韓國數學敎育學會誌〈數學敎育〉
1982. 12. Vol. XXI. No. 1

Journal of the Korea Society of Mathematical Education
Dec. 1982. Vol. XXI. No. 1

# On Group Algebras

by Yong Han, Shin
*Central Vocational Training Institute*

## 1. Introduction

Let $G$ be a group and let $F$ be a field. We denote by $GL_n(F)$ the group of all non-singular $n\times n$ matrices over $F$. A matrix representation of $G$ over $F$ is a group homomorphism

$$\varphi : G \longrightarrow GL_n(F)$$

The character $\chi_\varphi$ of such a representation $\varphi$ is the function of $G$ into $F$ defined by

$$\chi_\varphi(x) = tr\ \varphi(x), \text{ for all } x\in G.$$

The theory of representations is indispensible to study the structures of groups. If $F$ is a field of characteristic zero, the theory of representations over $F$ is called the ordinary representation theory.

The deeper properties of the characters of a finite group $G$ come from a study of the group algebra $F[G]$ of $G$ over the field $F$ and of modules over this algebra.

In this note we will prove the following two theorems.

**Theorem** 3.1. *If $G$ is the group of units of a ring $R$ and if $G$ is finite of odd order, the subring $S$ of $R$ generated by $G$ is a finite direct sum of Galois fields of characteristic* 2 :

$$S = GF(2^{k_1}) \oplus \cdots \oplus GF(2^{k_r}).$$

**Theorem** 3.2. *For any group $G$ (finite or infinite), the group algebra $C[G]$ of $G$ over the complex field $C$ is semisimple.*

## 2. Preliminaries

In this section, we will state some definitions and necessary theorems.

**Definition** Let $G$ be any group (finite or infinite) and let $F$ be a field. The *group algebra* $F[G]$ is an $F$-vector space with basis $G$ and with multiplication defined distributively using the given multiplication of $G$:

$$\Sigma a_x x + \Sigma b_x x = \Sigma (a_x + b_x) x$$
$$b(\Sigma a_x x) = \Sigma (ba_x) x$$
$$(\Sigma a_x x)\cdot(\Sigma b_y y) = \Sigma (a_x b_y) xy$$

**Definition** Let $R$ be a ring with 1. The *Jacobson radical* $J(R)$ of $R$ is the set of all elements of $R$ which annihilate all the irreducible left (right) $R$-modules:

$$J(R) = \{r\in R : rM=0 \text{ for all irreducible } R\text{-modules}\}$$

It is known that

$$J(R) = \{r\in R : 1-sr \text{ is invertible for all } s\in R\}$$

A ring $R$ is said to be *semisimple* if its Jacobson radical $J(R)$ is zero.

From the following theorem comes out the whole theory of group representation.

**Theorem** 2. 1. (*Wedderburn-Artin*) *Let R be a semisimple artinian ring. Then*

$$R \cong Mat_{n_1}(D_1) \oplus Mat_{n_2}(D_2) \oplus \cdots \oplus Mat_{n_r}(D_r)$$

*Where the $D_i$ are divison rings and the $Mat_{n_i}(D_i)$ are the rings of all $n_i \times n_i$ matrices over $D_i$.*

The following theorem is well-known

**Theorem** 2. 2. (Maschke) *Let G be a finite group. The group algebra F[G] of G over a field F is semisimple if and only if the characteristic of F does not divide the order of G.*

The proofs of the following lemmas are well-known.

**Lemma** 2. 3. (Wedderburn) *A finite division ring is a finite field.*

**Lemma** 2. 4. *The general linear group $GL_n(q)$ over the Galois field $GF(q)$ is of order*

$$|GL_n(q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

**Lemma** 2. 5. *The multiplicative group of the finite field is cyclic.*

## 3. Main theorems

In this section we will prove our main theorems.

**Theorem** 3. 1. *If G is the group of units of a ring R and if G is finite of odd order, then the subring S of R generated by G is a finite direct sum of Galois fields of characteristic* 2:

$$S = GF(2^{k_1}) \oplus \cdots \oplus GF(2^{k_r})$$

**Proof** Since $G$ is of odd order, $-1=1$; otherwise $\{-1, 1\}$ would be a subgroup of $G$ of order 2. Hence the subring $S$ generated by $G$ is the group algebra $F[G]$, where $F=GF(2)$ the Galois field with two elements. Since the characteristic of $F$ does not divide the order of $G$, Maschke's theorem implies that $F[G]$ is semisimple.

By the Wedderburn-Artin theorem, $F[G]$ is the finite direct sum of $\mathrm{Mat}_{n_i}(D_i)$, $i=1.....r$. By Lemma 2. 3, the finite division rings $D_i$ must be fields containing $GF(2)$. Hence each $D_i$ is a Galois field $GF\ (2^{k_i})$ for some $k_i$. By Lemma 2. 4, the number of units in $\mathrm{Mat}_{n_i}(D_i)$ is odd if and only if $n_i=1$ This completes the proof.

**Corollary** *A finite group G of odd order is the group of units of some ring if and only if G is abelian and is the finite direct product of cyclic groups $G_i$, where the order of each $G_i$ is of the form* $2^{k_i}$-1

**Proof** The assertion is an immediate consequence of Theorem 3. 1 and Lemma 2. 5.

Now we will prove the following theorem by the analytic method.

