Group Algebras in Coding Theory [1]

César Polcino Milies
and
Marins Guerreiro

Chapter 1

Group Rings

1.1 Introduction

A brief history[1]

In 1837, Sir William Rowan Hamilton formulated the first formal theory of complex numbers, defining them as ordered pairs of real numbers, just as is done nowadays.

The greatest problem of his time, motivated by physics, was to construct a language to develop dynamics; something similar to what was done by Newton when he invented calculus, creating adequate tools for the development of kinematics. To that end, it was necessary to create an algebra to operate with vectors in space.

After long efforts, he realized that it would not be possible to construct a three-dimensional algebra where division was possible and, based on geometrical considerations, he perceived that he would be able to describe an algebra, not of vectors, but of the operators that act on vectors in space, working with a four-dimensional algebra.

He then came to consider elements of the form $\alpha = a+bi+cj+dk$, which he called *Quaternions*, where the coefficients a, b, c, d represent real numbers and i, j, k are formal symbols called *basic units*. It was obvious to him that two such elements should be added componentwise, that is, according to the formula:

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')j+(d+d')k.$$

[1] This short history of the subject is based on [21, Section 3.1]. For more details on the history of group rings see [10] and [20].

The main difficulty was to define the product of two such elements in a reasonable way. Since this product should have the usual properties of a multiplication, such as the distributive law, it would actually be enough to decide how to multiply the symbols i, j, k among themselves. This again demanded considerable effort since from the very beginning Hamilton also assumed implicitly that the product should be commutative. (This is perfectly reasonable since he did not know, at the time, that he was about to discover the first noncommutative algebra structure in the history of mathematics.) Finally, in October 1843 he discovered the fundamental laws of the product of quaternions:

$$i^2 = j^2 = k^2 = ijk = -1,$$

which also imply the well-known formulas:

$$\begin{array}{ccccc} ij & = & k & = & -ji \\ jk & = & i & = & -kj \\ ki & = & j & = & -ik. \end{array}$$

The discovery of quaternions opened the possibilities of new extensions of the field of complex numbers, precisely when the recent discovery of the so-called Fundamental Theorem of Algebra seemed to indicate that the need for new extensions had come to an end.

In December of the same year, in an answer to a letter of Hamilton, the English mathematician John T. Graves introduced a new set of numbers, the *Octonions*, which can be defined as the set of elements of the form $a_0 + a_1e_1 + a_2e_2 + \cdots + a_7e_7$, where the coefficients a_i, $1 \leq i \leq 7$, are real numbers and the symbols e_i, $1 \leq i \leq 7$, are the *basic units*. Once again, the sum of two such elements is defined componentwise and the product is first defined on the basic units according to certain rules and then extended distributively. A striking fact about octonions is that the product so defined is not even associative. Graves actually did not publish his constructions and these numbers were discovered independently by Sir Arthur Cayley in 1845; for this reason, Qctonions are also known to this day as *Cayley Numbers*.

Hamilton himself realized that it was possible to extend even further this construction and he first defined *Biquaternions*, which are again elements of the form $\alpha = a+bi+cj+dk$, where the coefficients a, b, c, d are now assumed to be complex numbers. Soon afterwards he introduced the *Hypercomplex Systems*. Given a set of symbols, called *Basic Units* he considered the set of elements of the form $\alpha = a_1e_1 + a_2e_2 + \cdots + a_ne_n$, where the sum is once again defined componentwise and multiplication is defined by establishing

the values of the products of basic units pairwise. Since the product of two basic units must again be an element of this set, it must be of the form:

$$e_i e_j = \sum_{k=1}^{n} \gamma_k(i,j) e_k.$$

In other words, to give an algebra structure in this set, it is enough to choose conveniently the values of the coefficients $\gamma_k(i,j)$. Because of this fact, they are called the *structural constants* of the system.

These facts can be regarded as the first steps in the development of ring theory. Soon, many new systems were discovered and the need for a classification was felt. In a paper read in 1870 and published in lithographed form in 1871, entitled *Linear Associative Algebras*, Benjamin Peirce[2] gave a classification of the algebras known at the time and determined 162 algebras of dimension less than or equal to 6. As tools of his method of classification, B. Peirce introduced some very important ideas in ring theory, such as the notions of idempotent and nilpotent elements, and the use of idempotents to obtain a decomposition of a given algebra.

The first definition of an abstract group was given by A. Cayley in [4]; till then, only permutation groups had been considered in the literature. It is interesting to note that it is in this very same paper that the notion of a *group ring* appears for the first time. Almost at the end of the paper, Cayley states that if we consider the elements of a (finite) group as "basic units" of a hypercomplex system or, in his own words: "*if we consider them as quantities...such as the quaternions imaginaries*" then the group's product actually defines the product of these hypercomplex quantities.

The explicit definition, in the case of finite groups, is as follows.

Definition 1.1.1. *Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group (we agree to denote always by g_1 the identity element of G) and R a commutative ring with unity. Denote by RG the set of all elements of the form :*

$$a_1 g_1 + a_2 g_2 + \cdots + a_n g_n$$

where $a_1, a_2, \ldots, a_n$ are elements of R. The sum of two such elements is defined by

1.1.2.

$$(\sum_{i=1}^{n} a_i g_i) + (\sum_{i=1}^{n} b_i g_i) = \sum_{i=1}^{n} (a_i + b_i) g + i.$$

[2]The paper was finally published in the American Journal of Mathematics in 1881, then edited by J.J. Sylvester, with notes and addenda by Charles Sanders Peirce, son of the author[19].

Also, given two elements $\alpha = \sum_{i=1}^{n} a_i g_i$ *and* $\beta = \sum_{i=1}^{n} b_i g_i$ *in* RG *we define their* product *by*

1.1.3.
$$\alpha\beta = \sum_{i,j} (a_i b_j)(g_i g_j);$$

i.e.,
$$\alpha\beta = \sum_{i=1}^{n} c_h g_h$$

where c_h is the sum of products of the form $a_i b_i$ for all pairs of indexes i, j such that $g_i g_j = g_h$.

It is easily seen that, with the operations above RG is a ring, which has a unity; namely, the element $\mathbf{1} = \sum_{i=1}^{n} u_i g_i$ where $u_1 = 1$ and $u_i = 0$ if $i \neq 1$.

Notice that we can also define the product of elements $\alpha \in RG$ by scalars $r \in R$ by:

1.1.4.
$$r\left(\sum_{i=1}^{n} a_i g_i\right) = \sum_{i=1}^{n} (r a_i) g_i.$$

With this definition, RG becomes a module over R whhich is actually free, with basis G.

We have defined the concept of a group algebra only for finite groups because these are the ones that shall be useful when studying codes; however, it should be noted that they can be defined on the more general setting of groups which are not necessarily finite; see for example [18], [21] or [23].

Cayley's paper had no immediate influence on the mathematicians of the time and group rings remained untouched for still quite some time. They were introduced again by Theodor Molien when he realized that this was a natural setting in which to apply some of his earlier criteria for semisimplicity of rings.

The connection between group representation theory and the structure theory of algebras - which is obtained through group rings - was widely recognized after a most influential paper by Emmy Noether [16], some joint work of hers with Richard Brauer [3] and Brauer's paper [2].

We conclude this section with a few elementary results that will be useful in the sequel.

Lemma 1.1.5. *Let $f : G \to H$ be a group homomorphism. Then, there exists a unique ring homomorphism $f^* : RG \to RH$ such that $f^*(g) = f(g)$, for all $g \in G$. If R is commutative, then f^* is a homomorphism of R-algebras; moreover, if f is an epimorphism (monomorphism), then f^* is also an epimorphism (monomorphism).*

The proof is straightforward. A similar result is given in Exercise 1.

We remark that if $H = \{1\}$, then Lemma 1.1.5 shows that the trivial mapping $G \to \{1\}$ induces a ring homomorphism $\varepsilon : RG \to R$ such that $\varepsilon(\sum_{g\in G} a_g g) = \sum_{g\in G} a(g)$.

Definition 1.1.6. *The homomorphism $\varepsilon : RG \to R$ given by*

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

is called the **augmentation mapping** *of RG and its kernel, denoted by $\Delta(G)$, is called the* **augmentation ideal** *of RG.*

Notice that if an element $\alpha = \sum_{g\in G} a_g g$ belongs to $\Delta(G)$ then $\varepsilon(\alpha) = \sum_{g\in G} a_g = 0$. So, we can write α in the form:

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1).$$

Since clearly all elements of the form $g - 1,\ g \in G$, belong to $\Delta(G)$, the observation above shows that $\{g - 1 \ :\ g \in G,\ g \neq 1\}$ is a set of generators of $\Delta(G)$ over R. Also, notice that the linear independence of this set follows immediately, so we have actually shown the following.

Proposition 1.1.7. *The set $\{g - 1 : g \in G,\ g \neq 1\}$ is a basis of $\Delta(G)$ over R.*

Thus, we can write

$$\Delta(G) = \left\{ \sum_{g\in G} a_g(g-1) : g \in G,\ g \neq 1,\ a_g \in R \right\}.$$

Notice that, in particular, if R is commutative and G is finite, then $\Delta(G)$ is a free R-module of rank $|G| - 1$.

EXERCISES

1. Let $\mathbb{F}$ be a finite field with q elements and G a group of order n. Compute the number of elements of $\mathbb{F}G$.

