London Mathematical Society Lecture Note Series 84

Finite Group Algebras and their Modules

P. LANDROCK

London Mathematical Society Lecture Note Series 84

Finite Group Algebras and their Modules

P. LANDROCK

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor I.M. James,
Mathematical Institute, 24-29 St Giles, Oxford

1. General cohomology theory and K-theory, P.HILTON
4. Algebraic topology, J.F.ADAMS
5. Commutative algebra, J.T.KNIGHT
8. Integration and harmonic analysis on compact groups, R.E.EDWARDS
9. Elliptic functions and elliptic curves, P.DU VAL
10. Numerical ranges II, F.F.BONSALL & J.DUNCAN
11. New developments in topology, G.SEGAL (ed.)
12. Symposium on complex analysis, Canterbury, 1973, J.CLUNIE & W.K.HAYMAN (eds.)
13. Combinatorics: Proceedings of the British Combinatorial Conference 1973, T.P.McDONOUGH & V.C.MAVRON (eds.)
15. An introduction to topological groups, P.J.HIGGINS
16. Topics in finite groups, T.M.GAGEN
17. Differential germs and catastrophes, Th.BROCKER & L.LANDER
18. A geometric approach to homology theory, S.BUONCRISTIANO, C.P. ROURKE & B.J.SANDERSON
20. Sheaf theory, B.R.TENNISON
21. Automatic continuity of linear operators, A.M.SINCLAIR
23. Parallelisms of complete designs, P.J.CAMERON
24. The topology of Stiefel manifolds, I.M.JAMES
25. Lie groups and compact groups, J.F.PRICE
26. Transformation groups: Proceedings of the conference in the University of Newcastle-upon-Tyne, August 1976, C.KOSNIOWSKI
27. Skew field constructions, P.M.COHN
28. Brownian motion, Hardy spaces and bounded mean oscillations, K.E.PETERSEN
29. Pontryagin duality and the structure of locally compact Abelian groups, S.A.MORRIS
30. Interaction models, N.L.BIGGS
31. Continuous crossed products and type III von Neumann algebras, A.VAN DAELE
32. Uniform algebras and Jensen measures, T.W.GAMELIN
33. Permutation groups and combinatorial structures, N.L.BIGGS & A.T.WHITE
34. Representation theory of Lie groups, M.F. ATIYAH et al.
35. Trace ideals and their applications, B.SIMON
36. Homological group theory, C.T.C.WALL (ed.)
37. Partially ordered rings and semi-algebraic geometry, G.W.BRUMFIEL
38. Surveys in combinatorics, B.BOLLOBAS (ed.)
39. Affine sets and affine groups, D.G.NORTHCOTT
40. Introduction to Hp spaces, P.J.KOOSIS
41. Theory and applications of Hopf bifurcation, B.D.HASSARD, N.D.KAZARINOFF & Y-H.WAN
42. Topics in the theory of group presentations, D.L.JOHNSON
43. Graphs, codes and designs, P.J.CAMERON & J.H.VAN LINT
44. Z/2-homotopy theory, M.C.CRABB
45. Recursion theory: its generalisations and applications, F.R.DRAKE & S.S.WAINER (eds.)
46. p-adic analysis: a short course on recent work, N.KOBLITZ
47. Coding the Universe, A.BELLER, R.JENSEN & P.WELCH
48. Low-dimensional topology, R.BROWN & T.L.THICKSTUN (eds.)

49. Finite geometries and designs, P.CAMERON, J.W.P.HIRSCHFELD & D.R.HUGHES (eds.)
50. Commutator calculus and groups of homotopy classes, H.J.BAUES
51. Synthetic differential geometry, A.KOCK
52. Combinatorics, H.N.V.TEMPERLEY (ed.)
53. Singularity theory, V.I.ARNOLD
54. Markov processes and related problems of analysis, E.B.DYNKIN
55. Ordered permutation groups, A.M.W.GLASS
56. Journées arithmétiques 1980, J.V.ARMITAGE (ed.)
57. Techniques of geometric topology, R.A.FENN
58. Singularities of smooth functions and maps, J.MARTINET
59. Applicable differential geometry, M.CRAMPIN & F.A.E.PIRANI
60. Integrable systems, S.P.NOVIKOV et al.
61. The core model, A.DODD
62. Economics for mathematicians, J.W.S.CASSELS
63. Continuous semigroups in Banach algebras, A.M.SINCLAIR
64. Basic concepts of enriched category theory, G.M.KELLY
65. Several complex variables and complex manifolds I, M.J.FIELD
66. Several complex variables and complex manifolds II, M.J.FIELD
67. Classification problems in ergodic theory, W.PARRY & S.TUNCEL
68. Complex algebraic surfaces, A.BEAUVILLE
69. Representation theory, I.M.GELFAND et al.
70. Stochastic differential equations on manifolds, K.D.ELWORTHY
71. Groups - St Andrews 1981, C.M.CAMPBELL & E.F.ROBERTSON (eds.)
72. Commutative algebra: Durham 1981, R.Y.SHARP (ed.)
73. Riemann surfaces: a view towards several complex variables, A.T.HUCKLEBERRY
74. Symmetric designs: an algebraic approach, E.S.LANDER
75. New geometric splittings of classical knots (algebraic knots), L.SIEBENMANN & F.BONAHON
76. Linear differential operators, H.O.CORDES
77. Isolated singular points on complete intersections, E.J.N.LOOIJENGA
78. A primer on Riemann surfaces, A.F.BEARDON
79. Probability, statistics and analysis, J.F.C.KINGMAN & G.E.H.REUTER (eds.)
80. Introduction to the representation theory of compact and locally compact groups, A.ROBERT
81. Skew fields, P.K.DRAXL
82. Surveys in combinatorics: Invited papers for the ninth British Combinatorial Conference 1983, E.K.LLOYD (ed.)
83. Homogeneous structures on Riemannian manifolds, F.TRICERRI & L.VANHECKE
84. Finite group algebras and their modules, P.LANDROCK
85. Solitons, P.G.DRAZIN
86. Topological topics, I.M.JAMES (ed.)
87. Surveys in set theory, A.R.D.MATHIAS (ed.)
88. FPF ring theory, C.FAITH & S.PAGE
89. An F-space sampler, N.J.KALTON, N.T.PECK & J.W.ROBERTS
90. Polytopes and symmetry, S.A.ROBERTSON

