

Group-rings as *-algebras.

By I. N. HERSTEIN in Lawrence, U. S. A.

We consider the group-ring of a finite group over the field of complex numbers. Although the results we obtain are not new; in fact are very well-known, we believe our approach might be of some interest. The method we use depends almost entirely on the construction of an adjoint in the group-ring. The definition of this adjoint is fairly natural, and it leads us to some of the desired results both quickly and easily.

Let G be a finite group of order n , and let $1 = g_1, g_2, \dots, g_n$ be the elements of G . By the group-ring, Γ , of G over the the complex numbers K , we mean, the set of all formal sums $\sum \lambda_i g_i$ where $\lambda_i \in K$ and $g_i \in G$ and where:

1. $\sum \lambda_i g_i = \sum \mu_i g_i$ if and only if $\lambda_i = \mu_i$ for each i .
2. $\sum \lambda_i g_i + \sum \mu_i g_i = \sum (\lambda_i + \mu_i) g_i$.
3. $(\sum \lambda_i g_i)(\sum \mu_j g_j) = \sum_{i,j} \lambda_i \mu_j g_i g_j$ and where $g_i g_j$ is calculated in G .

By these definitions it is easily verified that Γ is a finite-dimensional algebra over K .

In Γ we define an adjoint operation, $*$, in the following manner:

If $A = \sum \lambda_i g_i$ then $A^* = \sum \bar{\lambda}_i g_i^{-1}$ where $\bar{\lambda}_i$ is the complex conjugate of λ_i .

From the definition of the $*$ and the operations of addition and multiplication in Γ it follows directly that

Theorem 1. For all $A, B \in \Gamma, \lambda, \mu \in K$

1. $A^{**} = A$
2. $(\lambda A + \mu B)^* = \bar{\lambda} A^* + \bar{\mu} B^*$
3. $(AB)^* = B^* A^*$.

Suppose that $A = \sum \lambda_i g_i$ and $B = \sum \mu_j g_j$. Hence $A^* = \sum \bar{\lambda}_i g_i^{-1}$ and $B^* = \sum \bar{\mu}_j g_j^{-1}$. Thus

$$AA^* + BB^* = \sum_i (|\lambda_i|^2 + |\mu_i|^2) + \sum_{i \neq j} \lambda_i \bar{\lambda}_j g_i g_j^{-1} + \sum_{i \neq j} \mu_i \bar{\mu}_j g_i g_j^{-1}.$$

Consequently $AA^* + BB^* = 0$ only if $\sum_i (|\lambda_i|^2 + |\mu_i|^2) = 0$; that is only if each $\lambda_i = \mu_i = 0$. So we have

Theorem 2. *If $A, B \in \Gamma$ then $AA^* + BB^* = 0$ if and only if $A = B = 0$.*

Since Γ is a finite-dimensional algebra over K , $A \in \Gamma$ is regular (that is possesses a multiplicative inverse) if and only if A is not a divisor of zero. Suppose for some A in Γ and some real $\lambda \in K, \lambda \neq 0$ that there exists a B in Γ such that $(AA^* + \lambda^2)B = 0$. Hence

$$B^*(AA^* + \lambda^2)B = (B^*A)(B^*A)^* + (\lambda B^*)(\lambda B^*)^* = 0;$$

thus by theorem 2 $\lambda B^* = 0$ and since $\lambda \neq 0$, it follows that $B^* = 0$, and so $B = 0$. Consequently for all $A \in \Gamma$ and $\lambda \neq 0 \in K, AA^* + |\lambda|^2$ is not a divisor of zero, and so

Theorem 3. *For all $\lambda \neq 0$ in K and $A \in \Gamma$, $AA^* + |\lambda|^2$ is regular.*

As an immediate consequence of theorem 2 we can also obtain the very well-known and important result that Γ is a semi-simple algebra; that is that Γ has no non-zero nilpotent left-ideals. To prove this we first prove that if A is self-adjoint, (i. e. $A = A^*$), then A is nilpotent only if $A = 0$. Let A be self-adjoint and different from zero; thus $A^2 = A^*A \neq 0$, by theorem 2 $(A^2)^* = A^*A^* = A^2 \neq 0$, and so $A^4 \neq 0$. Similarly $A^{2n} \neq 0$ for all integers n , and so A is not nilpotent. Suppose that I is a nilpotent left-ideal, and A is in I ; thus A^*A is in I and so is nilpotent. But $A^*A = (A^*A)^*$, whence $A^*A = 0$. Thus $A = 0$ and I is zero ideal, and Γ is semi-simple. Thus we have proved

Theorem 4. *Γ is a semi-simple algebra.*

Let I be a minimal left-ideal of Γ . As is well known for any semi-simple algebra, $I = Te$ where $e^2 = e$ is an idempotent. It is also easily shown that if Ie is a minimal left-ideal of Γ then eIe is a division ring (skew-field); since eIe contains the field Ke which is isomorphic to the complex numbers K , and is finite-dimensional over $Ke, eIe = Ke$; that is for all $A \in \Gamma, eAe = \lambda_A e$ where $\lambda_A \in K, e^*e$ is in I and $ee^*e = \lambda e$, where $\lambda \in K$. We claim that λ is real and different from zero. For

$$0 \neq (e^*e)^2 = e^*ee^*e = \lambda e^*e = (ee^*e)^*e = (\lambda e)^*e = \bar{\lambda} e^*e.$$

So $\lambda = \bar{\lambda} \neq 0$, and we have proved our contention.

