IDEMPOTENTS IN GROUP RINGS

By Walter Rudin and Hans Schneider

Introduction. Suppose G is a group and R is a ring. The *support* of a function f from G to R is the set of all $x \in G$ at which $f(x) \neq 0$. The *support group* of f is the smallest subgroup of G which contains the support of f. The *group ring* RG is the set of all R-valued functions on G whose support is finite, with pointwise addition and convolution as multiplication [2; 44]:

$$(f * g)(x) = \sum_{y \in G} f(xy^{-1})g(y) \qquad (x \in G). \tag{0.1}$$

It is then easily verified that RG satisfies the ring axioms; in fact, RG is a linear algebra over R.

(We write all groups multiplicatively, and denote group identities by 1; we also use 1 for the unit element of R if there is one.)

If R, in addition to being a ring, is a Banach algebra (i.e., an algebra over the complex field K, with a submultiplicative norm which makes R a Banach space), then we can consider the larger ring $R^1(G)$ which consists of those R-valued functions f on G, with possibly infinite support, for which the norm

$$||f|| = \sum_{x \in G} |f(x)| \tag{0.2}$$

is finite. (We have used absolute-value signs to denote the norm in R, and shall continue to do so. The superscript 1 in $R^1(G)$ is to indicate that we are dealing with an L^1-norm, i.e., that we are adding the *first* powers of $|f(x)|$ in (0.2).)

Convolution in $R^1(G)$ is defined by (0.1), and it is easy to see that the norm (0.2) is submultiplicative, i.e., that

$$||f * g|| \leq ||f||\,||g|| \qquad (f, g \in R^1(G)) \tag{0.3}$$

and that $R^1(G)$ is itself a Banach algebra.

An *idempotent* in a ring is an element of the ring which is its own square. Accordingly the idempotents in RG, or in $R^1(G)$, are those functions which satisfy

$$f(x) = \sum_{y \in G} f(xy^{-1})f(y) \qquad (x \in G). \tag{0.4}$$

For example, if G is a finite group, of order n, if γ is a *complex character* of G, i.e., a complex function on G such that $|\gamma(x)| = 1$ and

$$\gamma(xy) = \gamma(x)\gamma(y) \qquad (x, y \in G), \tag{0.5}$$

Received July 11, 1963. The research of the first author was supported by NSF Grant GP-249, that of the second author by NSF Grant G-19052, and by the Mathematics Research Center, U. S. Army, Madison, Wisconsin, under Contract No. DA-11-022-ORD-2059.

and if $f(x) = \gamma(x)/n$, then f is an idempotent in KG. (We recall that K denotes the complex field.)

The origin of the present paper lies in the following result [7] [1] [8]:

THEOREM A. *If G is a commutative group, then every idempotent in $K^1(G)$ has a finite support group.*

The existing proofs of this theorem deal with a more general situation (namely with idempotent measures on locally compact abelian groups; the conclusion is that every measure of this kind has a *compact* support group) and depend on the Pontryagin duality theory and on Fourier-Stieltjes transforms.

In the present paper we give very simple proofs of an extension of Theorem A (K is replaced by any commutative Banach algebra B) and of a purely algebraic analogue (Theorems 2.3 and 3.4.). We also give a fairly complete description (for any G) of the idempotents in $B^1(G)$ whose norm is 1. §IV contains examples which show to what extent commutativity is really needed in the preceding results. §§ V and VI contain results which are motivated by the proof of Theorem 3.4.

I. **Preliminaries.** We begin by assembling some facts which will be useful later.

If R has a unit element 1 and if $u \in RG$ is defined by

$$u(1) = 1, \qquad u(x) = 0 \quad \text{for} \quad x \neq 1, \tag{1.1}$$

then it is clear that u is the unit element of RG. The converse is also true:

1.1. THEOREM. *If G is a group and R is a ring, and if RG has a unit element, then so does R.*

Proof. Suppose e is the unit in RG. Fix $\alpha \in R$, define $f(1) = \alpha$, $f(x) = 0$ if $x \neq 1$, $x \in G$. Since $f * e = f = e * f$, and since the definition of convolution shows that $(f * e)(1) = \alpha e(1)$, $(e * f)(1) = e(1)\alpha$, we see that R has $e(1)$ as unit element.

1.2. THEOREM. *Suppose G is a group, ψ is a homomorphism of a ring R onto a ring $\bar{R}$, J is the kernel of ψ, and $\bar{\psi}$ is the mapping of RG into $\bar{R}G$ defined by*

$$(\bar{\psi}f)(x) = \psi(f(x)) \qquad (x \in G). \tag{1.2}$$

Then $\bar{\psi}$ is a homomorphism of RG onto $\bar{R}G$ with kernel JG.

In particular, $(R/J)G$ and RG/JG are isomorphic.

The proof is a matter of straightforward verification.

We turn to the characterization of the center of RG; recall that the *center* of a ring consists of those elements which commute with every element of the ring.

We let C_R be the center of R (this is a commutative subring of R) and we let N_R be the annihilator ideal of R, i.e., the set of those $\lambda \in R$ for which

$$\lambda\alpha = \alpha\lambda = 0 \tag{1.3}$$

for all $\alpha \in R$. Note that $N_R \subset C_R$.

A function $f \in RG$ is called a *class function* if f is constant on each conjugacy class of G. This means that

$$f(xy) = f(yx) \tag{1.4}$$

for all $x, y \in G$.

1.3. THEOREM. *The center of RG consists of all f of the form*

$$f = f_1 + f_2 , \tag{1.5}$$

where f_1 is a class function, $f_1 \in C_R G$, and $f_2 \in N_R G$.

If f is a central idempotent of RG, then f is a class function.

Proof. Suppose f is in the center of R. Fix $y \in G$, $\lambda \in R$, define $g(y) = \lambda$, $g(x) = 0$ for all other $x \in G$. Then

$$\lambda f(y^{-1}x) = (g * f)(x) = (f * g)(x) = f(xy^{-1})\lambda. \tag{1.6}$$

Taking $y = 1$, it follows that $\lambda f(x) = f(x)\lambda$ for all $x \in G$, so that $f \in C_R G$.