2. Let $\phi : R \to S$ be a homomorphism of rings and let G be a group. Show that the mapping $\phi^* : RG \to SG$ given by

$$\sum_{g\in G} a(g)g \mapsto \sum_{g\in G} \phi(a(g))g$$

is a ring homomorphism. Show that ϕ is a monomorphism (epimorphism) if and only if ϕ^* is also a monomorphism (epimorphism).

3. Let $R \subset S$ be rings with the same unit element and let G be a group. Show that $SG \simeq S \otimes_R RG$.

4. Let R be a commutative ring, let G, H be groups.

   (i) Show that $R(G \times H) \simeq (RG)H \simeq (RH)G$ (where $(RG)H$ denotes the group ring of H over the ring RG).

   (ii) Show also that $R(G \times H) \simeq RG \otimes_R RH$.

5. Let $\{R_i\}_{i\in I}$ be a family of rings and set $R = \oplus_{i\in I} R_i$. Show that, for any group G, we have that $RG \simeq \oplus_{i\in I} R_i G$.

6. Let I be a two-sided ideal of a ring R and let G be a group. Show that $IG = \{\sum_{g\in G} a(g)g \in RG \ : \ a(g) \in I\}$ is a two-sided ideal of RG and that $RG/IG \simeq (R/I)G$.

1.2 Augmentation Ideals

Definition 1.2.1. *Given a subgroup $H \in \mathcal{S}(G)$, we shall denote by $\Delta_R(G, H)$ the left ideal of RG generated by the set $\{h - 1 \ : \ h \in H\}$. That is,*

$$\Delta_R(G, H) = \left\{ \sum_{h\in H} \alpha_h(h - 1) \ : \ \alpha_h \in RG \right\}.$$

While working with a fixed ring R we shall omit the subscript and denote this ideal simply by $\Delta(G, H)$. Notice that the ideal $\Delta(G, G)$ coincides with the augmentation ideal $\Delta(G)$ introduced in the previous section.

Lemma 1.2.2. *Let H be a subgroup of a group G and let S be a set of generators of H. Then, the set $\{s - 1 \ : \ s \in S\}$ is a set of generators of $\Delta(G, H)$ as a left ideal of RG.*

Proof. Since S is a set of generators of H, every element $1 \neq h \in H$ can be written in the form $h = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_r^{\varepsilon_r}$ with $s_i \in S,\ \varepsilon_i = \pm 1,\ 1 \leq i \leq r$, for some positive integer r.

To prove the lemma, it suffices to show that all the elements of the form $h-1,\ h \in H$ belong to the left ideal I generated by the set $\{s-1\ :\ s \in S\}$. This can be seen by repeatedly applying the identities: $x^{-1}-1 = x^{-1}(1-x)$ and $xy-1 = x(y-1)+(x-1)$. □

To give a better description of $\Delta_R(G,H)$, let us denote by $\mathcal{T} = \{q_i\}_{i\in I}$ a complete set of representatives of left cosets of H in G, which we call a *transversal* of H in G. We shall always assume that we are choosing, as a representative of the particular coset H in $\mathcal{T}$, precisely the identity element of G. Thus, every element $g \in G$ can be written uniquely in the form $g = q_i h_j$ with $q_i \in \mathcal{T}$ and $h_j \in H$.

Proposition 1.2.3. *The set $B_H = \{q(h-1)\ :\ q \in \mathcal{T}, h \in H, h \neq 1\}$ is a basis of $\Delta_R(G,H)$ over R.*

Proof. First, we shall show that this set is linearly independent over R. Assume that we have a linear combination $\sum_{i,j} r_{ij} q_i (h_j - 1) = 0$, $r_{ij} \in R$. Then, we can write:

$$\sum_{i,j} r_{ij} q_i h_j = \sum_i \left(\sum_j r_{ij} \right) q_i.$$

Since $h_j \neq 1$ for all values of j, it follows easily that the members in the equation above have disjoint support. As the elements in G are linearly independent over R it readily follows that all coefficients must be 0. In particular, $r_{ij} = 0$, for all i, j.

To show that B_H also generates $\Delta_R(G,H)$, it will suffice to prove that every element of the form $g(h-1)$, with $g \in G$, $h \in H$, can be written as a linear combination of elements in B_H. Now, $g = q_i h_j$ for some $q_i \in \mathcal{T}$ and some $h_j \in H$. Then

$$g(h-1) = q_i h_j (h-1) = q_i (h_j h - 1) - q_i (h_j - 1)$$

and the result follows. □

Remark. Taking $H = G$, the corollary above is precisely Proposition 1.1.7.

In the case when H is a normal subgroup of G the ideal $\Delta(G,H)$ has an interesting meaning . In fact, if $H \lhd G$, then the natural homomorphism $\omega : G \to G/H$ can be extended to an epimorphism $\omega^* : RG \to R(G/H)$ such that

$$\omega^* \left(\sum_{g \in G} a(g)g \right) = \sum_{g \in G} a(g)\omega(g).$$

Proposition 1.2.4. *With the notations above, $Ker(\omega^*) = \Delta(G,H)$.*

Proof. Let $\mathcal{T}$ be a transversal of H in G. Then, every element $\alpha \in RG$ can be written as a finite sum $\alpha = \sum_{i,j} r_{ij}q_ih_j, r_{ij} \in R, q_i \in \mathcal{T}, h_j \in H$.

If we denote by $\overline{q_i}$ the image of q_i in the factor group G/H then we have

$$\omega^*(\alpha) = \sum_i (\sum_j r_{ij})\overline{q_i}.$$

Hence, $\alpha \in Ker(\omega^*)$ if and only if $\sum_j r_{ij} = 0$ for each value of i. So, if $\alpha \in Ker(\omega^*)$ we can write (adding some zeros):

$$\alpha = \sum_{i,j} r_{ij}q_ih_j = \sum_{i,j} r_{ij}q_ih_j - \sum_i \left(\sum_j r_{ij} \right) q_i = \sum_{i,j} r_{ij}q_i(h_j - 1) \in \Delta(G,H).$$

Thus, $Ker(\omega^*) \subset \Delta(G,H)$. The opposite inclusion follows trivially. □

Corollary 1.2.5. *Let H be a normal subgroup of a group G. Then, $\Delta(G,H)$ is a two-sided ideal of RG and*

$$\frac{RG}{\Delta(G,H)} \cong R(G/H).$$

As a special case, we see that $\Delta(G)$ is the kernel of the epimorphism ε induced by the trivial mapping $G \to \{1\}$ and thus

$$\frac{RG}{\Delta(G)} \cong R.$$

EXERCISES

1. Give the details of the proof of Lemma 1.2.2
2. Let $R \subset S$ be rings with the same unity and let G be a group. For any subgroup H of G, show that $\Delta_S(G,H) = S\Delta_R(G,H)$
3. Let R be a ring and let H be a subgroup of a group G. We can regard RH as a subring of RG and, consequently, $\Delta(H)$ as a subset of RG. Under this convention, show that:
   (i) $\Delta(G,H) = RG\Delta(H)$.
   (ii) $\Delta(G,H) = \Delta(H) + \Delta(G)\Delta(G,H)$.
4. Let H be a subgroup of a group G and assume that $\{H_i\}_{i\in I}$ is the set of all conjugates of H in G. Show that $U(H) = \sum_{i\in I}\Delta(G,H_i)$ and $V(H) = \cap_{i\in I}\Delta(G,H_i)$ are two-sided ideals of RG. Use this fact to give another proof of the fact that if $H \lhd G$ then $\Delta(G,H)$ is a two-sided ideal.
5. Given a left ideal $I \in \mathcal{I}(RG)$, set
$$\bigtriangledown(I) = \{g \in G \ : \ g-1 \in I\} = G \cap (1+I).$$
Prove that $\bigtriangledown(I)$ is a subgroup of G and that if I is a two-sided ideal of RG then $\bigtriangledown(I)$ is normal in G.
6. Prove that, if H is a subgroup of G, then $\bigtriangledown(\Delta(G,H)) = H$.
7. Let I be an ideal in RG. Prove that $\Delta(G, \bigtriangledown(I)) \subset I$.
   Show that $\Delta(G, \bigtriangledown(RG)) = \Delta(G) \neq RG$.
8. Let $\mathcal{T}$ be a transversal of a subgroup H in a group G. Show that, for any ring R, the group ring RG may be considered as a left RH-module. Show that this module is free over RH with basis $\mathcal{T}$.

1.3 Nilpotent Ideals

Let I be an ideal (left, right or two-sided) of a ring R. Set
$$I^n = \{\Sigma x_1 \cdots x_n \ : \ x_i \in I\} = 0;$$
i.e., I^n is the ideal, of the same type, generated by all products of n factors $x_1 \cdots x_n$ of elements in I

Definition 1.3.1. *We say that the ideal I is* **nilpotent** *if $I^n = 0$ for some n. The minimal positive integer n such that $I^n = 0$ is called the* **nilpotency index** *of I.*

Also, I is said to be **nil** *if, for every $x \in I$, there is an integer $n = n(x)$ such that $x^n = 0$.*

Proposition 1.3.2. *A ring R has a nilpotent right (or left) ideal if and only if R has a nilpotent (two-sided) ideal.*

Proof. Suppose $0 \neq I$ is a right ideal of R such that $I^n = 0$. Then RI is a two-sided ideal in R. Moreover,

$$(RI)^n = (RI)(RI)\dots(RI) = R(IR)(IR)\cdots(IR)I \subseteq R(I^n) = 0$$

and thus RI is a nilpotent ideal of R. The case when I is a left ideal is similar. □

Notice that, if there is a central element μ in a ring R with $\mu^2 = 0$, then μR is a two-sided ideal and $(\mu R)^2 = (\mu)^2 R^2 = 0$ so it is nilpotent.

