A dissertation submitted for the degree of
Master of Science in the University of Glasgow.

GROUP ALGEBRAS OF INFINITE GROUPS OVER ARBITRARY FIELDS.

by

LILIAN M. DUNLOP
The University of Glasgow

1966.

SUMMARY of a dissertation entitled "Group algebras of infinite groups over arbitrary fields" submitted for the degree of Master of Science of the University of Glasgow by Lilian M. Dunlop, 1966.

In this dissertation, we give an account of some recent work relating to group algebras.

In § 2, we define the lower and upper nil radicals and the Jacobson radical for the group algebra of any group over an arbitrary field and note that for a finite group these radicals coincide. In fact the radical of the group algebra of a finite group over a field is the zero ideal if (i) the field has characteristic zero or (ii) the field has characteristic p ($\neq 0$) and the group contains no p-elements.

In § 3, we show that for any algebra with an identity element, over a field whose cardinal number exceeds the dimension of the algebra over the field, the Jacobson and upper nil radicals coincide (1). These two radicals again coincide for any finitely generated algebra satisfying a polynomial identity (3). These results are used in conjunction with results on the upper nil radical of a group algebra in § 5. Passman (6) has proved that the upper nil radical of the group algebra of any group over a field of characteristic zero is the zero ideal and that if the field has characteristic $p \neq 0$, then the group algebra is semi-simple provided that the group contains no p-elements.

The main aim of the dissertation is to find conditions on the group or the field under which the Jacobson radical of a group algebra is the zero ideal. In § 4, we examine the behaviour of the Jacobson radical of an algebra over a field under extension of the field and establish two theorems by Amitsur on this subject (2).

Finally in § 6, using the results established in §§ 3-5, we establish that if the field over which the group algebra is formed is a non-algebraic extension of Q, the field of rational numbers, then the group algebra is semi-simple, whatever the group (4 and 6). We also prove two theorems by Passman (6) on group algebras over fields of characteristic p, in which he shows that if the field is a separably generated , non-algebraic extension of some subfield, or if it is non-denumerable, then the group algebra of any group with no p-elements is semi-simple.

Connell (5) has studied the slightly different problem of finding groups which give rise to semi-simple group algebras over arbitrary fields. If the group has no p-elements when the field has non-zero characteristic p then locally finite groups, ordered groups and abelian groups are such groups. Further, it can be shown that if two groups have semi-simple group algebras over a particular field, then the group algebra of the direct product of the groups over the same field is semi-simple, and ~~if the group algebra of a group over a field is semi-simple~~, that the group algebra of the direct product of any group with the infinite cyclic group over the field is also semi-simple, provided that if the field has non-zero characteristic p, then the group ~~may have~~ has no p-elements.

REFERENCES:

1. Amitsur S.A. : Algebras over infinite fields (Proc. American Math. Soc. 7 (1956) 35-46)

2. __________ : The radical of field extensions (Bull Research Council of Israel 7F (1957) 1-10)

3. __________ : A generalisation of Hilbert's Nullstellensatz. (Proc. American Math. Soc. 8 (1957) 649-656)

4. __________ : On the semi-simplicity of group algebras. (Michigan Math. J. 6 (1959) 251-254)

5. Connell, I.G. : On the group ring. (Canadian J. Math. 15 (1963) 650-685)

6. Passman, D.S. : Nil ideals in group rings. (Michigan Math. J. 9 (1962) 375-382).

PREFACE.

This dissertation is submitted in accordance with the regulations for the degree of Master of Science of the University of Glasgow. No part of it has previously been submitted by the author for a degree at any university.

I would like to thank my supervisor, Dr. D.A.R. Wallace, now of the University of Aberdeen, for his advice and encouragement during the past year.

CONTENTS.

Page.

1. Introduction.

In this thesis we shall give an account of some recent work relating to group algebras of infinite groups over arbitrary fields. At present, research is progressing in two apparently independent directions, both attempting to carry over to the case of infinite groups some of the features of the finite case.

First, there is the attempt to define a suitable radical for a general ring and then to find the conditions under which this radical is the zero ideal for a group algebra over a field; and secondly there is the investigation of group algebras with representations of bounded degree.

We shall, in this discussion, deal with the former only. In § 2, we define several radicals and indicate the relationship between them. Our main concern will be with the Jacobson radical of a group algebra but we shall also consider some properties of the upper nil radical, which will subsequently be used in proofs of theorems relating to the Jacobson radical.

For example, in § 3 we show that in certain cases, the Jacobson and upper nil radicals of a group algebra coincide and in § 5, we establish two results first proved by Passman (16) giving conditions under which the upper nil radical is the zero ideal. Passman has in fact proved that the upper nil radical of the group algebra of any group over any field of characteristic zero is zero (Theorem 5.2) and that if the group has no p-elements (i.e. elements of order p^n, n a positive integer), where p is the characteristic of the field/

field, then the upper nil radical is again the zero ideal. (Theorem 5.1)

In § 4, we examine the behaviour of the Jacobson radical of an algebra over a field when the field is extended and prove Amitsur's results (4) in Theorems 4.1 and 4.2.

Not all questions relating to the Jacobson radical have been answered yet. It is an unsolved problem whether the group algebra of any group over any field of characteristic zero is semi-simple.

It has been proved by Rickart (17), using the methods of Banach algebras, that if the field is the field of real numbers or the field of complex numbers, then the resulting group algebra is semi-simple. More recent work has given a more general class of fields of characteristic zero for which the group algebra of any group is semi-simple. In Theorem 6.1, Amitsur (6) has proved that if the field is a non-algebraic extension of Q, the field of rational numbers, then the group algebra is semi-simple.

For a field K of characteristic $p \neq 0$ and a group G with no p-elements, the group algebra is known to be semi-simple (16) when K is a separably generated, non-algebraic extension of some sub-field K_0 or when K is a non-denumerable field (Theorems 6.2 and 6.3).

These results refer to group algebras in which the group is arbitrary except that when the characteristic of the field is the non-zero prime p, the group has no p-elements.

We can regard group algebras from a slightly different point of view and investigate for which groups the group algebra over an arbitrary field is semi-simple. As before, we have no p-elements in the group if the field has characteristic p. It is known that provided/

provided this condition is imposed, the following classes of groups give rise to semi-simple algebras over any field: (i) locally finite groups {Corollary 6.5 (6)}, (ii) ordered groups {Theorem 6.7 (9)} and (iii) abelian groups {Corollary 6.6 (9)}.

As in Connell's paper "On the group ring" (9) we let $\mathcal{C}$ denote the class of all groups G with the property:

If K is a field of characteristic p (≥ 0) and if G has no p-elements if $p \neq 0$, then the group algebra of G over K is semi-simple.

The above three classes of groups then belong to $\mathcal{C}$. Other groups belonging to $\mathcal{C}$ can be constructed using Proposition 12 of (9)

(i) If each finitely generated subgroup of G is in $\mathcal{C}$, then $G \in \mathcal{C}$ (Theorem 6.4).

(ii) If $G, H \in \mathcal{C}$, then $G \times H \in \mathcal{C}$ (Theorem 6.8).

(iii) If G is any group and G_0 is the infinite cyclic group, then $G \times G_0 \in \mathcal{C}$ (Theorem 6.8).

(Note that in (iii) if the field has characteristic $p \neq 0$, then by the definition of $\mathcal{C}$, G may have no p-elements and so is not completely arbitrary).

§ 2. The radical of a group algebra.

Before defining the radical of a general ring, we must introduce the following concepts and definitions. Throughout, unless otherwise stated, we shall assume A to be an arbitrary ring.

M is a (right) A-module if

(i) M is an additive abelian group

(ii) there is a mapping from $M \times A$ to M, the image of (m,a) being denoted by ma.

The/

The mapping has the following properties:

(a) $m_1, m_2 \in M$; $a \in A \Rightarrow (m_1 + m_2)a = m_1a + m_2a$

(b) $m \in M$; $a_1, a_2 \in A \Rightarrow m(a_1 + a_2) = ma_1 + ma_2$

(c) $m \in M$; $a_1, a_2 \in A \Rightarrow (ma_1)a_2 = m(a_1a_2)$.

We shall deal with right A-modules only and so in general we omit the adjective "right".

A subset M' of M is called an A-submodule if (i) M' is an additive subgroup of M.

(ii) $m' \in M'$, $a \in A \Rightarrow m'a \in M'$.

If the ring A has an identity 1 and M is an A-module such that

$$m1 = m \text{ for all } m \in M,$$

then M is unitary or unital as in (13). We will eventually be concerned only with rings with an identity and we assume all modules unitary in that case.

The ideal of a module is closely linked with that of a representation.

A representation of a ring A is a homomorphism of A into the ring of endomorphisms of a commutative group M.

A representation is faithful if and only if it is one-to-one.

If there is a representation of A in terms of the endomorphisms of a commutative group M, then M may be regarded as an A-module. On the other hand, any A-module M gives rise to a representation of A (13, Chapter I).

The kernel of the representation defined by M is denoted by A(M) and is the set $\{a \in A: ma = 0 \ \forall \ m \in M\}$ so that the representation is faithful if and only if $A(M) = (0)$.

An/

An A-module M is irreducible if and only if

(i) $MA = \{ma : m \in M, \; a \in A\} \neq \{0\}$ (this is always so if M is unitary and $M \neq \{0\}$).

(ii) M has no proper submodules apart from $\{0\}$ and M.

We now define a subdirect sum: $\{A_i : i \in S\}$ is a possibly infinite set of rings, not necesserily distinct. We form the Cartesian product $\prod_{i \in S} A_i$ of the set. Addition and multiplication ar defined on $\prod A_i$ by

$$(a + b)_i = a_i + b_i, \; (ab)_i = a_i b_i$$

where $a, b \in \prod A_i$, a_i, b_i etc. $\in A_i$. (the "components" of a,b etc. in A_i).

The complete direct sum of the rings A_i is the product set with addition and multiplication as above, and is denoted by $\sum_C \oplus A_i$

A subring B of $\sum_C \oplus A_i$ is called a subdirect sum if and only if the homomorphism from B to A_i $(b \to b_i)$ is surjective for each $i \in S$. Then B is denoted by $\sum_S \oplus A_i$

We state the following result as Theorem 2.1. (13) The ring B can be represented as the subdirect sum $\sum_S \oplus A_i$ if and only if there is a set $\{B_i : i \in S\}$ of ideals in B such that $\bigcap_{i \in S} B_i = (0)$ and $A_i \cong B/B_i$.

The Wedderburn radical of a ring A is defined to be the sum of all the nilpotent ideals of A. However it is not always true that

$$W(A/W(A)) = (0).$$

For an artinian ring (i.e. one with descending chain condition on right ideals), W(A) is the maximal nilpotent ideal of A and W(A/W(A)) = (0). These properties of the Wedderburn radical of an artinian ring give us some idea of the properties which must be possessed by the radical of an arbitrary ring.

If ρ is a property which may be possessed by any ideal of a ring A, we call ρ a radical property if it satisfies the following conditions:

(i) If the ideal I is nilpotent, then I has ρ .

(ii) There is a unique maximal ideal with property ρ . We call this ideal the radical of A or Red A.

(iii) Red (A/Red A) = (0).

(iv) If A is artinian, Red A = W(A).

(v) If I has ρ , then so does every homomorphic image of I.

(Cf. Amitsur's definition of a π radical in (2)).

As we have already mentioned, the Wedderburn radical does not in general satisfy property (iii).

For any ring A we define a nil radical (a radical ideal according to Baer (7)), to be an ideal N such that

(i) N is nil

(ii) A/N contains no non-zero nilpotent ideals.

We define two nil radicals - the upper and lower nil radicals - for any ring A.

The lower nil radical of A, denoted by N(A), may be defined using transfinite induction in terms of the Wedderburn radical (7).

