ON THE STRUCTURE OF THE TORSION SUBGROUP OF THE GROUP OF UNITS OF A GROUP RING

Walter Lane Stanley

9 MAY 1977

From: CDR Walter L. Stanley, USN 245-52-2045/1410
To: Superintendant, U.S. Naval Postgraduate School
(Technical Library)
Monterey, California 93940

Subj: Doctoral Dissertation; forwarding of

Encl: (1) "On the Structure of the Torsion Subgroup of the Group of Units of a Group Ring"

1. I have been enrolled as a Direct Doctoral Student of the George Washington University. Enclosure (1) is my Dissertation submitted to and accepted by the University in partial fulfillment of the degree requirements, and is forwarded in accordance with verbal instructions from your Code 031.

On the Structure of the Torsion Subgroup of the Group of Units of a Group Ring

By

Walter Lane Stanley

B.F.A. February 1958, University of Florida

M.S. May 1965, U.S. Naval Post-Graduate School

M.Phil. September 1974, The George Washington University

A Dissertation submitted to

The Faculty of

The Graduate School of Arts and Sciences

of the George Washington University in partial satisfaction

of the requirements for the degree of Doctor of Philosophy

Dissertation Directed by

Myrna Pike Lee

Associate Professor of Mathematics

CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

This research was conducted in part under the auspices of the Doctoral Study Program of the U.S. Naval Postgraduate Education Program.

Mickey Lee taught me my first graduate course in algebra. Since then she has been my informal, then formal advisor and friend. She has guided rather than directed my research; allowing me to explore where intuition led, and steering me along a more fruitful path only when the blind alley had been illuminated. I hope her insistence that no assertion remain unchecked has finally sunk in.

I wish to express appreciation to Mr. John R. Lastova, Jr., for his help in locating reference material when others had been unsuccessful; and to Mrs. Judy Tedesco for her superb preparation of an exceptionally difficult manuscript.

Finally, to my wife, Eloise, and to my children, Debra and Roger, whose patience and understanding when Daddy had to study was seemingly without end: Thank you. Surely any family man completes doctoral studies only with the enthusiastic encouragement and assistance of the whole family unit.

ACKNOWLEDGEMENTS

This research was conducted in part under the auspices of the Doctoral Study Program of the U.S. Naval Postgraduate Education Program.

Mickey Lee taught me my first graduate course in algebra. Since then she has been my informal, then formal advisor and friend. She has guided rather than directed my research; allowing me to explore where intuition led, and steering me along a more fruitful path only when the blind alley had been illuminated. I hope her insistence that no assertion remain unchecked has finally sunk in.

I wish to express appreciation to Mr. John R. Lastova, Jr., for his help in locating reference material when others had been unsuccessful; and to Mrs. Judy Tedesco for her superb preparation of an exceptionally difficult manuscript.

Finally, to my wife, Eloise, and to my children, Debra and Roger, whose patience and understanding when Daddy had to study was seemingly without end: Thank you. Surely any family man completes doctoral studies only with the enthusiastic encouragement and assistance of the whole family unit.

CHAPTER I
INTRODUCTION AND BACKGROUND

Let G be a group and R a ring with unity element 1_R. The group ring of R over G is denoted RG, and is the collection of all formal sums

$$\sum_{g\varepsilon G} \alpha_g g$$

where $\alpha_g \varepsilon$ R, and for all but a finite number of terms, $\alpha_g = 0$.

Operations in the group ring are:

$$\sum_{g\varepsilon G} \alpha_g g + \sum_{g\varepsilon G} \beta_g g = \sum_{g\varepsilon G} (\alpha_g + \beta_g) g$$

and

$$(\sum_{g\varepsilon G} \alpha_g g)(\sum_{g\varepsilon G} \beta_g g) = \sum_{g\varepsilon G} \gamma_g g \quad \text{where } \gamma_g = \sum_{h\varepsilon G} \alpha_h \beta_{h^{-1}g}.$$

The element $0 = \sum_{g\varepsilon G} 0.g$ is the additive identity and the element $1 = 1_R e$ is the multiplicative identity, where e is the identity of G. The collections of elements $\{1_R \cdot g : g\varepsilon G\}$ and $\{\alpha \cdot e : \alpha\varepsilon R\}$ are isomorphic to G and R respectively, and we freely consider, therefore, that $R \subset RG$ and $G \subset RG$.

Any element $a \varepsilon RG$ which has the special form $a = \alpha g$, $\alpha\varepsilon R$, $g\varepsilon G$; is called a trivial element. Clearly G and $R \subset RG$ are composed of trivial elements. A unit in RG is, as expected, an element $u \varepsilon RG$ for which there exists an element $u^{-1} \varepsilon RG$ such that $uu^{-1} = 1$. A unit which is a trivial element is called a trivial unit. A unit of finite order k is an element satisfying $u^k = 1$, and $u^d \neq 1$ for every $0 < d \leq k$.

The question of the structure of units, and particularly of the structure of units of finite order, in the group ring has evoked considerable

interest. Knowledge of the structure of the units of finite order in ZG, where G is a finite Abelian group and Z is the ring of rational integers, leads directly to solution of the group ring isomorphism problem for this class of group rings. In particular, it is shown by Higman (4), that since the only trivial units of finite order in ZG are $\pm g$, then ZG $\simeq$ ZH if and only if G $\simeq$ H.

Most of the work to date has dealt with group rings RG in which R has been restricted to be either a field (usually an algebraic number field) or a ring of algebraic integers in an algebraic number field. Passman (6), for example, considers group algebras KG and shows that if G is not torsion free, and if $|K| \geq 3$, then KG has non-trivial units. A T.U.P. group (two-unique-product group) is one such that for any two finite non-empty subsets, A and B of G, with $|A| + |B| > 2$, there are at least two distinct elements $x, y \in G$ which have unique representations in the form $x = ab$; $y = cd$; with $a, c \in A$; $b, d \in B$.

Passman shows that if G is a T.U.P. group KG has only trivial units. Further, if G admits a strict linear ordering such that $x < y$ implies that $xz < yz$ for all $x, y, z \in G$, it is called an ordered group, and Passman proves that an ordered group is a T.U.P. group.

Continuing, he also shows that every torsion free Abelian group can be ordered. Thus, he has demonstrated that a large class of groups exists for which the group algebra KG has only trivial units. Clearly, for this same class of groups, RG has only trivial units where $R \subset K$.

Higman (4), in 1940, considered both units and units of finite order in group rings RG where R is an algebraic number field or its ring

of algebraic integers; in each case, of characteristic zero. For finite Abelian groups he showed that RG has only trivial units of finite order whenever R is a ring of algebraic integers, however even for ZG he showed the existence of non-trivial units unless G is the direct product of:

(1) s cyclic groups of order 2; and

(2) either (a) m cyclic groups of order 3 ($m \geq 0$) or

(b) n cyclic groups of order 4 ($n \geq 0$).

In the non-Abelian case he showed that if $G^* = G \times \langle h \rangle$ where $h^2 = e$, and all the units in ZG are trivial, then all the units in ZG* are trivial. He also proved that for G the group of quarternions, all the units in ZG are trivial.

Further results in the same paper include: If all the elements of a group G have finite order, then ZG has non-trivial units unless:

(1) G is an Abelian group, the orders of whose elements all divide four, or

(2) G is an Abelian group, the orders of whose elements all divide six, or,

(3) G is the direct product of a quarternion group and an Abelian group, the orders of whose elements all divide two.

Finally, he shows that if G is an infinite group which is indicable throughout, and R has no zero divisors, then RG has only trivial units. (A group is indicable throughout if for every non-trivial subgroup, there exists a homomorphism from the subgroup into Z whose image is not zero alone.)

Berman (1), in 1953, proved that the group ring ZG has non-trivial units of finite order unless G is Abelian or Hamiltonian of order a power of two. His work, then, in conjunction with Higman's results leads to this conclusion: If G is a finite group, neither Abelian nor Hamiltonian of order a power of two then RG has non-trivial units of finite order, where R is arbitrary of characteristic zero.

In 1974, Gerald Losey (5), proved that if G is a finite group and ZG contains a non-trivial unit of finite order, then it contains infinitely many of them. An excellent survey of results on units in the group ring has been prepared by Keith Dennis (3).

As can be seen, the major thrust of the work on units of finite order has thus far centered around the more familiar rings, and has explored the effect of the structures of various groups upon the problem. In view of the work of Higman and Berman, it would seem profitable to explore necessary and sufficient conditions on the ring to assure that all units of finite order are trivial in the group ring, where the group under consideration is either Abelian or Hamiltonian of order a power of two.

In this paper we restrict our consideration to the case of finite Abelian groups, but generalize the ring structure considerably; namely, we consider arbitrary integral domains of characteristic zero. Under these conditions on R and G we obtain necessary and sufficient conditions on the structure of R for RG to have only non-trivial units of finite order. This is the major result of Chapter II.

In Chapter III, we examine those group rings known to contain units of finite order which are non-trivial. For arbitrary integral domains R we find an upper bound on the order of the group of units of finite order

in RG. When K is a field, we construct the generators of the group of units of finite order of KG, and exhibit the structure of this group of units.

Appendix A contains results from the theory of group representations and group characters which are required in our proofs. Notation throughout is unavoidably cumbersome and an index of notation follows the Appendix.

Lemmas and theorems are numbered consecutively within each chapter and the appendix in the form X.n where X is the chapter number and n is the sequence of the theorem or lemma in the chapter. Referenced equations are numbered in parentheses at the extreme right, consecutively within a chapter. Reference to equations outside the chapter of the citation will always cite the chapter.

CHAPTER II
GROUP RINGS, ALL OF WHOSE UNITS OF FINITE ORDER ARE TRIVIAL

In this chapter, all rings are integral domains of characteristic zero, and all groups are Abelian with finite order. Let R be such a ring, G a group, and RG be the group ring of R over G. Let U(RG) be the group of units in RG, and TU(RG) be its torsion subgroup. An element of U(RG) is called trivial if it is of the form αg, where $\alpha \in U(R)$ and $g \in G$. We will determine necessary and sufficient conditions on R for all elements of TU(RG) to be trivial.

Lemma 2.1: $TU(RG) \subset TU(Q(\Delta)G)$ where Δ is a (not necessarily finite) set of roots of unity.

Proof: Let $[G:1] = n$ and exponent of $G = m$. Let K be the quotient field for R. Since char R = char K = 0, $Q \subset K$. Let ζ be a primitive m^{th} root of unity. Then $Q(\zeta) \subset K(\zeta)$, and since $Q(\zeta)$ is a splitting field for G, so is $K(\zeta)$. (See theorems A.13 and A.14 of Appendix A.) Hence we have an isomophism Φ:

$$\Phi: K(\zeta)G \to K(\zeta) \oplus \ . \ . \ . \ \oplus K(\zeta) \text{ (n-copies)} = K(\zeta)^n$$

Let $\Gamma^{(0)}, \ldots, \Gamma^{(n-1)}$ be the n mutually inequivalent one-dimensional $Q(\zeta)$ representations of G. We may associate each representation $\Gamma^{(i)}$, with its character $\chi^{(i)}$. (See the discussion preceding theorem A.13 Appendix A.) We will denote the value of $\chi^{(i)}$ at g_j by $\chi_j^{(i)}$. Now an element $a \in RG$ is mapped by Φ onto an n-tuple in $K(\zeta)^n$, say $\Phi(a) = (\beta_0, \ldots, \beta_{n-1})$, since $RG \subset K(\zeta)G$. From the corollary to theorem A.15

of Appendix A we may determine the β_j by the equation:

$$\beta_j = \sum_{i=0}^{n-1} \alpha_i \overline{\chi_i^{(j)}} \qquad (j = 0, \ldots, n-1) \qquad (1)$$

or conversely given $\Phi(a) = (\beta_0, \ldots, \beta_{n-1})$, we may determine the coefficients α_j from:

$$\alpha_j = 1/n \sum_{i=0}^{n-1} \beta_i \chi_j^{(i)} \qquad (j = 0, \ldots, n-1) \qquad (2)$$

Now let $u \in TU(RG)$. Since the order of finite units is preserved under Φ, and $\Phi(u) = (\beta_0, \ldots, \beta_{n-1})$, if $u^k = 1$, then $(\beta_0, \ldots, \beta_{n-1})^k = 1$. Hence $(\beta_0^k, \ldots, \beta_{n-1}^k) = 1$ from which we see that

$$\beta_i^k = 1 \qquad (i = 0, \ldots, n-1)$$

and each β_i must be a root of unity. Applying this constraint on the permissible values for the β_i to equation (2) illustrates that each α_j is a sum of products of roots of unity divided by an element of Z. Therefore we have shown that $u \in TU(RG)$ implies that $u \in TU(Q(\delta)G)$ for some root of unity δ.