In the case of a group algebra RG over a ring of positive characteristic p we can easily produce such an element μ when G contains a normal subgroup N of order divisible by the p. In fact, set $\mu = \sum_{x\in N} x$. Then

$$(\mu)^2 = (\sum\nolimits_{x\in N} x)\mu = \sum\nolimits_{x\in N} x\mu.$$

As $x\mu = \mu$ for all $x \in N$, we get $(\mu)^2 = |N|\mu = 0$. Hence, $I = \mu KG$ is an ideal in KG with $I^2 = 0$.

To fully describe the case when RG contains nilpotent ideals we need to introduce an important concept.

The regular representation

Let G be a finite group of order n and let R be a commutative ring. We shall consider RG as a free module over R, with basis G, and denote by $GL(RG)$ the set of all R-automorphisms of RG.

We can define a map $T : G \to GL(RG)$ as follows: to each element $g \in G$ we assign the linear map T_g which acts on the given basis by left multiplication. That is, $T_g(g_i) = gg_i$. It is easy to see that this is a homomorphism of G to $GL(RG)$; i.e., that :

$$T_{gh}(y) = (gh)y = g(h(y)) = T_g T_h(y).$$

The representation so defined is called the *regular representation* of G over R. Notice that we have defined the representation corresponding to an element $g \in G$ by using *left* multiplication by g on the elements of G, so this

should more properly be called the *left* regular representation of

As an illustration, we shall compute this representation for a couple of concrete examples. We first consider $G = \{1, a, a^2\}$, a cyclic group of order 3, whose elements we enumerate as $g_1 = 1,\ g_2 = a,\ g_3 = a^2$.

To find the image of a under the regular representation, we compute

$$ag_1 = g_2, \quad ag_2 = g_3, \quad ag_3 = g_1,$$

so we have that

$$T_a(g_1) = g_2, \quad T_a(g_2) = g_3, \quad T_a(g_3) = g_1.$$

Consequently, the matrix associated with T_a in the given basis is

$$\rho(a) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Consider now the Klein 4-group $G = \{1, a, b, ab\}$, whose elements we enumerate as: $g_1 = 1,\ g_2 = a,\ g_3 = b,\ g_4 = ab$. As above, we can obtain the matrix of $\rho(a)$

$$\rho(a) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

In a similar way

$$\rho(b) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \rho(ab) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \rho(1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Notice that, for an arbitrary finite group G, given an element $g \in G$, to find the matrix associated with T_g in the basis G we must compute, for each $g_i \in G$, the image $T_g(g_i)$ and its coefficients on the basis G will give the i^{th}-column of the matrix. Since $gg_i = g_j$, for some $g_j \in G$, the coefficients in this column will all be equal to 0, except for one of them, which will be equal to 1. Hence, this is a permutation matrix.

Also, if $g \neq 1$ then $gg_i \neq g_i$. This implies that when $g \neq 1$ all entries in the main diagonal of the corresponding matrix are equal to 0.

Thus, we have an easy formula for the matrix trace:

$$\begin{aligned} \mathrm{tr}(T_g) &= 0 \quad \text{if} \quad 1 \neq g \in G, \\ \mathrm{tr}(T_1) &= |G|. \end{aligned}$$

We are now ready to prove the main result in this section.

Theorem 1.3.3. (**Maschke's Theorem**) *Let RG be the group algebra of a finite group over a field K of characteristic $p \geq 0$. Then KG has a (nonzero) nilpotent ideal if and only if $p > 0$ and $p \mid |G|$.*

Proof. We have already seen above that if $p \mid |G|$ then taking $\mu = \sum_{x \in G} x$, the ideal $\mu KG = I$, is nilpotent.

We shall now assume that $p = 0$ or $p \nmid |G|$ and prove that KG has no nilpotent ideals. Let T be the regular representation of KG.

Let I be a nonzero nilpotent ideal of KG and let $\gamma = \sum \gamma_g g \in I$, be a nonzero element. Then $\gamma_{g_0} \neq 0$ for some $g_0 \in G$ and thus the element $\alpha = g_0^{-1}\gamma$ is in I and, writting $\alpha = \sum_{i=1}^{n} a_i g_i$ we have that $a_1 \neq 0$. Then, using the formulas for the trace of the regular representation, we have:

$$tr(T_\alpha) = tr\left(\sum_{i=1}^{n} a_i T_{g_i}\right) = a_1|G|.$$

On the other hand, since the trace of a nilpotent matrix is equal to 0, we get $a_1|G| = 0$, a contradiction since $|G|$ is invertible in K. □

This result was first obtained in 1898-99, in connection with finite groups of transformations, by Heinrich Maschke (1853 - 1908), and is the first important fact in representation theory. It was later extended to the general case of the group algebra of an arbitrary group over a commutative ring with unity by I.G. Connell [6] (see [21, Theorem 3,4,7]).

Nilpotent Augmentation Ideals

We shall now investigate for which groups G the augmentation ideal $\Delta(G)$ of KG is nilpotent.

Theorem 1.3.4. (Coleman [5]) *Let K be a field of characteristic $p \geq 0$ and G a finite group. Then, $\Delta(G)$ of KG is nilpotent if and only if $p > 0$ and G is a p-group.*

Proof. First, suppose that $\Delta(G)$ is nilpotent. Suppose that G has two non-identity elements x and y of relatively prime orders m and n respectively. Then

$$1 = x^m = (1 + x - 1)^m = 1 + m(x-1) + \binom{m}{2}(x-1)^2 + \cdots + (x-1)^m$$

and hence

$$m(x-1) + \binom{m}{2}(x-1)^2 + \cdots + (x-1)^m = 0.$$

Similarly,

$$1 = y^n = (1 + y - 1)^n = 1 + n(y-1) + \binom{n}{2}(y-1)^2 + \cdots + (y-1)^n$$

and

$$n(y-1) + \binom{n}{2}(y-1)^2 + \cdots + (y-1)^n = 0.$$

Choose integers u, v such that $mu + nv = -1$. Multiply the above equations by $u(y-1)$ and $v(x-1)$ respectively and add to obtain

$$\begin{aligned}(x-1)(y-1) &= u\binom{m}{2}(x-1)^2(y-1) + \cdots + u(x-1)^m(y-1) \\ &\quad + v\binom{n}{2}(x-1)(y-1)^2 + \cdots + v(x-1)(y-1)^n \\ &\quad \in \Delta(G)(x-1)(y-1) + (x-1)(y-1)\Delta(G).\end{aligned}$$

It follows that $(x-1)(y-1) \in (\Delta G)^s$ for all s. The element $(x-1)(y-1)$ is nonzero due to the choice of x and y. This is a contradiction and thus every element of G has prime power order.

If $char(K) \neq p$, then KG has no nilpotent ideals by Theorem 1.3.3. Hence $char(K) = p$, as claimed.

Conversely, let us assume that G is a finite p-group and K has characteristic p. We shall prove that $\Delta(G)$ is nilpotent by induction on $|G|$.

Choose an element $z \in \zeta(G)$, of order p. Then $\overline{G} = G/\langle z \rangle$ is a group of order smaller than $|G|$ and $(\Delta(\overline{G}))^{p^t} = 0$ for some t. This means that

$$(\Delta(G))^{p^t} \subseteq \Delta(G, \langle z \rangle) = (1-z)KG.$$

Then $(\Delta(G))^{p^{t+1}} \subseteq (1-z)^p KG = 0$, completing the proof. □

Corollary 1.3.5. *Let K be a field of characteristic p and let P be a normal subgroup of a finite group G. Then $\Delta(G,P)$ is nilpotent if and only if P is a p-group.*

Proof. Since $\Delta(G,P) = KG(\Delta(P)) = (\Delta(P))KG$, (see part (i) of exercise 3) we have

$$(\Delta(G,P))^n = (KG(\Delta(P)))^n = KG(\Delta(P))^n.$$

Hence, $\Delta(G,P)$ is nilpotent if and only if $\Delta(P)$ is nilpotent. The result now follows from the theorem. □

EXERCISES

1. Let $A = \{1, a, a^2, \ldots, a^{m-1}\}$ be a cyclic group of order m, and let T be its regular representation over a field K. Compute T_a.

2. Let $\mathcal{Q} = \langle a, b \mid a^4 == 1,\ a^2 = b^2,\ bab = a^{-1}\rangle$ be the quaternion group of order 8 and T the regular representation of $\mathcal{Q}$ over a field K. Compute T_a and T_b.

3. Let $D_4 = \langle a, b \mid a^4 = b^2 = 1,\ bab = a^{-1}\rangle$ be the dihedral group of order 8 T and T the regular representation of D_4 over a field K. Compute T_a and T_b.

4. Let $\mathbb{F}_2$ be the field with two elements. Compute the nilpotency index of $\mathbb{F}_2 D_4$ and of $\mathbb{F}_2\mathcal{Q}$.