A/

A simpler definition is:

$N(A) = \bigcap \{ N : N$ is an ideal of A such that A/N has no non-zero nilpotent ideals $\}$.

$N(A)$ is sometimes called the prime radical, a term which is derived from the fact that

$N(A) = \bigcap \{ P : P$ a prime ideal of $A \}$. (P is a prime ideal of A if and only if

$UV \subseteq P, U, V$ ideals of $A \Rightarrow U \subseteq P$ or $V \subseteq P$).

The equivalence of these characterisations of $N(A)$ is proved in Jacobson (13). Every nil radical of A does in fact contain $N(A)$ justifying the use of the term "lower".

From Theorem 2.1, we have that a ring A is isomorphic to a subdirect sum of prime rings if and only if $N(A) = (0)$, a prime ring being one in which (0) is a prime ideal.

If $N(A) = (0)$ we say that A is semi-prime.

The upper nil radical, $U(A)$, of a ring A is the sum of all the nil ideals of A and is the maximal nil ideal of A. $U(A/U(A)) = (0)$ and so $U(A)$ is indeed a nil radical. The property of being nil is a radical property.

In our initial definition of a radical, we made mention of a radical property ρ of ideals. The two radicals already dealt with are both nil radicals. Jacobson in (12) made the following observation, "Several investigations of nil ideals in arbitrary rings have been made recently but none of these has led to a structure theory for general semi-simple rings. This is one of the indications that in order to develop a satisfactory structure theory for arbitrary rings/

rings it is necessary to abandon the concept of a nil ideal in defining the radical".

Accordingly, the Jacobson radical of A is defined to be the sum of all quasiregular right ideals of A and is denoted by J(A).

A right ideal R is quasiregular, if for every $r \in R$, there is an $r' \in A$ such that $r + r' + rr' = 0$. Then r' is a right quasi-inverse of r. It may be proved that r' is also a left quasi-inverse i.e. $r + r' + r'r = 0$. In fact $r' \in R$ also. J(A) is the maximal quasiregular ideal of A and $J(A/J(A)) = (0)$. J(A) contains all nil ideals of A and we have the following inclusion relationship:

$$W(A) \subseteq N(A) \subseteq U(A) \subseteq J(A),$$

equality occurring when A is artinian.

Quasiregularity is clearly a radical property, giving rise to the corresponding radical J(A).

The following definitions are necessary for the statement of equivalent characterisations of J(A).

A right ideal R of A is modular if there is an element $t \in A$ such that $ta - a \in R$ for all $a \in A$. For any ring with an identity, all right ideals are modular.

A ring B is primitive if and only if it has a faithful irreducible module.

An ideal P of A is primitive if and only if A/P is a primitive ring

$$\text{Then } J(A) = \bigcap \{ A(M) : M \text{ an irreducible A module} \},$$

$$= \bigcap \{ R : R \text{ a maximal right ideal of A, which is modular} \},$$

$$= \bigcap \{ P : P \text{ a primitive ideal of A} \}.$$

If A has an identity,

$J(A) = \bigcap \{ R : R \text{ a maximal right ideal} \}$.

Also $z \in J(A) \Leftrightarrow (1 - az)^{-1}$ exists for all $a \in A$

$\Leftrightarrow (1 - za)^{-1}$ exists for all $a \in A$.

Jacobson proves the equivalence of these characterisations in (13).

By Theorem 2.1, $J(A) = (0)$ if and only if A is a subdirect sum of primitive rings.

It appears to be common practice to say that a ring A is semi-simple if $J(A) = (0)$, but in view of the use of the terms prime and semi-prime given above, it would be more consistent to use the term semiprimitive as Connell does (9). Connell defines a ring to be semi-simple if the intersection of its maximal ideals is the zero ideal, and in that case, the ring is a subdirect sum of simple rings. A is a simple ring if $A^2 \neq (0)$ and A has no ideals other than (0) and A.

However, as we shall from now on make reference to the upper nil and Jacobson radicals only, whenever the term semi-simple is used it will mean that the Jacobson radical of the ring in question is the zero ideal.

Our object is to study group algebras, but occasionally we shall have to refer to the group ring of a group over a ring, so we define this more general concept first.

The group ring of the group G over the ring A, denoted by R(G,A) consists of all finite sums of the form $\sum a(g)g$ where $g \in G$, $a(g) \in A$, i.e. only a finite number of the a(g) are non-zero.

R(G,A)/

R(G,A) is a ring if the operations of multiplication and addition are defined in the natural way, e.g.

$$\left(\sum_{g \in G} a(g)g \right) \left(\sum_{h \in G} b(h)h \right) = \sum_{g,h \in G} a(g)b(h)gh$$

If K is a field then R(G,K) is an algebra over K, with an identity. We denote the group algebra of the group G over the field K by A(G,K). The definitions for general rings given in the earlier part of the section may be applied to the special case of a group algebra A(G,K) over a field, noting that in this case, since the algebra has an identity, "ring ideal" may be replaced by "algebra ideal".

For any $x \in A(G,K)$ and $\lambda \in K$, $\lambda x = (\lambda e)x$ and so if $x \in I$, a ring ideal of A(G,K), $\lambda x \in I$, showing that I is an algebra ideal.

We denote the upper nil and Jacobson radicals of $A(G,K)$ by $U(G,K)$ and $J(G,K)$ respectively.

If G is a finite group, the group algebra of G over any field K is an algebra of finite dimension $|G|$, the order of G, over K.

Maschke's theorem (15) states that if G is a finite group and K is a field of characteristic $p \geqq 0$, then $A(G,K)$ is semi-simple if and only if $p > 0$ and $p \nmid |G|$, or $p = 0$.

If A is a semi-simple artinian ring, then

$$A = B_1 \oplus B_2 + \ldots \oplus B_n$$

where for $1 \leq i \leq n$, B_i is an ideal of A which is a simple artinian ring.

The Artin-Wedderburn theorem states that for any simple artinian ring B, there exist a positive integer n(unique) and a division ring D (unique up to isomorphism) such that

$$B \cong M_n(D)$$

where $M_n(D)$ is the ring of $n \times n$ matrices with coefficients from D. We then have that for any semi-simple artinian ring

$$A \cong M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \ldots \oplus M_{n_t}(D_t)$$

where $D_1, \ldots, D_t$ are division rings.

For any division ring D and positive integer n, $M_n(D)$ is isomorphic to the ring of linear transformations of an n-dimensional vector space over D, showing that any of the mappings $A \to M_{n_i}(D_i)$ is a representation of A in the sense defined earlier.

By/

By Maschke's Theorem if

(i) the characteristic of the field K is zero and G is any finite group or (ii) the characteristic of K is the non-zero prime p and $p \nmid |G|$, then A(G,K) may be represented as a direct sum of a finite number of simple algebras over K of the form $M_n(D)$ where D is a division algebra over K of finite dimension.

§ 3. The connection between the upper nil and Jacobson radicals.

As has already been pointed out, in a finite dimensional algebra, the upper nil and Jacobson radicals coincide. In certain other cases, these radicals coincide.

We commence by considering the spectrum S(a) (or $S_K(a)$) of an element $a \in A$, an algebra over the field K.

$$S(a) = \{ \lambda \in K: \ -\lambda^{-1}a \text{ is not quasi-regular in } A \}$$

as in Amitsur's paper (4), or alternatively, for an algebra A with an identity element,

$$S(a) = \{ \lambda \in \bar{K} : a - \lambda 1 \text{ has no inverse in } A \}.$$

This is the definition given by Jacobson in (13). Theorem 3.1, which we will eventually prove, is proved by Jacobson in (13) for an algebra with an identity and Jacobson then shows how the result may be extended to an algebra without an identity by adjoining an identity in the usual way.

The proof given by Jacobson is rather simpler than the original proof by Amitsur (4) and so we give the former here, omitting the extension of the result to algebras without an identity since we will only require to apply it to algebras with an identity.

Let C(a) be the complement of S(a) in K.

If/

If $\underline{a}$ is an algebraic element of A, then the subalgebra over K, generated by $\underline{a}$ is finite dimensional over K and there is a minimal polynomial $f(X)$ over K, of which $\underline{a}$ is a zero.

Lemma 3.1. If $\underline{a}$ is algebraic with minimal polynomial $f(X)$, then

$$S(a) = \{\lambda \in K : f(\lambda) = 0\}.$$

Proof: Let $\{\lambda_1, \ldots, \lambda_n\} = \{\lambda \in K : f(\lambda) = 0\}$.

Then for $1 \leq i \leq n$, there exists a polynomial $g_i(X)$ over K such that

$$(a - \lambda_i 1)g_i(a) = 0$$

$$\text{and} \qquad (X - \lambda_i)g_i(X) = f(X).$$

If $\lambda_i \notin S(a)$, then $a - \lambda_i 1$ has an inverse in A and so $g_i(a) = 0$. But the degree of $g_i(X)$ is less than the degree of $f(X)$ which is the minimal polynomial of $\underline{a}$. Thus we have a contradiction and so

$$\{\lambda_1, \ldots, \lambda_n\} \subseteq S(a).$$

Take $\lambda \in S(a)$, $\lambda \notin \{\lambda_1, \ldots, \lambda_n\}$.

Then $f(\lambda) \neq 0$ and $f(\lambda)^{-1}$ exists in K.

Let $g(X) = \dfrac{1 - f(\lambda)^{-1}f(X)}{X - \lambda}$ and $g(a) \in A$,

since $X - \lambda$ is a factor of $1 - f(\lambda)^{-1}f(X)$. Now $g(a)$ is an inverse of $(a - \lambda 1)$. But $\lambda \in S(a)$ and again we have a contradiction.

$$\text{So } S(a) \subseteq \{\lambda_1, \ldots, \lambda_n\}.$$

Combining the two results we have that $S(a) = \{\lambda \in K : f(\lambda) = 0\}$.

Lemma 3.2. Let $\mu_1, \ldots, \mu_r$ be distinct elements of $C(a)$ and $(a - \mu_1 1)^{-1}, \ldots, (a - \mu_r 1)^{-1}$ the corresponding inverses. Then either the elements, $(a - \mu_1 1)^{-1}, \ldots, (a - \mu_r 1)^{-1}$ are linearly independent or $\underline{a}$ is algebraic over K.

Proof:/

Proof: We assume that $(a - \mu_1 1)^{-1}, \ldots, (a - \mu_r 1)^{-1}$ are linearly dependent and prove that a is then algebraic over K.

By our assumption, there are $\alpha_1, \ldots, \alpha_r \in K$, not all zero, such that

$$\alpha_1(a - \mu_1 1)^{-1} + \ldots + \alpha_r(a - \mu_r 1)^{-1} = 0 \quad ;$$

we multiply by $\prod_{i=1}^{r}(a - \mu_i 1)$ obtaining

$$\alpha_1 g_1(a) + \alpha_2 g_2(a) + \ldots + \alpha_r g_r(a) = 0$$

where $g_i(X) = \prod_{j \neq i}(X - \mu_j)$ for a fixed i, $1 \leq i \leq r$.

Let $g(X) = \sum_{i=1}^{r} \alpha_i g_i(X)$. g(X) is not the zero polynomial, for if it were we would have

$$g(\mu_i) = 0 \qquad (1 \leq i \leq r)$$

and hence $\alpha_i g_i(\mu_i) = 0$ since $g_j(\mu_i) = 0$ when $i \neq j$.

But this is impossible since the μ's are distinct and not all the α's are zero.

Thus we have a non-zero polynomial over K, g(X), and g(a) = 0, so that a is algebraic.

Lemma 3.3. If A is an algebra over a field K and $a \in J(A)$, then a is either nilpotent or transcendental.

