Zero-Divisors and Idempotents in Group Rings

Bartosz Malman

Master's thesis
2014:E45

Lund University

Faculty of Engineering
Centre for Mathematical Sciences
Mathematics

Centrum Scientiarum Mathematicarum

Zero-divisors and idempotents in group rings

Bartosz Malman
Supervised by Johan Öinert

August 26, 2014

Abstract

After a brief introduction of the basic properties of group rings, some famous theorems on traces of idempotent elements of group rings will be presented. Next we consider some famous conjectures stated by Irving Kaplansky, among them the zero-divisor conjecture. The conjecture asserts that if a group ring is constructed from a field (or an integral domain) and a torsion-free group, then it does not contain any non-trivial zero-divisors. Here we show how a confirmation of the conjecture for certain fields implies its validity for other fields.

Acknowledgements

The author wants to sincerely thank Johan Öinert for his help with the choice of the topic, for the work and time he put in as the supervisor of this thesis, and finally for all the mathematical discussions, which concerned not only the material covered here.

Introduction

The study of group rings for their own sake began relatively recently, but nevertheless group rings appear implicitly even in foundational works on group theory. Arthur Cayley mentioned the group ring $\mathbb{C}S_3$ already in the arguably first paper on the subject of group theory, published in 1854. Group rings also appeared in Theodor Molien's work on complex algebras, which dates back to 1892. The contemporary definition of a group ring, for an arbitrary group and arbitrary ring, appeared a bit later. The definition had to wait, for it was not before the 1920s that the modern definition of a ring appeared. The definition of a group ring followed soon after.

Finite-dimensional complex group rings appear naturally in the study of representations of finite groups, and it is in the context of representation theory that they were first extensively studied. The study of arbitrary group rings for their own sake followed soon thereafter. The first monograph on the subject, entitled 'The algebraic structure of group rings', was written by Donald S. Passman and published in 1977.

Much of the development of theory of group rings was stimulated by the abundant amount of seemingly unapproachable problems. One such problem is to determine sufficient conditions for a group ring to be semisimple. In the case of a finite group, this question is answered by Maschke's famous result. Rickart showed in 1950 that if $K = \mathbb{C}$, then KG is semisimple regardless of the structure of G. The interesting case nowadays is the case of $K = \mathbb{Q}$.

Another interesting problem in the theory of group rings is the isomorphism problem. If R is a fixed ring, does $RG \cong RH$ imply that $G \cong H$? This is certainly not always the case, for if G is finite and $R = \mathbb{C}$, then the group ring $\mathbb{C}G$ is isomorphic to a direct product of full matrix rings, and in particular for two non-isomorphic abelian groups G, H of order n, we have $\mathbb{C}G \cong \mathbb{C}^n \cong \mathbb{C}H$. The problem for $R = \mathbb{Z}$ has been exceedingly difficult, and it was conjectured that the implication holds. In the end it was shown that the integral group ring does not determine the group. In 2001, Martin Hertweck published a paper in which he showed that a certain couple of two non-isomorphic groups of order $2^{25} \cdot 97^2$ have integral group rings which are isomorphic.

In the present text we shall present three conjectures related to zero-divisors, idempotents and units in group rings. All of these are concerned with non-existence problem, and the hypothesis imposed on the group ring RG is that the group G is torsion-free and R is a field. We will investigate how these conjectures are related to another and how the field K plays a role.

In Chapter 1 we define what a group ring is and go through some rudimentary facts about them, with focus on those facts which are useful in what comes next. We work with idempotents in Chapter 2. Large part of the chapter take up by a detailed proof of Kaplansky's theorem on traces of idempotent elements in complex group rings. Chapter 3 is concerned with zero-divisors, and in particular the zero-divisor conjecture. We show that we can slightly strengthen the assumptions in the statement of the original conjecture. In the brief final part, Chapter 4, we mention two conjectures related to units in group rings, and we show how Kaplansky applied his trace theorem to prove a special case of one of the conjectures.

Contents

Chapter 1

Basics

1.1 Definitions

The main objects of study here will be **group rings**. A group ring RG is a construction which involves a group G and a ring R. We will always assume that the ring R is associative and has a multiplicative identity element. The group ring is a ring and the underlying set consists of formal sums

$$\sum_{g\in G} a_g g \quad (a_g \in R, g \in G)$$

for which all but finitely many coefficients a_g are zero. We define the addition of two elements of RG point-wise

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g,$$

and the multiplication we define by

$$\big(\sum_{g\in G} a_g g\big)\big(\sum_{g\in G} b_g g\big) = \sum_{g\in G} c_g g,$$

where

$$c_g = \sum_{h\in G} a_g b_{g^{-1}h}.$$

If this multiplication seems strange, it will surely help to notice that this is exactly what we would get by requiring that $(a_g g)(b_h h) = (a_g b_h)gh$ and that the multiplication map $RG \times RG \to RG$ is additive in both arguments. The above definitions make RG into an associative and unital ring. The multiplicative identity element is $1_R \cdot 1_G$, where $1_R \in R$ is the unit of R and $1_G \in G$ is the identity element of the group. In general, RG is not commutative. It is commutative if and only if both R and G are commutative.

We can also define an action of the ring R on RG by

$$r \cdot \sum_{g\in G} a_g g = \sum_{g\in G} (r a_g) g \quad (r \in R).$$

This definition makes RG into a left R-module. The group ring is then a free R-module with basis consisting (of copies) of elements of G, and it is of rank $|G|$. It will often be the case that the ring R is a field, and we will often denote a field by the letter K. In that case, KG is a vector space over K, with a canonical basis consisting of the elements of G. If G is finite, then KG is a finite-dimensional K-algebra, and hence structure theorems apply, but we will often work without assumption on finiteness of G. In the literature, when $R = K$ is a field, the ring KG is often referred to as the *group algebra* KG.

The group ring RG is a ring extension of R, for we have a ring embedding $R \to RG$ given by $r \mapsto r \cdot 1_G$. Note that if R is commutative, then the image of R in RG is contained in the center of RG, and then RG is (by definition) an R-algebra. The mapping $g \mapsto 1_R \cdot g$ is a group embedding of G in the group of units of RG, and therefore we can also regard G as a subset of RG.

We will now consider some examples of group rings.

Example 1.1. Take K to be a field, $G = \{1_G, g, g^2, \ldots, g^{n-1}\}$ the cyclic group of order n, and form the group ring KG. The ring $K[x]$ of polynomials in one indeterminate x is a principal ideal domain, and assignment $x \to g$ gives us a ring homomorphism $\phi : K[x] \to KG$ which is obviously surjective. The polynomial $x^n - 1$ is clearly contained in the kernel of ϕ, and conversely if $p(x)$ is any polynomial in the kernel, then the expression $p(x) = q(x)(x^n - 1) + r(x)$, with $\deg(r) < n$ shows that $\ker \phi$ is the principal ideal generated by $x^n - 1$. Hence $KG \cong K[x]/(x^n - 1)$.

Example 1.2. Continuing the previous example, if in particular K is an algebraically closed field, then the polynomial $x^n - 1$ factors completely into irreducible factors

$$x^n - 1 = (x - \gamma_1)(x - \gamma_2) \ldots (x - \gamma_n).$$

If moreover n is a prime number and $K = \mathbb{C}$, then the roots of unity $\gamma_1, \gamma_2, \ldots, \gamma_n$ are all distinct. If M_i is the maximal ideal of $\mathbb{C}[x]$ generated by the polynomial $x - \gamma_i$ then we have, by the Chinese remainder theorem,

$$\mathbb{C}G \cong \mathbb{C}[x]/\prod_{i=1}^{n} M_i \cong \prod_{i=1}^{n} \mathbb{C}[x]/M_i \cong \mathbb{C}^n$$

and so $\mathbb{C}G$ is in this case isomorphic, as a ring, to the direct product of n copies of $\mathbb{C}$.

Example 1.3. By the Wedderburn-Artin structure theorem for finite-dimensional algebras, any group ring over a field K is isomorphic, as a K-algebra, to a direct product of finitely many full matrix rings over some finite-dimensional division algebras D_i:

$$KG \cong \prod_{i=1}^{n} M_{n_i}(D_i).$$

In particular, if K is algebraically closed, then $D_i = K$. The previous example is a special case of this.

Example 1.4. If $R = \mathbb{C}$ and $G = \mathbb{Z}$, then it is not hard to see that $\mathbb{C}\mathbb{Z} \cong \mathbb{C}[x, x^{-1}]$, the ring of formal sums $\sum_{n\in\mathbb{Z}} a_n x^n$ where only finitely many coefficients $a_n \in \mathbb{C}$ are non-zero.

Example 1.5. The group algebra KG is one of the central objects of study in the representation theory of finite groups. Any linear group representation $\rho : G \to GL(V)$, where V is a vector space over a field K, corresponds to a KG-module structure on V, and vice versa.

RG can be identified with the finitely supported R-valued functions on G. If $a = \sum_{g\in G} a_g g$ is an element of RG, then we can interpret it as a function $a : G \to R$ specified by $a(g) = a_g$. The corresponding addition operation would then be point-wise:

$$(a + b)(g) = a(g) + b(g) \quad (a, b \in RG, g \in G).$$

Multiplication in the group ring then corresponds to the convolution of functions:

$$(a * b)(g) = \sum_{h\in G} a(gh^{-1})b(h) \quad (a, b \in RG, g \in G). \tag{1.1}$$

It is sometimes convenient to think of a group ring in this way. When this viewpoint is particularly practical, we will denote the elements of RG by letters f, g (thinking of them as functions) and elements of G denoted by letters like x, y (thinking of them as points).

For a function $f \in RG$, the **support** of f, denoted $\mathrm{Supp}(f)$, consists of the finite subset of points $x \in G$ for which $f(x) \neq 0$. The **support group** of f is the smallest subgroup of G containing $\mathrm{Supp}(f)$. The element f can be seen as a function on its finitely generated support group H to the finitely generated subring R_1 (generated by the image of f). It is not hard to see that $f \in R_1 H \subseteq RG$.

Finally, if $R = \mathbb{C}$, we define a self-map * on $\mathbb{C}G$ by

$$a = \sum_{g\in G} a_g g \mapsto \sum_{g\in G} \overline{a_g} g^{-1} = a^*.$$

This map is an anti-isomorphism of rings which is conjugate-linear. It is also its own inverse, so it is an **involution**.

1.2 Homomorphisms of group rings

This section presents some standard and useful results concerning maps between group rings. Most of the results of this section will be used implicitly in the sequel. The below two propositions show how ring homomorphisms of the ring R and group homomorphisms of the group G induce homomorphisms of the corresponding group rings.

Proposition 1.6. *Let $\phi : S \to R$ be a ring homomorphism. Then ϕ extends uniquely to a homomorphism of group rings $\overline{\phi} : SG \to RG$ that is given by*

$$\overline{\phi}\big(\sum_{g\in G} a_g g\big) = \sum_{g\in G} \phi(a_g) g.$$

If ϕ is injective, then so is $\overline{\phi}$ and then SG can be interpreted as a subring of RG.

Proposition 1.7. *Let $\psi : H \to G$ be a group homomorphism. Then ψ extends uniquely to a homomorphism of group rings $\overline{\psi} : RH \to RG$ that is given by*

$$\overline{\psi}\big(\sum_{g\in G} a_g g\big) = \sum_{g\in G} a_g \psi(g).$$

If ψ is injective, then so is $\overline{\psi}$ and then RH can be interpreted as a subring of RG.

We see in particular that if H is a subgroup of G, then RH is naturally embedded in RG, and similarly if S is a subring of R, then SG is embedded in RG. This allows for very easy shifting of questions about group rings to smaller or bigger group rings. Many questions about group rings can be answered more easily by going down from G to a finitely generated support subgroup.

Now let R be a commutative ring. Then, as pointed out before, RG is an R-algebra. The below proposition exhibits a universal mapping property of the group ring. The notation $U(A)$ stands for the group of invertible elements of A.