London Mathematical Society Lecture Note Series: 84

Finite Group Algebras and their Modules

P. LANDROCK

Associate Professor of Mathematics

University of Aarhus, Denmark

CAMBRIDGE UNIVERSITY PRESS

Cambridge

London New York New Rochelle

Melbourne Sydney

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
32 East 57th Street, New York, NY 10022, USA
296 Beaconsfield Parade, Middle Park, Melbourne 3206, Australia

First published 1983

Printed in Great Britain at the University Press, Cambridge

Library of Congress catalogue card number: 83-15049

British Library Cataloguing in Publication Data

Landrock, P.
Finite group algebras and their modules -
(London Mathematical Society lecture note series,
ISSN 0076-0552; 84)
1. Finite groups
I. Title II. Series
512'.2 QA171

ISBN 0 521 27487 7

CONTENTS:

PREFACE

This book is concerned with the structure of group algebras of finite groups over fields of characteristic p dividing the order of the group, or closely related rings such as rings of algebraic integers and in particular their p-adic completions, as well as modules, and homomorphisms between them, of such group algebras.

Our principal aim has been to present some of the more recent ideas which have enriched and improved this beautiful theory that owes so much to Richard Brauer. In other words, we wish to account for a major part of what could be described as the post-Brauer period. The reader will find that once we get started, the majority of our proofs have not appeared before in any textbooks, and as far as Chapters II and III are concerned, a number of results and proofs which have not appeared before at all are included.

We do not at any stage restrict ourselves to particular methods, be they ring theoretic, character theoretic, etc. In each case we have attempted to present a proof or an approach which distinguishes itself in one way or another perhaps by being fast, elegant, illuminating, or with promising potentials for further advancement, or possibly all of this at the same time. (We are well aware of the fact that the reader may not always agree this has been achieved (unless of course he or she recognizes his or her own proof!)) One point though that has been important to us is to demonstrate the strong connection to cohomology which undoubtedly will be strengthened in the years to come. Another point to make is that we have tried very hard to avoid assumptions on the coefficient rings involved in the ambitious hope to attract non-specialists, perhaps even algebraic topologists and group theorists who may feel tempted to use the tools of modular representations more frequently.

Of course, to make the presentation as smooth, coherent and self-contained as possible, many classical results are included. Thus we only require knowledge with the theory of semisimple algebras and modules, including basic character theory (if this is not present, we recommend Feit (1967), Serre (1967) or Isaacs (1976)) and elementary facts about finite groups. Also to advance to the frontier as quickly as possible we have added suitable hypotheses at an early stage whenever convenient if it saves us some time. Just as an example, we only prove Krull-Schmidt for finite-dimensional algebras, not artinian rings in general. Usually, we will give a reference to Curtis and Reiner (1981) and (1985) for the more general results.

As the whole idea is to present--whenever appropriate--methods that Brauer avoided or did not even have at hand, the reader will find relatively few references to Brauer's work with the exception of more recent papers such as (1968), (1969) and (1971), and Brauer and Feit (1959). As references to Brauer's Main Theorems, we use the survey articles (1956) and (1959) rather than the original papers and otherwise refer to Feit (1982), which gives a very detailed account of Brauer's work and methods. The justification is that if we want to improve Brauer's theory substantially, we have to come up with something completely new. Recent contributions to which we have devoted particular attention are among others Alperin and Broué (1979), Benson and Parker (1983), Brauer (1968) and (1971), Brandt (1982b), Burry and Carlson (1982), Feit (1969), Green (1974), Knörr (1979), Landrock (1981c) and Scott (1973). This choice is no indication of an attempted evaluation of importance. These are simply the sources we have decided in particular to work with or discuss, leaving others out which equally well deserve careful attention such as Dade's deep work on endopermutation modules or Puig (1981) which is very far-reaching, as well as a number of other topics. Also we do not concern ourselves with the theory of blocks with cyclic defect groups, nor with p-solvable groups, which have recently been treated with great care and detail in Feit (1982). Likewise, Glauberman's powerful and important Z^*-Theorem, which has been indespensable in the classification of the finite simple groups has not been included for the simple reason that we have nothing new to contribute which is not already treated in the literature (see Feit (1982) again, for instance).

It is striking however how many of the deeper results in block theory were anticipated by R. Brauer and how hard we have to work to advance further. And we want to point out that some of Brauer's later work (quoted above) has been a major source of inspiration to a number of people over the last decade, which is the reason why a major part of Chapter III, Section 8, is devoted to these papers.

In 1971, Paul Fong gave a well-composed and inspiring course at Aarhus University on representation theory (see Fong (1971)), which in turn was partly inspired by Dade's lecture notes (1971) and Green's fundamental work in the sixties. Since 1975, I have given a number of lecture series at Aarhus on this subject, which gradually have developed from being close to Fong's lecture notes into part of the present book. Other direct or indirect sources of inspiration have been Michler (1972) and in particular Green (1974) apart from a great deal of Green's work in the sixties and seventies, which perhaps is the major general source of inspiration for Chapter II. Also I have profitted a lot from useful comments by and discussions with my students and others who have attended my lectures, in particular, Ivan Damgård and Carsten Hansen from the first category and Dave Benson from the second, all of whom helped me avoiding considerably more blunders than present now. Other results or approaches are inspired from my collaboration with G. Michler and discussions with J. L. Alperin, H. Jacobinski and D. Sibley and I have enjoyed comments from K. Fuller who read part of Chapter I and D. Burry who read part of Chapter II. The first version of Chapter II similar to the first half of the present was conceived and presented during my visit at University of Oxford in the spring of 1981 and I want to thank Michael Collins warmly for making this possible, and the British Science and Engineering Council for its financial support. But the major part of the final version was written during the academic year 1982-83 at the Institute for Advanced Study, Princeton. I am extremely grateful to the Institute, to NSF Grant MCS-8108814 (A01), and to Aarhus University for the help and financial basis for my stay there. And I want to thank Marianne for her support and understanding as well.