Proof: Any element of J(A) must be either algebraic or transcendental. Let $a \in J(A)$ be algebraic. Then the algebra A^* generated by a is finite dimensional over K and $A^* \subseteq J(A)$.

Now $a^k A^* \supseteq a^{k+1} A^*$ for $k = 0, 1, \ldots$. Since A^* has finite dimension over K, there exists an integer m, such that

$$a^{m-1} A^* = a^m A^*$$

$a^m \in a^{m-1}A^*$ and so there exists an element b of A^* such that

$$a^m = a^m b.$$

$b \in A^* \subseteq J(A)$ and so $-b \in J(A)$ and has a quasi-inverse $-b'$ such that $-b - b' + bb' = 0$.

$$\begin{aligned} \text{Then } 0 &= (a^m - a^m b) - (a^m - a^m b)b' \\ &= a^m + a^m(-b - b' + bb') \\ &= a^m \end{aligned}$$

and $\underline{a}$ is nilpotent.

We are now able to prove

<u>Theorem 3.1.</u> Let A be an algebra (with an identity element) over an infinite field K whose cardinal number exceeds $(A:K)$, the dimension of A over K. Then $J(A)$ is a nil ideal i.e. $J(A) = U(A)$.

<u>Proof:</u> Take any element $a \in J(A)$. Then $(1 - \lambda a)^{-1}$ exists for every $\lambda \in K$. Hence $\lambda^{-1} \in C(a)$ for every non-zero element λ of K. By lemma 3.2, if $\underline{a}$ is not algebraic, the set

$$\{ (a - \lambda^{-1}1)^{-1} : \lambda \in K, \lambda \neq 0 \}$$

is linearly independent over K.

But the cardinal number of the elements in this set is greater than $(A:K)$. Thus we have a contradiction showing that $\underline{a}$ is algebraic and so nilpotent by lemma 3.3.

Since every element of $J(A)$ is nilpotent, $J(A)$ is a nil ideal.

The following result is a corollary of Theorem 3.1, but because of its importance, we state it as a theorem.

<u>Theorem 3.2.</u> If A is a finitely generated algebra over an uncountable field then $J(A) = U(A)$.

Here the dimension of A over the field is countable and so is strictly/

strictly less than the cardinal number of the field.

Amitsur in (5) generalises Hilbert's Nullstellensatz and as an application proves that for finitely generated algebras of a particular type, the Jacobson radical is a nil ideal.

The classical form of the Nullstellensatz deals with the polynomial ring $F[x_1,\dots,x_n] = F[x]$ where F is a field and $x_1,\dots,x_n$ are commutative indeterminates. G is a subset of $F[x]$. If $f(x_1,\dots,x_n)$ $f(x) \in F[x]$ vanishes at all the zeros of G, then the Nullstellensatz states that there is a positive integer m such that $f^m(x)$ belongs to the ideal generated by the set G i.e. I(G).

Note: $(\lambda_1,\dots,\lambda_n)$ $(\lambda_i \in F)$ is a zero of G if and only if $g(\lambda_1,\dots,\lambda_n) = 0$ for all $g(x) \in G$.

The Nullstellensatz is extended as follows, using Amitsur's own notation.

$F[x] = F[x_1,\dots,x_n]$ is the free algebra generated by the finite set of <u>non-commutative</u> indeterminates over the field F.

$\bar{F}_k$ is the set of all k x k matrices over $\bar{F}$, the algebraic closure of F.

$\mathfrak{M}_k$ is the set of all polynomials $f(x_1,\dots,x_n) \in F[x]$ for which $f(x_1,\dots,x_n) = 0$ holds identically in $\bar{F}_k$. $\mathfrak{M}_k$ is an ideal in $F[x]$

R is an algebra over F. $(r_1,\dots,r_n)$ $(r_i \in R)$ is said to be a zero in R of the set of polynomials $G(\subseteq F[x])$ if $g(r_1,\dots,r_n) = 0$ for all $g(x) \in G$.

We say that $f(x) \in F[x]$ satisfies (Z_k) if $f(x_1,\dots,x_n)$ vanishes for all zeros of G which lie in $\bar{F}_k$,

and/

and $f(x) \in F[x]$ satisfies $(Z\infty)$ if $f(x_1,\ldots,x_n)$ vanishes for all zeros of G which lie in primitive rings.

Then the following two extensions of the Nullstellensatz are established.

I If $f(x)$ satisfies (Z_k) then $f^m(x)$ belongs to the union of the ideals $I(G)$ and $\mathcal{M}_k$ for some integer m.

II If $f(x)$ satisfies $(Z\infty)$ then $f^m(x) \in I(G)$ for some integer m.

Amitsur also proves that the Jacobson radical of $F[x]/Q_k$, where $Q_k = (I(G)+\mathcal{M}_k)$, is a nil ideal.

These results, along with Theorem 3.2 and earlier results proved by Amitsur in (1) are used to prove

Theorem 3.3.(5) The Jacobson radical of a finitely generated algebra which satisfies an identity is a nil ideal.

§ 4. The Jacobson radical under field extensions.

Before proceeding to examine the behaviour of the radical of an algebra under extension of the field, we give a short summary of definitions and results from the theory of fields which will be used in this and subsequent sections.

We consider extensions of a field C of arbitrary characteristic.

α is algebraic over C if α is the root of a non-trivial polynomial equation with coefficients in C, otherwise α is transcendental. An extension K of C is algebraic if every element of K is algebraic over C. K is a finite (algebraic) extension of C if K is a vector space of finite dimension over C.

We shall have occasion to consider some special types of algebraic extension of C.

K/

K is a <u>normal</u> extension of C if every irreducible polynomial over C which has at least one root in K, has all its roots in K. K is a finite normal extension of C if and only if K is the root field of some polynomial over C.

K is a <u>separable</u> extension of C if every element in K is the root of a separable polynomial over C i.e. one with distinct roots.

If C is a finite field or a field of characteristic zero, then any algebraic extension of C is a separable extension of C.

K is a <u>pure transcendental</u> extension of C if K is formed by the adjunction of elements, transcendental over C. A transcendence base $\{x_\mu\}$ (possibly infinite) may be chosen so that $K = C(x_\mu)$. The number of elements in a transcendence base is unique - the degree of transcendence of the extension. If $\{X_\mu\}$ is a set of commutative indeterminates of the same cardinality as $\{x_\mu\}$, then K is isomorphic to the field of rational functions $C(X_\mu)$.

If K is a transcendental (or non algebraic) extension of C, then there is a transcendence base $\{x_\mu\}$ such that $F = C(x_\mu)$ is a pure transcendental extension of C and K is an algebraic extension of F.

Let H be a normal separable extension of C and θ an automorphism of H, leaving elements of C invariant.

Let R be an algebra over C with $\{ r_i \}$ as a base of R over C. Every element of $R \otimes_C H = R_H$ may be expressed uniquely in the form $\sum_i r_i h_i$ $(h_i \in H$

We define a mapping θ' from R_H to R_H by

$$\left(\sum_i r_i h_i \right) \theta' = \sum_i r_i (h_i \theta).$$

θ' is an automorphism of R_H and leaves all elements of R invariant.

θ' is an extension of θ to R_H. It is the only extension leaving elements of R invariant and we denote it by θ in future.

The set of all automorphisms of H over C is a group. If G is a subgroup of this group, the set of elements of H left invariant by G is a subfield $F(\geq C)$ of H. If we extend the automorphisms in G to R_H then we obtain the group of all automorphisms of R_H leaving the elements of R_F invariant.

For every element $h \in H$, we shall denote by $tr(h)$, the trace of h which is defined to be $\sum h\theta$ where the sum is over all automorphisms of H over C. $\sum h\theta$ is clearly invariant under any automorphism of H over C and so $\sum h\theta \in C$ for all $h \in H$. Alternative, and more common, definitions are as follows: (i) Suppose that $g(x)$ is the minimal irreducible polynomial over C of which h is a root. Then if $n = (H:C)$, the degree of $g(x)$ divides n and so there is an integer r such that $G(x) = (g(x))^r$ is of degree n.
$G(x) = x^n - g_1x^{n-1} + \dots + (-1)^n g_n$ where $g_i \in C$. The trace of h is g_1, the sum of the roots of $G(x)$. (ii) Suppose that $(\lambda_1, \dots, \lambda_n)$ is a basis of H. Then

$$h\lambda_i = c_{i1}(h)\lambda_1 + \dots + c_{in}(h)\lambda_n.$$

Thus we have a matrix $[c_{ij}(h)]$ of type n x n and define trace of h to be

$$\sum_{i=1}^{n} c_{ii}(h).$$

We note that any automorphism of H over C maps h into a conjugate of itself i.e. a root of $g(x)$.

We form the matrix $[tr(\lambda_i\lambda_j)]$ of type n x n. Then $\det[tr(\lambda_i\lambda_j)]$ is non-zero if and only if H is separable over C.

These results are stated and proved by van der Waerden (18) and Jacobson (14).

<u>Lemma 4.1</u> A any ring. If for some $b \in J(A)$, and $a \in A$, $a + ba = 0$, then $a = 0$.

<u>Proof:</u> Since $b \in J(A)$, there exists $b' \in A$ such that $b + b' + b'b = 0$.

$$\text{Then} \quad ba + b'a + b'ba = 0.$$

Since $ba = -a$, we have

$$-a + b'a - b'a = 0 \quad \text{i.e. } a = 0.$$

<u>Lemma 4.2.</u> The quasi-inverse of $b \in J(A)$ is unique.

<u>Proof:</u> $b \in J(A)$. Then there is $b' \in J(A)$ such that $b + b' + bb' = 0$.

Suppose that there exists $b'' \in J(A)$ such that $b'' \neq b'$ and

$$b + b'' + bb'' = 0.$$

Then $(b' - b'') + b(b' - b'') = 0$ and, by lemma 4.1, it follows that $b' - b'' = 0$, a contradiction.

Then b' is the only quasi-inverse.

<u>Lemma 4.3.</u> Let $b \in J(A)$ and let b' be its quasi-inverse. Then the centraliser of b in A is the centraliser of b' in A.

<u>Proof:</u> $b + b' + bb' = 0.$

Let $a \in A$, such that $ab = ba$.

$$\text{Then } 0 = (b + b' + bb')a - a(b + b' + bb')$$

$$= ba - ab + (b'a - ab') + b(b'a - ab')$$

$$\text{i.e. } (b'a - ab') + b(b'a - ab') = 0.$$

By Lemma 4.1, $b'a - ab' = 0$.

We now consider any algebra A with an identity over a field C. Let C_n denote the ring of n x n matrices over C.

We denote the <u>tensor product</u> of two vector spaces U and V, both over a field K, by $U \otimes V$. $U \otimes V$ consists of all finite formal sums of/

of elements of the form

$$u \otimes v \qquad (u \in U,\ v \in V).$$

For convenience we denote $u \otimes v$ by uv and note that the product uv satisfies the laws

(i) $(u_1 + u_2)v = u_1 v + u_2 v \qquad (u_1, u_2 \in U;\ \ v \in V)$

(ii) $u(v_1 + v_2) = uv_1 + uv_2 \qquad (u \in U;\ \ v_1, v_2 \in V)$

(iii) $(\lambda u)v = u(\lambda v) = \lambda(uv) \qquad (u \in U;\ \ v \in V;\ \lambda \in K).$

<u>Lemma 4.4.</u> Let S be a subalgebra of C_n and S^* the centraliser of S in C_n. Then the centraliser of S in $A \otimes C_n$ is $A \otimes S^*$.

We denote $A \otimes C_n$ by A_n.

<u>Proof:</u> Let $\{a_i\}$ be a basis for A over C. Then any element of $A \otimes C_n$ is of the form $\sum_i a_i c_i$ where $c_i \in C_n$.