This shows that (1.6) can be rewritten in the form

$$[f(y^{-1}x) - f(xy^{-1})]\lambda = 0 \qquad (x, y \in G; \quad \lambda \in R). \tag{1.7}$$

Hence, replacing x by yx, we see that

$$f(x) - f(yxy^{-1}) \in N_R \qquad (x, y \in G). \tag{1.8}$$

If we now pick one element x_i in each conjugacy class of G, and if we define

$$f_1(yx_iy^{-1}) = f(x_i) \qquad (y \in G), \tag{1.9}$$

then f_1 is a class function, and (1.8) shows that $f - f_1 \in N_R G$. Thus f is of the form (1.5).

Conversely, if $f = f_1 + f_2$, as in (1.5), it is immediate that f_1 and f_2 are both in the center of RG; in fact $f_2 * g = g * f_2 = 0$ for every $g \in RG$. Hence if f is a central idempotent, we have

$$f_1 + f_2 = f = f * f = (f_1 + f_2) * (f_1 + f_2) = f_1 * f_1 .$$

It is easily seen that the convolution of two class functions is again a class function. Since $f_2 = f_1 * f_1 - f_1$, f_2 is a class function, and so is f.

This completes the proof.

Note. Theorem 1.3 is of course equally valid with $B^1(G)$ in place of RG, where B is any Banach algebra.

1.4 THEOREM. *Suppose G is the direct product of two groups G_1 and G_2, and R is a ring. Consider the elements of G as ordered pairs (x, y), with $x \in G_1$, $y \in G_2$.*

For each $f \in RG$ and for each $y \in G_2$, let $F(y)$ be the element of RG_1 defined by

$$(F(y))(x) = f(x, y) \qquad (x \in G_1). \tag{1.10}$$

Then $F \in (RG_1)G_2$, and the mapping $f \to F$ is an isomorphism of RG onto $(RG_1)G_2$.

Proof. Writing $F = \psi f$, it is easy to see that ψ is a $1 - 1$ mapping of RG onto $(RG_1)G_2$ and that ψ preserves sums. We have to check that ψ also preserves convolutions.

Suppose $F_1 = \psi f_1$, $F_2 = \psi f_2$. We have

$$(F_1 * F_2)(y) = \sum_{t \in G_2} F_1(yt^{-1}) * F_2(t) \qquad (y \in G_2). \tag{1.11}$$

Note that we have convolutions in the sum (1.11), since this is how multiplication is defined in RG_1 . By (1.11) we have

$$\begin{aligned}((F_1 * F_2)(y))(x) &= \sum_t (F_1(yt^{-1}) * F_2(t))(x) \\ &= \sum_{s,t} (F_1(yt^{-1}))(xs^{-1})(F_2(t))(s) \\ &= \sum_{s,t} f_1(xs^{-1}, yt^{-1}) f_2(s, t) = (f_1 * f_2)(x, y)\end{aligned}$$

for any $x \in G_1$, $y \in G_2$ (in the sums, s ranges over G_1 , t ranges over G_2). This completes the proof.

1.5. *Remark.* If H is a subgroup of G, then RH is clearly isomorphic with the subring of RG which consists of all $f \in RG$ whose support lies in H, and hence RH may be regarded as a subring of RG. In particular, the elements of RG whose support lies in the trivial subgroup $\{1\}$ form a subring of RG isomorphic to R.

II. Group rings over Banach algebras.

2.1. Lemma. *If x and y are distinct idempotents in a Banach algebra B, and if $xy = yx$, then*

$$|x - y| \geq 1.$$

Proof. Put $z = x - y$. Since x and y are commuting idempotents, we have $z^3 = z$. Since $z \neq 0$ and since the norm in B is submultiplicative, it follows that

$$0 < |z| = |z^3| \leq |z|^3.$$

Thus $|z| \geq 1$.

2.2. Theorem. *If H is the support group of a central idempotent $f \in B^1(G)$, where B is any Banach algebra and G is any group, and if H' is the commutator subgroup of H, then H/H' is finite.*

We recall that H' is the subgroup of H generated by the elements $aba^{-1}b^{-1}$ ($a, b \in H$), and that H' is the smallest normal subgroup of H such that H/H' is commutative.

Proof. Since every infinite commutative group has infinitely many complex characters, and since distinct characters of H/H' give rise to distinct characters of H, it is sufficient to prove that H has only finitely many complex characters.

Suppose $f \neq 0$. Then H is generated by the support S of f, and we may regard f as an element of $B^1(H)$.

Let γ be a complex character of H, and put $g(x) = \gamma(x)f(x)$. Since $|\gamma(x)| = 1$, $g \in B^1(H)$; in fact, $||g|| = ||f||$. Since $f * f = f$, we have, for $x \in H$,

$$(g * g)(x) = \sum_{y \in H} \gamma(xy^{-1})f(xy^{-1})\gamma(y)f(y) = \gamma(x) \sum_{y \in H} f(xy^{-1})f(y) = g(x),$$

so that g is idempotent.

By Theorem 1.3, f is a class function whose range is in the center of B. Since γ is a class function, the same is true of g, and so g is a *central* idempotent, by Theorem 1.3.

If γ_i and γ_j are distinct complex characters of H, then they must differ at some element of the generating set S; hence $\gamma_i f \neq \gamma_j f$. The preceding paragraph shows that $\gamma_i f$ and $\gamma_j f$ are commuting idempotents. Applying Lemma 2.1 to the Banach algebra $B^1(H)$, it follows that

$$||\gamma_i f - \gamma_j f|| \geq 1. \tag{2.1}$$

Assume now that H has infinitely many complex characters. Since S is at most countable, the diagonal process yields a sequence $\{\gamma_i\}$ of distinct characters of H such that $\lim \gamma_i(x)$ exists, as $i \to \infty$, for every $x \in S$. Since $|\gamma_i(x)| = 1$ and $\Sigma\, |f(x)| < \infty$, it follows that

$$\lim_{i \to \infty} ||\gamma_i f - \gamma_{i+1} f|| = \lim_{i \to \infty} \sum_{x \in S} |\gamma_i(x) - \gamma_{i+1}(x)|\, |f(x)| = 0,$$

in contradiction to (2.1).

Hence H has only finitely many complex characters, and the proof is complete.

2.3. THEOREM. *If G is a commutative group and B is a commutative Banach algebra, then every idempotent in $B^1(G)$ has finite support group.*

Proof. Since $B^1(G)$ is commutative, and since commutative groups have trivial commutator subgroups, this is a corollary of Theorem 2.2.