Clearly δ is dependent upon the particular $u \in TU(RG)$ under consideration. Let $\Delta = \{\delta : \delta \in R \text{ and } \delta^j = 1 \text{ for some } j\} \cup \{\zeta\}$

Now since K is the quotient field for R, any root of unity is in K if and only if it is in R. Hence for any unit $u \in TU(RG)$ the root of unity for which $u \in TU(Q(\delta)G)$ is either in R or is ζ. In either case it is in Δ. Thus $u \in TU(Q(\Delta)G)$.

Let ξ be an arbitrary root of unity and $G(Q(\xi)/Q)$ be the Galois group of $Q(\xi)$ over Q. For $\sigma \in G(Q(\xi)/Q)$ we extend the operation of σ to all of $Q(\xi)G$ by letting σ operate trivially on G and extending linearly.

Then for $a \in Q(\xi)G$, $a = \sum_{i=0}^{n-1} \alpha_i g_i$, $\sigma(a) = \sum_{i=0}^{n-1} \sigma(\alpha_i) g_i$.

Lemma 2.2: Let $[G:1] = n$, $u = \sum_{j=0}^{n-1} \alpha_j g_j \in TU(RG)$, $\alpha_j \in R$, $g_j \in G$. Let δ be a primitive root of unity of minimal order such that $u \in Q(\delta)G$. If no prime divisor of n is a unit in R, then the Norm from $Q(\delta)$ to Q of α_j, $N(\alpha_j)$, is a rational integer $(j=0, \ldots, n-1)$.

Proof: Consider an arbitrary but fixed α_j. By equation (2):

$$\alpha_j = 1/n \sum_{i=0}^{n-1} \beta_i \chi_j^{(i)}$$

Now by hypothesis, $\alpha_j \in Q(\delta) \cap R$ and certainly $N(\alpha_j) \in Q$. Consider the action of any $\sigma \in G(Q(\delta)/Q$ on α_j:

$$\sigma(\alpha_j) = 1/n \sum_{i=0}^{n-1} \sigma\beta_i \sigma\chi_j^{(i)}.$$

Since $\beta_i \in Q(\delta)$ and is in fact a power of δ, $\sigma\beta_i \in Z(\delta)$ and the same is true of $\sigma\chi_j^{(i)}$. Let

$$\gamma_j = \sum_{i=0}^{n-1} \beta_i \chi_j^{(i)}$$

Then $\sigma(\alpha_j) = (1/n)\,\sigma(\gamma_j) \in R(\delta)$ and $\sigma(\gamma_j) \in Z(\delta)$. Hence it is evident that $N(\gamma_j) \in Z$, say $N(\gamma_j) = c$, and so if $e = [G(Q(\delta)/Q:1]$:

$$N(\alpha_j) = \prod_{\sigma \in G(Q(\delta)/Q)} \sigma(\alpha_j) = c/n^e \in R(\delta) \cap Q, \text{ and so, } c/n^e \in R \cap Q$$

It remains to show that $c/n^e \in Z$. Suppose not. Then $(c, n^e) = d$ and we may write $c/n^e = c_o/n_o$ where $(c_o, n_o) = 1$, and $n^e = n_o d$, and $n_o \neq 1$. Then there exist $s, t \in Z$ such that $c_o s + n_o t = 1$, whence $(c_o/n_o)s + t = 1/n_o$. Now $c_o/n_o \in R$, so $(c_o/n_o)\, s \in R$ and since $t \in Z \subset R$, we have $1/n_o \in R$. There is a prime, p, dividing n_o since $n_o \neq 1$, and we may write $n_o = pr$. Then $r(1/n_o) = 1/p \in R$, contradicting the hypothesis that no prime divisor of n is a unit in R. Consequently, $n_o = 1$ and $c/n^e = N(\alpha_j) \in Z$ as required.

It is lemma 2,2 that allows Higman's theorem on trivial units of finite order to be extended to a much larger class of group rings (see Theorem 3 of Higman (4)). In fact, lemma 2.2 provides the means by which Higman's proof can be used intact.

Theorem 2.3 Let R be an integral domain of characteristic zero, and G be an Abelian group of order $n > 2$. If any prime divisor of n is a unit in R then RG has non-trivial units of finite order. Conversely, if no prime divisor of n is a unit in R then RG has only trivial units of finite order.

Proof: First, suppose $n = 2^k$ $(k > 1)$. If $\frac{1}{2} \in R$, there exist g, h; distinct elements of G. Then

$$\tfrac{1}{2}(1 - g - h - gh)$$

is a unit of order 2 in RG.

If $n \neq 2^k$, by the Fundamental Theorem of Abelian Groups, $G = C_1 \times \dots \times C_k$ where each C_i is cyclic of order a power of a prime divisor of n. Furthermore, for each $p|n$, there is some i such that C_i is of order a power of p, and C_i contains an element c_i of order p. Then

$$1/p(2\sum_{j=0}^{p-1} c_i^{\,j} - pc_i)$$ is a unit of order 2p if $p > 2$, otherwise of order 2.*

Assume conversely that no prime divisor of the order of G is a unit in R. Let $u = \sum_{i=0}^{n-1} \alpha_i g_i$ be a unit of finite order k in RG. By lemma 2.1 there is a cyclotomic extension of Q, $Q(\xi)$, containing each α_i $(i = 0, \dots, n-1)$, and such that $Q(\xi)$ is a splitting field for G.

---

*The two examples of non-trivial units do not depend upon the commutativity of the group. Thus this part of the theorem is also valid for non-Abelian groups.

By lemma 2.2, for any $\alpha_i \neq 0$, $N(\alpha_i)$ is a rational integer. The balance of the proof is due to Higman (4).

Since u is a unit, some $\alpha_j \neq 0$. For this j, since $\alpha_j \varepsilon\ Q(\xi)$, the absolute value function is well-defined.

$$|\alpha_j| = |(1/n)\sum_{i=0}^{n-1} \beta_i \chi^{(i)}(g_j)| \leq (1/n)\sum_{i=0}^{n-1} |\beta_i \chi^{(i)}(g_j)| = 1 \tag{4}$$

and the same is true for each conjugate of α_j, $\sigma(\alpha_j)$, $\sigma\ \varepsilon\ G(Q(\xi)/Q)$. The product

$$\prod_{\sigma\ \varepsilon\ G(Q(\xi)/Q)} \sigma(\alpha_j) = N(\alpha_j)$$

and this product is a rational integer. Hence, in (4) we must have equality ($|\alpha_j| = 1$) and therefore

$$\beta_o\chi^{(o)}(g_j) = \beta_1\chi^{(1)}(g_j) = \dots = \beta_{n-1}\chi^{(n-1)}(g_j) = \alpha_j$$

so
$$\beta_i = \alpha_j \overline{\chi^{(i)}(g_j)} \qquad (i = 0, \dots, n-1) \tag{5}$$

Consider α_k, $k \neq i$. From equation (2)

$\alpha_k = (1/n)\sum_{i=0}^{n-1} \beta_i \chi^{(i)}(g_k)$ and using (5):

$$\alpha_k = (1/n) \sum_{i=0}^{n-1} \alpha_j \overline{\chi^{(i)}(g_j)}\chi^{(i)}(g_k)$$

$$= (\alpha_j/n)\sum_{i=0}^{n-1} \overline{\chi^{(i)}(g_j)}\chi^{(i)}(g_k) = (\alpha_j/n)\delta_{jk}[G:1]$$

$$= 0 \qquad (k = 0, \dots, n-1;\ k \neq j)$$

by the orthogonality relations on group characters (see Appendix A equation (7)).

Hence $u = \alpha_j g_j$ and is a trivial unit.

Denote by ε: $RG \to R$ the augmentation map defined by

$$\varepsilon(a) = \varepsilon\left(\sum_{i=0}^{n-1} \alpha_i g_i\right) = \sum_{i=0}^{n-1} \alpha_i$$

Let $\operatorname{Ker} \varepsilon|_{U(RG)} = V(RG)$. For R a commutative ring as in the present case, we obtain the decomposition

$$U(RG) = V(RG) \times U(R)$$

In 1974 H. Zassenhaus (8) proved that if G is a finite group and R a commutative domain, then if no prime divisor of the order of G is a unit in R, the order of any torsion element of V(RG) is a divisor of the exponent of G.

<u>Corollary to Theorem 2.3:</u> Under the hypotheses of the theorem, if no prime divisor of the order of G is a unit in R, then the torsion subgroup of V(RG) is isomorphic to G.

Proof: Immediate from the theorem, since every element in TU(RG) is of the form αg where $\alpha \in U(R)$.

In the next chapter we will examine the structure of the torsion group of units of group algebras which have non-trivial elements. By a simple counting argument we shall also prove that all units of finite order when G has order 2 are trivial, thus including the one case excluded by the hypotheses of Theorem 2.3.

CHAPTER III

THE STRUCTURE OF TU(RG)

Again in this chapter, all rings are integral domains with characteristic zero, and all groups are Abelian of finite order. In chapter II we obtained a complete characterization of those group rings with only trivial units of finite order. Although this result greatly expands the class of group rings known to be so characterized, there remains a large class containing non-trivial units of finite order. In particular, all group algebras KG, where char K = 0, and G is finite Abelian, are in the latter class.

In this chapter we shall examine the torsion subgroup of the group of units of group rings known to contain non-trivial elements. We shall examine the structure of TU(RG) itself, determine its order, and when R = K, a field, derive its generators.

Information on the structure of TU(KG) is most readily determined from the decomposition of KG into a direct sum of fields. We recall that

$$KG \simeq K_0 \oplus \ldots \oplus K_{d-1} \qquad \text{where } d \leq [G:1],$$

and that a unit of finite order in this decomposition has the form $(\beta_0, \ldots, \beta_{d-1})$ where each β_i is a root of unity ($i \leq d-1$). Let us denote the isomorphism by:

$$\Phi: \; KG \to K_0 \oplus \ldots \oplus K_{d-1}.$$

<u>Theorem 3.1</u>: TU(Φ(KG)) is generated by the set of d-tuples

charac

chap

with

repeat

remai

partic

Abelian

of va

examin

R = l

from t

and tha

(Up

densty

Theore

$\{\Phi(u^{(i)}) = u_i = (1, \ldots, \beta_i, 1, \ldots, 1) : i = 0, \ldots, d-1$, and each β_i is a primitive root of unity of maximal order in $K_i\}$,

provided that K does not contain all roots of unity.

