carolina Press (1969)

[12] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, North-Holland Publishing Co. (1977).

[13] S. D. Berman, On the theory of group codes, Kibernetika, 3:31–39 (1967).

[14] R. W. Hamming, Error detecting and error correcting codes, The Bell System Technical Journal, 26:147–160 (1950).

[15] D. S. Passman, The algebraic structure of group rings, New York: Wiley, (1977).

[16] S. McKay, Finite p-groups, Queen Mary math notes (2000)

[17] G. Nebe, E. M. Rains, N. J. A. Sloane, Self-dual Codes and Invariant theory, Springer (2010)

Eigenstaendigkeitserklaerung

Hiermit versichere ich, Artur Schäfer, geboren am 03.04.1989, dass die vorliegende Arbeit von mir selbstständig und nur unter Zuhilfenahme der angegebenen Quellen und Hilfsmittel verfasst wurde.

Aachen, den 22. Oktober 2012

_____

Artur Schäfer