Proposition 1.8. *Let R be a commutative ring, G a group and A an R-algebra. If $\phi : G \to U(A)$ is a group homomorphism, then ϕ induces uniquely an R-algebra homomorphism $\overline{\phi} : RG \to A$ such that $\overline{\phi}(g) = \phi(g)$ for $g \in G$.*

Proof. The map clearly must be defined by

$$\overline{\phi}(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \phi(g).$$

The multiplicativity of $\overline{\phi}$ follows from multiplicativity of ϕ. The rest of the verifications are also straight-forward. □

Since RG is an R-module, we consider also the projections of RG onto the submodules RH, where H is a subgroup of G. We have a projection map $\pi_H : RG \to RH$ which maps the basis elements $g \in G \setminus H$ to 0. More explicitly, if $a = \sum_{g\in G} a_g g$, then

$$\pi_H(a) = \sum_{g\in H} a_g g.$$

The proposition below is especially important in the sequel.

Proposition 1.9. *Let H be a subgroup of the group G and let R be a ring. The projection map $\pi_H : RG \to RH$ is an R-module homomorphism with the property that if $a \in RG$ and $b \in RH$, then*

$$\pi_H(ab) = \pi_H(a)b$$

and

$$\pi_H(ba) = b\pi_H(a).$$

Proof. R-linearity of π_H is obvious, so we only prove the other property. Write

$$a = a' + \pi_H(a)$$

where $a' = a - \pi_H(a)$. Then the support of a' is disjoint from H. If $g \notin H$ and $h \in H$, then $gh \notin H$ must hold by the fact that H is closed under multiplication. It follows that the support of $a'b$ is disjoint from H. Hence

$$\pi_H(ab) = \pi_H[\pi_H(a)b] = \pi_H(a)b$$

where the last equality is true because π_H is the identity map on RH and, clearly, $\pi_H(a)b$ is an element in RH. The case of ba is treated in the same way. □

1.3 Group rings as functions spaces

The purpose of this section is to develop some tools which enable one to study group rings using analytic methods. These methods will be applied in the upcoming chapter to obtain a proof of Kaplansky's theorem on traces of idempotents, and later to prove for certain group rings a property called direct-finiteness.

If the ring R happens to be a normed algebra, real or complex, then it is particularly useful to identify the group ring with a ring of functions. The existence of a norm on R lets us define a larger ring containing RG, and this larger ring has been shown useful in the study of RG itself. When $R = \mathbb{C}$, for example, one can allow f to have infinite support, but instead require that $\|f\|_1 = \sum_{x \in G} |f(x)|$ is finite. This set of functions forms an algebra under point-wise addition and function convolution as multiplication. We will denote it by $L^1(G)$. Clearly $\mathbb{C}G \subseteq L^1(G)$ as $\mathbb{C}$-algebras. Of course, the notions of support and support groups still make sense for $L^1(G)$. The inherited norm $\| \cdot \|_1$ makes $\mathbb{C}G$ into a normed algebra.

Some important theorems concerning complex group rings, and in particular Kaplansky's theorem on traces which we will discuss later, have been proven using tools of functional and complex analysis. Some of the analytic tools could be applied because a complex group ring can be considered as a subalgebra of the bounded linear operators on a certain Hilbert space. We will define this Hilbert space, exhibit the embedding of $\mathbb{C}G$ in its space of bounded linear operators and prove properties of the embedding.

Let G be a group. We introduce the Hilbert space $L^2(G)$ of formal sums $a = \sum_{g\in G} a_g g$, with $a_g \in \mathbb{C}$ and for which $\sum_{g\in G} |a_g|^2$ is finite. We define addition, scalar multiplication and an inner product in the standard way. Hence, if $a, b \in L^2(G)$, $c \in \mathbb{C}$ then

$$\begin{aligned} a + b &= (\sum_{g\in G} a_g g) + (\sum_{g\in G} b_g g) = \sum_{g\in G} (a_g + b_g)g \\ c \cdot a &= \sum_{g\in G} (ca_g)g \\ (a, b) &= \big(\sum_{g\in G} a_g g, \sum_{g\in G} b_g g\big) = \sum_{g\in G} a_g \overline{b_g} \end{aligned}$$

One can verify that the above definitions make $L^2(G)$ into a Hilbert space.

It is easy to see that $\mathbb{C}G$ is embedded in $L^2(G)$ in the sense of vector spaces, and in particular $\mathbb{C}G$ inherits the above defined inner product. The norm corresponding to this inner product is

$$\|a\|_2^2 = (a, a) = \sum_{g\in G} |a_g|^2. \tag{1.2}$$

It is also easy to see that the completion of $\mathbb{C}G$ under this norm is $L^2(G)$. Furthermore, we will now see that we can regard $\mathbb{C}G$ as subalgebra of the algebra of bounded linear operators on $L^2(G)$.

Proposition 1.10. *Let $H = L^2(G)$ and $B(H)$ be the algebra of bounded linear operators on H. There is a $\mathbb{C}$-algebra monomorphism $I : \mathbb{C}G \to B(H)$ such that for $g \in G$, $I(g)$ acts by left translation on the basis G of H.*

Proof. For $h \in G$, denote by I_h the left translation operator on $L^2(G) = H$. That is, if

$$x = \sum_{g\in G} x_g g \in L^2(G),$$

then

$$I_h(x) = \sum_{g\in G} x_g (hg).$$

Clearly, I_h is a linear, bounded (with norm equal to 1) and invertible operator on H. The assignment $h \to I_h$ is easily seen to be a group homomorphism from G to its image in $B(H)$, and hence by Proposition 1.8 it extends to a $\mathbb{C}$-algebra homomorphism from $\mathbb{C}G$ to $B(H)$. Denote by I_a the image of $a \in \mathbb{C}G$ in $B(H)$ under the map I. We have $1 \in \mathbb{C}G \subseteq L^2(G)$, and for such a we have $I_a(1) = a$, since I_a is just multiplication by a. Hence no non-zero element of $\mathbb{C}G$ maps to the zero operator on H, and therefore I is injective. □

The above embedding is continuous with respect to the norm $\|\cdot\|_1$ on $\mathbb{C}G$ and operator norm $\|\cdot\|$ on $B(H)$. To see this, remember that $\|I_g\| = 1$ because I_g is just a shift. Then,

if $a = \sum_{g\in G} a_g g \in \mathbb{C}G$ we get

$$\|I(a)\| = \|I(\sum_{g\in G} a_g g)\| \leq \sum_{g\in G} |a_g|\|I_g\| = \|a\|_1.$$

Also note that since

$$\|I_a\| = \sup_{\|x\|=1, x\in H} \|I_a(x)\|_2 \geq \|I_a(1)\|_2 = \|a\|_2,$$

for the three norms on $\mathbb{C}G$ we have the inequalities

$$\|a\|_2 \leq \|I_a\| \leq \|a\|_1.$$

For an element $a = \sum_{g\in G} a_g g \in \mathbb{C}G$ we have earlier defined an involution

$$a^* = \sum_{g\in G} \overline{a_g} g^{-1}.$$

Recall that if H is a Hilbert space with an inner product $(\cdot,\cdot)$ and A is a bounded linear operator, then the **adjoint operator** A^* is the unique bounded linear operator on H for which we have

$$(Ax, y) = (x, A^* y)$$

for all $x, y \in H$. The map $A \mapsto A^*$ is an involution on $B(H)$. Of course, in finite-dimensional case every linear operator A on H corresponds to a matrix, and A^* corresponds to the conjugate transpose of the matrix corresponding to A.

With this definition of involution on $B(H)$ we can prove an important property of the above embedding. In the next lemma we keep denoting the embedding discussed above by I. Explicitly, for $a \in \mathbb{C}G$ we have

$$I(a) = I_a = \sum_{g\in G} a_g I(g) = \sum_{g\in G} a_g I_g.$$

Lemma 1.11. *For $a \in \mathbb{C}G$ we have $I(a^*) = I(a)^*$, and so I commutes with taking adjoints. In particular, the image of $\mathbb{C}G$ under I in $B(H)$ is closed under taking adjoints.*

Proof. It is clear that if $g \in \mathbb{C}G$, then $g^* = g^{-1}$. Also, one easily verifies from the definition of an adjoint operator that $I_g^* = I_{g^{-1}}$. Therefore, if $a = \sum_{g\in G} a_g g \in \mathbb{C}G$, we have

$$I(a^*) = I\Big(\sum_{g\in G} \overline{a_g} g^{-1}\Big) = \sum_{g\in G} \overline{a_g} I_{g^{-1}} = \Big(\sum_{g\in G} a_g I_g\Big)^* = I(a)^*.$$

□

Proposition 1.12. *The closure, with respect to the operator norm, of the subalgebra $I(\mathbb{C}G)$ in $B(H)$ is closed under taking adjoints of its elements.*

Proof. This result follows from the lemma. Let $U = \overline{I(\mathbb{C}G)}$. If $a \in U$, fix a sequence of elements $I(a_n) \in I(\mathbb{C}G)$ converging to a. Then

$$\|a^* - I(a_n^*)\| = \|a^* - I(a_n)^*\| = \|(a - I(a_n))^*\| = \|a - I(a_n)\|$$

and so $\|a^* - I(a_n)^*\|$ approaches zero as n gets big, so $a^* \in U$ since U is closed. □

We have established that the subalgebra $U = \overline{I(\mathbb{C}G}$ in $B(H)$ is a closed subalgebra which contains the adjoints of its elements. Such a subalgebra is usually called a *C^*-algebra*. Also note that if G is finite, then the above proposition implies that $\mathbb{C}G$ is isomorphic, as a $*$-algebra (an isomorphism of algebras with involution) to a subalgebra of the algebra of complex matrices of size $|G| \times |G|$. The above result does not depend on $\mathbb{C}$, so any group ring of a finite group over an arbitrary field is isomorphic to a subring of a matrix ring. But in the case of complex numbers and finite dimension, any subspace of $B(H)$ is closed, and so the image of $\mathbb{C}G$ under I is a norm-closed subspace of $B(H)$. This implies that $\mathbb{C}G$ is then a finite-dimensional C^*-algebra, with a norm induced by the embedding $\mathbb{C}G \to B(H) \cong M_{|G|}(\mathbb{C})$.

1.4 The augumentation ideal and the center

We will briefly discuss a certain proper non-trivial ideal that exists in every group ring over a non-trivial group. We also characterize the center of a group ring. This result will be applied in Chapter 3.

1.4.1 The augumentation ideal

For groups of order at least 2, group rings are never simple rings, in the sense that they always contain proper non-zero ideals. They always contain what is called the **augumentation ideal**. To exhibit the augumentation ideal, we apply Proposition 1.7 to the group homomorphism $G \to \{e\}$, the group with one element. The group ring of R over the one element group is easily seen to be isomorphic to R. From the result above we obtain a ring homomorphism $\epsilon : RG \to R$ that takes an element of RG to the sum of its coefficients. This map is the **augumentation map**. The kernel of the augumentation map,

$$\ker \epsilon = \Big\{ \sum_{g \in G} a_g g \mid \sum_{g \in G} a_g = 0 \Big\}$$

is what we call the augumentation ideal, and denote it by $\omega(RG)$. If R is a field, then the augumentation ideal of RG is clearly maximal, as it is the kernel of a ring homomorphism into a field.

1.4.2 The center

The center of a ring is the set of elements commuting (under multiplication) with every other element of the ring. In our case, the center is easy to characterize.

Proposition 1.13. *An element $a = \sum_{g\in G} a_g g \in RG$ is in the center of RG if and only if the coefficients a_g are contained in the center of R and $a_g = a_{x^{-1}gx}$ for all $x, g \in G$.*

Proof. First assume that a is central. If $g \in \mathrm{Supp}(a)$ and $x \in G$, then

$$x^{-1}gx \in \mathrm{Supp}(x^{-1}ax) = \mathrm{Supp}(a)$$

by centrality of a. From this we deduce that $g \in \mathrm{Supp}(a)$ implies that the entire conjugacy class of g in G is contained in $\mathrm{Supp}(a)$. Moreover, we see that for every pair of conjugate elements h, g we have $a_h = a_g$. Finally, for any $r \in R$ we have $ar = ra$ and this implies centrality (in R) of the coefficients of a.