2.4. We can complete the information contained in Theorem 2.3 by explicitly determining all idempotents in RG, if G is a finite commutative group and if R is a linear algebra over the complex field K; we do not require that R is normed, nor that R is commutative. The Fourier transform furnishes the natural tool for this purpose.

The following facts about characters are needed: The set Γ of all complex characters of G is a group (the *dual* group of G) under pointwise multiplication:

$$(\gamma_1\gamma_2)(x) = \gamma_1(x)\gamma_2(x) \qquad (x \in G). \tag{2.2}$$

If G has n elements, so does Γ, and if $x \in G$ and $x \neq 1$, then $\gamma_0(x) \neq 1$ for some $\gamma_0 \in \Gamma$. Since, for any $x \in G$ and any $\gamma_0 \in \Gamma$,

$$\sum_{\gamma \in \Gamma} \gamma(x) = \sum_{\gamma \in \Gamma} (\gamma_0\gamma)(x) = \gamma_0(x) \sum_{\gamma \in \Gamma} \gamma(x), \tag{2.3}$$

we obtain the orthogonality relation

$$\frac{1}{n} \sum_{\gamma \in \Gamma} \gamma(x) = \begin{cases} 1 & \text{if } x = 1, \\ 0 & \text{if } x \neq 1. \end{cases} \tag{2.4}$$

If now $f \in RG$, where R is a linear algebra over K, we define the Fourier transform of f by

$$\hat{f}(\gamma) = \sum_{y \in G} \gamma(y^{-1}) f(y) \qquad (\gamma \in \Gamma). \tag{2.5}$$

Then $\hat{f} \in R\Gamma$. If $h = f * g$, (2.2) shows that

$$\begin{aligned} \hat{h}(\gamma) &= \sum_{y} \gamma(y^{-1}) \sum_{z} f(z) g(z^{-1}y) \\ &= \sum_{z} \gamma(z^{-1}) f(z) \sum_{y} \gamma(y^{-1}z) g(z^{-1}y) \\ &= \sum_{z} \gamma(z^{-1}) f(z) \hat{g}(\gamma) = \hat{f}(\gamma)\hat{g}(\gamma) \end{aligned} \tag{2.6}$$

and (2.4) gives the inversion formula

$$\begin{aligned} \frac{1}{n} \sum_{\gamma} \gamma(x) \hat{f}(\gamma) &= \frac{1}{n} \sum_{\gamma} \gamma(x) \sum_{y} \gamma(y^{-1}) f(y) \\ &= \sum_{y} f(y) \frac{1}{n} \sum_{\gamma} \gamma(xy^{-1}) = f(x). \end{aligned} \tag{2.7}$$

If $f * f = f$, (2.6) shows that $\hat{f}(\gamma)$ is an idempotent in R, for each $\gamma \in \Gamma$; (2.7) shows how f is determined by its Fourier transform. Combining these facts, we have a proof of the following result:

2.5. THEOREM. *If G is a commutative group of order n, and if R is a linear algebra over the complex field, then the idempotents in RG are the functions of the form*

$$f(x) = \frac{1}{n} \sum_{\gamma \in \Gamma} \gamma(x) e_\gamma \qquad (x \in G), \tag{2.8}$$

where each e_γ is an idempotent in R, and where Γ is the dual group of G.

We conclude this section with a theorem [9] about idempotents of norm 1. Note that no non-zero idempotent in a Banach algebra can have norm less than 1, by Lemma 2.1.

2.6. THEOREM. *Suppose G is a group, B is a Banach algebra, $f \in B^1(G)$, $f * f = f$, and $\|f\| = 1$. Then the support of f is a finite subgroup H of G, and if n is the order of H, we have*

$$|f(x)| = 1/n \qquad (x \in H). \tag{2.9}$$

If, furthermore, the unit ball of B is strictly convex (in particular, if B is the complex field), or if B is commutative and semi-simple, then f satisfies the functional equation

$$f(xy) = nf(x)f(y) \qquad (x, y \in H). \tag{2.10}$$

Strict convexity of the unit ball of B means that the surface of the ball contains no straight line segment.

It is clear that every function which satisfies (2.10) is an idempotent; if (2.10) holds, the function nf is a homomorphism of G into a multiplicative subgroup of B. We do not know whether the additional conditions imposed on B are really needed to ensure (2.10).

Proof. Suppose $f \neq 0$, let S be the support of f, let M be the largest of the numbers $|f(x)|$, for $x \in G$, and let H be the set of all $x \in G$ at which $|f(x)| = M$. If $x \in H$, then

$$M = |f(x)| = |\sum_{y \in S} f(y)f(y^{-1}x)| \leq M \sum_{y \in S} |f(y)| = M. \tag{2.11}$$

Thus equality holds in (2.11), and this is only possible if $|f(y^{-1}x)| = M$ for all $y \in S$, $x \in H$. In other words, $S^{-1}H \subset H$. Since $H \subset S$, we have $H^{-1}H \subset H$, hence H is a group; it is obvious from the definition of H that H is finite. Since $1 \in H$ we have $S^{-1} \subset S^{-1}H$ and since $S^{-1}H \subset H$, we have $S^{-1} \subset H$. It follows that $S = H$, and if H has order n, then $M = 1/n$, since $\Sigma |f(x)| = 1$. This proves the first half of the theorem.

Each summand in the equation

$$f(x) = \sum_{y \in H} f(y)f(y^{-1}x) \qquad (x \in H) \tag{2.12}$$

has norm at most n^{-2}; there are n summands, and their sum has norm n^{-1}. It follows that each summand has norm exactly n^{-2}, and if we assume that the unit ball of B is strictly convex, then the n summands must all be equal (otherwise their sum would have norm less than n^{-1}). Hence

$$f(x) = nf(y)f(y^{-1}x) \qquad (x, y \in H), \tag{2.13}$$

which is equivalent to (2.10).

Finally, let φ be a homomorphism of B into the complex field K, and put $g(x) = \varphi(f(x))$. By Lemma 1.2, g is an idempotent in KH. Since complex homomorphisms of Banach algebra have norm at most 1 (as linear functionals), we have $|g(x)| \leq |f(x)|$. If strict inequality holds for some x, then $||g|| < 1$, hence $g = 0$, since g is idempotent. Otherwise, $||g|| = 1$, and since the unit ball of K is strictly convex, g satisfies (2.10). Since φ is a homomorphism, this says that

$$\varphi(f(xy) - nf(x)f(y)) = 0 \tag{2.14}$$

for all $x, y \in H$ and for all complex homomorphisms φ of B.