Take any $s \in S$. Then

$$s(\sum a_i c_i) - (\sum a_i c_i)s = \sum a_i(sc_i - c_i s)$$

$$= 0 \text{ if and only if } sc_i - c_i s = 0.$$

$$\text{i.e. if and only if } c_i \in S^*.$$

Thus any element of A_n commuting with all elements of S^* is in $A \otimes S^*$.

<u>Lemma 4.5.</u> If F is a finite extension of C of degree n, then F can be considered as a subfield of C_n and the centraliser of F in C_n is F itself.

<u>Proof:</u> F is an algebra of dimension n over C, and so it has a representation in C_n. (F is an F-module).

Moreover, this representation is clearly faithful and so we may consider F as a subfield of C_n.

Let F^* denote the centraliser of F in C_n.

C_n/

C_n is a central simple algebra over C, and F is a simple subalgebra containing a 1. Then (11, Chapt. V, Thm 19)

$(C_n : C) = (F:C)(F^* : C)$. But $(C_n : C) = n^2$ and $(F : C) = n$ so that $(F^* : C) = n$.

We then have $F^* \supseteq F$ and

$$(F^* : C) = (F : C).$$

Thus $F^* = F$.

Theorem 4.1.

If F is a separable extension of C, of finite or infinite degree, then

$$J(R_F) = J(R)_F,$$

Where R is an algebra with an identity over C and $R_F = R \otimes_C F$ etc.

Proof: We split the proof into several sections.

(i) If F is a finite algebraic extension of C, then $J(R_F) \supseteq J(R)_F$.

Suppose that $(F : C) = n$. As in Lemma 4.5, we regard F as a subfield of C_n. Jacobson proves in (13) that

$$J(R_n) = [J(R)]_n.$$

Since $F \subset C_n$, $J(R)_F \subset J(R) \otimes C_n = [J(R)]_n$.

All elements of $J(R)_F$ are quasiregular in $[J(R)]_n$.

Elements of $J(R)_F$ commute with elements of F and so by lemma 4.3, the quasi-inverses of the elements of $J(R)_F$ in $[J(R)]_n$ also commute with elements of F. By Lemmas 4.4 and 4.5 that the quasi-inverses of $J(R)_F$ in $[J(R)]_n$, in fact belong to R_F. So $J(R)_F$ is a quasiregular ideal of R_F and $J(R)_F \subseteq J(R_F)$.

We/

We intend to prove that when F is a finite separable extension of C, $J(R_F) \subseteq J(R)_F$, thus proving the theorem in the finite case. We assume that all extensions are separable throughout the remainder of the proof.

(ii) Let H be a finite normal extension of C and let $J(R) = (0)$. Then $J(R_H) = (0)$.

Let $r \in R \cap J(R_H)$. Then there exists $r' \in J(R_H)$ such that

$$r + r' + rr' = 0.$$

Let θ be an automorphism of H over C. Then θ may be regarded as an automorphism of R_H over R. Hence

$$(r + r' + rr')\theta = 0$$

$$\text{i.e. } r\theta + r'\theta + (r\theta)(r'\theta) = 0$$

But $r \in R$ and so $r\theta = r$.

Then $r + r'\theta + r.r'\theta = 0$ and $r'\theta$ is also a quasi-inverse of r in $J(R_H)$. But by Lemma 4.2 the quasi-inverse is unique and so $r'\theta = r'$. i.e. r' is invariant under all automorphisms of R_H over R and by earlier observations $r' \in R$.

Thus the quasi-inverse of every element of $R \cap J(R_H)$ is in R and so $R \cap J(R_H)$ is a quasiregular ideal of R.

$$\text{i.e. } R \cap J(R_H) \subseteq J(R) = (0)$$

and so. $R \cap J(R_H) = (0)$.

Let $\lambda_1, \ldots, \lambda_n$ be a basis for H over C; then any element $r \in J(R_H)$ can be expressed in the form

$$r = r_1\lambda_1 + \ldots + r_n\lambda_n \qquad (r_i \in R).$$

$J(R_H)$ is an ideal of R_H and is invariant under any automorphism of R_H.

Again/

Again we consider any automorphism θ of H over C. θ is also an automorphism of R_H over R. Then

$$(r\lambda_j)\theta = r_1(\lambda_1\lambda_j)\theta + \dots + r_n(\lambda_n\lambda_j)\theta \in J(R_H).$$

We sum this relationship for all automorphisms θ of H over C, obtaining

$$r_1 tr(\lambda_1\lambda_j) + r_2 tr(\lambda_2\lambda_j) + \dots + r_n tr(\lambda_n\lambda_j) \in J(R_H),$$

where for any $h \in H$, $tr\, h$ is as defined previously.

Since H is, by assumption, a separable extension of C, the matrix $\left[tr(\lambda_i\lambda_j) \right]$ is non-singular.

$$tr(\lambda_i\lambda_j) \in C \text{ and so}$$

$$r_1 tr(\lambda_1\lambda_j) + \dots + r_n tr(\lambda_n\lambda_j) \in R \quad \text{for } 1 \leq j \leq n.$$

Hence $r_1 tr(\lambda_1\lambda_j) + \dots + r_n tr(\lambda_n\lambda_j) \in R \cap J(R_H) = (0).$

Thus we have a set of n homogeneous linear equations in $r_1, \dots, r_n$. Since $\det\left[tr(\lambda_i\lambda_j) \right]$ is non-singular, these equations have only the trivial solution

$$r_1 = r_2 = \dots = r_n = 0.$$

Thus $r = r_1\lambda_1 + \dots + r_n\lambda_n = 0$ and r was any element of $J(R_H)$.

$$\text{Hence } J(R_H) = (0).$$

From (ii) we deduce

(iii) If H is a finite normal extension of C, then

$$\underline{J(R_H) \subseteq J(R)_H}.$$

Let $R^* = R/J(R)$. Then $J(R^*) = (0)$.

$R^*_H = R_H/J(R)_H$ and by (ii) $J(R^*_H) = 0$.

i.e. $J(R)_H$ is an ideal such that $R_H/J(R)_H$ is semi-simple. This implies that

$$J(R)_H \supseteq J(R_H),$$

since $J(R_H)$ is the minimal ideal Q such that R_H/Q is semi-simple.

From (i) and (iii) we have that if H is a finite normal (and separable) extension of C then

$$J(R_H) = J(R)_H \quad — \quad (A).$$

(iv) If F is a finite separable extension of C, then $J(R_F) = J(R)_F$.

We consider H to be a finite normal extension of C containing F. R_H may be considered as a field extension of R_F and by (A)

$$J(R_H) = J(R_F)_H.$$

From this we deduce that

$$J(R_F) \subseteq J(R_H)$$

and it follows immediately that

$$J(R_F) \subseteq J(R_H) \cap R_F.$$

Let $r \in J(R_H) \cap R_F$. Then r has a quasi-inverse $r' \in J(R_H)$. We consider any automorphism θ of R_H over R_F. Then $r'\theta$ is also a quasi-inverse of r, since $r\theta = r$. But r has a unique quasi-inverse and so $r'\theta = r'$. Thus $r' \in R_F$ and $J(R_H)$.

$J(R_H) \cap R_F$ is then a quasiregular ideal of R_F

i.e. $J(R_H) \cap R_F \subseteq J(R_F)$

Now $J(R_F) = J(R)_H \cap R_F$

$= J(R)_F.$

Thus $J(R)_F \supseteq J(R_F)$

Thus we have proved the theorem for separable extensions of finite degree.

(v) Let F be an infinite separable extension of C and $K \subset F$ a subfield of F of finite degree over C,

$$\text{then } J(R_F) \cap R_K \subseteq J(R_K).$$

Consider $r \in J(R_F) \cap R_K$. Then r has a quasi-inverse $r' \in J(R_F)$. $r' \in R_F$ and in fact $r' \in R_{K'}$, for some finite algebraic extension K' of C, $K' \subset F$.

We let H be the minimal normal field containing K, K' and H^* the minimal field containing H and F. $(H:C) < \infty$ and H is normal over C. So H^* is normal over F and $(H^*:F) < \infty$. Again by (A)

$$J(R_{H^*}) = J(R_F)_{H^*}$$

and $r, r' \in J(R_{H^*})$.

We consider θ, any automorphism of H over K. Then $r'\theta$ is a quasi-inverse of $r\theta = r$. $r \in J(R_{H^*})$ and so has a unique quasi-inverse in $J(R_{H^*})$. Both r', $r'\theta \in J(R_{H^*})$. Then $r' = r'\theta$, by Lemma 4.2. This implies that $r' \in R_K$ and that $J(R_F) \cap R_K$ is a quasiregular ideal in R_K

$$\text{i.e. } J(R_F) \cap R_K \subseteq J(R_K)$$

We are now able to complete the proof of the theorem:

(vi) If F is an infinite separable extension of C, then $J(R_F) = J(R)_F$.

(This proof applies to F, a finite separable extension of C, but we have already proved the result in that case).

If $r \in J(R_F)$, then $r \in R_K$ for some finite algebraic extension $K \subset F$ of C. By (v) $r \in J(R_K)$ and by (iv)

$$J(R_K) = J(R)_K$$

$$\text{i.e. } r \in J(R)_K \subset J(R)_F$$

since $K \subset F$.

Thus/

Thus $J(R_F) \subseteq J(R)_F$.

If $r \in J(R)_F$, then $r \in J(R)_K$ for some finite algebraic extension of C. K is a separable extension and so $J(R)_K = J(R_K)$ by (iv).

This implies that $r \in J(R_K)$ and so r has a quasi-inverse in $J(R_K)$. Thus every element of $J(R)_F$ has a quasi-inverse in R_F.
Then $J(R)_F$ is a quasiregular ideal of R_F. Therefore $J(R)_F \subseteq J(R_F)$.
Combining the two results we have that $J(R)_F = J(R_F)$ if F is an infinite (or finite) separable extension of C.

It is easy to extend the proof to cover algebras R over C, without an identity element. We omit this since we will only require to apply the theorem to algebras with an identity.

We now consider F, a pure transcendental extension of C. $F \simeq C(x)$ for some set of commutative indeterminates $\{x_i\}$ - possibly infinite.

Let $C[\ldots,x_i,\ldots] = C[x]$, the ring of all polynomials over C in the set $\{x_i\}$
$C(\ldots,x_i,\ldots) = C(x)$, the field of all rational functions over C in the set $\{x_i\}$.
Then $R[x] = R \otimes_c C[x]$, $R(x) = R \otimes_c C(x)$,
where $R(x) = \left\{ \dfrac{r(x)}{h(x)} : \begin{array}{l} r(x) \in R[x], \\ h(x) \in C[x] \end{array} \right\}$

In order to deal with pure transcendental extensions, we consider $R(x)$ as defined above, where R is an algebra with an identity over C. We first prove

Lemma 4.6 If $J(R(x)) \neq (0)$, then $J(R(x)) \cap R \neq (0)$,

Proof: We suppose that $h(x)^{-1}r(x) \quad J(R(x))$. and that $h(x)^{-1}r(x) \neq 0$.

$J(R(x))$ is an ideal of $R(x) \supseteq C(x)$.

Hence/

Hence $h(x)\, h(x)^{-1}\, r(x) \in J(R(x))$.

i.e. $r(x) \in J(R(x))$ and $r(x) \neq 0$.

Among all the polynomials $r(x) \in J(R(x))$ we choose the element of lowest degree and denote it by $r(x)$.

We assume that $r(x) \notin R$. Then it is of degree $k \geq 1$, for at least one indeterminate, x_1, say.