Conversely, assume that a has the indicated properties. It is clear that that $ra = ar$ for $r \in R$. Denote by $\tilde{g}$ the sum in RG of all conjugates of $g \in G$. Such elements obviously have the property that $x^{-1}\tilde{g}x = \tilde{g}$ for all $x \in G$. The hypothesis implies that

$$a = a_{g_1}\tilde{g_1} + \ldots + a_{g_k}\tilde{g_k}$$

for some $g_1, \ldots, g_k \in G$ with finite conjugacy classes. It follows that $x^{-1}ax = a$ for all $x \in G$ and hence a commutes with the linear combinations $\sum_{x\in G} r_x x$, so with all of RG. □

This result implies that if R is commutative, then the center of KG is a free R-module, with a basis consisting of elements on the form $\tilde{g}$ as defined in the proof of the proposition. It also implies that a central element $a \in RG$ must have a support consisting of elements $g \in G$ of finite conjugacy classes. We will return to this observation in Chapter 3, where we will show that if K is a field and G is torsion-free, then a central element $a \in KG$ cannot be a zero-divisor.

Chapter 2

Idempotents

The focus of this chapter is on idempotent elements of group rings. We will discuss some classical results. One of them is Kaplansky's theorem on the trace of idempotent elements, one of several results in the theory of group rings which so far only has been proven using methods of analysis. We will also discuss a famous theorem by Zalesskii.

2.1 Idempotents and related conjectures

An idempotent e is an element which equals its own square. That is, it satisfies the equation $e^2 = e$. If e is an idempotent, then so are all of its conjugates $x^{-1}ex$, where $x \in R$ is a unit. Also, $e' = 1 - e$ will be an idempotent, with the additional property that $ee' = e'e = 0$. The elements $0, 1 \in R$ are idempotents which exist in every (unital) ring. A non-trivial idempotent is one which is different from 0 and 1.

In the ring of square matrices, any diagonal matrix with entries restricted to 0 and 1 is an idempotent, and so is any matrix similar to such a matrix. More generally, if $M = N \oplus L$ is an R-module, then the projections π_N, π_L are idempotent elements of $\mathrm{Hom}_R(M)$. Conversely, if $\phi \in \mathrm{Hom}_R(M)$ is an idempotent, then it is a matter of verification that we have an R-module decomposition $M = \ker\phi \oplus \mathrm{im}\,\phi$. Idempotent elements are used throughout ring theory to construct similar decompositions, and so this is one way to motivate their study.

The existence of a non-trivial idempotent $e \in R$ implies the existence of zero-divisors, since $e(1 - e) = 0$. Therefore, the existence of non-trivial idempotents in R is a property stronger than the existence of non-trivial zero-divisors. It is strictly stronger, because there are rings, say $\mathbb{Z}/4\mathbb{Z}$, with non-trivial zero-divisors but no non-trivial idempotents.

2.1.1 The idempotent conjecture for group rings

We can ask what properties idempotent elements of RG possess, or we can ask what conditions guarantee the non-existence of non-trivial idempotents in a group ring RG. We show below that a certain important functional takes idempotent elements to rational

numbers between 0 and 1, for any field K of characteristic 0. As for the non-existence question, R clearly cannot contain idempotent elements. Also G must be torsion-free, for otherwise it certainly contains a finite subgroup H, and the element

$$a = \frac{1}{|H|} \sum_{h \in H} h$$

is an idempotent (to verify this, one can use the fact that $Hh = H$ for all $h \in H$).

Conjecture. *Let K be a field and G a torsion-free group. Then KG contains no non-trivial idempotent.*

The conjecture has been confirmed in some special cases. For example, in [4] Formanek uses a variant of the trace functional, discussed below, to prove the conjecture for Noetherian groups (that is, groups satisfying the ascending chain condition on subgroups) in the case when the field K is of characteristic 0.

Along the way to another result, we will show in the coming chapter that RG is an integral domain whenever R is an integral domain and G is torsion-free and abelian, so it will follow then that in this case RG cannot contain non-trivial idempotent.

2.1.2 The Kadison-Kaplansky conjecture

The idempotent conjecture for the complex group ring $\mathbb{C}G$ is a special case of another conjecture. We have seen earlier that the natural left translation action of G on $H = L^2(G)$ induces an algebra homomorphism of $\mathbb{C}G$ into $B(H)$, and that the closure of the image of this embedding is a C^*-algebra. This C^*-algebra is called the **reduced C^*-algebra** $C_r^*(G)$.

Conjecture (**Kadison-Kaplansky**). *Let G be a torsion-free group. The reduced C^*-algebra $C_r^*(G)$ contains no non-trivial idempotent.*

An affirmative solution to this conjecture of course implies an affirmative solution to the idempotent conjecture for group rings, since $\mathbb{C}G \subseteq C_r^*(G)$. It will follow from (Proposition 2.4) below that $C_r^*(G)$ contains a non-trivial idempotent if and only if it contains a non-trivial self-adjoint idempotent (an element x of $\mathbb{C}G$ is self-adjoint if it satisfies the equation $x^* = x$), and so the conjecture above can be re-phrased accordingly. It is (most likely) not known yet if the existence of a non-trivial idempotent in $\mathbb{C}G$, G torsion-free, implies the existence of a self-adjoint idempotent in $\mathbb{C}G$.

2.2 The trace map

In the remaining sections we deal only with group rings over fields. The field will be denoted by K. In this section we introduce the trace map, which is a linear functional on KG and which has been the subject of extensive study. As an application of this map and the analytic approach to complex group rings, we will prove in the next section a famous theorem of Kaplansky on the trace of idempotents.

2.2.1 Definition

We define a linear functional tr on KG, which we call the **trace** and which takes

$$a = \sum_{g \in G} a_g g \in KG$$

to a_1, the coefficient of the group identity element $1 \in G$,

$$\operatorname{tr} a = a_1. \tag{2.1}$$

If $a, b \in KG$, then we have the easily verifiable property

$$\operatorname{tr} ab = \operatorname{tr} ba \tag{2.2}$$

The above property is also enjoyed by the familiar matrix trace map, and actually there are more similarities. Regard $KG = V$ as a K-vector space. We have seen before that KG acts on V by left multiplication, and this action is K-linear. Every element of KG therefore defines a K-linear map on V, and we obtain in this way the *regular representation* of KG, a K-algebra monomorphism from KG to $\operatorname{Hom}_K(V)$, the algebra of linear maps on V. If G is a finite group, then V is finite-dimensional and we have the identification

$$\underset{K}{\operatorname{Hom}}(V) \cong M_n(K),$$

where $M_n(K)$ is the algebra of $n \times n$ matrices with entries from K.

Proposition 2.1. *Let G be a finite group and $\tau : KG \to M_n(K)$ the homomorphism discussed above. Then*

$$|G| \operatorname{tr} a = \operatorname{trace} \tau(a),$$

where trace *is the usual functional taking a matrix to the sum of the elements on the main diagonal.*

Proof. Let a basis for V consist of the elements of G. If

$$a = \sum_{g \in G} a_g g$$

then we have, by linearity of the maps,

$$\operatorname{trace} \tau(a) = \sum_{g \in G}^{n} a_g \operatorname{trace} \tau(g).$$

Since $G = gG$, we see that each $\tau(g)$ is a permutation matrix. Since left action of g on G leaves nothing fixed if $g \neq 1$ and leaves everything fixed if $g = 1$, clearly $\operatorname{trace} \tau(g) = 0$ for all $g \neq 1$, and $\operatorname{trace} \tau(1) = n = |G|$. □

Remark. The proposition can be applied to easily deduce that $0 < \operatorname{tr} e < 1$ whenever $e \in KG$ is a non-trivial idempotent, $|G|$ is finite and $\operatorname{char} K = 0$. The matrix $E = \tau(e)$ is idempotent and so satisfies $E^2 - E = 0$, hence is diagonalizable with eigenvalues restricted to 0,1 and E is neither the identity matrix nor the zero matrix (because e is non-trivial). Therefore, $\operatorname{trace} E = \operatorname{trace} \tau(e)$ is an integer k between 1 and $n - 1 = |G| - 1$, so the result follows from the above proven equation. As a bonus we get that $\operatorname{tr} e$ is a rational number, and that it is restricted to the values k/n, for $k = 1, \ldots, n-1$. For arbitrary groups it is also true that $\operatorname{tr} e$ lies in the prime subfield of K, regardless of characteristic. If the characteristic is 0, then $0 < \operatorname{tr} e < 1$ when $e \neq 0, 1$. These two facts are special cases of the two famous theorems by Kaplansky and Zalesskii that were mentioned in the introduction of this chapter and which we present below.

Proposition 2.2. *For $a, b, c \in \mathbb{C}(G)$ we have*

(i) $(a, b) = \operatorname{tr} ab^*$

(ii) $\operatorname{tr} aa^* = \|a\|_2^2$

(iii) $(a, bc) = (ac^*, b)$

(iv) $(a, cb) = (c^*a, b)$

Proof. The first one requires just a verification, and the second follows from the first by setting $b = a$. The last last two follow from the first one. For example, to prove (iii) we proceed as follows:

$$(a, bc) = \operatorname{tr} a(bc)^* = \operatorname{tr} ac^*b^* = (ac^*, b).$$

□

2.2.2 Kaplansky's theorem

The development in this section follows [7]. The theorem which we want to prove in this section is the following,

Theorem (Kaplansky). *Let $e \in \mathbb{C}G$ be an idempotent, $e \neq 0, 1$. Then $0 < \operatorname{tr} e < 1$.*

The important conclusion here is that the trace map is *faithful* in the sense that a non-zero idempotent maps to a non-zero element of K. Kaplansky's initial motivation was to apply the above result to deduce *direct finiteness* for the group ring KG where K has characteristic 0. Direct finiteness of a ring is the property that whenever $a, b \in R$ are such that $ab = 1$, then we also have that $ba = 1$. That is, one-sided invertible elements are invertible. This fact follows almost immediately from Kaplansky's theorem after it has been appropriately generalized to include the cases where K is any field of characteristic 0. The result is especially interesting because this (seemingly) purely algebraic statement has so far only been proven using analytic theory, and this is the proof presented here.

From before we know that there is an embedding $I : \mathbb{C}G \to B(H)$, the space of bounded linear operators on the Hilbert space $H = L^2(G)$. We will drop the notation $I(a)$ and simply consider $\mathbb{C}G$ as a subalgebra of $B(H)$. We have proven in the first chapter that the norm-closure $U = \overline{\mathbb{C}G}$ in $B(H)$ is closed under taking adjoints. The below statement, true in particular for U, is a well-known fact and a proof of it can be found in virtually any book on functional analysis or the theory of C^*-algebras.

Proposition 2.3. *Let $B(H)$ be the algebra of bounded linear operators on a Hilbert space H. If U is a norm-closed subspace of $B(H)$ that is also closed under taking adjoints, then for any element $x \in U$ we have that $1 + xx^*$ is invertible in U.*

We have earlier defined an involution map $^* : \mathbb{C}G \to \mathbb{C}G$. More generally, a map $^* : R \to R$ of a ring R is called an *involution* if it is an anti-isomorphism of R and is its own inverse. An element x is called **self-adjoint** if $x = x^*$ and x is also an idempotent then it is called a **projection**. For a projection we have the equalities

$$x^2 = x^*x = xx^* = x = x^*.$$

The two results below are due to Kaplansky [6].

Proposition 2.4. *Let R be a unital ring with involution such that for any $x \in R$, the element $1 + xx^*$ is invertible in R. For every idempotent $f \in R$, we can find a projection $e \in B$ such that $fR = eR$.*

Remark. The notation fR denotes the right principal ideal generated by f.