If now B is commutative and semi-simple, then 0 is the only element of B which is annihilated by every complex homomorphism of B. Thus (2.14) implies (2.10), and the proof is complete.

III. **Group rings over commutative rings.** The main result of this section is Theorem 3.4. Part of its proof can be given in a more general context and leads to Theorem 3.3. We begin by defining some relevant classes of groups.

3.1. *Definition.* (a) A group G is an ID-*group* if the absence of zero-divisors in a ring R implies that RG has no zero-divisors. (The letters "ID" stand for "integral domain.")

(b) A group G is an Ω-*group* if it has the following property: if A and B are non-empty finite subsets of G, then there exists at least one $x \in G$ which has a *unique* representation in the form $x = ab$ with $a \in A$ and $b \in B$.

(c) A group G is an O-*group* (ordered group) if it admits a linear ordering $<$ such that $x < y$ implies $xz < yz$ and $zx < zy$ for all $z \in G$. The best-known example of an O-group is of course the additive group Z of the rational integers.

(d) A group is called *torsion-free* if it has no elements of finite order (except, of course, the identity).

All torsion-free commutative groups are O-groups ([8; 194]; we have made no attempt to ascertain to whom this observation is originally due), and so are many non-commutative ones [6], for instance all free groups ([6], [4]) and all locally nilpotent torsion-free groups (Graham; unpublished).

It is trivial that every O-group is an Ω-group (simply take the largest elements of A and B for a and b); the converse is false, as we will see in § VI. It is easy to prove (see below) that every Ω-group is an ID-group and that every ID-group is torsion-free. It is conceivably true that every torsion-free group is an Ω-group. If so, then the results of §VI lose any interest which they may possess.

3.2. THEOREM. *Every Ω-group is an* ID-*group and every* ID-*group is torsion-free.*

Proof. Let G be an Ω-group and let R be a ring without zero-divisors. Suppose $f \in RG$, $g \in RG$, $f \neq 0$, $g \neq 0$, and let A, B be the supports of f, g. There exists $x \in G$ with a unique representation $x = ab$, where $a \in A$, $b \in B$; hence $(f * g)(x) = f(a)g(b)$, and since $f(a) \neq 0$, $g(b) \neq 0$ and R has no zero-divisors, we see that $(f * g)(x) \neq 0$. Thus $f * g \neq 0$, and we have proved that RG has no zero-divisors.

On the other hand, if G contains a finite non-trivial group H, and if R is any ring with at least two elements, let $f \in RH$ be a non-zero constant function and choose $g \in RH$, $g \neq 0$, so that $\sum_{x \in H} g(x) = 0$. Then $f * g = 0$, so that RH has zero-divisors, and by 1.5 the same is true of RG. Thus G is not an ID-group.

3.3. THEOREM. *If R is a commutative ring and G is an* ID-*group, then every idempotent $f \in RG$ has trivial support group.*

More explicitly, the conclusion is that $f(x) = 0$ if $x \neq 1$, $x \in G$, and that $f(1)$ is an idempotent in R.

Proof. Suppose $f \neq 0$, S is the support of f, and R_1 is the subring of R which is generated by the elements $f(x)$, for $x \in S$. Since S is finite, R_1 is finitely

generated, and since $f \in R_1G$, we may assume without loss of generality that R is finitely generated. We also lose no generality by assuming that R has a unit.

Every finitely generated commutative ring with unit is a homomorphic image of a ring of polynomials in finitely many indeterminates, with integral coefficients, and hence satisfies the ascending chain condition on ideals [10; 20, 21]. It follows that every primary ideal Q in R is contained in a prime ideal P such that $P^k \subset Q$ for some positive integer k (depending on Q) [10; 29] and that every ideal of R is an intersection of primary ideals [10; 32]. In particular, the intersection of *all* primary ideals of R consists of 0 alone.

Fix a primary ideal Q of R, let P be the corresponding prime ideal. Since P is prime, R/P has no zero-divisors; since G is an ID-group, $(R/P)G$ has no zero-divisors, and Theorem 1.2 shows that the same is true of RG/PG. In other words, if $f \in RG$, $g \in RG$, and $f * g \in PG$, then either $f \in PG$ or $g \in PG$.

Let u be the unit element of RG (see (1.1)). Since $f * f = f$, we have $f * (u-f) = 0$, so that either $f \in PG$ or $u - f \in PG$.

Suppose $f \in PG$. Then $f = f^k$, where f^k denotes the convolution of f with itself, k times. Since $P^k \subset Q$, and since $f^k(x)$ is, for each x, a sum of products of k factors, each belonging to P, it follows that $f \in QG$.

If $f \notin PG$, then $u - f \in PG$, and since $u - f$ is idempotent, the above argument shows that $u - f \in QG$.

In either case, we have proved that $f(x) \in Q$ for all $x \neq 1$. This is true for every primary ideal Q in R. Hence $f(x) = 0$ for all $x \neq 1$, and this proves the theorem.

3.4 THEOREM. *If R is a commutative ring and G is a commutative group, then every idempotent in RG has finite support group.*

Proof. Suppose $f \in RG$ and $f * f = f$. Since f has finite support, we may assume, without loss of generality, that G is finitely generated. But every finitely generated commutative group G is the direct product of a finite group H and the group Z^r, for some non-negative integer r. (Z^r denotes the direct product of r copies of the infinite cyclic group Z.)

Let ψ be the isomorphism of RG onto $(RH)Z^r$ described by Theorem 1.4. Then ψf is an idempotent in $(RH)Z^r$ (i.e., ψf is a function defined on Z^r, with values in RH) and since Z^r can be ordered (lexicographically, for instance), Z^r is an ID-group and hence ψf has trivial support group. The definition of ψ shows that this is equivalent to the statement that f has its support in H, and the proof is complete.

Remark. The proof shows that Theorem 3.4 actually holds for any group which is a direct product of a commutative group and an ID-group.

IV. **Examples.** In this section we exhibit some noncommutative situations in which RG has idempotents with more or less arbitrary supports. It is convenient to begin with a ring-theoretic lemma.