Proof: By lemma 2.1 $TU(KG) \subset TU(Q(\Delta))$ where Δ is the set of roots of unity contained in K. If Δ is a finite set, then there is a root of unity, η, such that $Q(\Delta) = Q(\eta)$. In the direct sum decomposition $\Phi(KG)$, therefore, each K_i contains a maximal cyclotomic extension of Q which is itself contained in $Q(\eta)$. Let the roots of unity which generate that extension be denoted ξ_i, $i = 0, \ldots, d-1$. Then every element of $TU(\Phi(KG))$ is of the form

$$(\xi_0^{n_0}, \ldots, \xi_{d-1}^{n_{d-1}}) = \prod_{i-0}^{d-1} u_i^{n_i}$$

It is clear that the set $\{u_i\}_{i=0}^{d-1}$ is independent.

<u>Corollary 1</u>: If K contains only a finite number of roots of unity, then $TU(KG)$ is isomorphic to a direct product of cyclic groups, $C_0 \times \ldots \times C_{d-1}$, where C_i is of the same order as ξ_i.

Proof: Obvious, since ξ_i generates a cyclic group of the required order.

<u>Corollary 2</u>: Let k_i be the order of ξ_i. Then the order of $TU(KG)$ is $\prod_{i=0}^{d-1} k_i$.

<u>Corollary 3</u>: Let G be a group of order 2. Then for any R, every $u \in TU(RG)$ is trivial.

Proof: Let K be any field containing R, and let η be a primitive root of unity of order k, such that $Q(\eta)$ is the maximal cyclotomic extension of Q contained in K. Since exp G = 2, Q is a splitting field for G, hence so is $Q(\eta)$. Then $KG \simeq K \oplus K$, and by corollary 2, the order of $TU(KG)$ is k^2. Now $G = \{e, g\}$ so the trivial units of finite order are $\eta^i g$ and $\eta^i e$ $(i = 0, \ldots, k-1)$. Hence there are exactly k^2 trivial units of finite order, exhausting the elements in $TU(KG)$.

Theorem 3.2: Let K be a field containing only finitely many roots of unity. Let G_1 and G_2 be Abelian groups of order n. Let k be the order of the maximal root of unity which is an element of K. Then if $\exp G_1 = \exp G_2 \leq k$, $TU(KG_1) \simeq TU(KG_2)$.

Proof: Since $\exp G_i \leq k$, it follows that K is a splitting field for G_i. Then by Corollary 1 to Theorem 3.1,

$TU(KG_1) \simeq C_1 \times \ldots \times C_{n-1}$; $TU(KG_2) \simeq C'_1 \times \ldots \times C'_{n-1}$ where the C_i and the C'_i are each of order k.

Hence, with an appropriate reindexing, $C_i \simeq C'_i$ $(i = 0, \ldots, n-1)$ and $TU(KG_1) \simeq TU(KG_2)$.

It is quite clear that even for an arbitrary field K, TU(KG) can be studied by restricting our attention to the largest cyclotomic extension of Q contained in K. Similarly, for an arbitrary ring R, it is sufficient to study the largest cyclotomic extension of Q contained in its quotient field in order to bound the order of TU(RG). We shall therefore continue our study of the torsion subgroup of the group of units by restricting attention to group rings of cyclotomic extensions of Q (and appropriate subrings thereof) over G.

While theorem 3.1 adequately describes the structure of TU(KG), it is clear that TU(KG) is unmaneageably large for even quite small groups. And unfortunately, theorem 3.1 tells us nothing of the form of an individual unit in TU(KG) as the more familiar formal sum. Our immediate purpose is to determine the form of the generators of TU(KG) as formal sums.

Let ζ be a primitive m^{th} root of unity where m is odd. Then if m is the exponent of G, $Q(\zeta)$ is the minimal splitting field for G.

Although $Q(-\zeta)$ is the same field as $Q(\zeta)$ and $-\zeta$ is a primitive $2m^{th}$ root of unity, the values of the characters of G will take on only values which are m^{th} roots of unity. Obviously the same difficulty does not prevail if the exponent of G is even. We can avoid consideration of special cases according to the value of the exponent of G, and at the same time consider other than minimal splitting fields by an appropriate adjustment of notation. We shall consistently use a small Greek letter (usually ζ) to denote a primitive root of unity of order the exponent of G, and a distinct Greek letter (usually η) to denote that primitive root of unity of maximal even order in K by which we extend Q. It is to be remembered, nonetheless, that so long as we consider splitting fields for G, ζ will always be some power of η.

<u>Theorem 3.3</u>: Let $K = Q(\eta)$ be any splitting field for G, an Abelian group of order n. Then the generators of TU(KG) are:

$$u^{(i)} = 1 - \frac{1-\eta}{n} \sum_{j=0}^{n-1} \chi^{(i)}(g_j)g_j \quad (i = 0, \ldots, n-1) \tag{1}$$

Proof: We identify the n linearly independent one-dimensional representations of G with their characters, $\chi^{(0)}, \ldots, \chi^{(n-1)}$ and agree that $\chi^{(0)}$ is the trivial character. From equation (2) of Chapter II, the coefficient of g_j for an arbitrary $a = \sum_{i=0}^{n-1} \alpha_i g_i \in KG$ is:

$$\alpha_j = (1/n) \sum_{r=0}^{n-1} \beta_r \chi^{(r)}(g_j) \qquad (j = 0, \ldots, n-1)$$

Let $u^{(i)}$ be that generator of TU(KG) whose image under Φ contains $\beta_i = \eta$ in the i^{th} component, and contains $\beta_k = 1$ whenever $k \neq i$. Then the coefficient of g_j in $u^{(i)}$ is:

$$\alpha_j^{(i)} = (1/n) \sum_{r=0, r\neq i}^{n-1} \chi^{(r)}(g_j) + \eta\chi^{(i)}(g_j)$$

$$= (1/n) \sum_{r=0}^{n-1} \chi^{(r)}(g_j) - \chi^{(i)}(g_j) + \eta\chi^{(i)}(g_j)$$

and so:

$$u^{(i)} = \sum_{j=0}^{n-1} [(1/n) \{\sum_{r=0}^{n-1} \chi^{(r)}(g_j) - \chi^{(i)}(g_j)(1-\eta)\}]g_j.$$

Since by equation (3) of Appendix A,

$$\sum_{r=0}^{n-1} \chi^{(r)}(g_j) = \begin{cases} 0 & (g_j \neq e) \\ n & (g_j = e) \end{cases}$$

$$u^{(i)} = (1/n)(n - (1 - \eta)) + \sum_{j=1}^{n-1} (1/n)(-\chi^{(i)}(g_j)\ (1 - \eta))g_j$$

$$= 1 - (1 - \eta)/n(1 + \sum_{j=1}^{n-1} \chi^{(i)}(g_j)\ g_j)$$

$$= 1 - (1 - \eta)/n - (1 - \eta)/n \sum_{j=1}^{n-1} \chi^{(i)}(g_j)\ g_j$$

Since $\chi^{(i)}(e) = 1$, we have:

$$u^{(i)} = 1 - (1 - \eta)/n(\sum_{j=0}^{n-1} \chi^{(i)}(g_j)g_j) \text{ as required.}$$

Based upon the set of generators derived in Theorem 3.3, we will find equations for the general form of any unit of finite order in KG whenever K is a splitting field for G. We seek an expression of the form:

$$u = \prod_{i=o}^{n-1} (u^{(i)})^{k_i} = \sum_{j=0}^{n-1} \alpha_j g_j \qquad \text{where each } k_i \leq [<\eta>:1]$$

The following computational lemma will be required in the derivation of the equations.

<u>Lemma 3.4</u>: Let $A = (\sum_{j=0}^{n-1} \chi^{(r)}(g_j)g_j)(\sum_{j=0}^{n-1} \chi^{(s)}(g_j)g_j)$. Then:

$$A = \delta_{rs} \cdot n \cdot \sum_{j=0}^{n-1} \chi^{(r)}(g_j)g_j \qquad \text{where } \delta_{rs} = \begin{cases} 1 & (r=s) \\ 0 & (r\neq s) \end{cases}$$

is the Kroneker Delta function.

Proof:

$$(\sum_{j=0}^{n-1} \chi^{(r)}(g_j)g_j)(\sum_{j=0}^{n-1} \chi^{(s)}(g_j)g_j)$$

$$= \sum_{j=0}^{n-1} \chi^{(r)}(g_j)g_j + \sum_{j=0}^{n-1} \chi^{(r)}(g_j)\chi^{(s)}(g_1)g_jg_1 + \dots$$

$$\dots + \sum_{j=0}^{n-1} \chi^{(r)}(g_j)\chi^{(s)}(g_{n-1})g_jg_{n-1}$$

Consider the coefficient of g_k for arbitrary k:

$$\alpha_k = \chi^{(r)}(g_k) + \chi^{(r)}(g_1^{-1}g_k)\ \chi^{(s)}(g_1) + \dots + \chi^{(r)}(g_{n-1}^{-1}g_k)\chi^{(s)}(g_{n-1})$$

$$= \chi^{(r)}(g_k)\ \{1 + \chi^{(r)}(g_1^{-1})\chi^{(s)}(g_1) + \dots + \chi^{(r)}(g_{n-1}^{-1})\ \chi^{(s)}(g_{n-1})\}$$

$$= [G:1]\delta_{rs}\ \chi^{(r)}(g_k) \quad \text{by equation (5) of Appendix A.}$$

Summing over all group elements yields:

$$A = n\delta_{rs}\sum_{j=0}^{n-1} \chi^{(r)}(g_j)g_j \qquad \text{as required.}$$

<u>Theorem 3.5</u>: Let $K = Q(\eta)$ (η a d^{th} root of unity) be a splitting field for G, a finite Abelian group. Let $u^{(0)}, \dots, u^{(n-1)}$ as defined in theorem 3.3 be the generators of TU(KG). Then:

a) $$(u^{(r)})^k = 1 - (1 - \eta^k)/n\sum_{j=0}^{n-1} \chi^{(r)}(g_j)g_j \tag{2}$$

b) $$u^{(r)}u^{(s)} = 1\ (1 - \eta)/n\sum_{j=0}^{n-1} (\chi^{(r)}(g_j) + \chi^{(s)}(g_j))g_j \quad (r \neq s) \tag{3}$$

c) $$u = (u^{(0)})^{k_o}(u^{(1)})^{k_1}\dots(u^{(n-1)})^{k_{n-1}}$$

$$= 1 - 1/n\sum_{j=0}^{n-1}\{\sum_{i=0}^{n-1}(1 - \eta^{k_i})\chi^{(i)}(g_j)\}g_j \tag{4}$$

$(k, k_o, \dots, k_{n-1} \leq d-1)$.

Proof:

a) By induction on k. If k = 1, then the form is just that of $u^{(r)}$.