Finally, I wish to thank Peggy Murray (who typed Chapter II) and in particular Kathy Lunetta (who typed the rest) for their excellent, fast and reliable typing as well as their patience with me and my manuscript.

A few remarks on notation and basic assumptions: If A is a ring, A_A means A considered as a right A-module, and except for a very few cases, a module is always right and finitely generated, free over the ring of coefficients. Also, if G is a group and $X \subseteq G$, $a \in_G X$ means $a^g = g^{-1}ag \in X$ for some $g \in G$. Likewise if $H, K \leq G$, $H \leq_G K$ means

$H^g \leq K$ for some $g \in G$. Furthermore, H/G means an arbitrary right transversal of H in G, $G\backslash H$ an arbitrary left and $H\backslash G/K$ an arbitrary transversal of double coset representatives.

One more thing: As one tool is used over and over again, it only seems fair to express our gratitude towards this as well. Therefore in more than one sense of the work, this book is dedicated to the trace map.

Princeton, New Jersey
June, 1983
Peter Landrock

CHAPTER I. THE STRUCTURE OF GROUP ALGEBRAS

1. Idempotents in rings. Liftings.

In this section, A is an arbitrary ring. Recall that an element $0 \neq e \in A$ is called an idempotent if $e^2 = e$. Two idempotents e_1 and e_2 are said to be orthogonal if $e_1e_2 = e_2e_1 = 0$, and an idempotent is called primitive if it is not the sum of two orthogonal idempotents.

Definition 1.1. Let A be a ring and M an A-module. Then M is said to be decomposable if there exist non-trivial submodules M_1 and M_2 of M such that $M = M_1 \oplus M_2$. Otherwise, M is called indecomposable.

Lemma 1.2. Let A be a ring and $e \in A$ an idempotent. Then eA is indecomposable as an A-module if and only if e is primitive.

Proof: One way is trivial. Conversely, assume $eA = A_1 \oplus A_2$ where $0 \neq A_i$ is a right ideal for $i = 1,2$. In particular, $e = e_1 + e_2$ for some $e_i \in A_i$, $i = 1,2$. Moreover, $ee_i = e_i$ for $i = 1,2$, as $e_i \in eA$. Hence

(1) $$e_1e_2 = (e-e_2)e_2 = e_2 - e_2^2 \in A_1 \cap A_2 = 0.$$

Thus $e_1e_2 = 0$ and $e_2^2 = e_2$. So by symmetry, $e_2e_1 = 0$ and $e_1^2 = e_1$ as well. Thus e is not primitive.

Definition 1.3. By an idempotent decomposition of 1 in A, we understand a set of pairwise orthogonal idempotents $e_1,\ldots,e_r$ such that $1 = \sum_{i=1}^{r} e_i$. An idempotent decomposition is called primitive if all the involved idempotents are primitive.

Remark. The importance of idempotent decompositions is of course, in view of Lemma 1.2, that they correspond to direct sum decompositions. If $A_A = \bigoplus_{i=1}^{t} A_i$, then $1 = \sum_{i=1}^{t} e_i$, where $e_i \in A_i$, is necessarily an idempotent decomposition, and vica verca. But even more holds, namely

Theorem 1.4 (Fitting). Let A be a ring and M an A-module. Denote the endomorphism ring of M over A by E. Then

i) There is a one-to-one correspondence between idempotent decompositions $1 = \sum_{i \in I} e_i$ in E and decompositions $M = \bigoplus_{i \in I} M_i$, where I is finite, characterized by the fact that e_j is the projection of M onto M_j with kernel $\bigoplus_{i \neq j} M_i$.

ii) Let $M = M_1 \oplus M_2 = N_1 \oplus N_2$, and let e be the projection onto M_1 with kernel M_2, f the projection onto N_1 with kernel N_2. Then $M_1 \simeq N_1$ if and only if $eE \simeq fE$ as E-modules.

iii) Let $e \in E$ be an idempotent. Then $e(M)$ is indecomposable if and only if eE is indecomposable.

Proof: i) and iii) are obvious.

ii) Let $\phi : M_1 \to N_1$ be an isomorphism. We may consider ϕ as an element of E by setting $\phi(M_2) = 0$. Then $\phi = f\phi e$. We therefore define $\Phi : eE \to fE$ by $\Phi(\alpha) = \phi\alpha$. As ϕ is an isomorphism, it easily follows that Φ is as well. Conversely, let $\Phi : eE \to fE$ be an isomorphism of E-modules. Let $\Phi(e) = f\phi_f$, $\Phi(e\phi_e) = f$, where $\phi_f, \phi_e \in E$. Then $f\phi_f e = \Phi(e)e = \Phi(e) = f\phi_f$. Similarly, $e\phi_e f = e\phi_e$, as $\Phi(e\phi_e f) = \Phi(e\phi_e)f = f = \Phi(e\phi_e)$. Also, $f = \Phi(e\phi_e) = \Phi(e)\phi_e = f\phi_f\phi_e$. Similarly, $e = e\phi_e\phi_f$, as $\Phi(e\phi_e\phi_f) = \Phi(e\phi_e)\phi_f = f\phi_f = \Phi(e)$. But then

$$(f\phi_f)(e\phi_e) = f\phi_f\phi_e = f \tag{2}$$

$$(e\phi_e)(f\phi_f) = e\phi_e\phi_f = e \tag{3}$$

which proves that $f\phi_f : M_1 \to N_1$ is an isomorphism.

We end this section with a very important theorem on lifting idempotents. Recall that an element $v \in A$ is called nilpotent if there

exists $n \in \mathbb{N}$ such that $v^n = 0$. If v is nilpotent, then obviously $1 + v$ is a unit.

Theorem 1.5. Let A be a ring and N a nilpotent ideal of A. Then

i) Let $\bar{e}$ be an idempotent of $\bar{A} = A/N$. Then there exists an idempotent e in A such that $e + N = \bar{e}$; ($\bar{e}$ is said to be lifted to e). If e' is another such idempotent, there exists $v \in N$ such that

$$e' = (1+v)^{-1} e(1+v). \tag{4}$$

ii) Units of $\bar{A}$ always lift to units of A.

iii) Let $\bar{1} = \sum_{i=1}^{t} \bar{e}_i$ be an idempotent decomposition in $\bar{A}$. Then there exists an idempotent decomposition $1 = \sum_{i=1}^{t} e_i$ in A such that $\bar{e}_i = e_i + N$ for all i. Again, if $\sum_{i=1}^{t} e_i'$ is another such decomposition in A, there exists $v \in N$ such that

$$e_i' = (1+v)^{-1} e_i(1+v) \tag{5}$$

for all i.

iv) Let $\bar{e} \in \bar{A}$ be an idempotent and let $e \in A$ be an idempotent such that $e + N = \bar{e}$. Then $\bar{e}$ is primitive if and only if e is primitive.