4.1. LEMMA. *If a ring R has a non-central idempotent e, then at least one of the following two statements is true*:

(a) *R contains an element $a \neq 0$ such that $ea = a$ but $ae = a^2 = 0$;*
(b) *R contains an element $b \neq 0$ such that $be = b$ but $eb = b^2 = 0$.*

Proof. Since e is not in the center of R, there exists $x \in R$ such that $ex \neq xe$, hence exe cannot be equal to both ex and xe.

If $exe \neq ex$, put $a = exe - ex$. If $exe \neq xe$, put $b = exe - xe$. Since $e^2 = e$, these elements have the desired properties.

Note that both $e + a$ and $e + b$ are idempotents, and that $e + a \neq 0$, $e + a \neq e$ if (a) holds, $e + b \neq 0$, $e + b \neq e$ if (b) holds. This gives the following.

COROLLARY. *If a ring R has a unique non-zero idempotent, then this idempotent lies in the center of R.*

An example is furnished by the 2×2 matrices

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

4.2. *Example.* Suppose R is a ring with a non-central idempotent e and suppose there exists $a \in R$ which satisfies condition (a) of Lemma 4.1. If x_1, x_2, x_3, $\cdots$ are arbitrary elements in a group G, define

$$f_0(x) = \begin{cases} e & \text{if } x = 1 \\ 0 & \text{if } x \neq 1 \end{cases} \qquad f_i(x) = \begin{cases} a & \text{if } x = x_i \\ 0 & \text{if } x \neq x_i \end{cases}. \tag{4.1}$$

Direct computation shows that

$$f_0 * f_i = f_i, \qquad f_i * f_j = 0 \qquad (i \geq 1, \quad j \geq 0). \tag{4.2}$$

Hence if

$$f = f_0 + f_1 + \cdots + f_n, \tag{4.3}$$

we see that $f * f = f$, and if $x_1, \cdots, x_n$ are distinct elements of G, f has $\{1, x_1, \cdots, x_n\}$ for its support.

Suppose next that R is a Banach algebra with a non-central idempotent (for instance, the algebra of all complex 2×2 matrices) and that G is any infinite group. Let $x_1, x_2, x_3, \cdots$ be distinct elements of G, choose complex numbers c_i such that $\Sigma |c_i| < \infty$, and define

$$f = f_0 + \sum_{i=1}^{\infty} c_i f_i. \tag{4.4}$$

Then f is an idempotent in $R^1(G)$, with infinite support.

Thus Theorem 2.3 cannot be extended to arbitrary Banach algebras, nor can Theorems 3.3 and 3.4 be extended to arbitrary rings. Our next aim is to show that the commutativity of G also cannot be omitted from Theorems 2.3 and 3.4. In fact, we can prove this for a rather large class of non-commutative groups.

(A simple example, which is a special case of the theorem which follows, was given in [9].)

4.3. THEOREM. *Suppose G is an infinite group which has a finite normal subgroup H. If H is not in the center of G, then $K^1(G)$ has idempotents with infinite support.*

Proof. For each $x \in G$ and $y \in H$, put

$$\sigma_x(y) = xyx^{-1}. \tag{4.5}$$

Since H is normal in G, each σ_x is an automorphism of H, and the mapping $x \to \sigma_x$ is a homomorphism of G into $A(H)$, the group of all automorphisms of H. Since H is finite, so is $A(H)$, and hence our homomorphism has an infinite kernel G_0. In other words, *G contains an infinite normal subgroup G_0 such that each element of G_0 commutes with each element of H.*

We now split the argument into two cases.

Case 1. *H is not commutative.* Then there exists $y_0 \in H$ which is not in the center of H. If n is the order of y_0, define

$$e(y_0^k) = \frac{1}{n} \exp\{2\pi ik/n\} \qquad (k = 0, 1, \cdots, n-1) \tag{4.6}$$

and put $e(y) = 0$ for all other $y \in H$. Then e is an idempotent in KH. Since $e(y) \neq e(y_0)$ for all $y \neq y_0$, and since y_0 is not in the center of H, e is not a class function, and we conclude from Theorem 1.3 that e is a non-central idempotent of KH. By Lemma 4.1, the ring KH contains a function a such that

$$e * a = a \quad \text{but} \quad a * e = a * a = 0 \tag{4.7}$$

and $a \neq 0$. (If not, there exists $b \neq 0$ in KH which satisfies conditions analogous to (b) in Lemma 4.1, and we could use b in place of a in what follows. Actually, *both* cases occur, since KH contains the ring of all 2×2 matrices, by the Wedderburn theorem.)

Extend the functions e and a to G, by defining them to be 0 outside of H. We then obtain functions in KG, with supports in H, which satisfy (4.7).

Now let $\{x_i\}$ be an infinite set of elements of G_0, each belonging to a different coset of H, put

$$\delta_i(x) = \begin{cases} 1 & \text{if } x = x_i \\ 0 & \text{if } x \neq x_i \end{cases} \tag{4.8}$$

and define

$$f = e + \sum_{i=1}^{\infty} c_i\, \delta_i * a, \tag{4.9}$$

where $\{c_i\}$ is a sequence of non-zero complex numbers such that $\Sigma |c_i| < \infty$.

Since each x_i commutes with each element of H, and since e and a have their

supports in H, it follows that

$$e * \delta_i = \delta_i * e, \qquad a * \delta_i = \delta_i * a \tag{4.10}$$

for $i = 1, 2, 3, \cdots$. Combining (4.7) and (4.10), we see that f defined by (4.9) is an idempotent in $K^1(G)$. Since $a \neq 0$ and since the functions $\delta_i * a$ have disjoint supports (each lies in a different coset of H), the support of f is infinite.