Assume the equation is true for k-1. Then: $(u^{(r)})^k = (u^{(r)})^{k-1}u^{(r)}$

$$= (1-(1-\eta^{k-1})/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j)(1-(1-\eta)/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j)$$

$$= 1 - (1-\eta^{k-1})/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j - (1-\eta)/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j)$$

$$+ (1-\eta)(1-\eta^{k-1})/n^2(n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j)$$

the final term being obtained by application of lemma 3.4.

$$(u^{(r)})^k = 1 - 1/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j[(1-\eta) + (1-\eta^{k-1}) - (1-\eta)(1-\eta^{k-1})]$$

$$= 1 - (1 - \eta^k)/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j \quad \text{as required for part a.}$$

b) $$u^{(r)}u^{(s)} = (1 - (1-\eta)/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j)(1 -(1-\eta)/n\sum_{j=0}^{n-1}\chi^{(s)}(g_j)g_j)$$

$$= 1 - (1-\eta)/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j - (1-\eta)/n\sum_{j=0}^{n-1}\chi^{(s)}(g_j)g_j$$

$$+ (1-\eta)/n\sum_{j=0}^{n-1}\chi^{(r)}(g_j)g_j\sum_{j=0}^{n-1}\chi^{(s)}(g_j)g_j.$$

By application of lemma 3.4, the final term is zero when $r \neq s$, and hence by collecting coefficients of each g_j we have the required equation for part b.

c) We shall prove part c by an induction argument on the number of generators which are raised to a non-zero power. There is no harm in renumbering the generators so that the first t of them are raised to a non-zero power while $u^{(t)}, \ldots u^{(n-1)}$ are raised to the zeroth power and are hence equal to one. Then if $t = 1$, the assertion is true by part a. Assume part c is true for t-1. Then if

$$u = (u^{(0)})^{k_0} \cdots (u^{(t-1)})^{k_{t-1}} (u^{(t)})^{k_t}$$

$$= (1 - 1/n \sum_{j=0}^{n-1} \{ \sum_{i=0}^{t-1} (1-\eta^{k_i}) \chi^{(i)}(g_j) \} g_j)(u^{(t)})^{k_t}$$

$$= 1 - 1/n \sum_{j=0}^{n-1} \{ \sum_{i=0}^{t-1} (1-\eta^{k_i}) \chi^{(i)}(g_j) \} g_j)(1 - (1-\eta^{k_t})/n \sum_{j=0}^{n-1} \chi^{(t)}(g_j) g_j)$$

$$= 1 - 1/n \sum_{j=0}^{n-1} \{ \sum_{i=0}^{t-1} (1-\eta^{k_i}) \chi^{(i)}(g_j) \} g_j - 1/n(1-\eta^{k_t}) \chi^{(t)}(g_j) g_j,$$

the cross-product term being zero by lemma 3.4. Hence

$$u = 1 - 1/n \sum_{j=0}^{n-1} \{ \sum_{i=0}^{t} (1-\eta^{k_i}) \chi^{(i)}(g_j) \} g_j \qquad \text{as required.}$$

Corollary: If G is cyclic of order m, and ζ is a primitive m^{th} root of unity, then parts a, b, and c of the theorem become:

a) $(u^{(r)})^k = 1 - (1-\eta^k)/m \sum_{j=0}^{m-1} \zeta^{rj} g^j$

b) $u^{(r)} u^{(s)} = 1 - (1-\eta)/m \sum_{j=0}^{m-1} (\zeta^{rj} + \zeta^{sj}) g^j$

c) $u = (u^{(0)})^{k_0} \cdots (u^{(n-1)})^{k_{n-1}}$

$$= 1 - 1/m \sum_{j=0}^{m-1} \{ \sum_{i=0}^{m-1} (1 - \eta^{k_i}) \zeta^{ij} g^j$$

Proof: Let G be generated by g. Then the characters, $\chi^{(r)}(g^j)$ are given by $\chi^{(r)}(g^j) = \zeta^{rj}$. Substitution in the theorem yields the required results.

Theorem 3.5 completely describes the elements of TU(KG) when K is a splitting field for G. In particular, the n elements $u^{(i)}$ ($i = 0, \ldots, n-1$) are the generators for TU(KG). We next expand the theory to group algebras, LG, where L is not a splitting field for G. We will find generators

$v^{(0)}, \ldots, v^{(d-1)}$ for TU(LG) and prove that each $v^{(i)}$ is of the form $\prod_{j=0}^{n-1} (u^{(j)})^{k_j}$.

Since L is a field, LG is semi-simple, and so is isomorphic to a direct sum of simple rings, say:

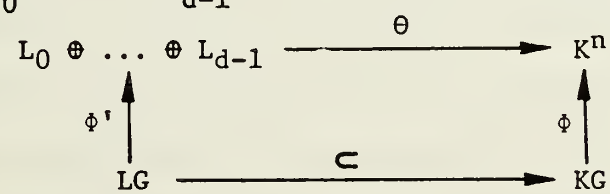
$$\Phi' : LG \rightarrow L_0 \oplus \ldots \oplus L_{d-1}.$$

Furthermore, these rings, L_r ($r = 0, \ldots, d-1$) are themselves fields. As before, we shall denote the minimal splitting field for G containing L by K. Clearly $LG \subset KG$, and the embedding is simply inclusion. Also, we have the isomorphism

$$\Phi: \ KG \ \rightarrow \ K^n$$

We wish to define an embedding:

Θ: $L_0 \oplus \ldots \oplus L_{d-1} \rightarrow K^n$ which will make the diagram



commute. The embedding must thus satisfy:

$$\Theta \circ \Phi' = \Phi|_{LG}.$$

By theorem 3.1, the generators of TU(LG) are given by $(1, \ldots, \beta_r, 1, \ldots, 1)_{r=0}^{d-1}$ considered as elements of $L_0 \oplus \ldots \oplus L_{d-1}$, where β_r is a primitive root of unity of maximal order contained in L_r and each component of the r^{th} generator is 1, except for the r^{th} one. To determine the form of the generators as elements $\sum_{i=0}^{n-1} \alpha_i g_i$ in LG, we must either determine Φ' or determine Θ, whence

$$v^{(r)} = \Phi'^{-1}(1, \ldots, \beta_r, 1, \ldots, 1) = \Phi^{-1}(\Theta(1, \ldots, \beta_r, 1, \ldots, 1))$$

Now Φ is known and was used in the previous work, and it turns out to be more straightforward to determine Θ than Φ'. This is the course we shall follow.

Higman's theorem 1 (4) shows the form of the direct sum decomposition of LG in that both the value of d and the structure of each L_r is exhibited. In the course of his proof, he also constructs the required embedding Θ, albiet somewhat obscurely for our purposes. In what follows, we have restructured his theorem and proof so as to clearly exhibit the required embedding.

We must work simultaneously in four rings, and the notation is not straightforward. It can be simplified and clarified somewhat by recasting some previous work in terms of matrices. For any ring R, and a finite group G, we may consider an element $a = \sum_{i=0}^{n-1} \alpha_i g_i$ in RG as an n-tuple $A = (\alpha_0, \ldots, \alpha_{n-1})$ in R^n, where addition is componentwise addition, and multiplication is a convolution, with the convolution rule established by the multiplication table of the group. Let, now, G be finite Abelian, and R = K, a splitting field for G. Let $B = (\beta_0, \ldots, \beta_{n-1})$ be the image of a in the direct sum decomposition of $KG \simeq K^n$. It is easy to verify that equations (2) of Chapter II may be replaced by the matrix equation

$$A = B\,(1/n)X \quad \text{where} \tag{5}$$

$$X = \begin{pmatrix} \chi^{(0)}(g_0) & \cdots & \chi^{(0)}(g_{n-1}) \\ \vdots & \ddots & \vdots \\ \chi^{(n-1)}(g_0) & \cdots & \chi^{(n-1)}(g_{n-1}) \end{pmatrix}$$

Similarly, equations (1) of Chapter II become the matrix equation

$$B = A\,\overline{X}^T \tag{6}$$

where $\overline{X}^T$ is the conjugate transpose of X.

Now let π be a permutation of (0, ..., n-1). It is obvious that if π is applied to the rows of X and the columns (components) of B in equation (5), that the vector A is unchanged. We observe that this fact permits the assigment of arbitrary indices to the characters of G so long as the corresponding indices are assigned to components of B.

Let $K = L(\zeta)$ be a minimal splitting field for G containing L. Hence ζ is a primitive m^{th} root of unity (m = exp G). Let G(K/L) be the Galois group of automorphisms of K leaving L fixed. The effect of any $\sigma \in G(K/L)$ on a root of unity of K is to map it to another root of unity of the same order. Then if $\chi^{(i)}$ is one of the characters of G, $\sigma(\chi^{(i)})$ is also one of the characters of G.
Suppose $\sigma(\chi^{(i)}) = \chi^{(j)}$. We denote the effect of σ then, by saying $\sigma(\chi^{(i)}) = \chi^{(\sigma(i))}$, that is, by defining $\sigma(i) = j$. This notation is convenient, but one must be careful to remember that i,j in this case are not to be considered as elements of L or K. Indeed, $i,j \in Z/(n)$.

We define a relation, <u>conjugacy</u>, among the characters of G by defining $\chi^{(i)}$ to be conjugate to $\chi^{(j)}$ if there is a $\sigma \in G(K/L)$ such that $\sigma(i) = j$. Clearly, conjugacy is an equivalence relation, and hence partitions the class of characters of G into classes which we shall denote $C_0, \ldots, C_{d-1}$. (We will show that the number of classes is, in fact, the number of fields in the decomposition of LG. In anticipation, then, we use d as this common number.) We let c_r be the cardinality of C_r.

Since we are free to index the characters of G at will, we do so as follows:

Let C_0 be the class containing the trivial character, $\chi(g_j) = 1 (j \leq n-1)$ and denote it $\chi^{(0)}$. It is trivial that for no $\sigma \in G(K/L)$ does $\sigma(\chi^{(i)}) = \chi^{(0)}$ $(i=1,\ldots,n-1)$ and so $c_o = 1$. Let C_1 be any conjugate class other than C_0 and index any character in C_1 by $\chi^{(1)}$. If there remain unindexed characters in C_1, index them sequentially $\chi^{(d)}, \ldots, \chi^{(d+c_1-1)}$. Having indexed all the characters in $C_0,\ldots,C_{r-1}$; let C_r be any class containing unindexed characters. Choose any character in C_r and index it $\chi^{(r)}$. Index the remaining characters in C_r by $\chi^{(j)}, \ldots, \chi^{(j+c_r-1)}$ where $j = (d + \sum_{i=1}^{r-1}(c_i - 1)$. Now let S_r be the set of indices of characters in C_r:

$S_0 = \{0\}$

$S_1 = \{1,d, \ldots, (d-1) + c_1-1\}$

.
.
.

$S_{d-1} = \{d-1;d+(c_1-1)+\ldots+(c_{d-2}-1);\ldots;(d-1)+(c_1-1)+\ldots+(c_{d-1}-1)\}$

As a final preparatory remark, for $\sigma \in G(K/L)$, Y an arbitrary finite dimensional matrix, $Y = (y_{ij})$; $y_{ij} \in K$; we define $\sigma(Y) = (\sigma(y_{ij}))$.

Lemma 3.6: Let $a = \sum_{i=0}^{n-1}\alpha_i g_i \in KG$; $B = (\beta_0, \ldots, \beta_{n-1}) = \phi(a)$.

Then $a \in LG$ if and only if for every $\sigma \in G(K/L)$, σ permutes the components of B, $\sigma B = \pi B$, where π is that permutation satisfying $\sigma X = \pi X$.

Proof: Suppose $a \in LG$ and write $A = (\alpha_0, \ldots, \alpha_{n-1})$. Since $\alpha_i \in L$, $(i=0, \ldots, n-1)$, $\sigma(A) = A$. Hence:

$$\sigma(A) = A = \sigma(B)\sigma(1/n)\sigma(X).$$

By the prior discussion, $\sigma(B) = \pi(B)$.