Proof. Consider the self-adjoint element

$$z = 1 + (f - f^*)(f^* - f)$$

and let $t = z^{-1}$. Then, of course, t is also self-adjoint. One can verify that the elements z and f commute, for indeed

$$zf = ff^*f = fz.$$

Hence it follows that t, being the inverse of z, also commutes with f. Since t is self-adjoint, it also commutes with f^*. From these properties it is seen readily that $e = ff^*t \in fR$ is self-adjoint. It is also an idempotent, for

$$e^2 = ff^*tff^*t = ff^*ff^*t^2 = zff^*t^2 = ff^*zt^2 = ff^*t = e.$$

Hence e is a projection. Since

$$ef = ff^*tf = (ff^*f)t = fzt = f$$

we get that $f \in eR$, and since $e = ff^*t \in fR$, we get the equality $eR = fR$. □

Proposition 2.5. *Let R be a unital ring and $e, f \in R$ two idempotents such that $eR = fR$. Then e and f are similar, i.e. there exists an invertible element $s \in R$ such that $s^{-1}fs = e$.*

Proof. It follows from the hypothesis that $ef = f$ and $fe = e$. Indeed, since $f \in eR$, we have that $f = ea$ for some $a \in R$. Hence

$$ef = e(ea) = e^2a = ea = f.$$

Similarly we can show that $fe = e$. The element $x = f - e$ has the properties $xf = 0$, $fx = x$ and $x^2 = 0$. From the last property we get $(1-x)(1+x) = 1$. Now we set $s = 1-x$ and get

$$s^{-1}fs = (1+x)f(1-x) = (f+xf)(1-x) = f(1-x) = f - fx = f - x = e.$$

□

It follows from the above two results that any idempotent in $\overline{\mathbb{C}G} = U \subseteq B(H)$ is similar to a projection. This is the crucial observation that leads to the proof of Kaplansky's theorem. Indeed, if both the projection p and the idempotent e that it is similar to would be elements of $\mathbb{C}G$, then by trace properties found in Proposition 2.2, we get

$$\operatorname{tr} e = \operatorname{tr} s^{-1}ps = \operatorname{tr} pss^{-1} = \operatorname{tr} p = \operatorname{tr} pp^* = \|p\|_2^2 > 0,$$

assuming that we're dealing with non-zero e, p. Since tr is linear and $1 - e$ is also an idempotent, the result would follow. The problem is that the interesting case is when the group ring $\mathbb{C}G$ is a proper subset of U, and so p is not necessarily an element of $\mathbb{C}G$. A way around this is to extend the trace map to U and prove that the properties that we have used above are preserved in the extension.

Using that tr is linear on $\mathbb{C}G$, it will extend (uniquely) to U if we can show that it is bounded (with respect to the operator norm on U), with the extension being bounded and linear. Let $\|\cdot\|_2$ denote the standard 2-norm on $H = L^2(G)$ and $\|\cdot\|$ the induced operator norm on $B(H)$. We have already seen in the first chapter that $\|a\| \geq \|a\|_2$ for $a \in \mathbb{C}G$. Of course we have $\|a\|_2 \geq |\operatorname{tr}(a)|$, which yields

$$\|a\| \geq \|a\|_2 \geq |\operatorname{tr} a|,$$

and in particular shows that tr is bounded on $\mathbb{C}G$, with respect to the operator norm. Hence tr can be extended to the operator norm closure of $\mathbb{C}G$, which is by definition U. We now verify that some of the properties of tr which hold for $\mathbb{C}G$ still hold for its extension to U. The extension of tr to U will also be denoted by tr.

Proposition 2.6. *For the extended map $tr : U \to \mathbb{C}$ and $a, b \in U$ we have*

(i) $\operatorname{tr}(ab) = \operatorname{tr}(ba)$

(ii) $\operatorname{tr}(aa^*) \geq 0$ *with equality if and only if* $a = 0$.

Proof. Of course the corresponding properties hold for elements of the group ring $\mathbb{C}G$, and this is a dense subset of U. Choose sequences $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ in $\mathbb{C}G$ converging to a and b respectively. By continuity of multiplication a_nb_n converges to ab, b_na_n converges to ba and by continuity of tr we get

$$\operatorname{tr}(ab) = \lim_{n\to\infty} \operatorname{tr}(a_nb_n) = \lim_{n\to\infty} \operatorname{tr}(b_na_n) = \operatorname{tr}(ba)$$

which proves (i).

By exactly the same argument, picking a sequence in $\mathbb{C}G$ converging to a we show easily by using the corresponding property for $\mathbb{C}G$ that $\operatorname{tr}(aa^*) \geq 0$ for any $a \in U$, which proves half of (ii).

Now assume that $\operatorname{tr}(aa^*) = 0$. Let again $\{a_n\}_{n=1}^{\infty}$ be a sequence with $a_n \in \mathbb{C}G$, and which converges to a. Then, since the involution is an isometry with respect to the operator norm, a_n^* converges to a and so $a_na_n^*$ converges to aa^*. Now, if $\|\cdot\|_2$ denotes the 2-norm on $\mathbb{C}G$, then using part (ii) of Proposition 2.2 we get that

$$0 = \operatorname{tr}(aa^*) = \lim_{n\to\infty} \operatorname{tr}(a_na_n^*) = \lim_{n\to\infty} \|a_n\|_2^2$$

Since a is a continuous operator on $L^2(G)$ and $\mathbb{C}G \subseteq L^2(G)$ is $\|\cdot\|_2$-dense, it will suffice to show that a is the zero operator on $\mathbb{C}G$. But since a is linear, it will further suffice to show that a is zero on $G \subset L^2(G)$. For all $n \geq 1$, we have

$$\begin{aligned} \|a(g)\|_2 &\leq \|(a-a_n)(g)\|_2 + \|a_n(g)\|_2 \\ &\leq \|a-a_n\|\|g\|_2 + \|a_ng\|_2 \\ &= \|a-a_n\| + \|a_n\|_2. \end{aligned}$$

By convergence of $\|a-a_n\|$ to 0 and of $\|a_n\|_2$ to 0 we get that $\|a(g)\|_2 = 0$, so the second half of (ii) is proven. □

With the above properties of the trace extension at hand, the proof of Kaplansky's theorem is basically just the repetition of what has already been explained above.

Theorem 2.7. ***(Kaplansky)*** *Let $e \in \mathbb{C}G$ be an idempotent, $e \neq 0, 1$. Then $0 < \operatorname{tr} e < 1$.*

Proof. With the setup $\mathbb{C}G \subseteq U \subseteq B(H)$ as before, e is an idempotent in a norm-closed subalgebra of $B(H)$ and this subalgebra is closed under taking adjoints. By the results above we can find an invertible element s such that $e = s^{-1}ps$, with $p = pp^*$ and $p \neq 0, 1$. Then we compute

$$\operatorname{tr} e = \operatorname{tr} s^{-1}ps = \operatorname{tr} pss^{-1} = \operatorname{tr} p = \operatorname{tr} pp^* > 0.$$

Since $1 - e$ is also a non-zero idempotent, we get $1 - \operatorname{tr} e = \operatorname{tr}(1-e) > 0$. □

This theorem can be generalized to the case where K is any field of characteristic 0.

Corollary 2.8. *Let $e \neq 0, 1$ be an idempotent in KG, where K is a field of characteristic 0. Then* $\operatorname{tr} e$ *is algebraic over $\mathbb{Q}$ and any embedding of $\mathbb{Q}(\operatorname{tr} e)$ in the complex numbers is contained in the reals, with* $\operatorname{tr} e$ *lying strictly between 0 and 1.*

Proof. Let $e = \sum_{i=1}^{n} a_i g_i$ with $g_1 = 1 \in G$. In chapter 3 we will show that the field $F = \mathbb{Q}(a_1, \ldots, a_n)$ can be embedded in $\mathbb{C}$ (see Proposition 3.20 there). Let ϕ be this embedding. Certainly $e \in FG \cong \phi(F)G \subseteq \mathbb{C}G$, and so $\phi(e)$ has trace strictly between 0 and 1 by the previous theorem. This means that $0 < \phi(\operatorname{tr} e) < 1$, since $\operatorname{tr} \phi(e) = \phi(\operatorname{tr} e)$. This proves half of the claim. Observe though that if $\operatorname{tr} e$ was transcendental, then by the proof of Proposition 3.20 we could have picked $\phi : F \to \mathbb{C}$ taking $\operatorname{tr} e$ to any transcendental in $\mathbb{C}$. In particular one outside of the real interval $(0, 1)$, which would lead to a contradiction to Kaplansky's theorem above. □

If the image of γ in $\mathbb{C}$ lies in the reals, for any embedding $\mathbb{Q}(\gamma)$ in $\mathbb{C}$, then γ is said to be *totally real algebraic*. Such a γ must necessarily be algebraic over $\mathbb{Q}$. The converse is not true. Adjoining to $\mathbb{Q}$ any root of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$ produces isomorphic fields, and so $2^{1/3}$ is not totally real algebraic, for its conjugates lie outside the reals. The theorem says that the traces of idempotent elements of group rings over fields of characteristic 0 can be interpreted as totally real algebraic numbers between 0 and 1. A deep theorem by Zalesskii asserts that traces of idempotents always lie in the prime subfield of K, regardless of the characteristic. This result is discussed below.

2.2.3 Zalesskii's theorem

The presentation in this section follows [9]. We treat the following result.

Theorem 2.9. *Let $e \in KG$ be an idempotent. Then* $\operatorname{tr} e$ *lies in the prime subfield of K.*

The special case of the theorem, for fields of prime characteristic, is proven by elementary and a very ingenious method. The general case follows from a technical result which shows existence of certain homomorphisms of rings. We will discuss the proof in the case of positive characteristic and indicate how the general case follows. The crucial observation is that the nice formula

$$(a + b)^p = a^p + b^p$$

which holds in commutative algebras of characteristic $p > 0$ can be generalized to the case of non-commutative ones. Recall that the **commutator subspace** $[A, A]$ of an algebra A is the linear span of commutators $xy - yx$ with $y, x \in A$. In the case that $A = KG$, we have

$$\operatorname{tr}(xy - yx) = \operatorname{tr}(xy) - \operatorname{tr}(yx) = 0,$$

so $[KG, KG]$ is contained in the kernel of tr.

Lemma 2.10. *Let $a_1, a_2, \ldots, a_k$ be elements of an algebra A over a field K of characteristic $p > 0$. Then if $q = p^n$, with n a positive integer, then*

$$(a_1 + a_2 + \ldots + a_k)^q = a_1^q + a_2^q \ldots + a_k^q \mod [A, A].$$

Proof. After expanding the left-hand side the expression can be identified with a sum of all words on the alphabet $a_1, a_2, \ldots, a_k$ which are of length exactly q. Hence, if S denotes this set of words, then we have

$$(a_1 + a_2 + \ldots + a_k)^q = \sum_{\omega \in S} \omega.$$

Note that the cyclic group $\mathbb{Z}/q\mathbb{Z}$ admits an action on S by right translation. For example,

$$(1 + q\mathbb{Z}) \cdot b_1 b_2 \ldots b_{n-1} b_n = b_n b_1 b_2 \ldots b_{n-1}.$$

Observe also that if $\omega' \in S$ is contained in the orbit $O(\omega)$ of $\omega \in S$ under this action, then the difference $\omega - \omega'$ is contained in the commutator $[A, A]$. Indeed, we can then write $\omega = \alpha\beta$ and $\omega' = \beta\alpha$ for some $\alpha, \beta \in A$. We deduce that

$$\sum_{\omega' \in O(\omega)} \omega' = |O(\omega)|\omega \mod [A, A]$$

where $|O(\omega)|$ denotes the number of elements in the orbit of ω. The group acting on the set S has order $q = p^n$, and therefore an orbit under its action either contains a single element, or a number of elements which is divisible by p. Hence by the above expression, for any non-trivial orbit $O(\omega)$, the sum of its elements vanishes modulo $[A, A]$. If the orbit is trivial, then it is easy to see that it must consist of a word on the form $a_i a_i \ldots a_i = a_i^q$. The claim now follows after summing over all the orbits. □

Theorem 2.11 (**Zalesskii, positive characteristic**). *Let $e \in KG$ be an idempotent, where K is a field of characteristic $p > 0$. Then* $\operatorname{tr} e$ *is contained in the prime subfield of K.*

Proof. Write

$$e = \sum_{x \in G} a_x x = b + \sum_{x \in P} a_x x,$$

where P is the set of elements in G of order which is a power of p. Setting $q = p^n$, for some $n > 0$, it follows from the lemma that

$$e = e^q = b^q + \sum_{x \in P} a_x^q x^q \mod [KG, KG].$$

Taking n large enough in $q = p^n$, we can ensure that $x^q = 1$ for all x in the expression above. We apply the lemma to b^q, where

$$b = \sum_{x \notin P} a_x x.$$

Note that since none of the elements of G in the support of b has an order which is a power of p, we get

$$b^q = \sum_{x \notin P} a_x^q x^q \mod [KG, KG]$$

and none of x^q equals 1_G, and hence $\mathrm{tr}(b^q) = 0$. The linearity of tr and the fact that $\mathrm{tr}[KG, KG] = \{0\}$ now implies

$$\mathrm{tr}\, e = \mathrm{tr}\, e^q = \sum_{x \in P} a_x^q = \big(\sum_{x \in P} a_x\big)^q.$$

The last equality holds because the arithmetic is now carried out in a field of characteristic $p > 0$. Note that the choice of n was arbitrary, as long as it was sufficiently big. Hence we can also set $q' = qp = p^{n+1}$. Then

$$\mathrm{tr}\, e = \mathrm{tr}\, e^{qp} = \sum_{x \in P} a_x^{qp} = \big(\sum_{x \in P} a_x\big)^{qp} = (\mathrm{tr}\, e)^p.$$

We see that the element $\mathrm{tr}\, e$ solves the equation $x^p - x = 0$ in K. Any such solution lies in the prime subfield, so the proof is complete. □

The general case of Zalesskii's theorem is a consequence of the following result, found in [9, Corollary 2.2.9] The lemma is non-trivial and can be established using methods of commutative algebra and algebraic number theory.