Proof: We first prove the theorem under the additional assumption that $N^2 = 0$.

i) Let $f \in A$ such that $f + N = \bar{e}$. Then $f^2 = f + y$ for some $y \in N$. Furthermore, for any $x \in N$,

$$(f+x)^2 = f^2 + xf + fx = (f+x) - x + y + xf + fx. \tag{6}$$

Thus we want to choose x such that $y = x - xf - fx$. To obtain this, we magically choose $x = (1-2f)y$. As $y = f^2 - f$, x commutes with f and

(7) $$x - xf - fx = (1-2f)y - 2f(1-2f)y = (1+4f^2-4f)y = (1+4y)y = y$$

as $y \in N$. Thus $e = f + (1-2f)(f^2-f)$ indeed is an idempotent in $\bar{e}$.

Next let e' be another idempotent in $\bar{e}$. Hence $e' = e + z$ for some $z \in N$. Then $e + z = e + ez + ze$ and thus $(1-e)z = ze$, which forces $eze = 0$. Likewise, $(1-e)z(1-e) = 0$. But now, for any $r \in A$,

(8) $$r = ere + er(1-e) + (1-e)re + (1-e)r(1-e).$$

Thus (8) reduces to

(9) $$z = ez(1-e) + (1-e)ze$$

for $r = z$. To finish, we need $v \in N$ such that

(10) $$e + z = (1-v)e(1+v) = e - ve + ev$$

since $vev \in N^2 = 0$. This forces $z = ev - ve$. So this time, we define

(11) $$v := ez(1-e) - (1-e)ze$$

which has the required property by (9).

ii) Let $u + N = \bar{u}$ for $\bar{u}$ a unit in $\bar{A}$. Then there exists $v \in A$ such that $\bar{u}\bar{v} = \bar{v}\bar{u} = \bar{1}$ with $\bar{v} = v + N$. Thus $uv = 1 + y$ and $vu = 1 + z$ for suitable $y,z \in N$. Hence uv and vu are units, which in turn forces u to be a unit.

iii) We use induction on t, the first step being i). Furthermore, by i) again, there exists an idempotent $e_t \in A$ such that $e_t + N = \bar{e}_t$. Let $A' = (1-e_t)A(1-e_t)$ which is a subring of A with $1 - e_t$ as unity. Moreover, $e_t r = re_t = 0$ for all $r \in A'$. The homomorphism $A \to \bar{A}$ induces a homomorphism of A' onto $(\bar{1}-\bar{e}_t)\bar{A}(\bar{1}-\bar{e}_t)$ with kernel $N' = A' \cap N$. In particular, $N'^2 = 0$. However, $\bar{e}_1,\ldots,\bar{e}_{t-1}$ all lie in $(\bar{1}-\bar{e}_t)\bar{A}(\bar{1}-\bar{e}_t)$, and $\bar{1}-\bar{e} = \sum_{i=1}^{t-1} \bar{e}_i$ is an idempotent decomposition in this ring. Hence induction yields the existence of an

idempotent decomposition $1 - e_t = \sum_{i=1}^{t-1} e_i$ in A', thus proving the first part of iii).

To show uniqueness in the sense as stated in iii), we again apply induction on t and as before, i) establishes the case $t=1$. Moreover, i) allows us to assume in the general case that $e_t = e_t'$. Induction now yields a $v \in N' \subseteq N$ such that $(1-v)e_i'(1+v) = e_i$ for all $i \leq t-1$. But as $v \in A'$, $e_t v = ve_t = 0$. Hence $(1-v)e_{t'}(1+v) = e_{t'} = e_t$ as well.

iv) One way is trivial. Conversely, assume $e = \bar{f}_1 + \bar{f}_2$ with $\bar{f}_1$ and $\bar{f}_2$ orthogonal idempotents. Now e is the unity of eAe and $A \to \bar{A}$ induces a homomorphism of eAe onto $\overline{eAe}$ with kernel $N \cap eAe$. Then i) asserts that $\bar{e} = \bar{f}_1 + \bar{f}_2$ can be lifted to eAe, and e is not primitive.

Finally, if N is an arbitrary nilpotent ideal with $N^r = 0$, we first lift to A/N^2 and apply induction on N^i to lift to $A/N^r = A$.

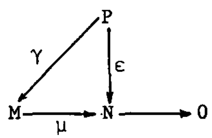
2. Projective and injective modules.

For the convenience of the reader, we recall the basic properties of projective and injective modules.

Let A be a ring. Then the direct summands of A_A have particularly nice properties. One of them is the property defined in

Definition 2.1. Let A be a ring. Then an A-module P is called *projective* if for any two A-modules M and N, and A-homomorphisms $\mu : M \to N$, which is surjective, and $\varepsilon : P \to N$, there exists a homomorphism $\gamma : P \to M$ such that

(1)



commutes.

Theorem 2.2. Let A be a ring, P_1, P_2 and P A-modules. Then we have

i) Any free A-module is projective. In particular, A_A is a projective A-module.

ii) $P_1 \oplus P_2$ is projective if and only if P_i is projective, $i = 1,2$.

iii) P is projective if and only if there exists an A-module M such that $P \oplus M$ is free.

iv) For any A-module M, there exists an exact sequence $0 \to N \to P_M \to M \to 0$ with P_M projective.

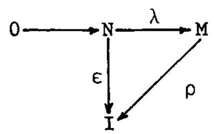
P is projective if and only if every exact sequence $0 \to N \to M \to P \to 0$ splits.

Proof: The reader is probably already familiar with these homological trivialities. Otherwise he or she is urged to produce the proofs.