Conversely, let $\sigma(X) = \pi(X)$ and suppose that $\sigma(B) = \pi(B)$. Then:

$\sigma(BX) = \sigma(B)\sigma(X) = \pi(B)\pi(X) = BX.$

Hence $\sigma(A) = (1/n\sigma(BX) = (1/n)BX = A$. Since σ was chosen arbitrarily, we have that $\sigma(\alpha_i) = \alpha_i$ $(i=0, \ldots, n-1)$ for every $\sigma \in G(K/L)$. Hence $\alpha_i \in L$ and $a \in LG$.

Let ξ_r generate the image of $\chi^{(r)}$ $(r=0, \ldots, d-1)$. Clearly ξ_r is an m^{th} root of unity, and in fact, for at least one r, ξ_r is a primitive m^{th} root of unity. For there is a $g \in G$ whose order is m. Write $G = \langle g \rangle \times G'$ and consider $\chi : G \to K$ by $\chi(g) \mapsto \zeta$; $\chi(g') \mapsto 1$ $(g' \in G')$. Then Im χ is generated by ζ and χ is one of the characters of G. ζ is a primitive m^{th} root of unity since g' has order m. This proves the last part of:

<u>Theorem 3.7 (Higman)</u>: Let $\chi^{(0)}, \ldots, \chi^{(d-1)}$ be a complete set of mutually inequivalent and with respect to L, non-conjugate characters of G. Then:

$$LG \simeq L_0 \oplus \cdots \oplus L_{d-1}$$

and there is an algebra monomorphism

$$\Theta: \ L_0 \oplus \cdots \oplus L_{d-1} \to K^n; \qquad (L_r \simeq L(\xi_r))$$

given as follows:

Choose for each $0 \leq i \leq n-1$, a fixed $\tau_i \in G(K/L)$ such that $\tau_i(i) = r$ if $i \in S_r$. If $0 \leq i \leq d-1$, let $\tau_i = id$. Let $\Lambda = (\lambda_{ij})$ be the d x n matrix of automorphisms $\lambda_{ij} = \begin{cases} id & (j \in S_i \\ 0 & (\text{otherwise}) \end{cases}$

Let Σ be an n x n diagonal matrix $\Sigma = \text{diag}\,(\tau_i)$. Then

$$\Theta = \Sigma \circ \Lambda$$

(Observe that the rows and columns of the matrices Σ and Λ are numbered from 0)

For at least one r, ξ_r is a primitive m^{th} root of unity.

Proof: We define the following notation: Let b_i be an element of a field, and let B_i be the vector $(b_i, b_i, \ldots, b_i)$ of length c_i-1. Then the vector $(b_0, \ldots, b_{d-1}, B_1, \ldots, B_{d-1})$ is defined to be the juxtaposition of the vectors $(b_0, \ldots, b_{d-1})$ with the vectors $B_1, \ldots, B_{d-1}$. Now let $(b_0, \ldots, b_{d-1}) \varepsilon K^d$. Then

$$\Lambda: (b_0, \ldots, b_{d-1}) \mapsto (b_0, \ldots, b_{d-1}, B_1, \ldots, B_{d-1}) \varepsilon K^n.$$

clearly then $\Lambda \varepsilon \mathrm{Hom}_K (K^d, K^n)$ and is a monomorphism.

Similarly, it is clear that $\Sigma \varepsilon \mathrm{Hom}_K(K^n, K^n)$. To show that each are algebra homomorphisms it is necessary to verify only the preservation of ring multiplication. Let $(b_0, \ldots, b_{d-1})$ and $(b'_0, \ldots, b'_{d-1}) \varepsilon K^d$. Then

$$\Lambda(b_0, \ldots, b_{d-1})(b'_0, \ldots, b'_{d-1})$$

$$= \Lambda(b_o b'_o, \ldots, b_{d-1}b'_{d-1})$$

$$= (b_0 b'_0, \ldots, b_{d-1}b'_{d-1}, B_1 B'_1, \ldots, B_{d-1}B'_{d-1})$$

$$= (b_0, \ldots, b_{d-1}, B_1, \ldots, B_{d-1})(b'_0, \ldots, b'_{d-1}, B'_0, \ldots, B'_{d-1})$$

$$= \Lambda(b_0, \ldots, b_{d-1})\Lambda(b'_0, \ldots, b'_{d-1})$$

Similarly, let $(b_0, \ldots, b_{n-1})$ and $(b'_0, \ldots, b'_{n-1}) \varepsilon K^n$. Then

$$\Sigma(b_0, \ldots, b_{n-1})(b'_0, \ldots, b'_{n-1})$$

$$= \Sigma(b_0 b'_0, \ldots, b_{n-1}b'_{n-1})$$

$$= (\tau_0(b_0 b'_0), \ldots, \tau_{n-1}(b_{n-1}b'_{n-1}))$$

$$= (\tau_0(b_0)\tau_0(b'_0), \ldots, \tau_{n-1}(b_{n-1})\tau_{n-1}(b'_{n-1}))$$

$$= (\tau_0(b_0), \ldots, \tau_{n-1}(b_{n-1}))(\tau_0(b'_0), \ldots, \tau_{n-1}(b'_{n-1}))$$

$$= \Sigma(b_0, \ldots, b_{n-1})\Sigma(b'_0, \ldots, b'_{n-1}).$$

Let $\Theta = \Sigma \circ \Lambda$. Then Θ is an algebra homomorphism

$$\Theta: K^d \to K^n$$

and is clearly a monomorphism. It remains to show that $LG \cong L_0 \oplus \ldots \oplus L_{d-1}$.

Let $a = \sum_{i=0}^{n-1} \alpha_i g_i \in LG \subset KG$ and let

$\Phi(a) = (\beta_0, \ldots, \beta_{n-1}) = B$

Now since $\alpha_i \in L$ and $\chi^{(i)}(g_j) = \xi_i^k$ for some integer k, it is clear that $\beta_i \in L(\xi_i)$ for each $i \leq n-1$. By lemma 3.6, $\sigma \in G(K/L)$ permutes the components of B. We fix an index, i, and consider:

$$\beta_i = \sum_{j=0}^{n-1} \alpha_j \overline{\chi^{(i)}(g_j)}. \quad \text{Then}$$

$$\tau_i^{-1}(\beta_i) = \tau_i^{-1}\left(\sum_{j=0}^{n-1} \alpha_j \overline{\chi^{(i)}(g_j)}\right)$$

$$= \sum_{j=0}^{n-1} \alpha_j \tau_i^{-1}\left(\overline{\chi^{(i)}(g_j)}\right)$$

and since $\chi^{(i)} \in C_r$ for some $r \leq d-1$, it follows that $\tau_i^{-1}(\beta_i) = \beta_r$. Hence $\Sigma^{-1}(B) = B' = (\beta_0, \ldots, \beta_{d-1}, B_1, \ldots, B_{d-1})$. Furthermore, since $\operatorname{Im} \chi^{(i)} = \operatorname{Im} \chi^{(r)}$, β_i and $\beta_r \in L(\xi_r)$. Hence $\Sigma^{-1}(\Phi(a)) \in \Lambda(L_o \oplus \ldots \oplus L_{d-1})$.

Conversely, let $D = (b_0, \ldots, b_{d-1}) \in L(\xi_0) \oplus \ldots \oplus L(\xi_{d-1})$. Then $\Lambda(D) = (b_0, \ldots, b_{d-1}, B_1, \ldots, B_{d-1}) \in K^n$. Now

$$\Sigma(\Lambda(D)) = (\beta_0, \ldots, \beta_{n-1}) \text{ where } \beta_i = \begin{cases} b_i & (i \leq d-1) \\ \tau_i(b_i) & (d \leq i \_ n-1) \end{cases}$$

Let $\sigma \in G(K/L)$ and suppose that $\sigma(i) = j$. Now $\tau_i^{-1}(i) = r$; $\tau_j^{-1}(j) = s$ where $r,s \leq d-1$; by our definition of the τ_i. Consider $\tau_j^{-1}\sigma\tau_i \in G(K/L)$. Obviously $\tau_j^{-1}\sigma\tau_i(r) = s$, and so $\chi^{(r)}$ is conjugate to $\chi^{(s)}$. Since $r,s \leq d-1$ we have $r = s$. But $\tau_j^{-1}\sigma\tau_i$ leaves L fixed, and $\operatorname{Im} \chi^{(r)} = \langle\xi_r\rangle$ fixed, hence leaves $L(\xi_r)$ fixed. Since $b_r \in L(\xi_r)$, then,

$$\tau_j^{-1}\sigma\tau_i(b_r) = b_r \text{ and so } \sigma\tau_i(b_r) = \tau_j(b_r).$$

But $\tau_i(b_r) = \beta_i$; $\tau_j(b_r) = \beta_j$ and so $\sigma(\beta_i) = \beta_j$. Thus σ permutes components of $\Sigma\Lambda(D) \in K^n$. By lemma 3.6, then, $\Phi^{-1}\Sigma\Lambda(D) \in LG$.

Hence we have shown a 1-1 correspondence between

elements of LG and elements of $L(\xi_0) \oplus \ldots \oplus L(\xi_{d-1})$. By the discussion preceding the theorem each ξ_r is an m^{th} root of unity and at least one of the ξ_r is primitive.

Theorem 3.7 enables us to compute the generators of TU(LG). Let δ be a root of unity of minimal even order s, which generates all roots of unity contained in L. Let ζ, as usual be a primitive m^{th} root of unity, and let η be a primitive root of unity of order $t = LCM(m,s)$. Then $K = L(\eta)$ is a minimal splitting field for G containing L. In the following, we retain the notation introduced in theorem 3.7.

Theorem 3.8: Let L be a field, G an Abelian group of order n; and let $K = L(\eta)$, be the minimal splitting field of G containing L. Let $\chi^{(0)}, \ldots, \chi^{(d-1)}$ be the complete set of non-conjugate characters of G with respect to L, and let $\chi^{(d)}, \ldots, \chi^{(n-1)}$ be the remaining characters of G. Let $u^{(i)}$, $(i=0, \ldots, n-1)$ be the generators of TU(KG). Then the generators $v^{(r)}$ $(r=0, \ldots, d-1)$ of TU(LG) are given by:

$$v^{(r)} = \prod_{i\varepsilon S_r} (u^{(i)})^{k_i}$$

where k_i is determined as follows: If $LG = L(\xi_0) + \ldots + (\xi_{d-1})$: $\xi_r = \eta^{k_r}$ and τ_i chosen as in theorem 3.7, then for $\tau_i(\chi^{(i)}) = \chi^{(r)}$;

$$\tau_i(\xi_r) = \eta^{k_i}.$$

Proof: By theorems 3.1 and 3.7 we know that if $v^{(r)}$, $r = 0, \ldots, d-1$ are the generators of TU(LG);

$$\Phi' (v^{(r)}) \varepsilon L(\xi_0) + \ldots + L(\xi_{d-1}), \text{ and}$$

$$\Phi' (v^{(0)}) = (\xi_0, 1, \ldots, 1)$$

$\Phi'(v^{(1)}) = (1, \xi_1, 1, \ldots, 1)$

.

.

.

$\Phi'(v^{(d-1)}) + (1, \ldots, 1, \xi_{d-1})$

where each ξ_r is of even order. Since $\xi_r \varepsilon K = L(\eta)$ and so $\xi_r = \eta^{k_r}$ for some integer k_r we can in fact write:

$\Phi'(v^{(r)}) = (1, \ldots, 1, \eta^{k_r}, 1, \ldots, 1)$ where v^{k_r} is in the r^{th} component. Now $\Theta\, \Phi'(v^{(r)}) = \Phi(v^{(r)})$ and hence $v^{(r)} = \Phi^{-1}\, \Theta\, \Phi'(v^{(r)})$ and we need only calculate $\Phi^{-1}\, \Theta\, \Phi'(v^{(r)})$.