Lemma 2.12. *Let K be a field of characteristic zero and $x_0, x_1, \ldots, x_n$ elements of K with $x_0 \notin \mathbb{Q}$. Then there exists a prime p, a valuation ring R of K containing $x_0, x_1, \ldots, x_n$ and a ring homomorphism ϕ from R to the algebraic closure of $GF(p)$ such that $\phi(x_0) \notin GF(p)$. The kernel of ϕ is the maximal ideal M of R.*

The above result is applied extensively in proofs of many theorems concerning group rings. Taking advantage of it leads in a straight-forward way to completion of the proof of Zalesskii's theorem.

Theorem 2.13 (**Zalesskii**). *Let $e \in KG$ be an idempotent, where K is a field. Then* $\mathrm{tr}\, e$ *is contained in the prime subfield of K.*

Proof. Since we have already proved the case when the characteristic of K is positive, we may assume that K has characteristic 0. Let $x_0 = \mathrm{tr}\, e, x_1, \ldots, x_n \in K$ be all the coefficients of the support of an idempotent $e \in KG$. If $x_0 \neq \mathbb{Q}$, then let R, ϕ, p be as in Lemma 2.12. Since the coefficients of e are contained in R, we have that $e \in RG \subseteq KG$. Moreover, if $M = \ker \phi$ and $F = R/M$ is the residue field, then the natural map $R \to F$ induces a ring homomorphism $RG \to FG$, where F has characteristic $p > 0$. As any ring homomorphism, it maps idempotents to idempotents, and by the assumption, the image of $x_0 = \mathrm{tr}\, e$ lies outside the prime subfield of F. This contradicts the result established for idempotents in group rings over fields of characteristic $p > 0$. Therefore $\mathrm{tr}\, e \in \mathbb{Q}$. □

Kaplansky's and Zalesskii's theorems are some of the most general results concerning traces of idempotents in group rings.

Chapter 3

Zero-divisors in group rings

This chapter presents an interesting question regarding group rings, namely the question of what conditions on the ring R and group G guarantee non-existence of non-trivial zero-divisors in the group ring RG. We present a long-standing conjecture, which claims that when G is a torsion-free group, then for an arbitrary field (or integral domain) K, the group ring KG contains no non-trivial zero-divisor. In section 2, we briefly discuss a very simple case of the conjecture, when G is assumed to be a unique product group. Next, by following work of B. H. Neumann [8] on FCC-groups and using the results of section 2, we are able to confirm that for arbitrary field K and a torsion-free group G the group ring KG contains no non-trivial central zero-divisor. In the last section we study systems of polynomial equations that arise when considering zero-divisors in group rings. We show how the zero-divisor conjecture for certain fields implies an answer to the conjecture for other fields.

3.1 The zero-divisor conjecture

Non-zero elements x, y of a ring R are non-trivial **zero-divisors** if $xy = 0 = yx$. To be more precise, if $xy = 0$ holds, but $yx \neq 0$, then x is a left zero-divisor and y a right zero-divisor. Matrix rings provide many simple examples of zero-divisors, and also examples where $AB = 0$ but $BA \neq 0$.

If RG is a group ring and R contains a zero-divisor, then clearly so does RG, because $R \subseteq RG$. Also, if G contains a non-identity element g of finite order $|g| = n \geq 2$, then zero-divisors always exist in RG. We simply take elements

$$a = 1 - g$$

and

$$b = 1 + g + \ldots + g^{n-1}.$$

Then it is easy to verify that $ab = ba = 0$.

We can ask ourselves what properties are possessed by zero-divisors in RG, or we could ask when a group ring RG lacks non-trivial zero-divisors. In the second case, by

the observations above, clearly R must be free of zero-divisors and G must be torsion-free. Since no pair of a field K and a torsion-free group G such that KG contained a zero-divisor had been found, Irving Kaplansky famously conjectured the following.

Conjecture (**Kaplansky**). *Let K be a field and G a torsion-free group. Then KG contains no non-trivial zero-divisor.*

Over the years some partial results have been obtained. The conjecture has been confirmed for some classes of groups. Perhaps the most interesting result is due to Brown, Farkas and Snider from 1976, which confirms the conjecture for the class of torsion-free polycyclic-by-finite groups and fields of characteristic 0. A polycyclic group is a solvable group with cyclic factors. That is, G is polycyclic if and only if we have a chain of subgroups

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_{n-1} \triangleleft G_n = G$$

where for $i = 0, 1, \ldots, n-1$ we have that G_{i+1}/G_i is a cyclic group. A polycyclic-by-finite group is a group G having a normal subgroup H of finite index which is polycyclic. In full generality, the conjecture is still open today. Attempts to confirm the conjecture for fixed fields K were also unsuccessful, and the situation here is just as hopeless. The conjecture has not been confirmed for any kind of field K, and indeed, it seems that the simplest imaginable case $K = \mathbb{F}_2$ is still out of reach.

3.2 The case of abelian and unique product groups

The special case of the zero-divisor conjecture when G is torsion-free abelian is particularly easy to handle, and it can be used to prove some further results. As noted before, if H is a subgroup of G, then we have the inclusion $RH \subseteq RG$. If we are given an equation $ab = 0$ with $a, b \in RG$ non-zero, then taking H to be the subgroup of G generated by the supports of a, b, we can construct the group ring RH. We have $a, b \in RH$ and H finitely generated. This shows that questions about non-existence of zero-divisors in group rings can be reduced to finitely generated groups. This observation leads to a quick proof of the zero-divisor conjecture for the special case when G is a torsion-free abelian group.

Proposition 3.1. *Let R be an integral domain and G a torsion-free abelian group. Then RG is an integral domain.*

Proof. By the remarks preceding the proposition we have already reduced the problem to the case where $G = \mathbb{Z}^n$, for this is how finitely generated torsion-free abelian groups look. Also, R can be replaced by its field of fractions. Consider the field of rational functions $R(x_1, x_2, \ldots, x_n)$. The elements of G are n-tuples of integers. Map such an n-tuple $(a_1, a_2, \ldots, a_n)$ to the rational function $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$. Certainly this is a group homomorphism, and so by Proposition 1.8 it extends to a ring homomorphism from RG. By construction the extended homomorphism is injective. Hence RG is contained in a field and this proves the assertion. □

As an application of the above proposition, we show that the size of the support of a zero-divisor in KG, when G is torsion-free, must be at least 3. We have seen that if $a \in RG$ is a zero-divisor, then it is a zero-divisor in a group ring RH constructed from a finitely generated group H. As a matter of fact, a is a zero-divisor even in the group ring over its support group. This follows from the following observation.

Proposition 3.2. *[9] Let $a \in RH \subseteq RG$, where H is a subgroup of G. Then a is a left (right) zero-divisor in RH if and only if it is a left (right) zero-divisor in RG.*

Proof. The "only if" statement is trivial, because $RH \subseteq RG$. Conversely, assume that $ab = 0$ where $b \in RG$. We can assume that the support of b intersects H, because $abg = 0$ for any $g \in G$, and so we can shift the support of the element b. Then by Proposition 1.9,

$$0 = \pi_H(ab) = a\pi_H(b),$$

and we are done, since $\pi_H(b) \neq 0$. □

As said before, the above result actually implies that a left zero-divisor in a group ring over a torsion-free group must necessarily have a support of size 3 or greater. Otherwise, if $a = rh + sg$ and $ab = 0$, with b non-zero, then it is easy to see that we can multiply the equation $ab = 0$ from the left by a suitable element to obtain the equation $a'b = 0$, where a' is on form $1 + (r^{-1}s)gh^{-1}$. The support group H of a' is infinite cyclic, generated by gh^{-1}. In particular, H is free abelian, and the above result tells us that a' is a left zero-divisor there. This contradicts the claim in Proposition 3.1.

A torsion-free abelian group is a special case of a **unique product group**, or a **up-group**. A group G is a up-group if for any two finite subsets A, B of G there exists at least one element $ab \in AB = \{xy : x \in A, y \in B\}$ which is represented uniquely in this way as a product of an element of A and an element of B. More precisely, if $ab = a'b'$ with $a' \in A, b' \in B$, then $a = a', b = b'$. It is easy to see that a finitely generated torsion-free abelian group is a up-group, just by linearly ordering its elements in some way. For example, let $n = (n_1, n_2, \ldots, n_k), m = (m_1, m_2, \ldots, m_k) \in \mathbb{Z}^k$. Then define $n > m$ if and only if $n_i > m_i$ for the smallest integer i for which $n_i \neq m_i$. This is a linear ordering on $\mathbb{Z}^k$ and it is trivial to see that $m, n, l \in \mathbb{Z}^k$ and $n > m$ implies $n + l > m + l$. Therefore, given two finite sets $A, B \subset \mathbb{Z}^k$ we simply choose a, b to be the maximal elements of A and B respectively, and conclude that $a + b$ is uniquely represented in this way in $A + B$ (additive notation). If G is an arbitrary torsion-free abelian group, then two finite sets A, B generate a finitely-generated torsion-free subgroup of G, and consequently G is a up-group.

Only torsion-free groups can be up-groups. This follows easily by noting that if $g \in G$ has order $n \geq 2$, then each element of AB, with $A = B = \{1, g, \ldots, g^{n-1}\}$, can be represented in n different ways as products of elements in A and B. Of course, up-groups satisfy the zero-divisor conjecture. For if a, b are non-zero elements of KG, then the hypothesis on G ensures that from the two finite subsets $A = \mathrm{Supp}(a)$, $B = \mathrm{Supp}(b)$ we obtain an element $xy \in \mathrm{Supp}(ab)$ and therefore $ab \neq 0$. If all torsion-free groups were indeed up-groups, then the zero-divisor conjecture would be true. Unfortunately, Promislow found in 1988 examples of torsion-free group without the unique product property [10].

3.3 FCC-groups and central zero-divisors

In this section we use group-theoretic arguments to show that if G is a torsion-free group, then the group ring KG does not contain non-trivial central zero-divisors. The theorem will follow from results of the previous section and the fact that the support group of a central element of KG, with G torsion-free, is an abelian group. The development in this section roughly follows [8]. Some similar ideas are also found in [9, section 4.1].

A group with the property that for every element $x \in G$, the set

$$x^G = \{g^{-1}xg : g \in G\}$$

of conjugates of x is finite will be called a **finite conjugacy class group**, or simply an **FCC-group**. Equivalently, a group is an FCC-group if for each $x \in G$ we have that the index $[G : C_G(x)]$ (the number of cosets of $C_G(x)$ in G) is finite, where

$$C_G(x) = \{g \in G : xg = gx\}$$

is the centralizer of x in G. The motivation for studying such groups is that the support groups of central elements of KG are FCC-groups.