5. Let R be a ring of characteristic p^t, $t \geq 1$. Prove that if G contains a finite normal p-subgroup P, then $\Delta(G,P)$ is a nilpotent ideal and $1+\Delta(G,P)$ is a normal subgroup of $\mathcal{U}(RG)$, the set of invertible elements of RG. Show also that it is a p-group.

6. Let $G = P \rtimes Q$, be the semi-direct product of the subgroups P and Q, where P is a p-group and Q contains no element of order p, and let R be a comutative ring of characteristic p. Prove that the quotient ring $G/\Delta(G,P)$ contains no nilpotent ideals.

7. Let $\mathbb{F}$ be a field of characteristic p and G a finite p group.

   (i) Show that every element $\alpha \in \mathbb{F}G$ such that $\varepsilon(\alpha) \neq 0$ is invertible.

   (ii) Prove that $\Delta(G)$ is the unique maximal ideal of $\mathbb{F}G$.

Chapter 2

Semisimplicity

2.1 Basic Facts

We saw, in the previous section, that if $\mathbb{F}$ is a field and G a finite group, then the group algebra $\mathbb{F}G$ contains no nilpotent ideals if and only if $char(\mathbb{F}) \nmid |G|$. This fact has very important consequences.

J.H.M. Wedderburn proved, in 1907 what became one of the most important theorems in the theory of structure of algebras. To state it, we need to introduce some concepts.

Definition 2.1.1. *An algebra A over a commutative ring R is called* **simple** *if it contains no proper two-sided ideals.*

The algebra A is called **semisimple** *if it is a direct sum of simple algebras.*

It can be shown that an algebra A is semisimple if and only if every left (or right) ideal is a direct summand (for a detailes account of these facts see [7, Chapter IV] or [21, Section 2.5]).

Weddurburns result states that a finite-dimensional algebra is semisimple if and only if it contains no nilpotent ideals. Moreover, he showed that simple algebras are isomorphic to full matrix rings over division rings. Combining this result with Maschke's Theorem, we obtain the following.

Theorem 2.1.2. ([21, Theorem 3.4.9]) *Let G be a finite group and let $\mathbb{F}$ be a field such that $char(\mathbb{F}) \nmid |G|$. Then:*

> *(i) $\mathbb{F}G$ is a direct sum of a finite number of two-sided ideals $\{A_i\}_{1 \leq i \leq r}$, called the* **simple components** *of KG. Each A_i is a simple algebra.*

(ii) Any two-sided ideal of $\mathbb{F}G$ is a direct sum of some of the members of the family $\{B_i\}_{1\leq i\leq r}$.

(iii) Each simple component A_i is isomorphic to a full matrix ring of the form $M_{n_i}(D_i)$, where D_i is a division ring containing an isomorphic copy of $\mathbb{F}$ in its center, and thus

$$\mathbb{F}G \;\cong\; \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

as $\mathbb{F}$-algebras.

Every ideal of a semisimple algebra is generated by an idempotent element; i.e., by an element e such that $e^2 = e$ and the ideal is two-sided if and only if the idempotent is central (see Exercise 2). Consequently, the theorem above can be translated as follows.

Theorem 2.1.3. *Let G be a finite group and let $\mathbb{F}$ be a field such that $char(\mathbb{F}) \nmid |G|$ and let $\mathbb{F}G = \oplus_{i=1}^{s} A_i$ be the decomposition of the group algebra as a direct sum of minimal two-sided ideals. Then, there exists a family $\{e_1, \ldots, e_s\}$ of elements of $\mathbb{F}G$ such that:*

(i) $e_i \neq 0$ *is a central idempotent,* $1 \leq i \leq t$.

(ii) If $i \neq j$ *then* $e_i e_j = 0$.

(iii) $1 = e_1 + \cdots + e_t$.

(iv) e_i *cannot be written as* $e_i = e_i' + e_i''$ *where* e_i', e_i'' *are central idempotents such that both* $e_i', e_i'' \neq 0$ *and* $e_i' e_i'' = 0$, $1 \leq i \leq t$.

(v) $A_i = Ae_i$, $1 \leq i \leq s$.

The idempotents in the theorem above are called the **primitive central idempotents** of $\mathbb{F}G$.

Since in a semisimple algebra A every left ideal is a direct summand, it is easy to show that, if A is finite-dimensional, then it can be written as a direct sum of minimal left ideals (as A-modules):

$$A = L_1 \oplus L_2 \oplus \cdots \oplus L_t.$$

As these are also of the form $L_i = Ae_i$, where e_i is an idempotent (not necessarily central) of A, $1 \leq i \leq t$, we also have the following.

Theorem 2.1.4. *Let G be a finite group and let $\mathbb{F}$ be a field such that $char(\mathbb{F}) \nmid |G|$ and let $\mathbb{F}G = \oplus_{i=1}^{s} L_i$ be a decomposition of the group algebra as a direct sum of minimal left ideals. Then, there exists a family $\{e_1, \ldots, e_s\}$ of elements of $\mathbb{F}G$ such that:*

(i) $e_i \neq 0$ *is an idempotent,* $1 \leq i \leq t$.

(ii) If $i \neq j$ *then* $e_i e_j = 0$.

(iii) $1 = e_1 + \cdots + e_t$.

(iv) e_i *cannot be written as* $e_i = e_i' + e_i''$ *where* e_i', e_i'' *are idempotents such that both* $e_i', e_i'' \neq 0$ *and* $e_i' e_i'' = 0$, $1 \leq i \leq t$.

(v) $L_i = Ae_i$, $1 \leq i \leq t$.

The idempotents in the theorem above are called a set of **primitive idempotents** of $\mathbb{F}G$.

Notice that part (ii) of Theorem 2.1.3 implies that the set of simple components of $\mathbb{F}G$ is precisely the set of minimal two-sided ideals of $\mathbb{F}G$. This implies, in particular, that the decomposition of the algebra as a sum of simple components is unique and, hence, that the set of primitive central idempotents is also unique. On the other hand, it can be shown that the decomposition of the algebra as a sum of minimal left ideal is unique, but only up to isomorphisms. Consequently sets of (non necessarily central) primitive idempotents, as in Theorem 2.1.4, are not unique.

EXERCISES

1. Let R be a commutative ring with unity and let $A = M_n(R)$ be the algebra of $n \times n$ matrices over R.

   (i) Show that $\mathcal{I}$ is an ideal of A if and only if $\mathcal{I} = M_n(I)$, where I is a two-sided ideal of R.

   (ii) Prove that if D is a division ring, then $A = M_n(D)$ is a simple algebra over the center of D.

2. Let R be a ring with unity.

(i) Show that an ideal I of R is a direct summand of R if and only of there exists an idempotent element $e \in R$ such that $I = Re$ and $R = Re \oplus R(1-e)$.

(ii)Prove that an ideal of the form $I = Re$ is two-sided if and only if e is central; i.e., $ex = xe$ for all $x \in R$.

(iii) The (left) **annihilator** of an ideal I in a ring R is the set:

$$ann(I) = \{x \in R \mid xy = 0,\ \forall y \in I\}.$$

Prove that the annihilator of Re is $R(1-e)$ and, conversely, the annihilator of $R(1-e)$ is Re.

3. Let D be a division ring and let $A = M_n(D)$, be the full ring of $n \times n$ matrices with entries in D.

   (i) Show that the set

$$I = \left\{ \begin{bmatrix} x_1 & 0 & \dots & 0 \\ x_2 & 0 & \dots & 0 \\ & & \dots & \\ x_n & 0 & \dots & 0 \end{bmatrix} \ :\ x_1, x_2, \dots, x_{n_i} \in \right\} \cong D^n$$

   is a minimal left ideal of A.

   (ii) Prove that every minimal left ideal of A is isomorphic to I.

4. Let I_1, I_2 be left ideals of a simple algebra A. Prove that either $I_1 I_2 = 0$ or $I_1 \cong I_2$.

5. Prove Theorem 2.1.3 assuming Theorem 2.1.2.

6. Assuming, once again, Theorem 2.1.2, prove that every central idempotent in a finite dimensional semisimple algebra is a sum of primitive central idempotents (which are called its **constituents**).

7. Prove that if a semisimple algebra A is finite-dimensional, then it can be written as a direct sum of minimal left ideals. Use this fact to prove Theorem 2.1.4.

8. Show that the center of a finite dimensional semisimple algebra is a direct sum of fields.

9. Let A be a finite dimensional semisimple algebra over an algebraically closed field $\mathbb{F}$. Prove that A is isomorphic to a direct sum of the form

$$A \cong M_{n_1}(\mathbb{F}) \oplus \cdots \oplus M_{n_s}(\mathbb{F}).$$

10. Let $(X^n - 1)$ denote the ideal of $\mathbb{F}[X]$ generated by $X^n - 1$. Prove that the quotient ring $\mathbb{F}[X]/(X^n - 1)$ is a semisimple algebra over $\mathbb{F}$.

11. Determine the structure of $\mathbb{Q}[X]/(X^n - 1)$ for $n = 3,\ 5$ and 6. Determine the structure of $\mathbb{C}[X]/(X^n - 1)$ for the same values of n.