Let $v_r = \Phi'(v^{(r)}) = (1, \ldots, \eta^{k_r}, 1, \ldots, 1)$. Then $\Lambda(v_r) = (\beta_0, \ldots, \beta_{n-1})$ where $\beta_i = 1$ if $i \not\varepsilon S_r$, and $\beta_i = \eta^{k_r}$ if $i \varepsilon S_r$; and

$$\Theta\Phi'(v^{(r)}) = \Sigma\Lambda(v_r) = (\tau_0(\beta_0), \ldots, \tau_{n-1}(\beta_{n-1})$$

$$= \prod_{i=0}^{n-1}(1, \ldots, 1, \tau_i(\beta_i), 1, \ldots, 1)$$

where $\tau_i(\beta_i) = \begin{cases} \tau_i(1) = 1 \text{ if } i \not\varepsilon S_r; \\ \beta_r = \eta^{k_r} \text{ if } i \varepsilon S_r \text{ and } i \leq d-1 \\ \tau_i(\eta^{k_r}) = \eta^{k_i} \text{ if } i \varepsilon S_r \text{ and } i \geq d. \end{cases}$

Clearly, if $i \geq d$, then η^{k_i} is a root of unity of the same order as η^{k_r} when $i \varepsilon S_r$.

Thus, $\Theta\Phi'(v^{(r)}) = \prod_{i \varepsilon S_r} (1, \ldots, 1, \eta^{k_i}, 1, \ldots, 1)$ where η^{k_i} is in the i^{th} component and all other components are equal to 1. But by theorems 3.1 and 3.5,

$\Phi^{-1}(1, \ldots, \eta^{k_i}, 1, \ldots, 1) = (u^{(i)})^{k_i}$ where $u^{(i)}$ is a generator of $TU(KG)$. Hence

$$v^{(r)} = \Phi^{-1}\Theta\Phi'(v^{(r)}) = \prod_{i \varepsilon S_r} (u^{(i)})^{k_i}.$$

An application will serve to make concrete the results of this chapter. Let G be the direct product of the cyclic groups of order 3 and of order $2^2 = 4$; $G = C_3 \times C_4$. Although G is itself cyclic, we compute the characters of G from those of C_3 and C_4 for illustration. In the computation we have indexed the characters according to the scheme outlined previously. Let $C_3 = \langle h \rangle$. Then its characters are:

$\chi'^{(0)}: h \mapsto 1$ (where δ is a cube root of unity)

$\chi'^{(1)}: h \mapsto \delta$

$\chi'^{(2)}: h \mapsto \delta^2$

If $C_4 = \langle k \rangle$, then its characters are:

$\chi''^{(0)}: k \mapsto 1$ (where Θ is a fourth root of unity)

$\chi''^{(1)}: k \mapsto \Theta$

$\chi''^{(2)}: k \mapsto \Theta^2$

$\chi''^{(3)}: k \mapsto \Theta^3$

Now exp G = 12, which is even, so let η be a primitive 12^{th} root of unity. Then $\delta = \eta^4$ and $\Theta = \eta^3$. The characters of G are found by taking all possible products of the characters of C_3 with the characters of C_4. The computed values of the characters of G are listed in table 1.

Let us find the generators of TU(QG). The minimal splitting field for G containing Q is $Q(\eta) = K$ and the automorphisms in G(K/Q) are listed in table 2. To read this table, find the exponent k of η in the first row. The exponent of $\sigma_i(\eta^k)$ is found at the intersection of the $i{+}1^{st}$ and the $k{+}1^{st}$ column.

TABLE 1

CHARACTER VALUES (EXPONENTS OF η) FOR $G = C_3 \times C_4$

Group element	$\chi^{(0)}$	$\chi^{(1)}$	$\chi^{(2)}$	$\chi^{(3)}$	$\chi^{(4)}$	$\chi^{(5)}$	$\chi^{(6)}$	$\chi^{(7)}$	$\chi^{(8)}$	$\chi^{(9)}$	$\chi^{(10)}$	$\chi^{(11)}$
(e,e)	0	0	0	0	0	0	0	0	0	0	0	0
(e,k)	0	3	6	3	0	6	3	9	9	6	9	0
(e,k^2)	0	6	0	6	0	0	6	6	6	0	6	0
(e,k^3)	0	9	6	9	0	6	9	3	3	6	3	0
(h,e)	0	4	4	0	4	0	8	4	8	8	0	8
(h,k)	0	7	10	3	4	6	11	1	5	2	9	8
(h,k^2)	0	10	4	6	4	0	2	10	2	8	6	8
(h,k^3)	0	1	10	9	4	6	5	7	11	2	3	8
(h^2,e)	0	8	8	0	8	0	4	8	4	4	0	4
(h^2,k)	0	11	2	3	8	6	7	5	1	10	9	4
(h^2,k^2)	0	2	8	6	8	0	10	2	10	4	6	4
(h^2,k^3)	0	5	2	9	8	6	1	11	7	10	3	4
ORDER	1	12	6	4	3	2	12	12	12	6	4	3

TABLE 2

THE AUTOMORPHISMS OF $G(Q(\eta)/Q)$

σ_0	0	1	2	3	4	5	6	7	8	9	10	11
σ_1	0	5	10	3	8	1	6	11	4	9	2	7
σ_2	0	7	2	9	4	11	6	1	8	3	10	5
σ_3	0	11	10	9	8	7	6	5	4	3	2	1

It is a trivial verification that:

$C_0 = \{\chi^{(0)}\}$

$C_1 = \{\chi^{(1)}, \chi^{(6)} = \sigma_1\chi^{(1)}, \chi^{(7)} = \sigma_2\chi^{(1)}, \chi^{(8)} = \sigma_3\chi^{(1)}\}$

$C_2 = \{\chi^{(2)}, \chi^{(9)} = \sigma_3\chi^{(2)}\}$

$C_3 = \{\chi^{(3)}, \chi^{(10)} = \sigma_1\chi^{(3)}\}$

$C_4 = \{\chi^{(4)}, \chi^{(11)} = \sigma\chi^{(4)}\}$

$C_5 = \{\chi^{(5)}\}$

and that $c_0 = 1$, $S_0 = \{0\}$; $c_1 = 4$, $S_1 = \{1,6,7,8\}$; $c_2 = 2$, $S_2 = \{2,9\}$; $c_3 = 2$, $S_3 = \{3,10\}$; $c_4 = 2$, $S_4 = \{4,11\}$; and $c_5 = 1$, $S_5 = \{5\}$. Furthermore, Image $\chi^{(0)} = \langle -1\rangle =$ Image $\chi^{(5)}$; Image $\chi^{(1)} = \langle\eta\rangle$; Image $\chi^{(2)} = \langle\eta^2\rangle$; Image $\chi^{(3)} = \langle\eta^3\rangle$; and Image $\chi^{(4)} = \langle\eta^4\rangle$.

Hence $QG \simeq Q \oplus Q(\eta) \oplus Q(\eta^2) \oplus Q(\eta^3) \oplus Q(\eta^4) \oplus Q$, and there are six generators of $TU(QG)$:

$$\Phi'(v^{(0)}) = (\eta^6,1,1,1,1,1,)$$

$$\Phi'(v^{(1)}) = (1,\eta,1,1,1,1)$$

$$\Phi'(v^{(2)}) = (1,1,\eta^2,1,1,1)$$

$$\Phi'(v^{(3)}) = (1,1,1,\eta^3,1,1)$$

$$\Phi'(v^{(4)}) = (1,1,1,1,\eta^4,1)$$

$$\Phi'(v^{(5)}) = (1,1,1,1,1,\eta^6)$$

Application of Θ to each $\phi'(v^{(r)})$ yields:

$$v_0 = (\eta^6,1,1,1,1,1,1,1,1,1,1,1)$$

$$v_1 = (1,\eta,1,1,1,1,\eta^5,\eta^7,\eta^{11},1,1,1)$$

$$v_2 = (1,1,\eta^2,1,1,1,1,1,1,\eta^{10},1,1)$$

$$v_3 = (1,1,1,\eta^3,1,1,1,1,1,1,\eta^3,1)$$

$$v_4 = (1,1,1,1,\eta^4,1,1,1,1,1,1,\eta^8)$$

$$v_5 = (1,1,1,1,1,\eta^6,1,1,1,1,1,1)$$

and it is immediate that the generators of TU(QG) are:

$$v^{(0)} = (u^{(0)})^6$$

$$v^{(1)} = (u^{(1)})(u^{(6)})^5\ (u^{(7)})^7\ (u^{(8)})^{11}$$

$$v^{(2)} = (u^{(2)})^2(u^{(9)})^{10}$$

$$v^{(3)} = (u^{(3)})^3(u^{(10)})^3$$

$$v^{(4)} = (u^{(4)})^4(u^{(11)})^8$$

$$v^{(5)} = (u^{(6)})^6$$

APPENDIX A
RESULTS FROM GROUP REPRESENTATION THEORY

In this appendix are collected various definitions and results from the theory of group representations which are used in the work of the paper. The theorems on group representations may be found in Curtis and Reiner (2). The discussion of group characters follows van der Waerden (7). In order to simplify the presentation, some theorems are proved in this appendix only for the case of finite Abelian groups; these theorems are applicable in greater generality.

GROUP REPRESENTATIONS

Definition: Let G be a group and M a finite dimensional vector space over a field K. A representation of G with representation space M is a homomorphism $\Gamma : G \to GL(M)$, where GL(M) is the group of units of $Hom_K(M,M)$. Two representations Γ and Γ' with representation spaces M and M', respectively, are called equivalent if there is a K-isomorphism $S : M \to M'$ such that $\Gamma'(g)S = S\Gamma(g)$, that is, $\Gamma'(g)S(m) = S(\Gamma(g)m)$ for every g in G, and m in M.

Definition: Let A be an algebra, finite dimensional over K. A representation of A with representation space M is an algebra homomorphism $\Gamma : A \to Hom_K(M,M)$ that is, a mapping Γ which satisfies:

$$\Gamma(a+b) = \Gamma(a) + \Gamma(b); \quad \Gamma(ab) = \Gamma(a)\Gamma(b);$$

$$\Gamma(\alpha a) = \alpha(\Gamma a); \qquad \Gamma(e) = 1 \qquad a,b \in A; \ \alpha \in K$$

Two algebra representations Γ and Γ' with representation spaces M and M' respectively, are called <u>equivalent</u> if there exists a K-isomorphism $S:M \to M'$ such that $\Gamma'(a)S = S\Gamma(a)$, $a \in A$. It is readily verified that KG is an algebra over K.

<u>Theorem A.1</u>: Every representation Γ of G with representation space M can be extended uniquely to a representation Γ^* of KG with representation space M. Conversely, every representation Γ^* of KG yields a unique representation of G.

Proof: Given $\Gamma: G \to GL(M)$, let

$$\Gamma^*(\sum_g \alpha_g g) = \sum_g \alpha_g \Gamma(g) \qquad \alpha_g \in K;\ g \in G$$

Since $GL(M) \subset Hom_K(M,M)$ and $Hom_K(M,M)$ is an algebra over K $\sum_g \alpha_g \Gamma(g) \in Hom_K(M,M)$. Preservation of addition and scalar multiplication are trivially checked. Consider

$$\begin{aligned}\Gamma^*\ (\sum_g \alpha_g g)(\sum_g \beta_g g) &= \Gamma^*(\sum_g \sum_t \alpha_t \beta_{t^{-1}g} g) \\ &= \sum_g \sum_t \alpha_t \beta_{t^{-1}g} \Gamma(g) \\ &= (\sum_g \alpha_g \Gamma(g))(\sum_g \beta_g \Gamma(g)) \\ &= \Gamma^*(\sum_g \alpha_g g)\Gamma^*(\sum_g \beta_g g)\end{aligned}$$

Conversely, given Γ^*, let $\Gamma = \Gamma^*(1 \cdot g)$, $\quad g \in G$.