We define $C'[x]$ and $C'(x)$ to be the ring of all polynomial functions and the field of all rational functions over the set $\{x_i : i \neq$

Then $R'[x] = R \otimes C'[x]$ and

$$R'(x) = R \otimes C'(x).$$

We note that $r(x) \in R[x]$ can be expressed in the form

$$r(x) = r_0 + r_1 x_1 + .. + r_k x_1^k \text{ where } r_k \neq 0$$

and $r_i \in R'[x]$ $(0 \leq i \leq k)$.

We now define an automorphism θ of $C(x)$ thus

$$\theta : x_1 \rightarrow x_1 + 1$$

$$\theta : x_i \rightarrow x_i \qquad (i \neq 1).$$

θ has a unique extension to $R(x)$, denoted by θ, such that all elements of R are invariant under θ.

$J(R(x))$ is invariant under all automorphisms of $R(x)$ and so

$$r(x)\,\theta \in J(R(x)).$$

$J(R(x))$ is an ideal and so the polynomial

$$S(x) = (r(x))\theta - r(x) \in J(R(x)).$$

We now have to consider the characteristic of C.

(i) <u>C has characteristic zero</u>

$$S(x) = \sum_{i=0}^{k} r_i \left[(x_1 + 1)^i - x_1^i \right].$$

is/

is of lower degree in x_1 than $r(x)$ and so $S(x)$ is of lower total degree than $r(x)$.

Since $k \geq 1$ and characteristic of $C = 0$, $S(x) \neq 0$ and $r(x)$ is not the element of $J(R(x))$ of lowest total degree, a contradiction.

Hence $r(x) \in R$

and $J(R(x)) \cap R \neq (0)$.

(ii) <u>C has characteristic $p \neq 0$</u>

Again $S(x)$ is of lower total degree than $r(x)$, but there is a possibility that $S(x) = 0$.

If $S(x) \neq 0$ we have a contradiction as above.

We suppose that $S(x) = 0$.

i.e. $r(x)\,\theta = r(x)$.

i.e. $g(x_1 + 1) = g(x_1)$ where g is a polynomial with coefficients in $R'[x]$.

We will show that $g(x_1) = g'(x_1^p - x_1)$ where g' is a polynomial in $x_1^p - x_1$ with coefficients in $R'[x]$.

We suppose that the degree of $g = k$, is less than p.

$$g(x_1 + 1) = g(x_1) \Rightarrow g(x_1 + m) = g(x)_1\, m \in Z.$$

$$g(x_1 + m) = g(m) + x_1 g_1(m) + \ldots + x_1^k g_k(m)$$

$$= r_0 + r_1 x_1 + r_2 x_1^2 + \ldots + r_k x_1^k = g(x_1).$$

Hence $g(m) = r_0$ for all integers m.

$GF[p] \subseteq R'[x]$ and so

$g(m) - r_0$ vanishes for all p-elements of $GF[p]$. But $g(x_1)$ has degree <

Therefore $g(x_1) = r_0 \in R'[x]$.

Take any polynomial $g(x_1)$ of degree $k \geq p$ such that $g(x_1 + 1) = g(x_1)$

Suppose that the result is true for any polynomial of degree $< k$.

$$g(x_1) = h(x_1)(x_1^p - x_1) + k(x_1)$$

where $h(x_1)$, $k(x_1)$ have coefficients in $R'[x]$ and the degree of k in x_1 is $<p$.

$$g(x_1 + 1) = g(x_1)$$

Hence

$$h(x_1 + 1)(x_1^P - x_1) + k(x_1 + 1) = h(x_1)(x_1^P - x_1) + k(x_1)$$

It follows that $(h(x_1 + 1) - h(x_1))(x_1^P - x_1) = k(x_1) - k(x_1 + 1)$.

Degree of right hand side is $< p$.

Degree of left hand side is $\geq p$ or 0.

For consistency, $h(x_1 + 1) = h(x_1)$

$$k(x_1 + 1) = k(x_1).$$

Then $k(x_1) = k_0 \in R'[x]$

and by induction,

$$h(x_1) = h'(x_1^P - x_1), \text{ where } h' \text{ has coefficients in } R'[x].$$

Then $g(x_1) = h'(x_1^P - x_1)(x_1^P - x_1) + k_0$

i.e. $r(x) = r'(x_1^P - x_1)$ with coefficients in $R'[x]$.

We now denote by $C_1[x]$, $C_1(x)$, $R_1[x]$, $R_1(x)$ the rings obtained by replacing x_1 in $\{x_i\}$ by $x_1^P - x_1$.

Then $C(x)$ is a finite extension of degree p over $C_1(x)$. θ is an automorphism of order p and leaves elements of $C_1(x)$ invariant. $C(x)$ is a separable extension of $C_1(x)$.

By (iv) Theorem 4.1,

$$J(R_1(x)) = J(R(x)) \cap R_1(x)$$

and so $r(x) \in J(R_1(x))$.

$C_1(x)$ is isomorphic to $C(x)$ under the mapping: $x_i \rightarrow x_i$ for $i \neq 1$

and $x_1^P - x_1 \rightarrow x_1$

This/

This mapping may be extended to an isomorphism between $R_1(x)$ and $R(x)$ and so it induces an isomorphism between $J(R_1(x))$ and $J(R(x))$. Under this isomorphism,

$$r(x) = r'(x_1^p - x_1) \to r'(x_1)$$

and so $r'(x_1) \in J(R(x))$.

The degree of $r'(x)$ in x_i, $i \neq 1$, is not greater than the degree of $r(x)$ in x_i and the degree of $r'(x_1)$ in x_1 is lower than the degree of $r(x)$ in x_1. So the degree of $r'(x_1)$ is lower than the degree of $r(x)$, a contradiction, since $r'(x_1) \neq 0$ and $r'(x_1) \in J(R(x))$.

Hence $r(x) \in R$.

and $J(R(x)) \cap R \neq (0)$.

We now prove the theorem:

<u>Theorem 4.2.</u> If F is a pure transcendental extension of C then $J(R_F) = N_F$ where $N = J(R_F) \cap R$ is a nil ideal.

<u>Proof:</u> $F = C(x)$. Then $R_F = R \otimes C(x) = R(x)$.

Let $N = J(R(x)) \cap R$.

Then $N_F = N(x)$.

$N \subseteq J(R(x))$ and so $N(x)R(x) = NR(x) \subseteq J(R(x))$.

It follows that $N(x) \subseteq J(R(x))$.

We map $R(x)$ onto $R(x)/N(x)$.

Also $R(x)/N(x) \cong (R/N)(x) = \bar{R}(x)$.

By (2), $J(R(x)/N(x)) = J(R(x))/N(x)$.

$$\text{Now } J(\bar{R}(x)) \cap \bar{R} \cong \frac{J(R(x))}{N(x)} \cap \left(\frac{R + N(x)}{N(x)}\right)$$

$$= \left[J(R(x)) \cap (R + N(x))\right] / N(x)$$

$$= \left[(J(R(x)) \cap R) + N(x)\right] / N(x)$$

$$= (N + N(x))/N(x) = N(x)/N(x) = \bar{0}.$$

Hence, since $J(\bar{R}(x)) \cap \bar{R} = \bar{0}$, by Lemma 4.6, $J(\bar{R}(x)) = \bar{0} \Rightarrow J(R(x)) \subseteq N(x)$.

Hence $J(R(x)) = N(x)$.

We must now prove N a nil ideal of R.

Let $r \in N \cap J(R(x))$ $(= N)$

Then $x(rx_1) \in J(R(x))$. Let $s = r^2$ and let $h(x)^{-1}r(x) \in J(R(x))$ be the quasi-inverse of sx_1.

Thus $sx_1 + h(x)^{-1}r(x) + h(x)^{-1}r(x)sx_1 = 0$

i.e. $h(x)sx_1 + r(x) + r(x)sx_1 = 0$ — (⊗)

Let $r(x) = r_0 + r_1x_1 + \dots + r_\nu x_1^\nu, r_\nu \neq 0, r_i \in R'[x]$

$h(x) = h_0 + h_1x_1 + \dots + h_\mu x_1^\mu, h_\mu \neq 0, h_j \in R'[x]$

Degree of $h(x)sx_1$ in x_1 is $\mu + 1$. By ⊗ the degree of $r(x)sx_1$ in x_1 is $\mu + 1$.

But degree of $r(x)sx_1 \leq \nu + 1$.

Hence $\mu \leq \nu$.

$r_i \in J(R'(x))$ since $J(R(x)) = N'(x_1)$,

Where $N' = J(R(x)) \cap R'(x)$, a consequence of applying the first part of the theorem to $R'(x)$ and $C'(x)$ instead of R and C and noting that the expression for $r(x)$ as a polynomial in x_1 with coefficients in $R'(x)$ is unique.

If $\mu = \nu$, by considering the coefficient of $x_1^{\nu+1}$, $h_\nu s + r_\nu s =$ Hence $s + h_\nu^{-1}r_\nu s = 0$. $h_\nu^{-1}r_\nu \in J(R'(x))$ and so Lemma 4.1 implies that $s = 0$ where $s = r^2$

i.e. r is nilpotent.

If $\mu < \nu$, by considering the coefficients of $x_1^{\nu+1}, \dots, x_1^{\mu+1}$, we obtain

$$r_\nu s = 0 \qquad (i)$$

$$r_\nu + r_{\nu-1} s = 0 \qquad (ii)$$

$$r_{\nu-1} + r_{\nu-2}\, s = 0 \qquad \text{(iii)}$$

$$\cdots$$

$$r_{\mu+2} + r_{\mu+1}\, s = 0$$

$$h_{\mu} s + r_{\mu+1} + r_{\mu} s = 0.$$

Multiply (ii) on right by s. Then by (i)

$$r_{\nu-1}\, s^2 = 0.$$

Multiply (iii) on right by s^2. Then by (ii)

$$r_{\nu-2}\, s^3 = 0.$$

Continue in this way, obtaining

$$r_{\nu-i+1}\, s^i = 0 \qquad i = 1, 2, \ldots, \nu - \mu.$$

Multiply last equation on right by $s^{\nu-\mu}$ and on left by h_{μ}^{-1}.

$$s^{\nu-\mu+1} + h_{\mu}^{-1} r_{\mu}\, s^{\nu-\mu+1} = 0.$$

$h_{\mu}^{-1} r_{\mu} \in J(R'(x))$ $\therefore$ By Lemma 4.1,

$$r^{s(\nu-\mu+1)} = s^{\nu-\mu+1} = 0$$

and r is nilpotent.

Hence N is nil.

Both these theorems will be used in later discussion. In (4), they are used to prove the following theorem

Theorem 4.3. If $A(G,Q)$ is semi-simple, then $A(G,F)$ is semi-simple for any field F of characteristic zero.

Proof: Note first that

$$A(G,K) = A(G,Q) \otimes_Q K \quad \text{where K is an extension field of Q.}$$

F may be regarded as an extension field of Q. There is a field $K \subseteq F$ such that K is a pure transcendental extension of Q and F is an algebraic extension/

extension of K. F is separable over K since the characteristic is zero.

$$J(G,K) = N \otimes_Q K \quad \text{by Theorem 4.2,}$$

where N is a nil ideal of $A(G,Q)$.

But $J(G,Q) = (0)$ and so $N = (0)$.

Then $J(G,K) = (0)$.

Now $J(G,F) = J(G,K) \otimes_K F = (0)$. by Theorem 4.1.

Hence the result.

§ 5. The upper nil radical.

In his paper "Nil ideals in group rings" (16), Passman is interested in group rings of groups over commutative rings with no non-zero nilpotent elements, but as our concern is with group rings over fields, we shall in general give only these results relating to this special case. In several places, we are as a result, able to simplify proofs of theorems.

In the first place, attention is directed to the upper nil radical of the group algebra. $U(G,K)$ is found to be the zero ideal in the two cases: (i) for any group G, if K has characteristic zero, (ii) for any group G with no p-elements, if the characteristic of K is the non-zero prime p.