Lemma 3.3. *Let G be a finitely generated group, with generators $g_1, g_2, \ldots, g_n$. If for each g_i the index $[G : C_G(g_i)]$ is finite, then the index $[G : Z(G)]$ is finite. In particular, $[G : C_G(g)]$ is finite for each $g \in G$ and so G is an FCC-group.*

Proof. The center $Z(G)$ of G is clearly the intersection of the finitely many subgroups $C_g(g_i), i = 1, \ldots, n$. Recall the fact that if H, K are subgroups of G of finite index in G, then $H \cap K$ is also of finite index in G. It then follows by induction that $Z(G)$ is a subgroup of finite index in G. If $g \in G$ is arbitrary, then we have

$$[G : C_G(g)][C_G(g) : Z(G)] = [G : Z(G)],$$

and this yields finiteness of $[G : C_G(g)]$. □

Remark. Here is an example that shows the necessity of the assumption that G is finitely generated. Let G be a countable product of the symmetry group of an equilateral triangle,

$$G = S_3 \times S_3 \times S_3 \ldots$$

and let H be the subgroup of G such that $x = (x_1, x_2, \ldots) \in H$ if and only if the x_n are all eventually the identity element e. If $x_n = e$ for all $n \geq N$, then $[H : C_H(x)] \leq 6^N$, yet H is infinite and has trivial center, so $[H : Z(H)] = \infty$.

Proposition 3.4. *Let $a \in KG$ be central and let H be the support group of a. Then H is an FCC-group.*

Proof. From Proposition 1.13 we know that for a central element $a = \sum_{g \in G} a_g g$ we have $a_g = a_{h^{-1}gh}$, for all $h, g \in G$. In particular, the elements of the support of a have finite conjugacy classes in G, and so also in H. The result now follows from Lemma 3.3. □

We will need the following well-known result due to Schur. Recall that the **commutator subgroup** G' of G is the smallest subgroup containing all elements of the form $g^{-1}h^{-1}gh$, for pairs $g, h \in G$.

Lemma 3.5 (**Schur**). *Let G be a group and $Z(G)$ be its center. If $[G : Z(G)]$ is finite, then the commutator subgroup G' of G is also finite.*

It follows from this lemma and the above results that the commutator subgroup G' of a finitely generated FCC group is finite.

The set $T(G)$ of elements of G which have finite order is the **torsion subset** of G. The torsion subset of an abelian group forms a subgroup, but this is not the case for a general non-abelian group.

Proposition 3.6. *Let G be a finitely generated FCC-group, $T(G)$ the torsion subset of G. Then $T(G)$ is a finite normal subgroup of G.*

Proof. As concluded above, G' is finite, and therefore we have the containment $G' \subseteq T(G)$. Of course, G/G' is abelian. Since it is also finitely generated, by a basic abelian group structure theorem we have that $T(G/G')$ is a finite subgroup of G/G'. The projection $\pi : G \to G/G'$ clearly maps $T(G)$ into $T(G/G')$. Conversely, if $a + G' \in T(G/G')$, then for some integer $n \geq 1$ we have that $a^n \in G' \subseteq T(G)$, and hence $a \in T(G)$. It follows that the inverse image of $T(G/G')$ under π is $T(G)$, and so by the standard fact that a homomorphic pre-image of a normal subgroup is normal, $T(G)$ is a normal subgroup of G. The finiteness of $T(G)$ follows from the equation $|T(G/G')| = |T(G)|/|G'|$. □

The result we are after now follows easily.

Corollary 3.7. *Let G be a finitely generated FCC-group, $T(G)$ its torsion subgroup. Then $G/T(G)$ is a finitely generated torsion-free abelian group.*

Proof. By Schur's lemma, we get $G' \subseteq T(G)$, so clearly $G/T(G)$ is abelian. Since G is finitely generated, so is $G/T(G)$. Since $G/T(G)$ is certainly torsion-free, basic structure theorems imply that $G/T(G)$ is free abelian. □

Remark. It follows from the above corollary that an arbitrary (not necessarily finitely generated) FCC-group G that is torsion-free must be abelian. This we see by taking $g, h \in G$ and considering the subgroup generated by g, h.

The main result of this section now follows easily.

Theorem 3.8. *Let G be a torsion-free group and K any field. Then KG contains no non-trivial central zero-divisor.*

Proof. Let a be any non-zero central element of KG and let H be the support group of a. Then we know that H is free abelian by Corollary 3.7, and so we know that KH contains no zero-divisors, by Proposition 3.1. By Proposition 3.2, we know that if a is a zero-divisor in KG, then it is also a zero-divisor in KH. This implies that a is not a zero-divisor in KG. □

The above result on the non-existence of central non-trivial zero-divisors in KG, where G is torsion-free, generalizes easily to the case of rings graded by a torsion-free group G in which homogeneous elements are not zero-divisors. We digress to briefly discuss this.

Definition 3.9. Let G be a group. A ring R is G-**graded** if R, as a group, can be expressed as a direct sum of subgroups indexed by G:

$$R = \bigoplus_{g \in G} R_g$$

and for $x \in R_g, y \in R_h$ we have that $xy \in R_{gh}$.

An element $x \in R_g$ is a **homogeneous element** of degree g. It is easy to see that if H is a subgroup of G, and R is a G-graded ring, then

$$R_H = \bigoplus_{h \in H} R_h$$

is a subring of R. Just as in the case of group rings, we have a projection map $\pi_H : R \to R_H$ given by

$$a = \sum_{g \in G} a_g \mapsto \sum_{h \in H} a_h.$$

Each element a of R is a finite sum of homogeneous elements $a_g \in R_g$, and the support of an element of a G-graded ring is defined naturally as the finite subset of $g \in G$ for which $a_g \neq 0$.

Lemma 3.10. *Let H be a subgroup of a group G. If R is a G-graded ring*

$$R = \bigoplus_{g \in G} R_g$$

and

$$R_H = \bigoplus_{h \in H} R_h$$

is the subring graded by H, then we have

$$\pi_H(ab) = \pi_H(a)b$$

and

$$\pi_H(ba) = b\pi_H(a)$$

whenever $a \in R$, $b \in R_H$.

Proof. The proof is essentially the same as in the case of the group ring, Proposition 1.9. We write $a = a' + \pi_H(a)$ and note that for any homogeneous element $x \in R_H$ the support of $a'x$ is disjoint from H. It follows that $a'b$ has support disjoint from H, and then the desired conclusion is obvious. □

Now we specialize to the case of G-graded rings in which homogeneous elements are not zero-divisors and where the subgroups R_g all contain non-zero elements. This type of G-graded ring is a generalization of the group ring RG when R is an integral domain.

Corollary 3.11. *Let R be a G-graded ring in which homogeneous elements are not zero-divisors and for which $R_g \neq \{0\}$, for all $g \in G$. Let H be a subgroup of G. An element $a \in R_H$ is a zero-divisor in R_H if and only if it is a zero-divisor in R.*

Proof. Suppose $ab = 0$ with $a, b \in R$ non-zero. Multiply from the right by a suitable homogeneous element to produce $ab' = 0$ and such that b' is non-zero and has a support which intersects H non-trivially. This can be done by picking $g \in \mathrm{Supp}(b)$, and multiplying by an element $x \in R_{g^{-1}h}$, $h \in H$. Now

$$\pi_H(ab') = a\pi_H(b') = 0$$

and $\pi_H(b') \in R_H$ is non-zero. □

Lemma 3.12. *Let R be a G-graded ring in which homogeneous elements are not zero-divisors and for which $R_g \neq \{0\}$ for all $g \in G$. Then the support group of a central element of R is an FCC-group.*

Proof. Let $a = \sum_{g \in G} a_g$ be a non-zero central element of R and let $0 \neq x \in R_h$ be homogeneous. By the non-vanishing property we have that $a_g x \neq 0, x a_g \neq 0$ for all $g \in \mathrm{Supp}(a)$ and so $\mathrm{Supp}(xa) = \mathrm{Supp}(ax) = \mathrm{Supp}(a)h = h\,\mathrm{Supp}(a)$. It follows that $\mathrm{Supp}(a)$ is closed under conjugation by elements of G. Since the support is a finite set, it follows that each element of the support of a has only finitely many conjugates. It then follows as before that the support group of a is an FCC-group. □

Lemma 3.13. *Let G be a unique product group and R a G-graded ring in which non-zero homogeneous elements are not zero-divisors. Then R contains no non-trivial zero-divisor.*

Proof. Let a, b be two non-zero elements of R and gh be an element of G that is uniquely expressed as a product of an element of $\mathrm{Supp}(a)$ and an element of $\mathrm{Supp}(b)$. By the non-vanishing property, $a_g b_g \neq 0$ and so $ab \neq 0$. □

Proposition 3.14. *Let G be a torsion-free group and R a G-graded ring in which homogeneous elements are not zero-divisors and for which $R_g \neq \{0\}$, for all $g \in G$. Then R contains no non-trivial central zero-divisor.*

Proof. A central element $a \in R$ is an element of the subring R_H, where H is the support group of a. Since H is free abelian by Lemma 3.12 and Corollary 3.7, R_H contains no non-trivial zero-divisors, by Lemma 3.13. Hence a is not a zero-divisor in R, by Corollary 3.11. □

3.4 Zero-divisors and systems of polynomial equations

In this section we show how the non-existence of zero-divisors in KG for some particular field K implies the non-existence of zero-divisors in group rings constructed from another field. We do this by considering the coefficients of two general elements $a, b \in KG$ as indeterminate and showing how the assumption of $ab = 0$ leads us naturally to the construction of systems of polynomial equations and an inequation. We show that $\mathbb{C}G$ contains no non-trivial zero-divisors if and only if $\overline{\mathbb{Z}}G$ contains no non-trivial zero-divisors. By using the same idea, we show also how the special case of the zero-divisor conjecture for K being an arbitrary finite field implies the general case.

3.4.1 The field of complex numbers and the ring of algebraic integers

We start by showing that if group ring $\mathbb{C}G$ contains no non-trivial zero-divisors if and only if the group ring $\overline{\mathbb{Z}}G$ contains no non-trivial zero-divisors, where by $\overline{\mathbb{Z}}$ we mean the integral closure of $\mathbb{Z}$ in $\mathbb{C}$. This will apply without any assumptions on G, so in particular it will apply when G is torsion-free.

Assume that $a, b \in KG$ are two arbitrary elements. By the definition of multiplication in a group ring, the coefficients of ab are polynomials in the coefficients of a and b.

Example 3.15. Let $G = \mathbb{Z}/3\mathbb{Z} = \{1, g, g^2\}$ and assume that we are looking for zero-divisors in $\mathbb{C}G$. Let

$$a = x_a \cdot 1 + y_a \cdot g + z_a \cdot g^2$$

and

$$b = x_b \cdot 1 + y_b \cdot g + z_b \cdot g^2$$

be two general elements of $\mathbb{C}G$. A brief computation yields that

$$ab = (x_a x_b + y_b z_a + y_a z_b) \cdot 1 + (x_a y_b + x_b y_a + z_a z_b) \cdot g + (x_a z_b + y_a y_b + x_b z_z) \cdot g^2.$$

If we consider $x_a, y_a, z_a, x_b, y_b, z_b$ as variables, and if the product ab is supposed to equal zero, then each of the three coefficients of ab must be zero. We obtain in this way a system of polynomial equations.

Assume again that $a, b \in \mathbb{C}G$, and that we have $ab = 0$. As in the example above, we obtain from the (non-zero) coefficients of a and b a solution

$$s = (s_1, s_2, \ldots, s_n) \in \mathbb{C}^n$$

to a system of polynomial equations, where n is the size of the union of supports of a and b, the first few s_i are the coefficients of a and the last few s_i are coefficients of b. Note also that $0 \in \mathbb{C}^n$ is a common zero of these polynomials, and actually many other points are too. Some of these correspond to cases when a or b are zero.

In the example above, the polynomials are integral. It is easy to see from the definition of multiplication in $\mathbb{C}G$ that in general the polynomials in the system are integral (coefficients are, indeed, all equal to 1), and hence lie in $\mathbb{Z}[x_1, \ldots, x_n]$. Since the coefficients of the supports of a and b are non-zero, we also have that none of the coordinates of the solution $s \in \mathbb{C}^n$ is zero, and we could express this as $R(s_1, \ldots, s_n) = \prod_{i=1}^{n} s_i \neq 0$. This puts us precisely in a setting of the famous (strong form of) Nullstellensatz.