Case 2. H is commutative. Since H is not in the center of G, the group G_0 constructed earlier in this proof is not all of G. Hence there is an infinite set of elements z_i which are not in G_0 but which lie in the same coset of G_0 and such that any two lie in distinct cosets of H. The construction of G_0 shows that there is an automorphism σ of H, *different from the identity mapping*, such that

$$z_i y z_i^{-1} = \sigma(y) \qquad (y \in H, \quad i = 1, 2, 3, \cdots). \tag{4.11}$$

Define $\sigma(x) = x$ if $x \in G$ but $x \notin H$. Since σ is not the identity mapping on H, there exists a complex character γ of H such that $\gamma \circ \sigma \neq \gamma$, where $\gamma \circ \sigma$ is the character defined by $(\gamma \circ \sigma)(x) = \gamma(\sigma(x))$. If n is the order of H, define $e \in KG$ by

$$e(x) = \begin{cases} n^{-1}\gamma(x) & (x \in H), \\ 0 & (x \notin H). \end{cases} \tag{4.12}$$

Since the convolution of any two distinct characters of H is 0, we have

$$e * e = e, \qquad (e \circ \sigma) * e = 0. \tag{4.13}$$

Define $\delta_i(z_i) = 1$, $\delta_i(x) = 0$ if $x \neq z_i$, let $\{c_i\}$ be a sequence of non-zero complex numbers such that $\Sigma |c_i| < \infty$, and put

$$f = e + \sum_{i=1}^{\infty} c_i \, \delta_i * e. \tag{4.14}$$

By (4.11) we have

$$(\delta_i^{-1} * e * \delta_i)(x) = e(z_i x z_i^{-1}) = (e \circ \sigma)(x) \tag{4.15}$$

for all $x \in G$, and hence

$$e * \delta_i * e = \delta_i * (e \circ \sigma) * e = 0, \tag{4.16}$$

by (4.13). It follows from these relations that f is an idempotent in $K^1(G)$, with infinite support.

Remarks. (a) If G/H contains a finitely generated infinite subgroup, the preceding construction can be modified so as to yield idempotents in KG with infinite support groups.

(b) Instead of the complex field K, other fields could have been used, provided they contain enough roots of unity to construct characters. However, Theorem 5.6 shows that *some* conditions (relating K and H) are needed.

(c) If none of the x_i lies in H, the norms of the functions f constructed in (4.9) and (4.14) are $1 + \Sigma |c_i| \, ||a||$ and $1 + \Sigma |c_i|$, respectively. They can be arbitrarily close to 1. Hence the norm-condition imposed in Theorem 2.6 cannot be relaxed.

V. **Group rings of ID-Groups.** Although Example 4.2 shows that Theorem 3.3 cannot be extended to *any* ring R which has a non-central idempotent, there nevertheless is a class of rings which includes some non-commutative ones and for which the conclusion does hold. Theorem 5.2 gives the precise result; 5.4 and 5.5 are applications of it.

All ideals mentioned below will be *two-sided* ideals. A ring R (or an ideal) is said to be *nil* if to each $x \in R$ there corresponds a positive integer $n(x)$ such that $x^{n(x)} = 0$; R is *nilpotent* if there is a fixed n such that the product of any n elements of R is 0; and R is *locally nilpotent* if every finitely generated subring of R is nilpotent.

5.1. THEOREM. (a) *If a ring R without zero-divisors has an idempotent $e \neq 0$, then e is the unit element of R, and R has no other idempotents except* 0.

(b) *Suppose N is a nil-ideal in a ring R and R/N has no zero-divisors. Then no two non-zero idempotents in R commute. Hence R has a unique non-zero idempotent if and only if R has a non-zero central idempotent.*

(c) *If N is a nil-ideal in a ring R and if there exists $r \in R$ such that $r^2 - r \in N$, then R has an idempotent e such that $e - r \in N$.*

Proof. (a) For every $x \in R$ we have

$$e(ex - x) = ex - ex = 0 = xe - xe = (xe - x)e,$$

since $e^2 = e$. But R has no zero-divisors and $e \neq 0$. Hence $ex - x = 0 = xe - x$. This says that R has a unit, namely e. If $x^2 = x \in R$, then $x(e - x) = 0$, hence either $x = 0$ or $x = e$.

(b) Suppose α and β are non-zero commuting idempotents in R. Since N is nil and since $\alpha^n = \alpha \neq 0$ for $n = 1, 2, 3, \cdots$, we have $\alpha \notin N$. Similarly $\beta \notin N$. Since R/N has no zero divisors, (a) shows that α and β are in the same coset of N, i.e., $\alpha - \beta \in N$. But $\alpha - \beta = (\alpha - \beta)^{2n-1}$ for $n = 1, 2, 3, \cdots$, and since N is nil, this is 0 for large enough n. Thus $\alpha = \beta$. The second part of (b) now follows immediately from the Corollary to Lemma 4.1.

(c) We paraphrase the argument used in [2; 161] in a slightly different context. Put

$$z = r^2 - r, \qquad r_1 = r + z - 2rz. \tag{5.1}$$

Then $z \in N$, $r_1 - r \in N$, z is a polynomial in r and so is r_1, hence r, r_1, z commute, and computation shows that

$$r_1^2 - r_1 = 4z^3 - 3z^2. \tag{5.2}$$

Thus $r_1^2 - r_1$ is divisible by z^2. Continuing this process, with r_1 in place of r, etc., we obtain elements r_k such that $r_k - r \in N$ and $r_k^2 - r_k$ is divisible by z^{2^k}. Since $z \in N$ and N is nil, it follows that $r_k^2 - r_k = 0$ if k is large enough.

It may be of some interest that the above proof actually yields an idempotent which is a polynomial in r, with integral coefficients.

5.2. THEOREM. *Suppose G is an* ID*-group and R is a ring which contains a locally nilpotent ideal N such that R/N has no zero-divisors.*

(a) *If R has no non-zero idempotent then RG has none.*
(b) *No two non-zero idempotents in RG commute.*
(c) *If R has a non-zero central idempotent then RG has a unique non-zero idempotent and this idempotent has trivial support group.*

Example 4.2 shows that the conclusions of (c) are false whenever R has a non-central idempotent.

Proof. Since every member of NG has finite support, its range lies in a finitely generated subring of N, and this subring is nilpotent by assumption. Thus *NG is a nil-ideal of RG,* and since G is an ID-group, we also see that *RG/NG has no zero-divisors,* by Theorem 1.2.

If R has no idempotent except 0, Theorem 5.1(c) shows that R/N has no idempotent, except 0, hence $(R/N)G$ has no unit, by Theorem 1.1. Hence RG/NG has no unit, and Theorem 5.1(a) implies that RG/NG has no idempotent, except 0. This says that every idempotent in RG lies in NG. But NG is nil. Hence 0 is the only idempotent in RG, and we have proved (a).