Having defined projectivity one may feel tempted to discuss the dual property, injectivity. We shall see later that for group algebras they are identical. Nevertheless, it is quite convenient to be aware of the formal difference. Moreover, if we turn to algebraic groups over infinite fields, there really is a difference.

Definition 2.3. An A-module I is called injective if for any two A-modules M and N, and A-homomorphisms $\lambda : N \to M$, which is injective, and $\epsilon : N \to I$, there exists a homomorphism $\rho : M \to I$ such that the following diagram commutes

(2)



Theorem 2.4. Let I_1, I_2 and I be A-modules. Then

i) $I_1 \oplus I_2$ is injective if and only if I_i is injective, $i = 1,2$.

ii) For any module N there exists an exact sequence $0 \to N \to I_N \to M \to 0$ with I_N injective.

iii) I is injective if and only if every exact sequence $0 \to I \to M \to N \to 0$ splits.

Proof: See the proof of Theorem 2.2. (ii) needs some elaboration.)

We will in the following use these basic properties of projective and injective modules without giving special reference, as a main rule.

3. The radical and artinian rings.

A discussion of the following definitions and basic results may be found in a great number of books on ring theory, of which Artin, Nesbitt and Thrall (1944) is the classical source. For a more contemporary treatment which is in concurrence with our discussion here, we suggest Anderson and Fuller (1973). Anyway, before embarking on the study of this section, the reader should make sure to be familiar with the theory of semisimple rings and modules.

Definition 3.1. Let A be a ring. The radical of A, which will be denoted by J(A), is defined as the intersection of all maximal right ideals of A.

Lemma 3.2. Let A be a ring. Then

i) Let E be a simple A-module. Then $EJ(A) = 0$.

ii) Let $x \in A$ and assume $Ex = 0$ for all simple A-modules E. Then $x \in J(A)$.

iii) J(A) is a 2-sided ideal.

Proof: Let E be an arbitrary but fixed simple A-module, and choose $v \in E$ with $vA \neq 0$. Then $a \to va$ defines a module homomorphism $A \to E$. Denote the kernel of this map by M_E. As E is simple, M_E is a right maximal ideal in A, and thus contains J(A) by definition. This proves i) and ii), which together characterize J(A) as the set of elements in A which annihilates all simple A-modules, from which iii) follows.

Definition 3.3. Let A be a ring, M and A-module. Then M is called (right) artinian, if any descending chain of submodules becomes stationary at some point. M is also said to satisfy the d.c.c. (descending chain condition), or the minimal condition.

Likewise, A is called a right (left) artinian ring, if A_A $({}_AA)$ is artinian. If A is right and left artinian, A is called artinian.

Definition 3.4. A descending chain

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0 \tag{1}$$

of submodules of the A-module M is called a composition series if M_i/M_{i+1} is simple for all i.

Remark. If M is not finitely generated, M may not have a composition series, even if A is right artinian. In fact, if M is not finitely generated, M may not even have a maximal submodule. However, if M is finitely generated, there is no problem as we proceed to see. The point is

Lemma 3.5. Let A be a ring, and let M be a finitely generated A-module. Then M has a maximal submodule. In particular, $MJ(A) \subset M$.

Proof: The reader is probably familiar with the fact that the first statement follows from Zorn's lemma. Now the second follows from Lemma 3.2i).

Theorem 3.6. Let A be a right artinian ring. Then

i) $J(A)$ is nilpotent.

ii) Let M be a finitely generated A-module. Then $M/MJ(A)$ is semisimple.

iii) $A/J(A)$ is a semisimple ring.

Proof: i) If $J(A)$ is not nilpotent, there exists an $n \in \mathbb{N}$ with $J(A)^n = J(A)^{n+1} \neq 0$ by definition. Hence there exists $a \in J(A)$

with $aJ(A)^n \neq 0$. Moreover, as A is artinian, we may even assume that $I = aA$, I a minimal ideal such that $IJ(A)^n \neq 0$. Thus in fact $aA = aJ(A)$ by minimality of I, as $aJ(A)^{n+1} = aJ(A)^n$, and thus $aAJ(A) = aA$, a contradiction by Lemma 3.5.

To prove ii) and iii), it suffices to prove that $A/J(A)$ is a semisimple A-module. But as A is artinian, there exists finitely many right maximal ideals $M_1,\ldots,M_r$ such that $J(A) = \bigcap_{i=1}^{r} M_i$ by the characterization of $J(A)$ in the proof of Lemma 3.2. Hence the canonical homomorphism $A/J(A) \to \bigoplus_{i=1}^{r} A/M_i$ is injective.

Corollary 3.7. Let A be a right artinian ring and M a finitely generated A-module. Then $MJ(A)$ is the unique minimal submodule with $M/MJ(A)$ semisimple.

Notation: In view of Corollary 3.6, we set $J(M) := MJ(A)$ and call this the radical of M.

Corollary 3.8. Let A be a right artinian ring and M a finitely generated A-module. Then

i) M is isomorphic to a direct sum of indecomposable modules.

ii) M has a composition series.

Proof: This follows immediately from the fact that $J(A)$ is nilpotent and $A/J(A)$ and $M/MJ(A)$ are semisimple, as does

Corollary 3.9 (Nakayama's lemma). Same assumptions as above. Let L be a submodule of M such that $L + MJ(A) = M$. Then in fact $L = M$.

The following is now straightforward though tedious to establish using the fundamental homomorphism theorem and we (wisely) omit the proof.

Theorem 3.10 (Jordan-Hölder). Let A be a ring and M an A-module. If M possesses a composition series, any two composition series contain the same number of members, and the simple factor modules arising from these series may be arranged to be pairwise isomorphic.

Definition 3.11. Let A be a ring, and assume $A_A = \bigoplus_{i=1}^{t} P_i$, where P_i is indecomposable. (This, for instance, holds if A is right artinian, as we have just seen.) These summands are called the principal indecomposable modules (p.i.m.'s) of A.

It is now clear from Lemma 1.2 that a right ideal P in a ring A, with the above property, is a p.i.m. if and only if there exists a primitive idempotent e such that $P = eA$.