Theorem 3.16 (**Hilbert's Nullstellensatz**). *Let K be an algebraically closed field, and $P_1, \ldots, P_r, R$ finitely many polynomials in $K[x_1, \ldots, x_n]$. If the system*

$$\begin{aligned} P_1(x_1, \ldots, x_n) = \ldots = P_r(x_1, \ldots x_n) &= 0, \\ R(x_1, \ldots, x_n) &\neq 0, \end{aligned}$$

has no solution in K^n, then R is contained in the radical ideal generated by $P_1, \ldots, P_n$, i.e., there exist $Q_1, \ldots, Q_r \in K[x_1, \ldots, x_n]$ and an integer $m > 0$ such that

$$Q_1 P_1 + \ldots + Q_r P_r = R^m.$$

We will apply the Nullstellensatz to prove that if there are no non-trivial zero-divisors in the group ring $\overline{\mathbb{Q}}G$, then there are none in $\mathbb{C}G$. By $\overline{\mathbb{Q}}$ we mean the algebraic closure of the field of rational numbers. We have $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$ and $\overline{\mathbb{Q}}$ is an algebraically closed field.

Proposition 3.17. *The group ring $\overline{\mathbb{Q}}G$ contains no non-trivial zero-divisor if and only if $\mathbb{C}G$ contains no non-trivial zero-divisor.*

Proof. Of course, since $\overline{\mathbb{Q}} \subset \mathbb{C}$, one of the implications is obvious. To obtain the other implication, we will argue that if $\mathbb{C}G$ contains non-trivial zero-divisors, then $\overline{\mathbb{Q}}G$ also contains non-trivial zero-divisors. The proof will be constructive. So let us assume that

$$a = \sum_{i=1}^{k} s_i g_i,$$

$$b = \sum_{i=k+1}^{n} s_i g_i$$

are non-zero elements of $\mathbb{C}G$, and that $ab = 0$. We can of course assume that the coefficients $s_1, \ldots, s_n$ are non-zero. As indicated in the example above, the coefficients of ab are polynomials in the coefficients $s_1, \ldots, s_k$ of a and $s_{k+1}, \ldots, s_n$ of b. As explained above, we have a finite number of integral polynomials

$$P_1, \ldots, P_r, R \in \mathbb{Z}[x_1, \ldots, x_n]$$

and a solution $s = (s_1, \ldots, s_n) \in \mathbb{C}^n$ to the system of equations

$$P_1(s) = P_2(s) = \ldots = P_r(s) = 0,$$

and an inequation

$$R(s) = \prod_{i=1}^{n} s_i \neq 0.$$

Since $P_1, \ldots, P_r, R$ are integral polynomials, this system makes sense over $\overline{\mathbb{Q}}$ too. Seeking a contradiction, assume that the system has no solution in $\overline{\mathbb{Q}}^n$. Then we can apply Hilbert's Nullstellensatz, and obtain polynomials

$$Q_1, \ldots, Q_r \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$$

such that

$$Q_1 P_1 + \ldots + Q_r P_r = R^m.$$

But evaluating this at s, we obtain

$$0 = (R(s))^m \neq 0,$$

a contradiction. Therefore, we must have a point

$$t = (t_1, \ldots, t_n) \in \overline{\mathbb{Q}}^n$$

for which

$$P_1(t) = \ldots = P_n(t) = 0$$

and

$$R(t) \neq 0.$$

Now let a', b' be the elements of $\overline{\mathbb{Q}}G$ with supports equal to a and b respectively, and with coefficients obtained from $t = (t_1, \ldots, t_n)$. More precisely, we let

$$a' = \sum_{i=1}^{k} t_i g_i$$

and

$$b' = \sum_{i=k+1}^{n} t_i g_i.$$

By construction, the coefficients of the product $a'b'$ are equal precisely to $P_i(t) = 0$. The equation

$$R(t) = \prod_{i=1}^{n} t_i \neq 0$$

means that neither a' or b' is equal to zero. Hence $a'b' = 0$, and we have obtained zero-divisors in $\overline{\mathbb{Q}}G$. □

Remark. Note that we did not really use any intrinsic properties of the fields $\overline{\mathbb{Q}}$ except for the containment $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$ and the property that the former is an algebraically closed field. In particular, this argument is independent of the characteristic of the fields involved. We will use this more general result in the forthcoming sections (see Lemma 3.27 below).

Remark. The supports of the elements a', b', constructed in the course of the proof of the proposition equal, the supports of a and b, respectively. This is because $\prod_{i=1}^{n} t_i \neq 0$ which means that none of the t_i is zero.

Showing that $\overline{\mathbb{Q}}$ contains no non-trivial zero-divisor if $\overline{\mathbb{Z}}G$ does not requires only an elementary argument. It is shown by clearing denominators of coefficients of possible zero-divisors in $\overline{\mathbb{Q}}G$, because $\overline{\mathbb{Q}}$ is the field of fractions of $\overline{\mathbb{Z}}$. In general, if K is the field of fractions of an integral domain D, then DG contains a non-trivial zero-divisor if and only if KG contains a non-trivial zero-divisor.

Proposition 3.18. *$\overline{\mathbb{Q}}$ is the field of fractions of $\overline{\mathbb{Z}}$. Moreover, for any $a \in \overline{\mathbb{Q}}$ there exists an integer n such that $na \in \overline{\mathbb{Z}}$.*

Proof. It suffices to prove the second claim. If $a \in \overline{\mathbb{Q}}$ then we have an equation

$$a^m + c_{m-1}a^{m-1} + \ldots + c_1 a + c_0 = 0,$$

where the c_i's are rational. There certainly exists an integer n such that $nc_i \in \mathbb{Z}$ for all i, for example, the product of the denominators of the c_i. Multiply the equation above by n^m to obtain

$$(na)^m + c_{m-1}n(na)^{m-1} + \ldots + c_1 n^{m-1}(na) + c_0 n^m = 0,$$

which shows that $na \in \overline{\mathbb{Z}}$. □

We arrive at the following proposition.

Proposition 3.19. *Let G be a group. The following assertions are equivalent:*

(i) *$\mathbb{C}G$ contains no non-trivial zero-divisor;*

(ii) *$\overline{\mathbb{Q}}G$ contains no non-trivial zero-divisor;*

(iii) *$\overline{\mathbb{Z}}G$ contains no non-trivial zero-divisor.*

3.4.2 Fields of characteristic zero

It is well-known that the validity of the zero-divisor conjecture in the case of $\mathbb{C}$ also implies its validity for any field of characteristic 0. This is a consequence of the below observation, which is often useful, and which we already used in the proof of the corollary to Kaplansky's theorem in Chapter 2.

Proposition 3.20. *Let F be a countable field of characteristic 0. Then there exists an embedding of F into the field of complex numbers $\mathbb{C}$.*

Proof. Since we certainly can embed the prime subfield of F into $\mathbb{C}$, we can use an elementary argument involving Zorn's lemma to obtain a pair (K, σ) of a subfield K of F and a field embedding $\sigma : K \to \mathbb{C}$ that is maximal in the sense that if $K \subseteq K'$ and $\sigma' : K' \to \mathbb{C}$ is an embedding which coincides with σ on K, then $K = K'$ and $\sigma = \sigma'$.

Let K be a field that is maximal in the above sense. If $K \subsetneq F$, then take some $a \in F \setminus K$. We must consider two cases. If a is algebraic over K, then it has a corresponding minimal polynomial $p(x) \in K[x]$, and the degree of $p(x)$ must be at least 2 by the assumption that $a \in F \setminus K$. The embedding $\sigma : K \to \mathbb{C}$ induces naturally an isomorphism of rings $K[x] \cong \sigma(K)[x]$ and so the isomorphic image of $p(x)$ must be irreducible of degree at least 2. Since $\sigma(K) \subset \mathbb{C}$ and $\mathbb{C}$ is algebraically closed, we have a corresponding root $b \in \mathbb{C} \setminus \sigma(K)$. Then we easily obtain an extension isomorphism $K(a) \cong \sigma(K)(b)$ by mapping a to b. This contradicts the maximality of the pair (K, σ).

On the other hand if a is transcendental over K, then noting that since K is countable, $\sigma(K)$ has a countable algebraic closure in $\mathbb{C}$, and so there are plenty of elements in $\mathbb{C}$ which are transcendental over $\sigma(K)$. Take any such element and extend the isomorphism σ by mapping a to any element of $\mathbb{C}$ which is transcendental over $\sigma(K)$. This again contradicts the maximality of (K, σ). We conclude that $K = F$. □

Corollary 3.21. *Assume that the complex group ring $\mathbb{C}G$ contains no non-trivial zero-divisor. Then for any field K of characteristic 0 the group ring KG contains no non-trivial zero-divisor.*

Proof. For any non-zero $a, b \in KG$ we can construct a finitely generated subfield

$$F = \mathbb{Q}\big(\operatorname{Supp}(a), \operatorname{Supp}(b)\big)$$

of K such that $a, b \in FG \subseteq KG$. Since F is countable, the proposition implies that we have an embedding $\phi : F \to \mathbb{C}$. This induces a ring embedding of $\phi(F)G$ into $\mathbb{C}G$. Since $FG \cong \phi(F)G \subseteq \mathbb{C}G$, we must have $ab \neq 0$, and therefore KG contains no non-trivial zero-divisor. □

It would be interesting to know if the case of $K = \mathbb{C}$ also implies the conjecture for fields of positive characteristic, and hence if the zero-divisor conjecture can be solved by considering $\mathbb{C}$ alone. Currently there is nothing that indicates that this should be the case, and indeed for many classes of groups G, the non-existence of non-trivial zero-divisor has only been established for fields of characteristic 0.

3.4.3 Reduction to finite fields

Next we show that if the zero-divisor conjecture holds for all finite fields, then it holds for all fields. Hence we show that if for all finite fields K the group ring KG contains no non-trivial zero-divisors, then non-trivial zero-divisor conjecture holds in general, for all fields. In essence, this is a consequence of the Nullstellensatz and the fact that fields which are finitely generated $\mathbb{Z}$-algebras are always finite fields. For the proof we need a couple of well-known results from commutative algebra.

Proposition 3.22. *Let A, B, C be commutative rings with identity, with A being Noetherian and*

$$A \subseteq B \subseteq C.$$

If C is a finitely generated as an A-algebra and C is finitely generated as a B-module, then B is finitely generated as an A-algebra.

Proposition 3.23 (**Zariski's lemma**)**.** *Let A be a field and K a finitely generated A-algebra which is a field. Then K is a finite algebraic extension of A.*

Proofs of the above two statements can be found in many textbooks on commutative algebra, for example in [1]. The below lemma below is listed as an exercise in [1].

Lemma 3.24. *Let F be a field that is finitely generated as a ring. Then F is a finite field.*

Remark. By a *finitely generated ring* R we mean a ring which is finitely generated over some quotient ring of $\mathbb{Z}$.

Proof. First we show that the characteristic of F must be prime. Otherwise it is zero, and with that assumption we will reach a contradiction. Indeed, we then have the inclusions

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq F = \mathbb{Z}[x_1, x_2, \ldots, x_n]$$

where $x_1, x_2, \ldots, x_n$ are the finitely many generators of F over $\mathbb{Z}$. In particular, F is a finitely generated $\mathbb{Q}$-algebra, so it is a finite algebraic extension of $\mathbb{Q}$ by Zariski's lemma. Therefore, it is a finite-dimensional vector space over $\mathbb{Q}$. Since $\mathbb{Z}$ is certainly Noetherian, we apply the first of the above two propositions to conclude that $\mathbb{Q}$ is a finitely generated $\mathbb{Z}$-algebra. But this certainly cannot be the case, for then only finitely many primes could be found among factors of the denominators of rational numbers. It follows that F must have characteristic $p > 0$, and so $F = \mathbb{F}_p[x_1, x_2, \ldots, x_n]$. Applying Zariski's lemma again, to $\mathbb{F}_p \subseteq F$, we get that F is a finite-dimensional vector space over $\mathbb{F}_p$, and therefore finite. □

Proposition 3.25. *If the zero-divisor conjecture holds for all finite fields, then it holds for the field of complex numbers $\mathbb{C}$.*

Proof. Take any two non-zero elements $a, b \in \mathbb{C}G$. We will show that $ab \neq 0$. Let R be the subring of $\mathbb{C}$ generated over $\mathbb{Z}$ by the coefficients of a and b and by the inverses of these coefficients. Then a, b are elements of RG. Take any maximal ideal M of R and construct the quotient ring R/M. Since R is a finitely generated ring, R/M is a finitely generated field, and so it is a finite field by Lemma 3.24. Let $\pi : RG \to (R/M)G$ be the group ring homomorphism induced by the natural projection map. Since the coefficients of both a and b are units in R, they are not contained in M, and so $\pi(a)$ and $\pi(b)$ are non-zero in $(R/M)G$. They satisfy $0 \neq \pi(a)\pi(b) = \pi(ab)$. It therefore follows that $ab \neq 0$, and so $\mathbb{C}G$ contains no non-trivial zero-divisor. □

The following result is now an immediate consequence of Corollary 3.21.