These two results are proved separately, each requiring several lemmas.

For any ring R, we denote by Comm R the set of all finite sums of elements of the form $ab - ba$, where $a,b \in R$.

<u>Lemma 5.1.</u> For any ring R, if k and n are positive integers, and p a prime, then for every set $r_1,\ldots,r_n$ of n elements of R,

$$(r_1 + r_2 + \ldots + r_n)^{p^k} = r_1^{p^k} + \ldots + r_n^{p^k} + pr + z,$$

Where $r \in R$ and $z \in$ Comm R.

<u>Proof:</u> $(r_1 + \ldots + r_n)^{p^k} = r_1^{p^k} + \ldots + r_n^{p^k} + t$ where t is a sum of elements of R of the form

$$r_{i_1} r_{i_2} \ldots r_{i_{p^k}}$$

where at least two of the subscripts are different.

Consider two words w_1, w_2 of the form

$$w_1 = r_{i_1} r_{i_2} \ldots r_{i_{p^k}},$$

$$w_2 = r_{i_j} r_{i_{j+1}} \dots r_{i_{pk}} r_{i_1} \dots r_{i_{j-1}}$$

i.e. they are cyclic permutations of each other.

Then $w_1 - w_2 = ab - ba \in \text{Comm } R$ where $a = r_{i_1} \dots r_{i_{j-1}}$,

$$b = r_{i_j} \dots r_{i_{pk}} .$$

Hence $w_1 \equiv w_2$ (modulo Comm R).

Thus all the cyclic permutations of a word are congruent modulo Comm R and the number of such words is divisible by p. Hence the result.

We now consider Comm R(G,R), where R(G,R) is the group ring of the group G over the ring R which is commutative. Comm R(G,R), by definition, consists of sums of elements of the form ab − ba, where $a,b \in R(G,R)$.

Suppose $a = r_1g_1 + \dots + r_mg_m$

and $b = s_1h_1 + \dots + s_nh_n$

where $r_i, s_j \in R$ and $g_i, h_j \in G$.

$$ab - ba = \sum_{i,j} r_is_jg_ih_j - \sum_{i,j} s_jr_ih_jg_i$$

$$= \sum_{i,j} r_is_j(g_ih_j - h_jg_i),$$

since R is commutative.

Thus Comm R(G,R) is spanned over R^2 by all elements of the form

$$gh - hg \qquad (g,h \in G) .$$

Any element of R(G,R) is of the form $x = \sum_{g} r(g)g \quad (r(g) \in R, g \in G)$

with/

with only a finite number of non-zero terms. Let $\theta(x)$ denote the coefficient of the identity of G in the expression for x.

Let $z \in$ Comm $R(G,R)$. The elements of G form a linearly independent set over R. Thus if $\theta(z) \neq 0$, $1 = gh$ for some $g,h \in G$. But then $hg = 1$ and so $gh - hg = 0$. This clearly leads to a contradiction, and we have the result that if $z \in$ Comm $R(G,R)$ then $\theta(z) = 0$.

<u>Lemma 5.2.</u> If $x = \lambda_1 1 + \lambda_2 g_2 + \dots + \lambda_n g_n \in A(G,K)$, where K is a field of characteristic $p (\neq 0)$ and no g_i is a p-element, and x is nilpotent, then

$$\theta(x) = \lambda_1 = 0.$$

<u>Proof:</u> If $x^m = 0$, choose a positive integer k such that $p^k \geq m$. Then $x^{p^k} = 0$.

Using Lemma 5.1,

$$0 = x^{p^k} = \lambda_1^{p^k} 1 + \lambda_2^{p^k} g_2^{p^k} + \dots + \lambda_n^{p^k} g_n^{p^k} + py + z,$$

Where $y \in A(G,K)$ and $z \in$ Comm $A(G,K)$, $py = 0$ since the characteristic of K is p.

No g_i is a p-element and so $g_i^{p^k} \neq 1 \quad (2 \leq i \leq n)$

Thus $\theta(x^{p^k}) = 0$

i.e. $\lambda_1^{p^k} + \theta(z) = 0$.

By the remarks preceding this lemma, $\theta(z) = 0$ and so

$$\lambda_1 = 0 \qquad (\lambda_1 \in K, \text{ a field}).$$

$$\text{i.e. } \theta(x) = 0.$$

<u>Theorem 5.1.</u> If K is a field of characteristic $p (\neq 0)$ and G is a group with no p-elements, then

$$U(G,K) = (0).$$

Proof/

Proof: Consider any $x \in U(G,K)$, $U(G,K)$ is a nil ideal. Then for any element $g \in G \subseteq A(G,K)$,

$$xg^{-1} \in U(G,K), \text{ and so is nilpotent.}$$

By Lemma 5.2,

$$\theta(xg^{-1}) = \text{coefficient of } g \text{ in } x$$
$$= 0.$$

It follows that $x = 0$ and

$$U(G,K) = (0).$$

Before going on to prove the corresponding result for a field of characteristic zero, we make a few remarks on algebraic number theory (10). Let K be a finite field extension of Q, the field of rational numbers. An algebraic integer in K is an element of K which is a zero of a monic polynomial with coefficients in Z, the ring of integers.

Let D be the set of all algebraic integers in K. Then D is a subring of K and so is an integral domain. Further K is the quotient field of D.

Since K is a finite extension of Q of dimension (K:Q), D is a finitely generated Z-module and (D:Z) = (K:Q). Further, any Z-basis for D is also a Q-basis for K.

i.e. if $\{u_1,\dots,u_t\}$ is a basis for D as a Z-module, then
i.e. if $\{u_1,\dots,u_t\}$ is a basis for D as a Z-module, then $K = Qu_1 \oplus \dots \oplus Qu_t$. Let $\lambda \in K$.

$$\lambda u_i = \sum_{j=1}^{t} \rho_{ij}(\lambda) u_j \qquad (1 \leq i \leq t,\ \rho_{ij}(\lambda) \in Q)$$

We/

We denote by $R(\lambda)$, the $t \times t$ matrix $[\rho_{ij}(\lambda)]$ with coefficients in Q. Then the norm of λ, denoted $N(\lambda)$, is $\det R(\lambda)$.

In particular, if $\lambda \in D$, $N(\lambda) \in Z$. $N(\lambda)$ is independent of the choice of the basis $\{u_1,\dots,u_t\}$ for any $\lambda \in K$.

For any $\alpha, \beta \in K$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

For $\alpha \in K$, $q \in Q$, $N(q\alpha) = q^t N(\alpha)$.

We use these results from the theory of algebraic numbers in Lemma 5.

If K is a finite field extension of Q and G is any group, then

$$U(G,K) = (0)$$

(Note that K is necessarily of characteristic zero).

Proof: D is, as above, the set of all algebraic integers in K.

Suppose that

$$x = d_1 1 + d_2 g_2 + \dots + d_n g_n \in U(G,K)$$

and that $d_1 \neq 0$. $(d_1,\dots,d_n \in D)$. Such an element belonging to $U(G,K)$ may be found since K is the quotient field of D.

If $z = \lambda_1 1 + \lambda_2 g_2 + \dots + \lambda_n g_n \in U(G,K)$ where $\lambda_1,\dots,\lambda_n \in K$, for each λ_i, there exists $m_i \in Z$ such that $m_i\lambda_i \in D$ for $1 \leq i \leq n$.
Let $m = m_1 m_2 \dots m_n$. Then $mz \in R(G,D)$. If $z \neq 0$, then $\lambda_i \neq 0$ for som

$$g_i^{-1}z = \lambda_1 g_i^{-1} + \lambda_2 g_i^{-1} g_2 + \dots + \lambda_i 1 + \dots + \lambda_n g_i^{-1} g_n$$

and the coeficient of 1 in $g_i^{-1}z$ is non-zero.

Hence $mg_i^{-1}z$ is of the same form as x and since $U(G,K)$ is an ideal, $x \in U(G,K)$.

We choose a prime p satisfying the conditions:

(i) $p > |N(d_1)|$

(ii) $p >$ the order of every g_i with finite order,

then/

then $g_i^p \neq 1$ $(1 < i \leq n)$

(iii) $p >$ the degree of nilpotence of x.

Then by Lemma 5.1,

$$0 = x^p = d_1^p 1 + d_2^p g_2^p + .. + d_n^p g_n^p + py + z$$

where $y \in R(G,D)$ and $z \in$ Comm $R(G,D)$. By earlier remarks, $\theta(z) = 0$.

$\theta(x^p) = 0$ since $x^p = 0$.

i.e. $d_1^p + \theta(py) = 0$.

and hence $d_1^p = -p\ \theta(y) = pd$ for some $d \in D$.

$N(d_1^p) = N(d_1)^p$ and $N(pd) = p^t N(d)$.

$N(d_1), N(d) \in Z$ since $d_1, d \in D$. $N(d_1^p) = p^t N(d) \Rightarrow p \mid N(d_1)$.

But $p > |N(d_1)|$. Thus we have a contradiction and so $x = 0$.

For any $z \in U(G,K)$, there is an $x \in U(G,K)$ and $x = mg_1^{-1}z \in R(G,D)$.

Now $x = 0$ and it is clear that $z = 0$.

Therefore $U(G,K) = (0)$.

<u>Theorem 5.2.</u> For any field, K of characteristic zero and any group, G,

$$U(G,K) = (0).$$

<u>Proof:</u> K can be regarded as an extension field of Q.

Let $x = \lambda_1 g_1 + .. + \lambda_n g_n \in U(G,K)$.

$(\lambda_i \in K,\ g_i \in G, \quad 1 \leq i \leq n)$.

Let R be the ring $Q[\lambda_1, ..., \lambda_n]$. If $\lambda_1, ..., \lambda_i$ are algebraic over Q and $\lambda_{i+1}, ..., \lambda_n$ are transcendental over Q $(0 \leq i \leq n)$ then $Q[\lambda_1, ..., \lambda_i]$ is a finite algebraic extension of Q and is the maximal subfield of R.

Let $x \in U(G,R)$ and let M be any maximal ideal of R. The natural mapping/

mapping $R(G,R) \rightarrow A(G, R/M)$ maps x onto an element of $U(G, R/M)$. R/M is a field and so R/M is isomorphic to some subfield of R i.e. to some subfield of $Q[\lambda_1, \ldots, \lambda_i]$. Thus R/M is a finite algebraic extension of By Lemma 5.3, $U(G, R/M) = (0)$ and so the image of x under the natural mapping $R(G,R) \rightarrow A(G, R/M)$ is 0. Hence $\lambda_1, \ldots, \lambda_n \in M$, M any maximal ideal of R.

But $J(R) = \bigcap \{ M : M$ a maximal ideal of $R \}$ since R is commutative and has an identity. So $\lambda_1, \ldots, \lambda_r \in J(R)$.
R is a finitely generated commutative algebra over Q. i.e. R is a finitely generated algebra which satisfies an identity and so $J(R)$ is a nil ideal by Theorem 3.3.

Therefore, for every integer i, $1 \leq i \leq n$ there exists a positive integer m_i such that

$$\lambda_i^{m_i} = 0.$$

but $\lambda_i \in R \subseteq K$, a field.

Hence $\lambda_i = 0 \quad (1 \leq i \leq n)$

Then $x = 0$ and $U(G,K) = (0)$.

Maschke's Theorem (§ 2) shows that if G is a finite group of order divisible by p and K is a field of characteristic p, then $U(G,K) \neq (0)$. $U(G,K)$ need not be the zero ideal when K has characteristic p and G has p-elements, even when G is an infinite group, as can be seen from this example:

$G = H \times C$, the direct product of $H = \{1, g\}$, the group of order 2, and C, the infinite cyclic group generated by x. If we consider the group/

group algebra of G over a field K of characteristic 2,

$$(1 - g)^2 = 1 - g^2 = 0$$

and $1 - g$ generates a nilpotent ideal of $A(G,K)$, which is non-zero.