If we apply Theorem 5.1(b) with RG and NG in place of R and N, we obtain (b).

To prove (c), assume $e^2 = e \neq 0$ and e is in the center of R. If $f \in RG$ is defined by $f(1) = e$, $f(x) = 0$ for $x \neq 1$, then $f \neq 0$, $f * f = f$, and f is in the center of RG. By (b), RG cannot contain any other non-zero idempotent. This completes the proof.

5.3. THEOREM. *Suppose G is a group $\{R_\alpha\}$ is a collection of rings such that every idempotent in $R_\alpha G$ has trivial support group, and R is the complete direct sum of the rings R_α. Then every idempotent in RG has trivial support group.*

Proof. Each $r \in R$ is an indexed set $\{r_\alpha\}$, with $r_\alpha \in R_\alpha$. Addition and multiplication in R are componentwise. If $f \in RG$ and if $f_\alpha(x)$ denotes the α-th component of $f(x)$, for $x \in G$, the mapping $f \to f_\alpha$ is a homomorphism of RG onto $R_\alpha G$. Thus if f is idempotent, so is each f_α, and the hypothesis implies that $f_\alpha(x) = 0$ for all α and for all $x \neq 1$. Thus $f(x) = 0$ if $x \neq 1$.

5.4. *Remark.* Theorems 5.2 and 5.3 yield an alternative proof of Theorem 3.3. For if $\{Q_\alpha\}$ is a collection of primary ideals in R whose intersection is $\{0\}$, and if $\{P_\alpha\}$ is the collection of the associated prime ideals, the rings R/Q_α satisfy the hypotheses of Theorem 5.2, with $N = P_\alpha/Q_\alpha$. Also, Theorem 5.3 applies since R is isomorphic to a subring of the direct sum of the rings R/Q_α, as is

shown by the mapping $r \to \{\varphi_\alpha(r)\}$, where φ_α is the natural homomorphism of R onto R/Q_α.

The same technique is used in the following proof. We recall that a ring R is defined to be *regular* if to each $a \in R$ there exists $x \in R$ such that $axa = a$.

5.5. THEOREM. *Suppose R is a regular ring and G is an* ID*-group. Then all idempotents in RG have trivial support group if and only if R has no nilpotent elements (except* 0*).*

Proof. Forsythe and McCoy [3] proved that every regular ring R without nilpotent elements is a subring of a ring R' which is a complete direct sum of division rings D_α. Every division ring satisfies the hypotheses of Theorem 5.2 (with the zero-ideal for N), and since 0 and 1 are the only idempotents in a division ring, 5.2 and 5.3 show that every idempotent in $R'G$ has trivial support group. The same is of course true of the smaller ring RG.

On the other hand, if a regular ring R has a nilpotent element different from 0 then R has a non-central idempotent [3], and so the second half of the theorem follows from Example 4.2.

We conclude this section with a more special result, which should be compared with Theorem 4.3. We recall that a *p-group* is one in which the order of every element is a power of p.

5.6. THEOREM. *Let p be a prime. Suppose G has a finite normal subgroup H which is a p-group, and suppose G/H is an* ID*-group. If F is a field of characteristic p, then FG has only the trivial idempotents* 0 *and* 1.

Proof. For any $x \in G$ let $\bar{x}$ be the coset of H which contains x, and define

$$(\sigma f)(\bar{x}) = \sum_{y \in H} f(xy). \tag{5.4}$$

The proof that σ is a homomorphism of FG onto $F(G/H)$ is a matter of straightforward verification. If M is the kernel of σ, then FG/M is isomorphic to $F(G/H)$, and since G/H is an ID-group and F is a field, it follows that FG/M has no zero-divisors.

If we can show that M is a nil-ideal in FG, then Theorem 5.1(b) implies that FG cannot have two distinct commuting non-zero idempotents. But F is a field, hence has a unit, hence so does FG, and this gives the desired result.

Let M_0 be the set of all $g \in FH$ such that

$$\sum_{y \in H} g(y) = 0. \tag{5.5}$$

Then M_0 is a nilpotent ideal in FG [2; 189]. (In the cited reference, the result is stated for algebraically closed fields; we can of course replace F by its algebraic closure, without any loss of generality.) As usual, we will regard members of FH as members of FG which are 0 outside H.

Let $\{x_i\}$ be a collection of elements of G, exactly one in each coset of H, and define $\delta_i(x_i) = 1$, $\delta_i(x) = 0$ if $x \neq x_i$. Then every $f \in M$ can be represented in

the form

$$f = \sum \delta_i * g_i \tag{5.6}$$

where the g_i are in M_0. The sum in (5.6) is of course finite.

If δ is any function on G which is 1 at one point and is 0 elsewhere (let us call such functions *one-point functions*) and if $g \in M_0$, then $\delta * g * \delta^{-1}$ is easily seen to be in M_0, hence $\delta * g = g' * \delta$, where $g' \in M_0$. Since the convolution of two one-point functions is again a one-point function, we see that any product of the form

$$\delta_{i_1} * g_{i_1} * \cdots * \delta_{i_k} * g_{i_k}, \tag{5.7}$$

where the g_i are in M_0, is equal to

$$g'_{i_1} * \cdots * g'_{i_k} * \delta, \tag{5.8}$$

where the g'_i are in M_0 and δ is a one-point function. Since M_0 is nilpotent, (5.6) now shows that M is also nilpotent.

This completes the proof.

VI. ID-groups and Ω-groups.

6.1. THEOREM. *If G has a normal subgroup H such that both H and G/H are Ω-groups, then G is an Ω-group.*

Proof. Let A, B be finite non-empty subsets of G, let $\bar{A}$ be the set of all cosets of H which intersect A, define $\bar{B}$ similarly. Then $\bar{A}$ and $\bar{B}$ are finite non-empty subsets of G/H, and since G/H is an Ω-group, there exist $\bar{a} \in \bar{A}$, $\bar{b} \in \bar{B}$, such that $\bar{a}\bar{b}$ has no other factorization $\bar{a}_1\bar{b}_1$ with $\bar{a}_1 \in \bar{A}$, $\bar{b}_1 \in \bar{B}$.