Let $e' = \frac{e^*e}{\lambda}$. Since λ is real $(e')^* = e'$. Also

$$(e')^2 = \frac{e^*e}{\lambda} \frac{e^*e}{\lambda} = \frac{e^*e}{\lambda} = e'.$$

From this we obtain

Theorem 5. *Every minimal left-ideal of Γ can be generated by a self-adjoint idempotent.*

We suppose that $l = \Gamma e, e^* = e$, is a minimal left-ideal of Γ . Thus l is a finite-dimensional vector space over K . In l we will now define an "inner product" so that l becomes a unitary space over K .¹⁾

Suppose that $a, b \in l = \Gamma e$, l a minimal left-ideal. We define $I(a, b) = eb^*ae = \lambda_{ab}e$ where $\lambda_{ab} \in K$. We define the inner product of a and b , which we denote by (a, b) , by $(a, b) = \lambda_{ab}$. For this inner product we prove:

$$1. (a, b) = \overline{(b, a)}.$$

For $I(a, b) = eb^*ae = (ea^*be)^* = (\lambda_{ba}e)^* = \overline{\lambda_{ba}}e = \lambda_{ab}e$, so from the definition of the inner product we obtain that $(a, b) = \overline{(b, a)}$.

$$2. (\mu a + \omega b, c) = \mu(a, c) + \omega(b, c).$$

For $I(\mu a + \omega b, c) = ec^*(\mu a + \omega b)e = \mu ec^*ae + \omega ec^*be$
 $= \mu I(a, c) + \omega I(b, c).$

Thus $(\mu a + \omega b, c) = \mu(a, c) + \omega(b, c).$

$$3. (a, a) \geq 0; (a, a) = 0 \text{ if and only if } a = 0.$$

From 1. $(a, a) = \overline{(a, a)}$, and so (a, a) is real. We next show that if $a \neq 0$, $(a, a) \neq 0$. Since $a \in l$, $ae = a$. Thus $I(a, a) = ea^*ae = (ae)^*(ae) = a^*a \neq 0$ if $a \neq 0$; this implies $(a, a) = 0$ only if $a = 0$. We still have left to show that (a, a) is positive. Suppose that $I(a, a) = ea^*ae = -\omega^2e$ where ω is real. Then $(ae)^*(ae) + (\omega e)^*(\omega e) = 0$, whence $\omega = 0$ and $a = 0$.

So we have shown that our inner product is an inner product in the sense of HALMOS¹⁾ and that l is a unitary space. This is

Theorem 6. *Every minimal left-ideal of Γ is a unitary vector space over K .*

Since Γ is the vector-space direct sum of its minimal left-ideals, each of which is a unitary space:

Theorem 7. *Γ is a unitary space over K .*

Since Γ is an algebra over K , every $A \in \Gamma$ acts as a linear transformation on the minimal left-ideal $l = \Gamma e, e = e^*$. The usual definition of the adjoint of a linear transformation A on a unitary space is by: $(a, A^*b) = (Aa, b)$ for all $a, b \in l$. We show that our definition is consistent with this. For

$$I(Aa, b) = eb^*Aae = e(A^*b)^*ae = I(a, A^*b) \text{ and so } (Aa, b) = (a, A^*b).$$

We say a linear transformation on a unitary space is a unitary transformation if $(Aa, Aa) = (a, a)$ for all a in the space. Now

$$I(ga, gb) = e(gb)^*gae = eb^*g^{-1}gae \text{ for all } g \in G, a, b \in \Gamma e. \text{ That is, } \\ I(ga, gb) = I(a, b) \text{ for all } g \in G, a, b \in \Gamma e, \text{ whence } (ga, gb) = (a, b).$$

¹⁾ For these concepts see: P. P. HALMOS, *Finite-dimensional vector spaces* (Princeton, 1948.).

So every group element acts as a unitary transformation on the minimal left-ideals of I . This enables us to prove the classic theorem

Theorem 8. *Every irreducible representation of a finite group, taken in the field of complex numbers, is equivalent to a unitary representation.²⁾*

Every irreducible representation of G can be taken so as to have a minimal left-ideal of I as representation space. Since every group element acts on the minimal left-ideals of I as a unitary transformation, theorem 8 is proved.

(Received June 12, 1950.)

²⁾ similar statement follows immediately for all representations from Theorem 8.