Before we prove a number of important structure theorems describing the p.i.m.'s of a right artinian ring, we need the following important consequence of Theorem 1.5:

Theorem 3.12. Let A be a right artinian ring. Then

i) Let $1 = \sum_{i=1}^{t} e_i = \sum_{j=1}^{s} f_j$ be primitive idempotent decompositions. Then $s = t$ and there exists a unit u in A such that $u^{-1}e_i j = f_{\phi(i)}$ for all i, where ϕ is some permutation of $\{1,2,\ldots,s\}$.

ii) Let e,f A be idempotents. Then $eA \simeq fA$ if and only if there exists a unit $u \in A$ such that $u^{-1}eu = f$.

Proof: We assume these results are familiar to the reader if A is semisimple. But then i) follows from Theorem 1.5 while for ii) we have to remark in addition that if $eA \sim fA$, then $eA/eJ(A) \simeq fA/fJ(A)$.

Corollary 3.13. Let A be a right artinian ring. Then

i) The p.i.m.'s of A_A are uniquely determined up to isomorphism. In other words, if

$$A_A \simeq \bigoplus_{i \in I} P_i \simeq \bigoplus_{j \in J} Q_j \tag{2}$$

where the P_i's and Q_j's are all indecomposable, then there exists a bijection $\phi : I \to J$ such that $P_i \simeq Q_{\phi(i)}$ for all i.

ii) A finitely generated indecomposable A-module is projective if and only if it is isomorphic to a p.i.m. of A_A.

Proof: i) is just a reformulation of Theorem 3.12i) in view of the remark following Definition 1.3.

ii) follows from the general properties of projective modules.

The following result is of extreme importance in what follows.

Theorem 3.14. Let A be a right artinian ring and $\{e_i\}$ a set of primitive idempotents. Set $P_i = e_iA$. Then

i) P_i contains a unique maximal submodule, namely $e_iJ(A)$.

ii) The following are equivalent

a) $P_i/e_iJ(A)$ and $P_j/e_jJ(A)$ are isomorphic

b) P_i and P_j are isomorphic

c) There exists a unit $\bar{u}$ in $A/J(A)$ such that $\bar{u}^{-1}\bar{e}_i\bar{u} = \bar{e}_j$, where $\bar{e}_k = e_k + J(A)$ for $k = i,j$

d) There exists a unit u in A such that $u^{-1}e_iu = e_j$.

Proof: i) Let M be a maximal right ideal in P_i. Then P_i/M is a simple A-module. In particular, $e_iJ(A) = P_iJ(A) \subset M$ by Lemma 3.2i). However, as $\bar{e}_i = e_i + J(A)$ is a primitive idempotent in $A/J(A)$ and $e_iA \cap J(A) = e_iJ(A)$, we have that $e_iA/e_iJ(A)$ is simple. Thus, in fact, $e_iJ(A) = M$.

ii) The equivalence of b) and d) was proved in Theorem 3.12, and c) and d) are equivalent by Theorem 1.5. Finally, the equivalence of c) and a) is a well-known property of semisimple rings.

In particular, we have proved

Corollary 3.15. There is a one-to-one correspondence between the isomorphism classes of the p.i.m.'s of A and the isomorphism classes of the simple A-modules.

4. Cartan invariants and blocks.

We proceed to define the so-called Cartan invariants of an arbitrary artinian ring.

Definition 4.1. Let $e_1,\dots,e_m$ be primitive idempotents of the artinian ring A such that $\{e_iA\}$ form a complete set of representatives of isomorphism classes of p.i.m.'s of A (in particular, they are all orthogonal to each other). Let $P_i = e_iA$, and set $E_i = P_i/e_iJ(A)$.

The Cartan invariant c_{ij} is defined as the multiplicity of E_j as a composition factor in P_i. The $m \times m$ matrix $\{c_{ij}\} = C$ is called the Cartan matrix.

Later we shall prove several important results on Cartan invariants for group algebras. Here, in the general case where much less holds, we only prove

Lemma 4.2. The principal indecomposable P_i has a composition factor isomorphic to E_j if and only if P_ie_j $(= e_iAe_j) \neq 0$.

Proof: Assume $P_ie_j \neq 0$, and let $0 \neq x \in P_ie_j$. Then $xe_j = x$, and we may define an A-homomorphism $\phi : P_j \to P_ie_jA \subseteq P_i$ by $\phi(v) = xv$. Since P_j has a unique maximal submodule, namely $e_jJ(A)$, the kernel of ϕ must be contained in $e_jJ(A)$, and thus $\phi(P_j)/\phi(e_jJ(A)) \simeq E_j$ is a composition factor of P_i.

Conversely, if E_j is a composition factor of P_i, there exists a submodule M of P_i with a submodule N such that $M/N \simeq E_j$. As P_j is projective, the map $P_j \to E_j$ may be factored through M. In particular, there exists a non-trivial homomorphism $\phi : P_j \to P_i$. Hence $\phi(e_j) \neq 0$. But then $\phi(e_j) = \phi(e_j)e_j \neq 0$ which shows that $P_ie_j \neq 0$.

Definition 4.3. Let Q_1 and Q_2 be p.i.m.'s of A. Then Q_1 and Q_2 are said to be linked, if there exists a sequence of p.i.m.'s $Q_1 = P_1, P_2, \dots, P_s = Q_2$ such that P_i and P_{i+1} have a composition factor in common for all i. For notation, we use $Q_1 \equiv Q_2$.

Clearly, $\equiv$ is an equivalence relation on the set of p.i.m.'s of A. Let $\mathbb{P}_1,\dots,\mathbb{P}_r$ denote the equivalence classes under $\equiv$. By the block $\mathbb{B}_i$ of A associated with $\mathbb{P}_i$, we understand

(1) $$\mathbb{B}_i = \{\Sigma Q \mid Q \in \mathbb{P}_i,\ Q \subseteq A\}.$$

Theorem 4.4. The blocks of A are indecomposable 2-sided ideals of A and artinian rings. Moreover,

(2) $$A = \bigoplus_{i=1}^{r} \mathbb{B}_i$$

and (2) is the unique decomposition of A into a direct sum of indecomposable ideals. In particular, if e_i is the unity of $\mathbb{B}_i$, then $e_1,\dots,e_r$ are the only centrally primitive idempotents in A.