12. Given a polynomial $f \in \mathbb{F}[X]$ let $f = f_1^{n_1} f_2^{n_2} \cdots f_t^{n_t}$ be its decomposition as a product of irreducible polynomials of $\mathbb{F}[X]$. Prove that $\mathbb{F}[X]/(f)$ is a semisimple algebra over $\mathbb{F}$ if and only if $n_i = 1,\ 1 \leq i \leq t$.

13. Let A and B be finite abelian groups. Prove that $\mathbb{C}A \cong \mathbb{C}B$ if and only of $|A| = |B|$.

14. For an arbitrary positive integer n, let $\mathbb{F}$ be a field of characteristic not dividing n and let C_n denote the cyclic group of order n.

    (i) Compute the decomposition of $\mathbb{F}C_2$ and of $C_2 \times \cdots \times C_2$.

    (ii) Compute the decomposition of $[\mathbb{F}C_2 \times C_3]$.

2.2 The number of simple components

There is a situation when the number of simple components of a finite dimensional, semisimple algebra is quite easy to determine.

Definition 2.2.1. *Let A be a finite dimensional semisimple algebra over a field F. The field $\mathbb{F}$ is called a* **splitting field** *for A if all the simple components of A are isomorphic to full matrix rings over $\mathbb{F}$ itself; i.e., $\mathbb{F}$ is a splitting field for A if*

$$A \cong \bigoplus_{i=1}^{s} M_{n_i}(\mathbb{F}).$$

Let G e a finite group. If a field $\mathbb{F}$ is a splitting field for the group algebra $\mathbb{F}G$, then we say that $\mathbb{F}$ is a **splitting field for** *G.*

Notice that Exercise 9 of the previous section shows that algebraically closed fields are splitting fields for finite dimensional semisimple algebras. There is a better result due to R. Brauer which we quote withiot proof (see [7, Theorem 41.1], [8, pp. 127-128]).

Theorem 2.2.2. (Brauer) *Let G be a finite group of exponent m and let θ be a primitive root of unity of order m. If K is a field such that $char(K) \nmid |G|$ then $K(\theta)$ is a splitting field for G.*

The center of a matrix ring $M_n(\mathbb{F})$ over a field $\mathbb{F}$ is isomorphic to $\mathbb{F}$ (see Exercise 1). Hence, if $\mathbb{F}$ is a splitting field for a finite dimensional semisimple algebra A and

$$A \cong \bigoplus_{i=1}^{s} M_{n_i}(\mathbb{F})$$

we have that

$$\mathcal{Z}(A) \cong \bigoplus_{i=1}^{s} \mathcal{Z}(M_{n_i}(\mathbb{F})) \cong \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{s \text{ times}}.$$

Consequently, we have the following.

Corollary 2.2.3. *Let $\mathbb{F}$ be a splitting field for a finite dimensional semisimple algebra A. Then, the number of simple components of A equals the dimension of $\mathcal{Z}(A)$ over $\mathbb{F}$.*

In the case of the group algebra, this dimension is easy to compute, as we show below. To do so, we introduce some very important elements.

Definition 2.2.4. *Let G be a group, R a commutative ring and let $\{C_i\}_{i\in I}$ be the set of conjugacy classes of G which contain only a finite number of elements. For each index $i \in I$ set $\gamma_i = \sum_{x\in C_i} x \in RG$. These elements are called the* **class sums** *of G over R.*

Theorem 2.2.5. *Let G be a group and let R be a commutative ring. Then, the set $\{\gamma_i\}_{i\in I}$ of all class sums forms a basis of $\mathcal{Z}(RG)$, the centre of RG, over R.*

Proof. First, notice that given an arbitrary element $g \in G$, we have that $g^{-1}\gamma_i g = \sum_{x\in C_i} g^{-1}xg$. Since conjugation by g is an automorphism of G which fixes class sums (that is, $C_i^g = C_i$ for every index $i \in I$), we see that $\sum_{x\in C_i} g^{-1}xg = \sum_{y\in C_i} y = \gamma_i$. Hence, $\gamma_i g = g\gamma_i$, for all $g \in G$, showing that $\gamma_i \in \mathcal{Z}(RG)$, $\forall i \in I$.

To show that these elements are linearly independent, assume that we have a finite sum $\sum_i r_i\gamma_i = 0$. We can write this equation as $\sum_i r_i \sum_{x\in C_i} x = 0$ and, since different class sums have disjoint supports, the linear independence of the elements in G shows that we must have $r_i = 0$, for all $i \in I$.

Finally, suppose $\alpha = \sum_{g\in G} a_g g \in \mathcal{Z}(RG)$. We shall show that if $g \in supp(\alpha)$, then any other element h in the conjugacy class of g also belongs to $supp(\alpha)$ and $a_g = a_h$. In fact, if $h = x^{-1}gx$ for some $x \in G$, since α is central, we have that $\alpha = x^{-1}\alpha x$. That is,

$$\sum_{g\in G} a(g)g = \sum_{g\in G} a(g)x^{-1}gx.$$

By comparing the coefficient of h on both sides of this equation, we get that $a_h = a_g$. This shows that we may factor the coefficients of elements in each conjugacy class and write

$$\alpha = \sum_i a_i\gamma_i.$$

Hence, $\{\gamma_i\}_{i\in I}$ is also a set of generators for $\mathcal{Z}(RG)$. □

Corollary 2.2.6. *Let $\mathbb{F}$ be a splitting field for a finite group G. Then, the number of simple components of $\mathbb{F}G$ is equal to the number of conjugacy classes of G.*

Example 2.2.7. Let S_3 denote the group of permutations of three elements. We wish to describe its group algebra over $\mathbb{C}$, the field of complex numbers. We can write $S_3 = \{I,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$. It is well-known that two permutations are conjugate if and only if they have the same cycle structure, so we can compute the conjugacy classes of S_3:

$$\begin{aligned} C_1 &= \{I\} \\ C_2 &= \{(1\ 2),\ (1\ 3),\ (2\ 3)\} \\ C_3 &= \{(1\ 2\ 3),\ (1\ 3\ 2)\} \end{aligned}$$

Thus $\mathbb{C}S_3$ must contain three simple components which are full matrix rings of the form $M_n(\mathbb{C})$. If we write $\mathbb{C}G \simeq A_1 \oplus A_2 \oplus A_3$ we see that $[A_1 : \mathbb{C}] + [A_2 : \mathbb{C}] + [A_3 : \mathbb{C}] = [\mathbb{C}S_3 : \mathbb{C}] = 6$. Notice that if, for a given summand, we have that $n > 1$, then the corresponding dimension is greater than or equal to 4. Hence, it is easily seen that the only possibility is

$$\mathbb{C}S_3 \simeq \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}).$$

If $\mathbb{F}$ is not a splitting field, the number of simple components of $\mathbb{F}G$ is not so easy to obtain. However, D.S. Berman [1] and E. Witt [24] were able to compute this number in the general case, using character theory ([7, Theorems 21.5 and 21.25]). In this section we shall give a proof of this result entirely in terms of the inner structure of the group algebra, due to R.A. Ferraz [9].

Let G be a finite group of exponent m containing s different conjugacy classes and let θ be a primitive root of unity of order m. Using Theorem 2.2.2 we can write

$$K(\theta)G \cong \bigoplus_{i=1}^{s} M_{n_i}(K(\theta)).$$

Let φ denote the isomorphism above. If we denote by $T_i : \mathbb{K}(\theta)G \to M_{n_i}(K(\theta)),\ 1 \leq i \leq s$ the composition of φ with the natural projection onto the corresponding simple component, we can write $\varphi = T_1 \oplus \cdots \oplus T_s$ where the maps $T_1,\ 1 \leq i \leq s$, are precisely the irreducible representations of G over $K(\theta)$ and T_i is not equivalent to T_j whenever $i \neq j$. We denote by χ_i the character afforded by the representation $T_i,\ 1 \leq i \leq s$.

If we restrict this isomorphism to $\mathcal{Z}(K(\theta)G)$ we get:

$$\varphi(\mathcal{Z}(K(\theta)G)) = \underbrace{K(\theta) \oplus \cdots \oplus K(\theta)}_{s \text{ times}}.$$

Let σ be an automorphism in $Gal(K(\theta), K)$. We can extend σ to $\varphi(\mathcal{Z}(K(\theta)G))$ in a natural way as follows. Given $(k_1, \ldots, k_t) \in \varphi(\mathcal{Z}(K(\theta)G))$ we set:

$$\sigma(k_1, \ldots, k_t) = (\sigma(k_1), \ldots, \sigma(k_t)).$$

Notice that $\sigma(\theta) = \theta^i$, where i is an integer such $1 \leq i \leq m-1$ and $(m, i) = 1$. Let $U(\mathbb{Z}_e)$ denote the set of invertible elements in $\mathbb{Z}_e$ and let $i : Gal(K(\theta), K) \to U(\mathbb{Z}_e)$ be the monomorphism defined by $i(\sigma) = \bar{i}$. For an element $g \in G$ we set $g^\sigma = g^{i(\sigma)}$.