Fix $a \in \bar{a}$, $b \in \bar{b}$, let $ax_1, \cdots, ax_m$ be the members of $A \cap \bar{a}$, let $y_1 b, \cdots, y_n b$ be the members of $B \cap \bar{b}$. Then $x_1, \cdots, x_m, y_1, \cdots, y_m$ are in H, and since H is an Ω-group, there exist x_i and y_j such that $x_i y_j \neq x_r y_s$ if $r \neq i$ or $s \neq j$.

Then $ax_i y_j b$ is an element of G which is uniquely represented as a product of an element of A and an element of B. Hence G is an Ω-group.

Remark. A very similar proof shows that G is an ID-group if H is an ID-group and G/H is a Ω-group. Also, the direct product of two ID-groups is an ID-group; this follows trivially from Theorem 1.4.

The following example shows that Theorem 6.1 cannot be stated for O-groups, and that there are Ω-groups which are not O-groups.

6.2. EXAMPLE. Let G be the set of all ordered pairs (m, n) with $m \in Z$, $n \in Z$ (recall that Z is the additive group of the rational integers) and multiplication defined by

$$(m, n)(a, b) = (m + (-1)^n a, n + b). \tag{6.1}$$

Let $H = \{(m, 0) : m \in Z\}$. Then H is the kernel of the homomorphism $(m, n) \to n$,

so that H is normal. Since both H and G/H are isomorphic to Z, Theorem 6.1 shows that G is an Ω-group.

If $x = (0, 1)$ and $y = (1, 0)$, then $x^2 = (0, 2)$, $y^2 = (2, 0)$, and

$$xy = (-1, 1) \neq (1, 1) = yx,$$

$$x^2y^2 = (2, 2) = y^2x^2.$$

Thus G contains two elements which do not commute but whose squares do commute, and this cannot happen in an O-group [6].

Theorem 3.2 showed that every Ω-group is an ID-group. We conclude with a stronger result, modeled after a theorem of Higman [4]; he uses Z where we use Ω-groups:

6.3. THEOREM. *Let G be a group in which every non-trivial finitely generated subgroup can be mapped homomorphically onto a non-trivial Ω-group. Then G is an* ID*-group.*

Proof. Let R be a ring without zero-divisors. If $f \in RG$, let $\nu(f)$ be the number of elements in the support of f. If there exist $f, g \in RG$ such that $f \neq 0$, $g \neq 0$, but $f * g = 0$, then there is such a pair for which $\nu(f) + \nu(g)$ is minimal. Suppose f and g are so chosen; let A and B be their supports.

Replacing $f(x)$ by $f(ax)$ and $g(x)$ by $g(xb)$ affects none of the above properties. We can therefore assume, without loss of generality, that $1 \in A$ and $1 \in B$. Since R has no zero-divisors, it is clear that both A and B must have at least two elements. Let G_0 be the group generated by A and B. By assumption, there is a homomorphism η of G_0 onto a non-trivial Ω-group H, and therefore $\eta(A)$ contains an element $\bar{a}$ and $\eta(B)$ contains an element $\bar{b}_1$ such that $\bar{a}\bar{b}$ has no other representation in the form $\bar{a}_1\bar{b}_1$ with $\bar{a}_1 \in \eta(A)$, $\bar{b}_1 \in \eta(B)$.

Let $A_1 = A \cap \eta^{-1}(\bar{a})$, $B_1 = B \cap \eta^{-1}(\bar{b})$, and define

$$f_1(x) = \begin{cases} f(x) \text{ on } A_1 \\ 0 \text{ elsewhere} \end{cases} \qquad g_1(x) = \begin{cases} g(x) \text{ on } B_1 \\ 0 \text{ elsewhere.} \end{cases} \tag{6.2}$$

For $x \in A_1B_1$, our choice of $\bar{a}$, $\bar{b}$ shows that

$$(f_1 * g_1)(x) = (f * g)(x). \tag{6.3}$$

Thus $f_1 \neq 0$, $g_1 \neq 0$, $f_1 * g_1 = 0$.

But $\eta(A)$ and $\eta(B)$ generate H, hence they cannot both reduce to the identity of H, hence either A_1 is a proper subset of A or B_1 is a proper subset of B (or both). This shows that

$$\nu(f_1) + \nu(g_1) < \nu(f) + \nu(g), \tag{6.4}$$

in contradiction to the assumed minimal property of the pair f, g.

Postscript

The preceding work suggests the following questions which are left unanswered.

(1) Is the conclusion (2.10) of Theorem 2.6 true without any assumptions on the Banach algebra B?
(2) Is every torsion-free group an Ω-group or an ID-group?
(3) Can Theorem 3.3 be extended to group rings over Banach algebras? More specifically, if G is a noncommutative ID-group (or an Ω-group, or an O-group), does every idempotent in $K^1(G)$ have trivial support group?
(4) Does every central idempotent in RG or in $B^1(G)$ have finite support group?
(5) If RG has a non-zero idempotent, must R have one? (Compare Theorem 5.2(a).)
(6) If RG has a unique non-zero idempotent, must its support be $\{1\}$? (The answer is of course yes if the answer to (5) is yes.)

References

1. P. J. Cohen, *On a conjecture of Littlewood and idempotent measures*, American Journal of Mathematics, vol. 82(1960), pp. 191–212.
2. C. W. Curtis and Irving Reiner, *Representation Theory of Finite Groups and Associative Algebras*, New York, 1962.
3. Alexander Forsythe and N. H. McCoy, *On the commutativity of certain rings*, Bulletin of the American Mathematical Society, vol. 52(1946), pp. 523–526.
4. Graham Higman, *The units of group rings*, Proceedings of the London Mathematical Society, (2), vol. 46(1940), pp. 231–248.
5. Friedrich Levi, *Über die Untergruppen der freien Gruppen*, Mathematische Zeitschrift, vol. 37(1933), pp. 90–97.
6. B. H. Neumann, *On ordered groups*, American Journal of Mathematics, vol. 71(1949), pp. 1–18.
7. Walter Rudin, *Idempotent measures on abelian groups*, Pacific Journal of Mathematics, vol. 9(1959), pp. 195–209.
8. Walter Rudin, *Fourier Analysis on Groups*, New York, 1962.
9. Walter Rudin, *Idempotents in group algebras*, Bulletin of the American Mathematical Society, vol. 69(1963), pp. 224–227.
10. B. L. van der Waerden, *Moderne Algebra*, vol. 2, New York, 1943.

University of Wisconsin