Proof: By definition, $A = \Sigma\, \mathbb{B}_i$, and

(3) $$\mathbb{B}_i = \{\Sigma eA \mid eA \in \mathbb{P}_i,\ e \text{ a primitive idempotent}\}$$

which is a right ideal. Moreover, if $e \in \mathbb{B}_i$ and $f \in \mathbb{B}_j$ are primitive idempotents and $i \neq j$, Lemma 4.2 asserts that $eAf = 0$, by definition of blocks. Hence (3) yields that $\mathbb{B}_i\,\mathbb{B}_j = 0$. Consequently,

(4) $$A\mathbb{B}_i = (\Sigma\, \mathbb{B}_j)\mathbb{B}_i \subseteq \mathbb{B}_i\,\mathbb{B}_i \subseteq \mathbb{B}_i$$

and thus $\mathbb{B}_i$ is in fact a 2-sided ideal. Next we claim that the sum $\Sigma\mathbb{B}_i$ is direct. Indeed, this is a standard argument: Let $1 = \Sigma e_i$, where $e_i \in \mathbb{B}_i$, and let $0 = \Sigma a_i$, where $a_i \in \mathbb{B}_i$. Then

(5) $$a_j = a_j(\Sigma e_i) = a_je_j = (\Sigma a_i)e_j = 0$$

for all j, as $\mathbb{B}_i\mathbb{B}_j = 0$ for $i \neq j$. It is now straightforward to show that e_i is a unity of $\mathbb{B}_i$ and that $\mathbb{B}_i$ is an artinian ring. Finally, let $A = \mathfrak{A} \oplus \mathfrak{B}$ where $\mathfrak{A}$ and $\mathfrak{B}$ are 2-sided ideals and $\mathfrak{B}$ is indecomposable as such. Let $1 = e + f$ with $e \in \mathfrak{A}$ and $f \in \mathfrak{B}$. Again it follows that $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} = 0$, and consequently f is a central idempotent, and primitive as such as $\mathfrak{B}$ is indecomposable. Hence there exists exactly one i with $e_if \neq 0$. Thus $e_i = f$ as they are both primitive, and $\mathfrak{B} = \mathbb{B}_i$, from which the rest of the theorem follows.

We now leave the general theory of artinian rings to concentrate first on finite dimensional algebras and then group algebras and, to some extent, symmetric algebras.

5. Finite dimensional algebras.

First of all, we want to make the convention that for the rest of this book, a module is finitely generated.

In this particular section, we furthermore assume A to be a finite dimensional algebra over a field F. Obviously, A is an artinian ring then, and we will use the notation of Definition 4.1.

An important point we want to make in our whole discussion is how a number of crucial properties of a module M over A are closely related and often entirely determined by those of its endomorphism ring. We have already seen a demonstration of this in Theorem 1.4.

For M and N A-modules, we denote $\mathrm{Hom}_A(M,N)$ by $(M,N)^A$.

Lemma 5.1. With the notation above, we have

i) $(M,M)^A$ is a finite dimensional algebra over F.

ii) $J((M,M)^A) \supseteq \{\phi \in (M,M)^A \mid \phi(M) \subseteq MJ(A)\}$.

Proof: i) is trivial.

ii) Let $\mathfrak{n}$ denote the right hand side of ii), which obviously is an ideal. Let $\phi \in \mathfrak{n}^r$ for some r. Then $\phi(M) \subseteq MJ(A)^r$ and thus $\mathfrak{n}$ is nilpotent, which proves that $\mathfrak{n} \subseteq J((M,M)^A)$.

Remark. Equality does not always hold in ii) above.

Recall there is a one-to-one correspondence between idempotent decompositions $1 = \Sigma e_i$ in $(M,M)^A$ and decompositions $M = \bigoplus_i M_i$, characterized by the fact that e_i is the projection of M onto M_i with kernel $\bigoplus_{j\neq i} M_j$. Also $(M,M)^A$ is artinian, of course.

Theorem 5.2. Same notation as above. Then

i) (Krull-Schmidt.) The indecomposable direct summands of M are uniquely determined up to isomorphism. In other words, if

$$(1) \qquad M \simeq \bigoplus_{i\in I} M_i' \simeq \bigoplus_{j\in J} M_j''$$

where the M_i' 's and M_j'' 's are indecomposable A-modules, there exists a bijection $\phi : I \to J$ such that $M_i' \simeq M''_{\phi(i)}$ for all i.

ii) Let $M = M_1 \oplus M_2 = N_1 \oplus N_2$, and let $1 = e+1-e = f+1-f$ be the corresponding idempotent decompositions in $(M,M)^A$. Then $M_1 \simeq N_1$ if and only if there exists a unit $u \in (M,M)^A$ such that $e = u^{-1}fu$.

Remark: Krull-Schmidt in fact holds even if A is only (right) artinian, but then the proof is no longer just an application of Theorem 3.12 (see for instance Curtis and Reiner (1981)), as we then lack the information that $(M,M)^A$ is artinian.

Proof: The decomposition in (1) corresponds to primitive idempotent decompositions in $(M,M)^A$. However, as we saw in the proof of Theorem 3.12 any such two decompositions are conjugate via a unit in $(M,M)^A$, from which i) follows.

ii) By Theorem 1.4, it suffices to prove that this holds for direct summands of E_E, where $E = (M,M)^A$. But again this follows from Theorem 3.12.

As an application of Theorem 3.14, we get

Lemma 5.3. Same notation as above. Then M is indecomposable if and only if $(M,M)^A/J((M,M)^A)$ is a division algebra over F.

Remark. A more general result, which again is beyond the scope of this book, states that if A is a ring and M is an A-module with a composition series, then M is indecomposable if and only if $(M,M)^A$ is local (see Curtis and Reiner (1981)).

Lemma 5.4. Let $e \in A$ be an idempotent and let M be any A-module. Then

$$(2) \qquad (eA,M)^A \simeq Me$$

as F-spaces.

Proof: We define $T : (eA,M)^A \to M$ by $T(\phi) = \phi(e)$. Then T is an F-linear map. Moreover, $\phi(e) = 0$ forces $\phi(e)a = \phi(ea) = 0$ for all $a \in A$, thus forcing $\phi = 0$, i.e., T is injective. Furthermore, $\phi(e) = \phi(e)e \in Me$, so T maps into Me. Conversely, if $x \in M$, we define $\phi_x \in (eA,M)^A$ by $\phi_x(a) = xa$. Then $T(\phi_x) = \phi_x(e) = xe$. Thus T is an isomorphism.