Also, we set $\sigma^\varphi = \varphi^{-1} \circ \sigma \circ \varphi$. These maps can be visualized in the diagram bellow.

$$\begin{array}{ccc} \varphi(\mathcal{Z}(K(\theta)G)) & \xrightarrow{\sigma^\varphi} & \varphi(\mathcal{Z}(K(\theta)G)) \\ \downarrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi^{-1}} \\ \underbrace{K(\theta) \oplus \cdots \oplus K(\theta)}_{s \text{ times}} & \xrightarrow{\sigma} & \underbrace{K(\theta) \oplus \cdots \oplus K(\theta)}_{s \text{ times}} \end{array}$$

Theorem 2.2.8. *With the notation above, we have that $\sigma(\varphi(\gamma_g)) = \varphi(\gamma_{g^\sigma})$ and, consequently, $\sigma^\varphi(\gamma_g) = \gamma_{g^\sigma}$.*

Proof. It is easily seen that $T_i(\gamma_g) = |\Gamma_g|\chi_i(g)/n_i I$ ([8, p. 30]) and thus

$$\varphi(\gamma_g) = \left(\frac{|\Gamma_g|\chi_1(g)}{n_1}, \cdots, \frac{|\Gamma_g|\chi_s(g)}{n_s} \right).$$

So, to prove our statement we must show that

$$\sigma\left(\frac{|\Gamma_g|\chi_i(g)}{n_i} \right) = \frac{|\Gamma_g|\chi_i(g^\sigma)}{n_i},\ 1 \leq i \leq s,$$

and, to do so, it suffices to prove that $\sigma(\chi_i(g)) = \chi_i(g^\sigma)$.

Since $T_i(g)^e = T_i(g^e) = 1$, the linear map $T_i(g)$ is diagonalizable so, there exists $L_i \in GL(k(\theta), n_i)$ such that

$$T_i(g) = L_i \begin{bmatrix} \theta^{t_1} & & & \\ & \theta^{t_2} & & \\ & & & \\ & & & \theta^{t_{n_i}} \end{bmatrix} L_i^{-1}.$$

Hence $\chi_i(g) = \theta^{t_1} + \theta^{t_2} + \cdots + \theta^{t_{n_i}}$. Notice that $\{\theta^{t_1}, \theta^{t_2}, \ldots, \theta^{t_{n_i}}\}$ is the set of all distinct units of the irreducible polinomial of $T_i(g)$ and σ permutes this set. Thus $\chi_i(g) = \theta^{t_1 i(\sigma)} + \theta^{t_2 i(\sigma)} + \cdots + \theta^{t_{n_i} i(\sigma)}$.

On the other hand

$$\begin{aligned} T_i(g^j) &= L_i \begin{bmatrix} \theta^{t_1} & & & \\ & \theta^{t_2} & & \\ & & & \\ & & & \theta^{t_{n_i}} \end{bmatrix}^{i(\sigma)j} L_i^{-1} \\ &= L_i \begin{bmatrix} \theta^{t_1 i(\sigma)j} & & & \\ & \theta^{t_2 i(\sigma)j} & & \\ & & & \\ & & & \theta^{t_{n_i} i(\sigma)j} \end{bmatrix} L_i^{-1}, \end{aligned}$$

so the desired equality follows. □

The result above shows that the elements of $Gal(K(\theta), K)$ act on $\mathcal{B} = \{\gamma_g \mid g \in G\}$ as permutations. Let S_g denote the orbit of γ_g under the action of $Gal(K(\theta), K)$, i.e.

$$S_g = \{\sigma^\varphi(\gamma_g) \mid \sigma \in Gal(K(\theta), K)\} = \{\gamma_{g^\sigma} \mid \sigma \in Gal(K(\theta), K)\}.$$

We also set $\eta_g = \sum_{\gamma \in S_g} \gamma$ and notice that it follows directly from the definitions of S_g and η_g that $\sigma^\varphi(S_g) = S_g$ and $\sigma^\varphi(\eta_g) = \eta_g$, for all $\sigma \in Gal(K(\theta), K)$.

Let V_g denote the K-vector subspace of KG spanned by the elements in S_g. Since each element γ_g is central, it is clear that $V_g \subset \mathcal{Z}(KG))$.

Proposition 2.2.9. *Let V_g be a subspace as above and let α be an element in V_g. If $\sigma^\varphi(\alpha) = \alpha$ for all σ in $Gal(k(\theta), K)$, then $a = k\eta_g$, for some $k \in K$.*

Proof. We enumerate $S_g = \{\gamma_1, \gamma_2, \ldots, \gamma_\mu\}$. For each γ_j and each $\sigma \in Gal(K(\theta), K)$ we have $\sigma^\varphi(\gamma_j) = \gamma_{j'}$, for some j', $1 \leq j' \leq \mu$.

Write $= \sum_{j=1}^{\mu} k_j\gamma_j$, with $k_j \in K$. It follows from the definition of S_g that, for each index i, there exists an automorphism $\sigma_i \in Gal(K(\theta), K)$ such that $\sigma_i^\varphi(\gamma_1) = \gamma_i$. Then, as $\sigma_i^\varphi(\alpha) = \alpha$, we have

$$\sum_{j=1}^{\mu} k_j\gamma_j = \alpha = \sigma_i\left(\sum_{j=1}^{\mu} k_j\gamma_j\right) = \sum_{j=1}^{\mu} k_j\sigma_i^\varphi(\gamma_j).$$

Notice that the coefficient of γ_i in the right-hand side of the equation above is k_1 while its coefficient in the left-hand side of the equation is k_i. As this holds for every index i, $1 \leq i \leq \mu$, we see that $\alpha = k_1\eta_g$, as stated. □

We denote by ν the number of different orbits S_g, $g \in G$ and let $T = \{g_1, \ldots, g_\nu\}$ a set of elements in G such that $\{\gamma_1, \ldots, \gamma_\nu\}$ is a set of representatives of these orbits. Then $\mathcal{B} = \cup_{g\in T} S_g$.

Since $\mathcal{B}$ is a basis of $\mathcal{Z}(KG)$ over K, we have that

$$\mathcal{Z}(KG) = \bigoplus g \in T V_g.$$

Furthetmore, since $\sigma^\varphi(S_g) = S_g$, we have that $\sigma^\varphi(V_g) = V_g$ for every $\sigma \in Gal(K(\theta), K)$ and every $g \in G$.

Corollary 2.2.10. *Let α be an element in $\mathcal{Z}(KG)$. Then $\sigma\varphi(\alpha) = \alpha$ for every $\sigma \in Gal(K(\theta), K)$ if and only if α is a linear combination of the elements in $\{\eta_g \mid g \in T\}$.*

Proof. Take $a \in \mathcal{Z}(KG)$. Then $\alpha = \sum_{g\in T} v_g$, with $v_g \in V_g$. As noted above, $\sigma^\varphi(v_g) \in V_g$, for every $\sigma \in Gal(K(\theta), K)$ and every $g \in T$. Then, if $\sigma^\varphi(\alpha) = \alpha$, it follows that $\sigma^\varphi(v_g) = v_g$.

Proposition 2.2.9 above shows that this implies $v_g = k_g\eta_g$ for suitable $k_g \in K$. Hence, $a = \sum_{g\in T} k_g\eta_g$.

The converse is trivial. □

Now, let $\mathcal{A}$ denote the K-vector subspace of KG spanned by the elements of the set $\{\eta_g \mid g \in T\}$ which, in view of Corollary 2.2.10, is

$$\mathcal{A} = \{\alpha \in \mathcal{Z}(KG) \mid \sigma^\varphi(\alpha) = \alpha,\ \forall\sigma \in Gal(K(\theta), K)\}.$$

Proposition 2.2.11. *Let α be an element of KG. Then $\alpha \in \mathcal{A}$ if and only if $\varphi(\alpha) \in \underbrace{K \oplus \cdots \oplus K}_{s \text{ times}} \subset K(\theta) \oplus \cdots \oplus K(\theta) = \varphi(\mathcal{Z}(K(\theta)G))$.*

Proof. Let $\alpha \in KG$. Then

$$\alpha \in \mathcal{A} \quad \text{if and only if } \sigma^{\varphi}(\alpha) = \alpha \text{ for all } \sigma \in Gal(K(\theta), K)$$

and this occurs if and only if $\sigma(\varphi(\alpha)) = vf(\alpha)$ for all $\sigma \in Gal(K(\theta), K)$. Recall that $\varphi(\alpha) = (a_1, \ldots, a_s),\ a_i \in K(\theta),\ 1 \leq i \leq s$, and that $\sigma(a_1, ..., a_s) = (\sigma(a_1), \ldots, \sigma(a_s))$ for all $\sigma \in Gal(K(\theta), K)$. It follows that $\sigma(\varphi(\alpha)) = \varphi(\alpha)$ if and only if $\sigma(a_i) = a_i$ for all $\sigma \in Gal(K(\theta), K)$, and this happens if and only if $a_i \in K, 1 \leq i \leq s$. □

Lemma 2.2.12. *Let $p_\alpha(X) \in K[X]$ denote the minimal polynomial of an element $\alpha \in \mathcal{Z}(KG)$. Then $\alpha \in \mathcal{A}$ if and only if*

$$p_\alpha(X) = (X - k_1) \cdots (X - k_t),\ k_i \in K, 1 \leq i \leq t,$$

is the product of distinct linear factors.