Uniqueness of both constructions is obvious.

<u>Definition</u>: Let N be a K-subspace of a representation space M, and let $\Gamma: G \to GL(M)$. N is called a <u>G-subspace</u> of M if $\Gamma(g)n \in N$ for every $g \in G$; $n \in N$.

<u>Remark</u>: If we define $\Gamma_1(g) = \Gamma(g)|_N$ for every $g \in G$, then $\Gamma_1 : G \to GL(N)$.

<u>Definition</u>: Let $\Gamma : G \to GL(M)$ and $\Gamma^* : KG \to Hom_K(M,M)$ be its corresponding representation of KG. We call a K-subspace N of M a <u>KG-subspace</u> if $\Gamma^*(a)N \subset N$ for every $a \in KG$. Clearly N is a KG-subspace if and only if N is a G-subspace.

<u>Definition</u>: Let G be a group and M an additive Abelian group. The group M is called a <u>left G-module</u> if for each $g \in G$; $m \in M$, a product gm is defined such that

$$g(m+m') = gm+gm'; \quad (gg')m = g(g'm); \quad em = m$$

for every $g,g' \in G$; $m,m' \in M$.

<u>Theorem A.2</u>: Let KG be the group algebra of a finite group over a field K. Then there is a 1-1 correspondence between the K-representations of G and the left KG-modules M. Two left KG-modules are isomorphic if and only if the corresponding representations are equivalent.

Proof: Let $\Gamma : KG \to Hom_K(M,M)$ and for each $a \in KG$; $m \in M$, define $am = \Gamma(a)m$. Then clearly:

$$a(m+m') = am+am'; \; (a+a')m = am+a'm; \; (aa')m = a(a'm);$$

$$em = m; \quad (\alpha a)m = \alpha(am) = a(\alpha m) \qquad a,a' \in KG; \; m,m' \in M; \; \alpha \in K$$

Thus Γ has made M into a left KG-module.

Conversely, let M be a K-subspace which is a left KG-module. For each $a \in KG$, define:

$$\Gamma(a) : M \to M \text{ by } \Gamma(a)m = am$$

Then it is readily checked that Γ is a representation of KG.

<u>Definition</u>: A KG-module M ($\neq (0)$) is called <u>irreducible</u> if M contains no non-trivial submodules, otherwise it is called <u>reducible</u>.

It is indecomposable if it is impossible to express M as a direct sum of two non-trivial submodules, and is called completely reducible if every submodule of M is a direct summand, that is, for every submodule N of M, there is an N' such that $M = N \oplus N'$. KG representations are called irreducible, reducible, indecomposable, and completely reducible according as to their corresponding KG modules.

Let L be an extension field of K and let A be an algebra over K. Then if Γ is a K-representation of A, it is obviously an L-representation of A. Let A^L be the L-linear combinations $\sum l_i a_i$ of the elements of A. Then A^L is an algebra and Γ may be extended to an L-representation of A^L by setting:

$$\Gamma(\sum l_i a_i) = \sum l_i \Gamma(a_i).$$

Definition: Let A be a K-algebra and V an irreducible A module. We call V absolutely irreducible if V^L is an irreducible A^L- module for every extension field L of K.

Definition: An extension field L of K is called a splitting field for G if every irreducible KG module is absolutely irreducible.

Definition: A ring has the minimum condition if it satisfies the descending chain condition (D.C.C.) on left ideals, that is, if every chain of left ideals $I_1 \supset I_2 \supset \ldots$ terminates in the sense that there is a j such that $I_j = I_{j+1} = \ldots$

Theorem A.3.(Maschke): Let $\Gamma: G \to GL(M)$ be a representation of a finite group G by linear transformations on a vector space M over a field K, and assume that char (K) $\nmid$ [G:1]. Then Γ is completely reducible.

Theorem A.4: Every algebra A, finite dimensional over K has the minimum condition.

Proof: For $\alpha \in K$ and $b \in A$,

$$\alpha b = \alpha(1)b, \text{ and}$$

$$(\alpha 1)b = \alpha(1b) = \alpha(b1) = b(\alpha 1), \qquad (2)$$

Hence the set of elements $K_0 = \{\alpha 1 : \alpha \in K\}$ is contained in the center of A and is a field isomorphic to K. We identify K and K_0. Then (2) shows that every left, right, or two-sided ideal in the ring A is also a K-subspace of the vector space A. Since the subspaces of a finite dimensional vector space satisfy the D.C.C., it follows that the left ideals of A do also.

Definition: A ring is said to be semi-simple if it satisfies the minimum condition, and if Rad R = (0), where Rad R is the sum of all nilpotent left ideals I of R, that is, all left ideals I for which $I^m = (0)$ for some m. A ring is simple if it contains no non-trivial two-sided ideals.

Theorem A.5: A ring R which satisfies the minimum condition is semi-simple if and only if every R-module is completely reducible.

Proof: See Curtis and Reiner (2) pp 164-6.

Theorem A.6: Let G be a finite group and K a field such that char K $\nmid [G:1]$. Then KG is semi-simple.

Proof: This is immediate from Maschke's theorem (A.3) together with theorems A.4 and A.5.

Theorem A.7: Let R be a semi-simple ring, and let L be a minimal left ideal of R. The sum B_L of all the minimal left ideals of R which are isomorphic to L is a simple ring, and a two-sided ideal of R. Furthermore, R is the direct sum of all the ideals B_L obtained by letting L range over a full set of non-isomorphic minimal left ideals of R.

Proof: See (2) Theorem 25.15.

Theorem A.8 (Wedderburn): Let A be a simple ring with minimum condition. then $A \simeq \mathrm{Hom}_D(M,M)$ for some finite dimensional right vector space M over a skew-field D. The dimension (M:D) and the skewfield D are uniquely determined by A.

We next determine an upper bound on the number of irreducible representations of KG. Let K be a field, A an algebra over K with unity element. Let M be a left-A-module. Then M is a vector space over K if we define:

$$\alpha m = (\alpha 1_A)m \qquad \alpha \in K;\ m \in M$$

and assume that (M:K) is finite.

For each $a \in A$, let a_L: $m \to am$ $m \in M$. Then $a_L \in \mathrm{Hom}_K(M,M)$, and the map $a \to a_L$ is a homomorphism of A onto $A_L = \{a_L : a \in A\}$

Now A_L is a subalgebra of $\mathrm{Hom}_K(M,M)$. M can be viewed as a left A_L module, and the subspaces of M which are A-submodules are precisely the same as the subspaces which are A_L -submodules.

A_L is a finite dimensional algebra over K even when A is not, and M is a faithful A_L module, that is, no non-zero element of A_L annihilates M.

Consider $D = \mathrm{Hom}_A(M,M)$. In (2) p 180 it is shown that $D \subset \mathrm{Hom}_K(M,M)$ and is a subalgebra of $\mathrm{Hom}_K(M,M)$. Hence $(D:K) \leq (M:K)^2$.

Theorem A.9 (Schur's Lemma): Let A be a finite dimensional algebra over an algebraically closed field K, and let M, N be irreducible A-modules. Then $\mathrm{Hom}_A(M,N) = (0)$ if M and N are not isomorphic, whereas $\mathrm{Hom}_A(M,M) = K \cdot 1_M$.

Let A be a semi-simple algebra which is finite dimensional over K as a vector space. Then all left, right, and two-sided ideals of A are K-subspaces of A. Let $M_1, \ldots, M_n$ be a full set of non-isomorphic left ideals of A; each M_i is then a finite dimensional vector space over K. Let $D^{(i)} = \mathrm{Hom}_A(M_i,M_i)$. Let A_i denote the simple component of A containing M_i. Then M_i is a faithful irreducible A_i module and

$$A_i \simeq \mathrm{Hom}_{D^{(i)}}(M_i,M_i).$$

Define $u_i = (M_i:D^{(i)})$. Then $A_i \simeq D^{(i)}_{u_i}$, a full matrix ring over the division algebra $D^{(i)}$. A_i is a direct sum of u_i copies of M_i:

$$A = A_i \oplus \ldots \oplus A_n \qquad\qquad A_i \simeq D^{(i)}_{u_i}$$

and M_i may be taken to be a minimal left ideal in the simple ring A_i. It is shown in (2) p 185 that

$$(A:K) = \sum_{i=1}^{n} u_i^2\ (D^{(i)}:K).$$

If K is algebraically closed it follows from Schur's Lemma that each $D^{(i)}$ coincides with K so

$$A = A_1 \oplus \ldots \oplus A_n \quad A_i \simeq K_{u_i},\ u_i = (M_i:K).$$

Furthermore, M_i occurs with multiplicity u_i in the decomposition of A into a direct sum of minimal left ideals.

Let $[G:1] = n$, and let K be algebraically closed. Let $M_1, \ldots, M_n$ be a full set of non-isomorphic KG-modules. Then $KG \simeq A_1 \oplus \ldots \oplus A_n$, where the A_i are the simple components of KG and $A_i \simeq K_{u_i}$, with $u_i = (M_i:K)$. Also KG contains u_i copies of M_i in its decomposition into minimal left ideals. Hence

$$[G:1] = \sum_{i=1}^{n} u_i^2, \text{ since KG has K-dimension } [G:1].$$

Theorem A 10: Let G be a finite group and K an algebraically closed field such that char K $\nmid$ $[G:1]$. Then the number of non-isomorphic irreducible left KG-modules is the same as the number of conjugate classes of G.

Proof: Since the rings A_i annihilate each other we have

$$\text{center } KG \simeq (\text{center } A_1) \oplus \ldots \oplus (\text{center } A_n).$$

Now $A_i \simeq K_{u_i}$ and since the only matrices which commute with all matrices in the full matrix ring K_{u_i}, are scalar multiples of the identity matrix,

$$(\text{center } A_i:K) = 1$$

Hence $n = ((\text{center } KG):K)$. Let $G_1, \ldots, G_s$ denote the conjugate classes of G and define $c_i = \sum_{g \varepsilon G_i} g$. The following theorem yields $s = n$, and proves our required result:

Theorem A.11: Let K be an arbitrary field. The elements c_i form a K-basis for center KG.

Proof: $c_i \varepsilon$ center KG since for every $h \varepsilon G$,

$$hc_i h^{-1} = \sum_{g \varepsilon G_i} hgh^{-1} = c_i.$$

$\{c_i\}$ are clearly linearly independent since each g is an element of the

sum of only one c_i. For each $h \in G$,

$$\sum \alpha_g g = y = hyh^{-1} = \sum \alpha_g hgh^{-1} \text{ from which } \alpha_{h^{-1}gh} = \alpha_g. \quad g \in G$$

Then $\alpha_g = \alpha_{g'}$ whenever g, g' are in the same conjugate class. This shows that y is a K-linear combination of the c_i.

NOTE: When K is not algebraically closed, the above two theorems still yield that the number of non-isomorphic irreducible left KG-modules is less than or equal to the number of conjugate classes of G. Then the equivalence of KG-modules and representations establishes the desired upper bound on the number of irreducible representations of KG.

GROUP CHARACTERS

The results of this section are taken from van der Waerden (7). The results are applicable only to finite Abelian groups, and are used in the paper only in that context. A more general development of the theory of group characters can be found in (2) Chapter V.