Corollary 5.5. Let $e \in A$ be an idempotent. Then

$$(eA,eA)^A \simeq eAe \tag{3}$$

and $T : (eA,eA)^A \to eAe$ defined by $T(\phi) = \phi(e)$ is an F-algebra isomorphism.

Lemma 5.6. Let $e \in A$ be an idempotent. Then

$$J(eAe) = eJ(A)e = J(A) \cap eAe. \tag{4}$$

Proof: The last equality is obvious. Moreover, $eJ(A)e$ is a nilpotent ideal in eAe, hence contained in $J(eAe)$. Finally,

$$(AJ(eAe)A)^r = (AeJ(eAe)eA)^r = AJ(eAe)^r A. \tag{5}$$

Thus $J(eAe)$ generates a nilpotent ideal in A, which shows that $J(eAe) \subseteq J(A)$.

This enables us to improve Lemma 5.1 for modules of the form eA, e an idempotent.

Corollary 5.7. Let $e \in A$ be an idempotent. Then

$$J((eA,eA)^A)^r \subseteq \{\phi \in (eA,eA)^A \mid \phi(eA) \subseteq eA \cap J(A)^r\} \tag{6}$$

for all r, and equality holds for $r = 1$.

Proof: By Lemma 5.6,

$$J(eAe)^r = (J(A) \cap eAe)^r \subseteq J(A)^r \cap eAe. \tag{7}$$

Moreover, $\phi \in J((eA,eA)^A)^r$ if and only if $\phi(e)$ $J(eAe)^r$ by Corollary 5.5, from which (6) follows. The equality for $r = 1$ is then obtained from Lemma 5.1.

Lemma 5.8. Assume F is a splitting field of $A/J(A)$, and let E_i be a simple A-module. Let M be an arbitrary A-module, and denote the multiplicity of E_i as a composition factor of M by a_i. Then

$$a_i = \dim_F((P_i,M)^A) \tag{8}$$

where P_i is the p.i.m. corresponding to E_i.

Proof: Recall that by Theorem 3.14i) and Schur's lemma,

$$(P_i,E_i)^A \simeq F \tag{9}$$

as an F-space. Let

$$M = M_1 \supset M_2 \supset \cdots \supset M_n = 0 \tag{10}$$

be a filtration of M with M_j/M_{j+1} simple for all j. Choose j_1 maximal so that no composition factor of M/M_{j_1} is isomorphic to E_i. It immediately follows that

$$W := (P_i,M)^A = (P_i,M_{j_1})^A \tag{11}$$

as any factor module of P_i has E_i as a composition factor. Hence induction on $\dim_F M$ allows us to assume that $j_1 = 1$, and moreover that the dimension over F of $W_1 := (P_i,M_2)^A$ is $a_i - 1$. Furthermore, as P_i is projective, there exists $\phi_1 \in W$ with $\phi_1 \in W_1$, or in other words

$$(\phi_1(P_i)+M_2)/M_2 = M_1/M_2 \simeq E_i. \tag{12}$$

Now let $\phi \in W$ be arbitrary. Then (9) and (12) imply the existence of $\lambda \in F$ such that

(13) $$([\phi-\lambda\phi_1](P_i) + M_2)/M_2 = 0.$$

Hence $\phi-\lambda\phi_1 \in W_1$, and we are done.

Corollary 5.9. Assume F is a splitting field of $A/J(A)$. Then the Cartan invariants c_{ij} of A satisfy

(14) $$c_{ij} = \dim_F((P_j,P_i)^A)$$

with the notation of Section 4.

Remark. The proof above shows that in general, if F is arbitrary, then

(15) $$c_{ij} \leq \dim_F((P_j,P_i)^A)$$

and equality holds if and only if $(E_i,E_i)^A \simeq F$, i.e., if and only if F is a spliting field of the Wedderburn component of $A/J(A)$ corresponding to E_i.

6. Duality.

We are now ready to take advantage of the fact that a group algebra over a finite group not only is a finite dimensional algebra but has a basis which forms a group! The following simple and yet extremely important definition takes advantage of that fact. It immediately leads us to a strong property of projective modules of a group algebra.

Definition 6.1. Let R be a commutative ring and G a finite group. By an $R[G]$-module M, we will always mean a module which considered as an R-module is free and finitely generated.

By the dual or contragredient, M^* of M, we understand

(1) $$(M,R)^R$$

with the following action by G: for all $\phi \in (M,R)^R$ and all $g \in G$, we define

(2) $$(\phi g)(x) = \phi(xg^{-1})$$

for all $x \in M$. (The reader is urged to check that this makes $(M,R)^R$ into an $R[G]$-module of the same rank over R as M.) Finally, M is called self-dual if $M \simeq M^*$ as $R[G]$-modules.

Example: Let $R = \mathbb{C}$, and let χ be the character afforded by M. Then the character of M^* is $\bar{\chi}$.

We have the following evident properties of dual modules.

Lemma 6.2. Same notation as above. Then

i) $(M^*)^* \simeq M$.

ii) $(M \oplus N)^* \simeq M^* \oplus N^*$.

iii) M is indecomposable if and only if M^* is indecomposable.

iv) $M \simeq N$ if and only if $M^* \simeq N^*$.

Proof: Exercise.

Recall that for a group G, G and G^{op} are isomorphic, and $g \to g^{-1}$ is an isomorphism. For the same reason, we have

Theorem 6.3. Same notation as above. For any $g \in G$, define $\phi_g : R[G] \to R$ by

(3) $$\phi_g(\Sigma\alpha_g g) = \alpha_g.$$

Then $(R[G])^* = \underset{g}{\oplus} R\phi_g$, and $(\phi_g)h = \phi_{gh}$. Moreover

(4) $$\Sigma\alpha_g g \to \Sigma\alpha_g\phi_g$$

is an $R[G]$-isomorphism between $R[G]$ and $R[G]^*$. In other words, $R[G]$ is self-dual.

Proof. Only (4) has to be checked. But