Proof. Clearly α and $\varphi(\alpha)$ have the same minimal polynomial. Assume first that $\alpha \in \mathcal{A}$. Then $\varphi(\alpha) = (a_1, \ldots, a_s)$, so $f(X) = (X - a_1) \cdots (X - a_s)$ is a polynomial in $K[X]$ such that $f(\alpha) = 0$. Let $\{k_1, \ldots, k_t\}$ be the set of all distinct elements in $\{a_1, \ldots, a_s\}$. Then $g(X) = (X - k_1) \cdots (X - k_t) \in K[X]$ satisfies $g(\alpha) = 0$, and clearly this is the minimal such polynomial. Conversely, assume that $p_\alpha(X) = (X - k_1) \cdots (X - k_t), k_i \in K$, and write $\varphi(\alpha) = (a_1, \ldots, a_s), a_i \in K(\theta), 1 \leq i \leq s$. Then $p_\alpha(\alpha) = 0$ implies that $p_\alpha(a_i) = 0, 1 \leq i \leq s$ which, in turn, implies that each a_i is an element of $\{k_1, \ldots, k_t\}$. So $\alpha \in \mathcal{A}$. □

Now let $\varphi : KG \to \oplus_{i=1}^{r} M_{n_i}(D_i)$ be an isomorphism as in Theorem 2.1.2.

Let K_i denote the center of $D_i, 1 \leq i \leq r$, which is an extension of K. Then $\varphi(\mathcal{Z}(KG)) = \oplus_{i=1}^{r} K_i$. It follows that $\mathcal{Z}(KG)$ *and* KG *have the same number of simple components.*

Also notice that, With notation as above, $\varphi(\mathcal{A}) = \oplus_{i=1}^{r} K \subset \oplus_{i=1}^{r} K_i$.

Finally, we are ready to prove the main result in this section.

Theorem 2.2.13. *The set $\{\varphi(\eta_g) | g \in T\}$ is a basis of $\oplus_{i=1}^{r} K$, so the number of simple components of KG is the number of different orbits of the class sums γ_g under the action of $Gal(K(\theta), K)$.*

Proof. . As we saw in the previous lemma, the subspace $\mathcal{A}$ is precisely the set of elements $\alpha \in \mathcal{Z}(KG)$ whose minimal polynomial $p_\alpha(X)$ is a product of distinct linear factors in $K[X]$. So $\sigma(\mathcal{A})$ is the set of all elements $\beta \in oplus_{i=1}^r K_i$ whose minimal polynomial is the product of distinct linear factors in $K[X]$, and this occurs if and only if $\beta \in \oplus_{i=1}^r K$ as stated.

As a consequence, $\{\varphi(\eta_g)|g \in T\}$ is a basis of $\oplus_{i=1}^r K$, so the number of orbits is $|\{\eta_g|g \in T\}| = dim \oplus_{i=1}^r K = r$ □

Example 2.2.14. Let us consider again the group S_3 of permutations of three elements. We wish to describe its group algebra over $\mathbb{F}_q$, a finite field with q elements such that $gcd(q, 6) = 1$. As in Example 2.2.7, we can write its conjugacy classes as

$$\begin{aligned} C_1 &= \{I\} \\ C_2 &= \{(1\ 2),\ (1\ 3),\ (2\ 3)\} \\ C_3 &= \{(1\ 2\ 3),\ (1\ 3\ 2)\} \end{aligned}$$

so, the class sums are:

$$\gamma_1 = I,\ \gamma_2 = (1\ 2) + (1\ 3) + (2\ 3),\ \ \gamma_3 = (1\ 2\ 3) + (1\ 3\ 2).$$

If θ denotes a q^{th}-root of unity, the Galois group of $\mathbb{F}_q(\theta)$ over $\mathbb{F}_q$ is generated by the map $\sigma : \mathbb{F}_q(\theta) \to \mathbb{F}_q(\theta)$ given by $x \mapsto x^q$.

Since q is odd, it is clear that, for an element $g \in S_3$ of order 2, we have that $g^\sigma = g$. On the other hand, as $3 \nmid q$ we have that $q \equiv 2$ or $3 \pmod 6$, so for elements $g \in S_3$ of order 3 we get $g^\sigma = g$ or g^2.

This shows that all class sums are fixed by $Gal(\mathbb{F}_q(\theta) : \mathbb{F}_q)$; thus S_3 has three $\mathbb{F}_q$-classes and $\mathbb{F}_q S_3$ has three simple components. Consequently

$$\mathbb{F}_q S_3 \simeq \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_2(\mathbb{F}_q).$$

Hence, every finite field such that $gcd(q, 6) = 1$ is a splitting field for S_3.

EXERCISES

1. Let R be a ring. Show that a matrix $A \in M_n(R)$ is central if and only if A a scalar matrix with entries in $\mathcal{Z}(R)$, the center of R; i.e., it is of the form

$$A = \begin{bmatrix} x & 0 & \cdots & 0 \\ 0 & x & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & x \end{bmatrix},$$

   with $x \in \mathcal{Z}(R)$.

2. Let $D_4 = \langle a, b \mid a^4 = a^2 = 1,\ bab = a^{-1} \rangle$ denote the Dihedral group of order 8. Determine structure of $\mathbb{F}D_4$, for any finite field of characteristic different from 2.

3. Let $\mathcal{Q} = \langle a, b \mid a^4 = 1,\ a^2 = b^2,\ bab = a^{-1} \rangle$ denote the Quaternion group of order 8. Determine structure of $\mathbb{F}\mathcal{Q}$, for any finite field of characteristic different from 2 and deduce that $\mathbb{F}D_4 \cong \mathbb{F}\mathcal{Q}$ for these fields.

Chapter 3

Idempotent Elements

3.1 Subgroup idempotents

There is a standard way of constructing idempotents in a group ring from the subgroups of the given group.

Let G be a finite group, R a commutative ring and H a subgroup of G such that such the $|H|$ is invertible in R (notice that this is always the case if R is a field and $char(R) \nmid |G|$). We shall denote by $\widehat{H}$ the element

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h \in RG.$$

Lemma 3.1.1. *Let R be a ring with unity and H a subgroup of a group G. If $|H|$ is invertible in R, then $\widehat{H} = \frac{1}{|H|}\widehat{H}$ is an idempotent of RG. Moreover, if $H \lhd G$ then e_H is central.*

Proof. First, we prove that $\widehat{H}$ is an idempotent. To do so, we consider the product:

$$\begin{aligned} \widehat{H}\widehat{H} &= \frac{1}{|H|}\left(\sum_{h \in H} h\right)\widehat{H} = \frac{1}{|H|}\sum_{h \in H}(h\widehat{H}) \\ &= \frac{1}{|H|}\sum_{h \in H}\widehat{H} = \frac{1}{|H|}.|H|\widehat{H} = \widehat{H}. \end{aligned}$$

Finally, if $H \lhd G$, for any $g \in G$ we have that $g^{-1}Hg = H$; therefore

$$g^{-1}\widehat{H}g = \frac{1}{|H|}\sum_{h \in H} g^{-1}hg = \frac{1}{|H|}\sum_{h \in H} h = \widehat{H}.$$

Thus, $\widehat{H}g = g\widehat{H}$, for all $g \in G$, which implies that $\widehat{H}\alpha = \alpha\widehat{H}$ for all $g \in G$. Thus, $\widehat{H}$ is central in RG. □

We wish to know how does the decomposition obtained from one idempotent of this kind looks like. We need a preliminary result.

Lemma 3.1.2. *The annihilator of an ideal of the form $I = RG.\widehat{H}$ is*

$$ann(I) = \Delta(G, H).$$

Proof. Set $\alpha \in \mathbb{F}G.\widehat{H}$. Then $\alpha = \beta\widehat{H}$, for some $\beta \in \mathbb{F}G$.

According to Proposition 1.2.3, if $\mathcal{T}$ denotes a transversal of H in G, we can write any element γ in the form

$$\gamma = \sum_{\substack{t\in\mathcal{T}\\ h\in H}} r_{t,h}t(h-1), \quad r_{t,h} \in R.$$

Hence

$$\alpha\gamma = \beta\widehat{H}\left(\sum_{\substack{t\in\mathcal{T}\\ h\in H}} r_{t,h}t(h-1)\right) = \beta\left(\sum_{\substack{t\in\mathcal{T}\\ h\in H}} r_{t,h}t\widehat{H}(h-1)\right) = 0.$$

This argument shows that $\Delta(G, H) \subset ann(I)$.

To prove the converse, recall that, if $\omega^* : RG \to R(G/H)$ denotes the extension of the natural homomorphism $\omega : G \to G/H$, Proposition 1.2.4 shows that $\Delta(G, H) = Ker(\omega^*)$. Given $\gamma \in ann(I)$ we have, as in Exercise 2 that $\gamma \in |RG(1 - \widehat{H})$ so it is of the form $\gamma = \beta\widehat{H}$ for some $\beta \in RG$.

So, $\omega^*(\gamma) = \omega^*(\beta)\omega^*(1 - \widehat{H}) = 0$. Consequently $\gamma \in Ker(\omega^*) = \Delta(G, H)$. □

Proposition 3.1.3. *Let R be a ring and let H be a normal subgroup of a group G. If $|H|$ is invertible in R, then*

$$RG = RG.\widehat{H} \oplus RG.(1 - \widehat{H})$$

where

$$RG.\widehat{H} \cong R(G/H) \text{ and } RG.(1 - \widehat{H}) = \Delta(G, H).$$

Proof. Since we have shown above that $\widehat{H}$ is a central idempotent, it is clear that $RG = RG.\widehat{H} \oplus RG.(1 - \widehat{H})$ (see Exercise 2 of section § 2.1).