As yet, necessary and sufficient conditions for the existence of non-zero nil ideals have not been found, but in the paper (16) at present under discussion, Passman has established necessary and sufficient conditions for the existence of non-zero nilpotent ideals in group algebras. By Theorem 5.2, it is clear that only the case in which the characteristic of the field is non-zero need be considered.

We shall see that the theorem predicts that the particular group algebra considered above will have a non-zero nilpotent ideal.

The result follows only after proving several preliminary lemmas.

Lemma 5.4. Let J be a group and $H_1,\ldots,H_n$ a finite number of subgroups of J. Suppose that there exists a finite set of elements g_{ij} of $J(j = 1,\ldots,n;\ i = 1,2,\ldots,f(j))$ with

$$J = \bigcup_{i,j} H_j g_{ij} \quad - (i)$$

then for some index j, $[J:H_j] < \infty$.

Proof: Without loss of generality, the n subgroups may be assumed distinct. If $n = 1$, the result is obvious. We prove the result by induction, assuming it to be true for m distinct subgroups H_j, where $m < n$.

If a full set of cosets of H_n appears in the expression for J as a union of cosets, then clearly $[J:H_n] < \infty$, since the total number of cosets involved in the expression (i) is finite.

To complete the proof, we must consider the case in which the coset $H_n g$ of H_n does not occur in (i)

Now/

Now $H_n g \subseteq J = \bigcup_{i,j} H_j g_{ij}$.

But $H_n g \cap H_n g_{in} = \emptyset \quad (1 \leq i \leq f(n))$ so that $H_n g \subseteq \bigcup_{j \neq n, i} H_j g_{ij}$

Further

$$H_n g_{in} = (H_n g) g^{-1} g_{in}$$

and so $H_n g_{in}$ is also contained in a finite union of cosets of the remaining n − 1 subgroups. Thus we have obtained an expression for J as a union of cosets of less than n subgroups and by the induction assumption, the result follows.

Before proceeding to the next lemma, several definitions must be made. (i) for any group G, let

$$G_0 = \{ g \in G : g \text{ has only a finite number of conjugates in } G \}.$$

$$= \{ g \in G : [G : C(g)] < \infty \},$$

Where $C(g)$ is the centraliser of g in G. G_0 is a subgroup of G, since if $g_1, g_2 \in G_0$, then for every $h \in G$,

$$h^{-1}(g_1 g_2^{-1})h = (h^{-1} g_1 h)(h^{-1} g_2^{-1} h)$$

$$= (h^{-1} g_1 h)(h^{-1} g_2 h)^{-1}$$

and there is only a finite number of elements of G of the forms

$$h^{-1} g_1 h, \quad h^{-1} g_2 h \qquad (g_1, g_2 \in G_0, h \in G).$$

(ii) Let ψ be a mapping from $A(G,K)$ to $A(G_0,K)$, defined thus:

$$\text{if } x = \sum_{g \in G} \lambda(g) g \in A(G,K)$$

$$\text{then } \psi(x) = \sum_{g \in G_0} \lambda(g) g \in A(G_0,K).$$

(iii)/

(iii) For any element $x = \sum_{g \in G} \lambda(g)g \in A(G,K)$, let the support of x be the subset of G,

$$\text{Supp } x = \{ g \in G : \lambda(g) \neq 0 \}.$$

Lemma 5.5. Let $x \in A(G,K)$ such that for every $g \in G$, $\psi(g^{-1}xgx) = 0$. Then if we denote $\psi(x)$ by x_0,

$$x_0^2 = 0.$$

Proof: We may express x uniquely in the form $x = x_0 + y$ where $\psi(y) = 0$

For every element $g \in \text{Supp } x_0$,

$$[G:C(g)] < \infty .$$

Let $J = \bigcap_{g \in \text{Supp } x_0} C(g)$, then $[G:J] < \infty$

For every element h of J,

$$h^{-1}x_0h = x_0.$$

Suppose that

$$y = \lambda_1 h_1 + \dots + \lambda_n h_n (\lambda_i \in K, h_i \notin G_0)$$

and let $H_i = J \cap C(h_i) (i = 1,2,\dots,n)$. We assume $x_0^2 \neq 0$ and try to obtain a contradiction arising from this assumption.

There exists a non-zero element $z \in \text{Supp}(x_0^2)$.

Take any $g \in J$. Then

$$g^{-1}xgx = (x_0 + g^{-1}yg)(x_0 + y)$$

$$= x_0^2 + g^{-1}ygx_0 + x_0y + g^{-1}ygy$$

$$\psi(g^{-1}xgx) = 0.$$

Hence there must be a term in z in one of the last three summands to cancel the term in z in x_0^2.

$$\text{Supp}(g^{-1}ygx_0) \cap G_0 = \text{Supp}(x_0y) \cap G_0 = \emptyset$$

since $\psi(y) = 0$.

$z \in G_0$ and therefore $z \in \mathrm{Supp}(g^{-1}ygy)$.

i.e. there exist h_i, h_j such that $g^{-1}h_i g h_j = z$, $(1 \leq i, j \leq n)$

and $g^{-1}h_i g = zh_j^{-1}$. $, g \in J$.

Then $g_{ij}^{-1} h_i g_{ij} = zh_j^{-1}$, some $g_{ij} \in J$ and $g \in H_i g_{ij}$.

But g was any element of J, so that $J = \bigcup_{i,j} H_i g_{ij}$.

By Lemma 5.4, for some i, $[J:H_i] < \infty$. But $H_i \subseteq C(h_i)$ by definition so that $[G:C(h_i)] < \infty$.

This implies that $h_i \in G_0$, a contradiction.

Hence $x_0^2 = 0$.

<u>Lemma 5.6.</u> Let $S = \{g_1, \ldots, g_n\}$ be a finite normal subset of the group G. If H is the subgroup generated by S, then H is normal in G and for every $h \in H$,

$$h = g_1^{m_1} g_2^{m_2} \ldots g_n^{m_n} \quad (m_i \in Z).$$

If each g_i is of finite order, so is H.

<u>Proof:</u> It is clear that H is a normal subgroup of G, since S is normal in G.

Any element of H is of the form

$$h = g_{i_1}^{\pm 1} g_{i_2}^{\pm 1} \ldots g_{i_t}^{\pm 1} \quad (g_{i_j} \in S)$$

We prove the result by induction on t. The theorem is obviously true for $t = 1$, and we assume it true for a "word" of "length" s, where $s < t$.

Let j be the smallest subscript occurring in the representation of h.

Then/

$$\text{Then } h = h_1 g_j^{\pm 1}(g_j^{\mp 1} h_1 g_j^{\pm 1})h_2$$

$$= g_j^{\pm 1} h_2 .$$

Since S is normal, h_2 is a word of the same form as h but involving one less element of S.

By the induction assumption,

$$h_2 = g_k^{m_k} g_{k+1}^{m_{k+1}} \ldots g_n^{m_n} \quad (m_i \in Z),$$

omitting all the terms with zero exponent occurring before the first term with non-zero component.

If $j \leq k$, we have an expression for h of the required form. Otherwise, in this representation, there is an element of subscript less than j . We apply the process again. Since there is only a finite number of elements in S, after a finite number of applications, a representation of h of the required form will be obtained.

Since each $h \in H$ can be expressed in the form

$$h = g_1^{m_1} g_2^{m_2} \ldots g_n^{m_n},$$

if each element of S is of finite order, then it is clear that H is of finite order.

Theorem 5.3. If K is a field of characteristic $p \neq 0$, then A(G,K) has a non-trivial nilpotent ideal if and only if G contains a finite normal subgroup H whose order is divisible by p.

Note that this theorem gives conditions on K,G under which it is impossible for the lower nil radical to be zero and so these are also sufficient conditions for a non-zero upper nil or Jacobson radical.

Proof/

Proof (i) Sufficiency Suppose that H is a finite normal subgroup

<u>Proof (i) Sufficiency</u> Suppose that H is a finite normal subgroup of G of G and that $p \,\big|\, |H|$ where p is the characteristic of K.

$$\text{Let } H = \{h_1, \ldots, h_n\}, \qquad n = |H|.$$

For any $\lambda \in K$, $\lambda \neq 0$, let

$$x = \sum_{i=1}^{n} \lambda h_i = \lambda \sum_{i=1}^{n} h_i \in A(G,K).$$

Then
$$x^2 = \lambda^2 \Big(\sum_{i=1}^{n} h_i\Big)\Big(\sum_{j=1}^{n} h_j\Big)$$

$$= \lambda^2 n \Big(\sum_{i=1}^{n} h_i\Big)$$

$$= 0 \text{ since } p \mid n.$$

Also for any element $g \in G$,

$$gxg^{-1} = g\Big(\sum_{i=1}^{n} \lambda h_i\Big) g^{-1}$$

$$= \lambda \sum_{i=1}^{n} g h_i g^{-1}$$

$$= \lambda \sum_{i=1}^{n} h_i \quad \text{since H is a finite normal subgroup}$$

$$= x.$$

Then $gx = xg$ for all $g \in G$. It follows that x commutes with every element of $A(G,K)$ and is nilpotent so that x generates a non-trivial nilpotent ideal in $A(G,K)$.

(ii) <u>Necessity.</u> Suppose that N is a non-trivial nilpotent ideal in $A(G,K)$. Then there exists a positive integer m such that

$$N^m \neq (0) \quad \text{and } N^{m+1} = (0).$$

Choose/

Choose $x \in N^m$ with $\theta(x) \neq 0$. Then for every $g \in G$,

$$gxg^{-1} \in N^m, \text{ an ideal,}$$

and $gxg^{-1}x \in N^{m+1} = (0)$.

$$\text{i.e. } gxg^{-1}x = 0.$$

x satisfies the conditions of Lemma 5.5 so that $x_0^2 = 0$, where $x_0 = \psi(x)$

i.e. x_0 is nilpotent.

$1 \in G_0$ therefore $\theta(x_0) = \theta(x) \neq 0$. By Lemma 5.2, there must be a p-element in Supp x_0. Let this p-element be h_1. Supp $x_0 \subseteq G_0$. Thus $h_1 \in G_0$ and $S = \{h_1, \ldots, h_t\}$, the set of all conjugates of h_1, is finite and is a normal subset of G. Lemma 5.6 now states that the subgroup H generated by S is a normal subgroup of G. Each element of S has finite order and so H also has finite order. h_1 is a p-element and $h_1 \in H$.

Hence $p \,\|\, |H|$, as required.

---

§ 6 The Jacobson Radical

The results proved for the upper nil radical of the group algebra cover a wide range of groups and fields. The only case which is uncertain is that in which the characteristic of the field is a non-zero prime p and there are p-elements in the group. This problem is solved to some extent by Theorem 5.3. The significant fact is that there is no restriction on the field apart from characteristic as mentioned above.

However, in considering the Jacobson radical of a group algebra, we find that in order to have semi-simplicity, additional restrictions must/

must be placed on either the group or the field.

For fields of characteristic zero, we have a result proved by Amitsur (6)

Theorem 6.1. If K is a field of characteristic zero and is a non-algebrai extension of Q, then $J(G,K) = (0)$ for any group G.

Proof: $K \supseteq F$, where F is a pure transcendental extension of Q, and K is an algebraic extension of F. (by remarks on the theory of fields in § 4). In fact since K has characteristic zero, K is a separable extension of F.

By Theorem 4.2,

$$J(G,F) = N \otimes_Q F$$

where N is a nil ideal of $A(G,Q)$.

By Theorem 5.2, $U(G,Q) = (0)$ i.e. $A(G,Q)$ has no non-zero nil ideals and so $N = (0)$.