**Theorem** 3. 2. *Fcr any group G (finite or infinite), the group algebra C[G] over the complex field C is semisimple.*

**Proof** We define a trace map $tr$ on $C[G]$ into $C$ by

$$tr\ (\Sigma a_x x) = a_1$$

Clearly $tr$ is a $C$-linear functional on $C[G]$ and $tr\ \alpha\beta = tr\ \beta r$. A Hermitian inner product on $C[G]$ can be defined by

$$(\alpha, \beta) = \Sigma a_x \bar{b}_x$$

where $\alpha = \Sigma a_x x$ and $\beta = \Sigma b_x x$. Let $\|\alpha\| = (\alpha, \alpha)^{1/2}$ Furthermore we define a map * on $C[G]$

into $C[G]$ by

$$\alpha^*=\Sigma\bar{a}_x x^{-1},\ \ if\ \ \alpha=\Sigma a_x x$$

Then it is easy to see that

$$(\alpha,\alpha)=tr\ \alpha\alpha^*=\|\alpha\|^2$$

Moreover, we introduce an auxiliary norm on $C[G]$ by defining $|\alpha|=\Sigma|a_x|$ if $\alpha=\Sigma a_x x$. Clearly $|\alpha+\beta|\leqq|\alpha|+|\beta|$ and $|\alpha\beta|\leqq|\alpha||\beta|$.

Now let $\alpha$ be a fixed element of $JC[G]$. Then for all complex number $\zeta$, the element $1-\zeta\alpha$ is invertible, and we can consider the map

$$f(\zeta)=tr(1-\zeta\alpha)^{-1}$$

We will show that $f$ is an entire function and we will find its Taylor series about the origin.

For convenience we set $g(\zeta)=(1-\zeta\alpha)^{-1}$ so that $f(\zeta)=tr\ g(\zeta)$. Then we have the basic identity

$$g(\zeta)-g(\eta)=(\zeta-\eta)\alpha g(\zeta)g(\eta).$$

We first show that $|g(\eta)|$ is bounded in a neighborhood of $\zeta$. Now by the above $g(\eta)=g(\zeta)-(\zeta-\eta)\alpha g(\zeta)g(\eta)$ so $|g(\eta)|\{1-|\zeta-\eta||\alpha g(\zeta)|\}\leqq|g(\zeta)|$.

In particular, if we choose $\eta$ sufficiently close to $\zeta$ then we have

$$|g(\eta)|\leqq 2|g(\zeta)|$$

Next we show that $f(\zeta)$ is an entire function. From the basic identity it follows that

$$g(\zeta)-g(\eta)=(\zeta-\eta)\alpha g(\zeta)\{g(\zeta)-(\zeta-\eta)\alpha g(\zeta)g(\eta)\}.$$

Hence by dividing this equation by $\zeta-\eta$ and by taking traces, we obtain

$$\frac{f(\zeta)-f(\eta)}{\zeta-\eta}-tr\ \alpha g(\zeta)^2=-(\zeta-\eta)tr\ \alpha^2 g(\zeta)^2 g(\eta).$$

Finally since $|tr\ \gamma|\leqq|\gamma|$ we conclude from the boundeness of $|g(\eta)|$ in a neighborhood of $\zeta$ that

$$\lim_{\eta\to\zeta}\frac{f(\zeta)-f(\eta)}{\zeta-\eta}=tr\ \alpha g(\zeta)^2$$

Hence $f(\zeta)$ is an entire function with $f'(\zeta)=tr\ \alpha g(\zeta)^2$

Now we can show that

$$f(\zeta)=\sum_{i=0}^{\infty}\zeta^i\ tr\ \alpha^i$$

is the Taylor series expansion for $f(\zeta)$ in a neighborhood of the origin. Furthermore, $f$ is an entire function and hence the above series describes $f(\zeta)$ and converges for all $\zeta$. In particular we have

$$\lim_{n\to\infty} tr\ \alpha^n=0$$

and this holds for all $\alpha\in JC[G]$.

We conclude the proof by showing that if $JC[G]\neq 0$ then there exists an element $\alpha\in JC[G]$ which does not satisfy the above. Indeed, suppose $\beta$ is a nonzero element of $JC[G]$ and set $\alpha=\beta\beta^*/\|\beta\|^2$. Then $\alpha\in JC[G]$ since the Jacobson radical is an ideal. Moreover, we have $\alpha=\alpha^*$ and

$$tr\ \alpha=\|\beta\|^{-2}tr\ \beta\beta^*=\|\beta\|^{-2}\|\beta\|^2=1.$$

Now the powers of $\alpha$ are also symmetric under $*$so for all $m\geqq 0$ we have

$$tr\ \alpha^{2^{m+1}}=tr\ \alpha^{2^m}(\alpha^{2^m})^*=\|\alpha^{2^m}\|^2\geqq(tr\ \alpha^{2^m})^2.$$

Hence by induction $tr\ \alpha^{2^m}\geqq 1$ for all $m\geqq 0$, and this contradicts the fact that $tr\ \alpha^n\to 0$. Thus $JC[G]=0$ and the result follows.

## References


1. Curtis, C.W. and Reiner, I., *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.
2. Dornhoff, L., *Group representation theory*, Marcel Dekher, New York, 1971.
3. Ditor, S.Z., On the group of units of ring, *Amer. Month Math.*, 1971. 522-523.
4. Feit, W. *Characters of finite groups*, Benjamin, New York 1967.
5. Gorenstein, D., *Finite groups*, Harper and Row, New York, 1968.
6. Herstein, I.N., *Non commutative rings*, Carus Mathematical Monographs, No. 15, Math. Assoc. Amer., 1971.
7. Passman, D.S., *Group rings*, Marcel Dekker, New York, 1972.