Corollary 3.26. *If the zero-divisor conjecture holds for all finite fields, then it holds for all fields of characteristic 0.*

We have hence shown that the validity of the conjecture for all finite fields implies the validity of the conjecture for all fields of characteristic 0. What is left to do is to show that if a non-trivial zero-divisor exists in an group ring KG, where K is an infinite field of characteristic $p > 0$, then there also exists a zero-divisor in a group ring FG where F is a finite field. This follows again from the Nullstellensatz.

Lemma 3.27. *Let K be a field of characteristic $p > 0$ and a, b non-zero elements of KG for which we have $ab = 0$. Then there exists a finite field F of characteristic $p > 0$ and elements a', b' of FG for which we have $a'b' = 0$.*

Proof. Let $S \subseteq K$ be the finite set which is the union of coefficients of a and b. Let Ω be the algebraic closure of $\mathbf{F}_p$, the prime subfield of the field K. Let L be some field containing both Ω and S. For example, take L to be the algebraic closure of K. We have $a, b \in LG$, $ab = 0$ in LG, and so LG contains non-trivial zero-divisors. Arguing exactly as we did in the proof of Proposition 3.17, this gives us a system of polynomial equations and an inequation, with coefficients in $\mathbf{F}_p$. If no non-zero point of Ω^n was a solution to this system of polynomial equations, then again we reach a contradiction exactly in the same way as we did in the proof of the aforementioned proposition. Hence there exists a solution $t = (t_1, t_2, \ldots, t_n) \in \Omega^n$ such that $t_i \neq 0$ for all i. Again, repeating the argument of Proposition 3.17, we construct from the coordinates of t a pair of non-zero elements $a', b' \in \Omega G$ such that $a'b' = 0$. Since the coefficients of a' and b' are algebraic over $\mathbf{F}_p$, we can construct a finite field F by adjoining the coefficients of a', b' to $\mathbf{F}_p$. Then $a', b' \in FG$ and $a'b' = 0$, so the proof is complete. □

Using Corollary 3.26, Lemma 3.27 and Corollary 3.21, we arrive at the following result.

Theorem 3.28. *Let G be a group. The following two assertions are equivalent:*

(i) *For any field K, the group ring KG contains no non-trivial zero-divisor;*

(ii) *For any finite field K, the group ring KG contains no non-trivial zero-divisor.*

In particular, this holds for G torsion-free.

While this result might be slightly amusing, it surely brings us nowhere closer to a proof of Kaplansky's zero-divisor conjecture. This is partly because the 'harder' of the cases seems to be when the characteristic is indeed prime, as evidenced by works of Formanek, Farkas and Snider, which settle related questions for characteristic 0, but not for characteristic $p > 0$. It would be far more interesting to show that the case of $K = \mathbb{C}$ implies results for fields of non-zero characteristic.

One could also claim that, in some sense, the main difficulty of the problem lies in the complexity of the class of torsion-free groups. Any partial results so far obtained have dealt with a subclass of torsion-free groups. For example, the polycyclic-by-finite

ones or supersolvable ones. In both cases the additional hypotheses imply some finiteness conditions on the groups in question. By playing around with the coefficient rings we are avoiding the main difficulty, which has to be handled sooner or later.

Chapter 4

Unit and direct-finiteness conjectures

In this last brief chapter we introduce the last of the three famous conjectures concerning elements in group rings. We show that, perhaps a little surprisingly, it implies the other two. We briefly discuss the question of direct-finiteness of group rings and how Kaplansky's trace theorem settles this question for the case of characteristic 0.

4.1 Units and the unit conjecture

Clearly $G \subseteq RG$ consists of units, and if $r \in R$ is a unit, then $rg \in RG$ is a unit for each $g \in G$. Such units of RG we call *trivial*. Are there any others? Again, in the case when R is a field and G is torsion-free, no examples of non-trivial units are known to exist. If $K = \mathbb{C}$, then the slightly larger ring $L^1(G)$ contains plenty of units. This is because $L^1(G)$ is a Banach algebra, and so any element at small distance from 1 is invertible.

Conjecture. *Let K be a field and G a torsion-free group. Then KG contains no non-trivial unit.*

This third conjecture is actually the strongest of the three conjectures presented in this paper, the other two being the ones regarding zero-divisors and idempotent elements. This follows from a theorem of Connell [3], which asserts that if G is torsion-free, then KG is a *prime ring*.

Lemma 4.1. *[3] Let G be a torsion-free group and K a field. Then KG is a prime ring, i.e., if A, B are two non-zero ideals of KG, then $AB \neq \{0\}$.*

Proposition 4.2. *[9] Let G be a torsion-free group. If KG contains non-trivial zero-divisors, then it contains non-trivial units.*

Proof. By the above result of Connell's, we know that KG is a prime ring. If $ab = 0$ in KG, with $a, b \neq 0$, then consider the principal ideals A and B, generated by a and b respectively. Then A is the set of finite sums of elements on the form rar', for $r, r' \in KG$, and similarly for B. Since $BA \neq \{0\}$, a product of at least one pair of such sums from

B and from A is non-zero. In particular, an element on the form $rbr'ar'', r, r', r'' \in KG$ must be non-zero, and hence $br'a$ must be non-zero. Then the element $c = br'a$ has square zero, for $c^2 = br'(ab)ra = 0$ and hence $1 - c, 1 + c$ are inverses of each other. One sees that c must have an element in its support which is different from $1 \in G$, for otherwise it could not possibly square to zero. Hence it follows that $1 - c, 1 + c$ are non-trivial units in KG. □

It is true that *global* invertibility of an element $a \in RG$ is equivalent to *local* invertibility of a for each subgroup H of G such that RH contains a. Therefore, like in the case of zero-divisors, invertibility of an element can be studied on the level of its support group.

Proposition 4.3. *[9] Let H be a subgroup of G. Then $a \in RH$ is (left/right) invertible in RH if and only if it is (left/right) invertible in RG.*

Proof. One direction is obvious. Now let $b \in RG$ be such that $ab = ba = 1$. By Proposition 1.9, we see that

$$1 = \pi_H(ab) = a\pi_H(b).$$

Similarly we have $\pi_H(b)a = 1$. □

Remark. As was the case with the corresponding result for zero-divisors, it also follows easily from the above result that no (left/right) invertible element of KG, G torsion-free, could have a support of size 2. If the claim would be false, then there is no loss of generality in assuming that a hypothetical unit a is on form $a = 1 + rg$. By the proposition this is a unit in the group ring KH, where H is the support group of a. Then H is infinite cyclic generated by g. But in that case $KH \cong K[x, x^{-1}]$, with a corresponding to the element $1 + rx$. One can fairly easily check that such an element could not possibly be invertible in $K[x, x^{-1}]$. This is a contradiction.

4.2 Direct-finiteness of group rings

Another very interesting conjecture related to invertibility is the question of direct finiteness of KG. A ring R is *directly finite* if whenever $a, b \in R$ are such that $ab = 1$, then we also have that $ba = 1$. All rings are not directly finite, as evidenced by the left and right shift operators on the space of sequences $(a_0, a_1, a_2, \ldots)$.

Conjecture. *Let K be a field and G a group. Then KG is directly finite.*

Playing around with the equations one sees that $ab = 1$ implies $(ba - 1)b = 0$, and so if a ring lacks non-trivial zero-divisors, then it is directly finite. Therefore, the direct finiteness conjecture is implied by both the zero-divisor conjecture and the unit conjecture. The case of fields of characteristic 0 has been settled by Kaplansky, using traces, and we show this below. The case of fields of positive characteristic is open up until today, and even the seemingly simpler case when $K = \mathbb{F}_2$ has not yet been settled. We remark that the case of G being finite is trivial, regardless of characteristic.

Proposition 4.4. *Let A be a finite-dimensional unital algebra over a field K. Then A is directly finite.*

Proof. Because every element of A acts on A by left (or right) multiplication and does so faithfully, we get an injective ring homomorphism of A into the ring of linear transformations on the vector space A, and hence into a matrix ring. Now the claim follows from the basic fact that $MN = 1$ implies $NM = 1$ for matrices. □

Remark. A slight generalization of the above is possible, for we can replace a finite-dimensional algebra by any left-Noetherian ring. To see this, note that the equation $ab = 1$ induces a left(!) R-module homomorphism $S : R \to R$ given by $x \mapsto xb$. By the assumption, this map is surjective, for $S(xa) = x$. But since R is left-Noetherian, S is also injective. To see this, note that $\ker(S) \subseteq \ker(S^2) \subseteq \dots$ forms an ascending chain of left ideals of R, which must stabilize at some $n > 1$. Now take some $x \in \ker(S)$. By surjectivity, we find $y \in R$ such that $S^n(y) = x$, which implies $S^{n+1}(y) = S(x) = 0$. Hence $y \in \ker(S^{n+1}) = \ker(S^n)$, and so $x = S^n(y) = 0$, so $\ker(S)$ contains only the zero element. It follows that for all non-zero $x \in R$, we have $xb \neq 0$. But then $ab = 1 \Rightarrow bab = b \Rightarrow (ba - 1)b = 0$ and so $ba - 1 = 0$.

Kaplansky's theorem on trace of idempotents is enough to prove that KG is directly finite if the characteristic of K is zero.

Theorem 4.5. *Let K be a field of characteristic 0. Then KG is directly finite.*

Proof. Let $ab = 1$. Then ba is easily seen to be an idempotent. But

$$1 = \mathrm{tr}(ab) = \mathrm{tr}(ba)$$

so ba is an idempotent of trace 1. If F is the subfield of K generated over $\mathbb{Q}$ by the coefficients of the support of ba, then K can be embedded into $\mathbb{C}$. Consequently FG embeds into $\mathbb{C}G$ and as an element of $\mathbb{C}G$, ba still has trace 1, and so $ba = 1$ in $\mathbb{C}G$ by Kaplansky's theorem. Since the embedding respects units, $ba = 1$ in FG, and hence in KG. □

Hence a statement of algebraic nature has been settled using Kaplansky's theorem, a results so far only proven by methods of analysis. Another interesting example of such beneficial interaction between algebra and analysis can be found in the proof of Jacobson semisiplicity of the complex group ring $\mathbb{C}G$, found in [9]. In that work, Passman presents the result, which was initially obtained by Rickart, and its proof relies on elementary complex analysis.

Bibliography

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*. Westview Press, 1969.

[2] R. G. Burns, *Central idempotents in group rings*. Canad. Math. Bull. Vol 13 (4), 1970.

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

[4] E. Formanek, *Idempotents in Noetherian group rings*. Canad. J. Math. 25 (1973), 366-369.

[5] N. Jacobson *Basic Algebra II*. Dover Publications, Inc., Mineola, New York, 2009.

[6] I. Kaplansky, *Rings of operators*. W. A. Benjamin Inc., New York, 1968

[7] M. S. Montgomery, *Left and right inverses in group algebras*. Bull. Amer. Math. Soc. Volume 75, Number 3 (1969), 471-624

[8] B. H. Neumann, *Groups with finite classes of conjugate elements*. Proc. London. Math. Soc 1 (1951), 178-187.

[9] D. S. Passman, *The Algebraic Structure of Group Rings*. Dover Publications, Inc., Mineola, New York, 2011

[10] S. D. Promislow, *A simple example of a torsion-free, nonunique product group*. Bull. London Math. Soc. 20 (1988), no. 4, 302-304.

[11] W. Rudin, H. Schneider, *Idempotents in group rings*. Duke Math. J. 31 (1964), 585-602

Master's Theses in Mathematical Sciences 2014:E45
ISSN 1404-6342

LUTFMA-3265-2014

Mathematics
Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund, Sweden

http://www.maths.lth.se/