Let G be a group and K a field. A character of G in K is a homomorphism $\chi: G \to K^*$, where K^* is the multiplicative group of K.

Let G be cyclic of order n, say $G = \langle a \rangle$. Let $\chi(a) = \zeta$. Then $g \in G$ implies that $g = a^j$ for some $j \leq n-1$, and so $\chi(g) = \zeta^j$. Since $a^n = e$, we must have that $\zeta^n = 1$, showing that ζ is an n^{th} root of unity. Now if K contains all n^{th} roots of unity and char K $\nmid [G:1]$, then there is a character $\chi: a \to \zeta$ where ζ is a primitive n^{th} root of unity. It is easy to see that all characters of G must be a power (j=0, ..., n-1) χ^j of χ and that the set of characters of G $\{\chi^j: j=0, \ldots, n-1\}$ forms a cyclic group of order n, and hence isomorphic to G.

Now let $G \simeq H_1 \times \ldots \times H_s$ be the direct product, of s cyclic groups H_i of orders n_i. Let ζ_i be primitive n_i^{th} roots of unity. Let $H_i = \langle a_i \rangle$. If χ is a character of G, then $\chi(a_i)$ is an n_i^{th} root of unity for each i, and therefore, $\chi(a_i) = \zeta_i^{k_i}$ for some k_i. But since $g \in G$ implies that $g = a_1^{z_1} \ldots a_s^{z_s}$ we have that $\chi(g) = \chi(a_1^{z_1}) \ldots \chi(a_s^{z_s})$

$$= \zeta_1^{k_1 z_1} \ldots \zeta_s^{k_s z_s}.$$

Now each k_i may take any of the numbers 0, ..., $n_i - 1$ for its value, and for each value we obtain a different character. Hence there are $n = \prod n_i$ distinct characters of G, each taking values in a field containing a primitive root of unity of order LCM(n_1, ..., n_s). But this is exactly exp G. The character group is thus a direct product of cyclic groups of orders n_1, ..., n_s, and so is isomorphic to G. By the Fundamental Theorem of Abelian Groups, every Abelian group is isomorphic to the direct product of cyclic groups. We have thus shown that:

Theorem A.12: Let G be a finite Abelian Group, $G = H_1 \times \ldots \times H_s$. Then the character group of G is isomorphic to G, and any character of G is the product of s characters one from each of the character groups of H_i, $i = 1, \ldots, s$.

If ζ is any n^{th} root of unity, it is well known that

$$1 + \zeta + \zeta^2 + \ldots + \zeta^{n-1} = \begin{cases} 0 & (\zeta \neq 1) \\ n & (\zeta = 1) \end{cases}$$

From this follows immediately the following relations, known as the orthogonality relations of characters:

$$\sum_k \chi_k(a) = \begin{cases} n & (a=e) \\ 0 & (a \neq e) \end{cases} \qquad (3)$$

$$\sum_z \chi_k(a) = \begin{cases} n & (k=0) \\ 0 & (k \neq 0) \end{cases} \qquad (4)$$

$$\sum_k \chi_k(a)\chi_k(b) = \begin{cases} n & (a=b^{-1}) \\ 0 & (\text{otherwise}) \end{cases} \qquad (5)$$

$$\sum_a \chi_k(a)\chi_j(a) = \begin{cases} n & (k=j) \\ 0 & (\text{otherwise}) \end{cases} \tag{6}$$

$$\sum_k \chi_k(a)\chi_k(b) = \begin{cases} n & (a=b) \\ 0 & (\text{otherwise}) \end{cases} \tag{7}$$

Now let K be a field containing $\zeta_1, \ldots, \zeta_s$ and G be an Abelian group. Consider the 1-dimensional representations of KG; $\Gamma: G \to \mathrm{Hom}_K(K,K) \simeq K$. Evidently, each character of G may be identified with a one-dimensional representation and we have shown that G has [G:1] distinct characters. Since G is Abelian, the number of conjugate classes of G is also [G:1].

SPLITTING FIELDS FOR ABELIAN GROUPS

Theorem A.13: Let [G:1] = n; exp G = m, and ζ be a primitive m^{th} root of unity. Then $K = Q(\zeta)$ is a splitting field for G when G is Abelian.

Proof: All characters of G take their values in K. Since a character is identified with each one-dimensional representation of KG, there are n distinct one dimensional KG-representations and hence n distinct non-isomorphic irreducible KG-modules. By theorem A.9, and the remarks following it, the n non-isomorphic irreducible KG-modules have dimension 1 over K, and a complete set of one-dimensional representations has been obtained. Since for any extension field $L \supset K$, the module extensions are irreducible as LG modules, they are absolutely irreducible, and hence K is a splitting field by definition.

Theorem A.14: An extension field of a splitting field is a splitting field.

Proof: See (2) theorem 29.21.

Let K be a splitting field for G, $[G:1] = n$. Then $KG \simeq K^n$. Write
$$A = \sum_{i=0}^{n-1} \alpha_i g_i \to (\beta_0, \ldots, \beta_{n-1}) \in K^n.$$

<u>Theorem A.15</u>: Let K be a splitting field of characteristic zero for G, a finite Abelian group. Let Z_j be a minimal ideal in the simple component A_j of KG. Then $A_j = (KG)c_j$ for a uniquely determined idempotent c_j in KG and

$$c_j = [G:1]^{-1} \sum_{i=0}^{n-1} \overline{\chi^{(j)}(g_i)} g_i$$

where $\chi^{(j)}$ is the character afforded by Z_j.

Proof: Let $KG \simeq A_0 \oplus \ldots \oplus A_{n-1}$ be the direct sum decomposition of KG into simple components and $1 = c_o + \ldots + c_{n-1}$ be the corresponding decomposition of 1 as a sum of idempotents. Then c_j annihilates A_k for $k \neq j$ and is the identity element for A_j. This proves that

$\underline{Z}_k(c_i) = \delta_{ik}\underline{I}^{(z_k)}$ where the underscore denotes a matrix; $\underline{Z}_k$ is the matrix representation afforded by $\chi^{(k)}$; and $z_k = (A_k:K)$.

On the other hand, each g_i is a K-linear combination of the c_j. Since
$$\underline{Z}_k(g_i) = \frac{\chi^{(k)}(g_i)}{z_k} \underline{I}^{(z_k)} \qquad \text{(see (2) p 235)}$$

it follows that

$$g_i = \sum_{k=0}^{n-1} \frac{\chi^{(k)}(g_i)}{z_k} c_k \qquad 0 \leq i \leq n-1$$

But $(A_k:K) = 1 = z_k$, and hence

$$[G:1]^{-1} \sum_i \overline{\chi^{(j)}(g_i)} g_i = [G:1]^{-1} \sum_{i,k} \overline{\chi^{(j)}(g_i)} \chi^{(k)}(g_i)\, c_k$$

$$= \sum_k \delta_{jk} c_k$$

$$= c_j$$

as required.

Corollary: Let $A \in KG$, $A = \sum_{i=0}^{n-1} \alpha_i g_i = \sum_{k=0}^{n-1} \beta_k c_k$. Then

$$\alpha_j = [G:1]^{-1} \sum_{i=0}^{n-1} \beta_i \overline{\chi^{(i)}(g_j)} \qquad j=0, \ldots, n-1 \tag{8}$$

and

$$\beta_k = \sum_{i=0}^{n-1} \alpha_i \chi^{(k)}(g_i) \qquad k=0, \ldots, n-1 \tag{9}$$

Proof: Immediate by substituting values for the g_j and the c_k and equating coefficients.

INDEX OF NOTATION

This index lists letters and symbols with fixed useage throughout the paper. Arrangement is by Roman letters, then Greek letters alphabetically; followed by expressions and symbols.

C_i -- The set of characters of G which are conjugate to $\chi^{(i)}$.

c_i -- The cardinality of C_i.

Q -- The field of rational numbers.

S_i -- The set of indices of characters in C_i.

$u^{(i)}$ -- A generator of TU(KG) where K is a splitting field for G.

$v^{(i)}$ -- A generator of TU(LG) where L is <u>not</u> a splitting field for G.

Z -- The ring of rational integers.

Γ -- A representation of a group, G. $\Gamma_j^{(i)}$ denotes the value of $\Gamma^{(i)}$ at g_j.

δ_{ij} -- The Kroneker delta function; $\delta_{ij} = \begin{cases} 1 & (i=j) \\ 0 & (i\neq j) \end{cases}$

ζ -- A primitive m^{th} root of unity where m = exp G.

η -- A primitive root of unity of even order. $Q(\eta)$ is the largest cyclotomic extension of Q contained in a given splitting field for G.

Θ -- The monomorphism Θ: $K^d \to K^n$ by which $LG \simeq L_0 \oplus \dots \oplus L_{d-1}$ is embedded in $KG \simeq K^n$. $\Theta = \Sigma \Lambda$

Λ -- The monomorphism Λ: $K^d \to K^n$ given by the matrix (λ_{ij}); λ_{ij} = id if $\chi^{(j)} \varepsilon C_i$.

Σ -- The isomorphism Σ: $K^n \to K^n$ given by the matrix diag (τ_i).

τ_i	--	The automorphism, $\tau_i \in G(K/L)$ for which $\tau_i(i) = r$; $i \in S_r$.
Φ	--	The isomorphism Φ: $KG \to K^n$ where K is a splitting field for G.
Φ'	--	The isomorphism Φ': $LG \to L_o \oplus \ldots \oplus L_{d-1}$ where L is not a splitting field for G.
exp G	--	The exponent of G, the order of the element of G with maximal order.
G(K/L)	--	The Galois group of automorphisms of K leaving L fixed.
GL(M)	--	The general linear group of a vector space M. GL(M) is the group of invertible transformations in Hom_K (M,M).
Im f	--	The set of values of a function f, contained in the codomain of f.
TU(RG)	--	The torsion subgroup of the group of units of a group ring.
[G:1]	--	The order of the group G.
$\| \ \|$	--	The absolute value function; also, the cardinality of a set.
< >	--	The group generated by the elements listed within the brackets.
$\overline{\chi}$	--	The complex conjugate of a number or a complex valued function. If χ is a character of G then $\overline{\chi} = \chi^{-1}$.
$\|$	--	is a divisor of, as in $a \| b$.
$\dagger$	--	is not a divisor of, as in $a \dagger b$.
(M:N)	--	The dimension of M over N as vector spaces.
$\oplus$	--	Direct sum

REFERENCES

1. S. D. Berman, On the Equation $x^m = 1$ in an Integral Group Ring, Ukrain. Math Z. 7(1955), 253-61.

2. C.W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, New York, Interscience, 1962.

3. R.K. Dennis, The Structure of the Unit Group of Group Rings, (to appear in the Proceedings of the Ring Theory Conference, University of Oklahoma, Norman, March 11-13, 1976, which is to be published by Marcel Dekker.)

4. G. Higman, The Units of Group Rings, Proc. London Math. Soc. 46(1940), 231-48.

5. G. Losey, A Remark on the Units of Finite Order in the Group Ring of a Finite Group, Canad. Math. Bull. 17(1974), 129-30.

6. D. S. Passman, Infinite Group Rings, New York, Marcel Dekker, 1971.

7. B. L. van der Waerden, Algebra, 2 vols. 7 ed., New York, Fredrick Ungar, 1970.

8. H. Zassenhaus, On the Torsion Units of Finite Group Rings, Studies in Mathematics (in honor of A. Almeida Costa), Instituo de Alta Cultura, Lisbon, 1974.