Set $G.\widehat{H} = \{g\widehat{H} \mid g \in G\}$, which is a multiplicative group inside RG. To see that $R(G/H) \equiv RG.\widehat{H}$ we shall first show that $G/H \cong G.\widehat{H}$ as groups.

In fact, clearly the map $\phi : G \to G.\widehat{H}$ given by $g \mapsto g\widehat{H}$ is a group epimorphism. Since it is easy to see that $Ker(\phi) = H$, the result follows.

As $G.\widehat{H}$ is a basis of $RG.\widehat{H}$ over R the group isomorphism above extends linearly to an algebra isomorphism so $RG.\widehat{H} \cong R(G/H)$.

The fact that $RG.(1 - \widehat{H}) = \Delta(G, H)$ follows from the previous Lemma. □

Definition 3.1.4. *Let R be a ring and let G be a finite group such that $|G|$ is invertible in R. The idempotent $e_G = \frac{1}{|G|}\widehat{G}$ is called the* **principal idempotent** *of RG.*

As an immediate consequence of the result above, using the principal idempotent of RG we can show that semisimple group algebras always contain at least one simple component which is isomorphic to the ring of coefficients.

Corollary 3.1.5. *Let R be a ring and let G be a finite group such that $|G|$ is invertible in R. Then, we can write RG as a direct sum of rings*

$$RG \cong R \oplus \Delta(G).$$

To prove our next result we shall need the following.

Lemma 3.1.6. *Let R be a commutative ring and let I be an ideal of a group algebra RG. Then the quotient ring RG/I is commutative if and only if $\Delta(G, G') \subset I$, where G' denotes the commutator subgroup of G.*

Proof. Let I be an ideal in RG such that RG/I is commutative. Then, $\forall g, h \in G$ we have that $gh - hg \in I$ so $hg(g^{-1}h^{-1}gh - 1) \in I$. Since hg is invertible, we also have that $g^{-1}h^{-1}gh - 1 = (g, h) - 1 \in I$. It follows from Lemma 1.2.2 that $\Delta(G, G') \subset I$.

Conversely, since $gh - hg = hg((g, h) - 1) \in \Delta(G, G')$, if $\Delta(G, G') \subset I$, we have that $gh \equiv hg \pmod{I}$, for all $g, h \in G$ and thus RG/I is commutative. □

Proposition 3.1.7. *Let RG be a semisimple group algebra. If G' denotes the commutator subgroup of G, then we can write*

$$RG = RGe_{G'} \oplus \Delta(G, G'),$$

where $RGe_{G'} \simeq R(G/G')$ is the sum of all commutative simple components of RG and $\Delta(G, G')$ is the sum of the non commutative ones.

Proof. Both the fact that RG can be decomposed as stated and that $RGe_{G'} \simeq R(G/G')$ follow from Proposition 3.1.3.

It is clear that $RGe_{G'} \simeq R(G/G')$ is commutative, so it is certainly a sum of commutative simple components of RG. To complete the proof of our statement, it will be enough to show that there are no commutative simple components in $\Delta(G, G')$. So assume, by way of contradiction, that we can decompose it as $\Delta(G, G') = A \oplus B$, where A is a commutative simple component and B its complement. Then, $RG = RGe_{G'} \oplus A \oplus B$ so we have that $RG/B \simeq RGe_{G'} \oplus A$ is commutative. It follows from Lemma 3.1.6 that $\Delta(G, G') \subset B$, a contradiction. □

Example 3.1.8.

Let S_3 be the group of permutations of three elements. We wish to describe now its group algebra over $\mathbb{Q}$, the field of rational numbers. At this point, we do not know whether the simple components will be matrix rings over $\mathbb{Q}$ itself or if they will also involve some division rings containing $\mathbb{Q}$. We first compute $S_3' = \{I,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ so $|S_3/S_3'| = 2$, consequently $\mathbb{Q}(S_3/S_3')$ is of dimension 2 over $\mathbb{Q}$. Since we have seen above that it must always contain at least one component isomorphic to $\mathbb{Q}$ we see that $\mathbb{Q}S_3$ contains exactly two commutative simple components, both of them isomorphic to $\mathbb{Q}$. Since the dimension of $\Delta(S_3, S_3')$ is at least 4 and the dimension of the whole group algebra over $\mathbb{Q}$ is $|S_3| = 6$ we see that we must have

$$\mathbb{Q}S_3 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus B,$$

where B is a simple component of dimension 4 over $\mathbb{Q}$. Since $\mathbb{Q}S_3$ contains nilpotent elements (for example, $\gamma = (1 - (1\ 2))(1\ 2\ 3)(1 + (1\ 2))$ is such that $\gamma^2 = 0$), it cannot be a direct sum of division rings; thus, we have

$$\mathbb{Q}S_3 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}).$$

Notice that the arguments above are still valid if we take coefficients in any field $\mathbb{F}$ such that $\mathbb{F}S_3$ is semisimple. So it follows, *a fortiori*, that $\mathbb{Q}$ is also a splitting field for S_3.

Example 3.1.9.

Let $\mathbb{F}$ be any finite field of characteristic not 2 and consider the Dihedral group of order 8:

$$D_4 = \langle a, b \mid a^{=}b^2 = 1,\ bab = a^{-1} \rangle.$$

A direct computation shows that $D_4' = \{I, a^2\}$. Hence:

$$\frac{D_4}{D_4'} \cong C_2 \times C_2.$$

As,

$$\mathbb{F}C_2 \times C_2 \cong \mathbb{F} \oplus\ \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F},$$

we get

$$\mathbb{F}D_4 \cong \mathbb{F} \oplus\ \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \Delta(D_4, D_4').$$

An argument on dimensions now shows that $\Delta(D_4, D_4') \cong M_2(\mathbb{F})$ so

$$\mathbb{F}D_4 \cong \mathbb{F} \oplus\ \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F} \oplus M_2(\mathbb{F}).$$

EXERCISES

1. Let H be a normal subgroup of a group G, such that $|H|$ is invertible in a commutative ring R. Prove that $ann(\Delta(G, H) = RG.\widehat{H}$.

Bibliography

[1] S.D. Berman, The number of irreducible representations of a finite group over an arbitrary field, *Dokl. Akad. Nauk*, **106** (1956), 767-769.

[2] R. Brauer, *Über Systeme Hypercomplexer Zahlen*, Math. Z. **30** (1929), 79–107.

[3] R. Brauer and E. Noether, *Über minimale Zerfällungskörper irreduzibler Darstellungen*, Sitz. Preuss. Akad. Wiss. Berlin (1927), 221–228.

[4] A. Cayley, *On the theory of groups as depending on the symbolic equation* $\theta^n = 1$, Phil. Mag. **7** (1854), 40–47.

[5] D.B. Coleman, *On the modular group ring of a p-group*, Proc. Amer. Math. Soc. **15** (1964), 511–514.

[6] I.G. Connell, *On the group ring*, Can. J. Math. **15** (1963), 650–685.

[7] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York, 1962.

[8] L. Dornhoff, *Group Representation Theory*, Part A, M. Dekker, New York, 1971.

[9] R.A. Ferraz, Simple components and central units in group algebras. *J. Algebra*, **279** (2004), 191-203.

[10] T. Hawkins, *Hypercomplex numbers, Lie groups and the creation of group representation theory*, Archive Hist. Exact Sci. **8** (1972), 243–287.

[11] I. Kaplansky, *Problems in the theory of rings*, Nas–NRC Publ. 502, Washington, 1957, pp. 1–3.

[12] I. Kaplansky, *"Problems in the theory of rings" revisited,* Amer. Math. Monthly **77** (1970), 445–454.

[13] J. Lambek, *Lectures on Rings and Modules*, Blaisdell, Toronto, 1966.

[14] T. Molien, *Über Systeme höherer complexer Zahlen*, Math. Ann. Bd. **41** (1893), 83–156.

[15] T. Molien, *Über die Invarianten der Linearen Substitutionsgruppen*, S'ber Akad. d. Wiss. Berlin (1897), 1152–1156.

[16] E. Noether, *Hypercomplexe Grössen und Darstellungtheorie*, Math. Z. **30** (1929), 641–692.

[17] D.S. Passman, *Infinite Group Rings*, Marcel Dekker, New York, 1971.

[18] D.S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977.

[19] B. Peirce, *Linear associative algebras*, Amer. J. Math. **4** (1881), 97–215.

[20] C. Polcino Milies, *A glance at the early history of group rings*, in Groups—St. Andrews 1981, ed. by C.M. Campbell and E.F. Robinson, London Math. Soc. Lecture Notes Series 71, Cambridge Univ. Press, London, 1982, pp. 270–280.

[21] C. Polcino Milies and S.K. Sehgal, *An Introduction to Group Rings*, Algebras and Applications, Kluwer Academic Publishers, Dortrecht, 2002.

[22] P. Ribenboim, *Rings and Modules*, Interscience, New York, 1969.

[23] S.K. Sehgal, *Topics in Group Rings*, Marcel Dekker, New York, 1978.

[24] E. Witt, Die Algebrische Structur des Gruppenringes einer endlichen Gruppe über einem Zahlenkörper, *J. für Math,* **190** (1952), 231-245.