It follows that $J(G,F) = (0)$.

By Theorem 4.1,

$$J(G,K) = J(G,F) \otimes_F K = (0).$$

In particular, if K is a non-denumerable field of characteristic zero, $J(G,K) = (0)$. This theorem includes Rickart's results in (17) in which K was the field of real or complex numbers.

We now return to the case in which the characteristic of the field is non-zero. Passman (16) has proved the following two theorems:

Theorem 6.2. If K is a field of characteristic $p \neq 0$ and is a separably generated, non-algebraic extension of some subfield K_0, then $J(G,K) = (0)$ for any group G, with no p-elements.

Proof/

Proof: There is a field $K_1 \subseteq K$ such that K_1 is a pure transcendental extension of K_0 (not necessarily of finite transcendence degree) and K is a separable algebraic extension of K_1 (§4).

By Theorem 4.2,

$$J(G,K_1) = N \otimes_{K_0} K_1$$

where $N \subseteq U(G,K_0)$. But by Theorem 5.1, $U(G,K_0) = (0)$ and so

$$J(G,K_1) = (0).$$

By Theorem 4.1,

$$J(G,K) = J(G,K_1) \otimes_{K_1} K$$

and it follows that $J(G,K) = (0)$.

Lemma 6.1. If H is a subgroup of a group G, then

$$A(H,K) \cap J(G,K) \subseteq J(H,K)$$

for any field K.

Proof: Let $x \in A(H,K) \cap J(G,K)$. There exists $y \in A(G,K)$ such that

$$x + y + xy = 0.$$

Let $y = h + k$ where $h \in A(H,K)$ and k involves no elements of H.

Then $x + h + k + xh + xk = 0$,

i.e. $(x + h + xh) + (k + xk) = 0$.

$x + h + xh \in A(H,K)$ and $k + xk$ involves no elements of H.

Hence $x + h + xh = 0$ (and $k + xk = 0$) and so $x \in J(H,K)$.

We now have

Theorem 6.3.(16). If K is a non-denumerable field of characteristic $p > 0$ and G is a group having no p-elements then

$$J(G,K) = (0).$$

Proof/

Proof: Let $x = \sum_{g \in G} \lambda(g)g \in J(G,K)$

If H is the subgroup generated by Supp x, then H is finitely generated and $x \in J(H,K)$ by Lemma 6.1.

Now A(H,K) is a finitely generated algebra over a non-denumerable field and by Theorem 3.2,

$$J(H,K) = U(H,K)$$

and so $x \in U(H,K)$.

By Theorem 5.1, U(H,K) = (0) which implies that x = 0 and that

$$J(G,K) = (0).$$

So far we have found conditions on the field K which are sufficient to make A(G,K) semi-simple for any group G, with the usual restriction on the order of the group elements in relation to the characteristic of the field.

In keeping the field arbitrary and looking for sufficient conditions on the group, the following theorem will be of use.

Theorem 6.4. If J(H,K) = (0) for every finitely generated subgroup H of G, then J(G,K) = (0).

Proof: By Lemma 6.1, if $x \in J(G,K)$ and H is the subgroup generated by Supp x, then $x \in J(H,K)$.

Now H is a finitely generated subgroup of G and so J(H,K) = (0)

Hence x = 0 and so J(G,K) = (0).

Corollary 6.5. If G is a locally finite group, then J(G,K) = (0) for any field K, where if the characteristic of K is $p \neq 0$, then G has no p-elements.

Proof/

Proof: Since G is a locally finite group, any finitely generated subgroup of G is of finite order. The result follows immediately from Maschke's Theorem and Theorem 6.4.

Corollary 6.6. If G is a commutative group, then $J(G,K) = (0)$ for any field K, where if the characteristic of K is $p \neq 0$, then there are no p-elements in G.

Proof: Let H be any finitely generated subgroup of G. Then H is commutative and the group algebra $A(H,K)$ is a finitely generated algebra, satisfying the identity, $F(X,Y) \equiv XY - YX = 0$.

By Theorem 3.3,

$$J(H,K) = U(H,K).$$

But by Theorem 5.2,

$$U(H,K) = (0) \text{ and so } J(H,K) = (0).$$

Now $A(G,K)$ satisfies the conditions of Theorem 6.4 and we may deduce that $J(G,K) = (0)$.

This result is proved by Amitsur (characteristic of K = 0) in (6) and by Connell in (9) using different proofs from this. Connell actually deals with the more general case of the group ring over a commutative ring. We may prove easily that the group algebra of an ordered group is semi-simple.

An ordered group G is one in which there is a binary relationship, $<$ with properties:

(i) $a \nless a$ for any $a \in G$.

(ii) $a > b,\ b > c \Rightarrow a > c \quad (a, b, c \in G)$.

(iii) If $a \nless b$ and $a \ngtr b$, then $b > a$.

(iv) $a > b \Rightarrow ca > cb$ and $ac > bc \quad (a, b, c \in G)$.

Theorem/

Theorem 6.7.(9) If G is an ordered group, then $J(G,K) = (0)$ for any field K.

Proof: Consider the following two elements of $A(G,K)$.

$$a = \lambda_1 g_1 + \dots + \lambda_m g_m, \ \lambda_i \in K, \ \lambda_i \neq 0$$

$$\text{and } g_1 < g_2 < \dots < g_m \ (g_i \in G)$$

$$a' = \mu_1 h_1 + \dots + \mu_n h_n, \ \mu_j \in K, \ \mu_j \neq 0$$

$$\text{and } h_1 < h_2 < \dots < h_n \ (h_j \in G).$$

Then $aa' = \lambda_1 \mu_1 g_1 h_1 + \dots + \lambda_m \mu_n g_m h_n$

$$\lambda_1 \mu_1 \neq 0, \quad \lambda_m \mu_n \neq 0 \ (K \text{ a field})$$

and $g_1 h_1 < \dots < g_m h_n$.

Thus $aa' = 1 \Rightarrow m = n = 1$.

Since $a \in J(G,K)$, $1 + ag$ has an inverse for all $g \in G$.

By the above discussion, $1 + ag$ must involve only one element of G. There are $g \in G$, $g \neq 1$ and so $a = 0$ which implies that $J(G,K) = (0)$.

Before proving the final theorem, we prove

Lemma 6.2. If G_0 is the infinite cyclic group and A is a ring such that $U(A) = (0)$, then $J(G_0,A) = (0)$.

Proof: Let G_0 be generated by g. Then any element of $R(G_0,A)$ is of the form $x = \sum_{i=-\infty}^{\infty} a_i g^i$ with only a finite number of the a's non-zero. $(a_i \in A)$. If the highest power of g in x having non-zero coefficient is g^n, then n is the degree of x. The element of least degree of a non-zero ideal I of $R(G_0,A)$ is the element of the form

$$\sum_{i=0}^{m} a_i g^i \text{ with } a_0, a_m \neq 0,$$

of least degree.

We prove first that if $x = \sum_{i=0}^{m} a_i g^i$ is an element of least degree in the non-zero ideal I of $R(G_0,A)$ and $y \in R(G_0,A)$ is such that

$$a_m^k\, y = 0 \text{ for some } k \geq 1,$$

then $a_m^{k-1} xy = 0$.

Suppose that $y = \sum_{i=-\infty}^{\infty} b_i g^i \quad (b_i \in A)$.

Then $a_m^k\, y = 0 \Leftrightarrow a_m^k\, b_i = 0$ for all i.

Thus it is sufficient to prove the result for $y = b \in A$. Suppose that $a_m^k\, b = 0$. $a_m^{k-1} xb$ has $a_m^k b$ as coefficient of g^m and so the degree of $a_m^{k-1} xb$ is less than m. Thus we have an element of the same form as x but of lower degree (not necessarily $a_m^{k-1} xb$). By the definition of x,

$$a_m^{k-1} xb = 0.$$

We are now able to proceed with the proof of the lemma. We assume $J(G_0,A) \neq (0)$. and let M be the set of elements of $J(G_0,A)$ of least degree. The "leading coefficients" of all elements of M, together with 0, form an ideal N of A. We will show that N is nil.

Let $x = a_0 + a_1 g + \dots + a_m g^m \in M$.

Then $xga_m \in J(G_0,A)$ and so is quasiregular. Hence there is an element $z \in R(G_0,A)$ such that

$$xga_m + z + xga_m z = 0$$

$$\text{and } xga_m + z + zxga_m = 0$$

$$\text{i.e. } xa_m + zg^{-1} + xa_m z = 0 \qquad \text{--- (i)}$$

$$\text{and } xa_m + zg^{-1} + zxa_m = 0 \qquad \text{--- (ii)}$$

We denote zg^{-1} by t and assume that $a_m^k\, t \neq 0$ for $k = 1,2,\dots$. We choose/

choose the element of the set $\{a_m^k t : k = 1,2,\ldots\}$ of lowest degree. Let the degree be n. Then $t = t_1 + g^{n+1} t_2$ where t_1 has degree n.

i.e. $t_1 = \sum_{i=-\infty}^{n} b_i g^i$ where $b_n \neq 0$. By the definition of n, for k sufficiently large $a_m^k g^{n+1} t_2 = 0$ but $a_m^k t_1 \neq 0$. Then $a_m^k t_2 = 0$. $a_m^k b_n \neq 0$ for any positive integer k.

By the remarks at the beginning of the lemma we may now deduce that

$$a_m^{\ell} t_2 = 0 = a_m^{\ell} x a_m t_2 \text{ for } \ell \text{ sufficiently large.}$$

We multiply (i) on the left by a_m^{ℓ}.

$$a_m^{\ell} x a_m + a_m^{\ell}(t_1 + g^{n+1} t_2) + a_m^{\ell} x a_m (t_1 + g^{n+1} t_2) g = 0$$

Hence $a_m^{\ell} x a_m + a_m^{\ell} t_1 + a_m^{\ell} x a_m t_1 g = 0$.

The coefficient of g^{m+n+1} on the left hand side of this expression is $a_m^{\ell+2} b_n$. Hence $a_m^{\ell+2} b_n = 0$, a contradiction. So $a_m^k t = 0$ for some k.

We multiply (ii) on the left by a_m^k.

i.e. $a_m^k x a_m + a_m^k t + a_m^k t g x a_m = 0$

i.e. $a_m^k x a_m = 0$.

Hence $a_m^{k+2} = 0$ and so N is a non-zero nil ideal.

(The proof of this lemma is adapted from the proof of the corresponding result for the polynomial ring A[X] in one indeterminate over the ring A, as given by Jacobson in (13)).

Theorem 6.8 (9) allows us to construct other groups having semi-simple group algebras using Theorem 6.6 and Corollaries 6.5, 6.7. $\mathcal{C}$ is as defined in § 1.

Theorem/

<u>Theorem 6.8.</u> (i) If $G, H \in \mathcal{C}$ then $G \times H \in \mathcal{C}$.

(ii) If G is arbitrary and G_0 is the infinite cyclic group, then $G \times G_0 \in \mathcal{C}$

<u>Proof</u> (i) Let K be a field of characteristic p. There are no p-elements in $G \times H$ which implies that there are no p-elements in either G or H.

We form $A(G,K) \otimes_K A(H,K)$. This is a ring in which both factors are free K-modules. Hence each element of the tensor product has a unique representation of the form

$$\sum \lambda (g \otimes h) \quad (\lambda \in K,\ g \in G,\ h \in H)$$

The mapping $\sum \lambda (g \otimes h) \rightarrow \sum \lambda\, gh$ maps $A(G,K) \otimes_K A(H,K)$ onto $A(G \times H,K)$ and is an isomorphism.

$A(G,K)$ is separable i.e. for every extension field F of K, $A(G,K) \otimes_K F$ is semi-simple, since $G \in \mathcal{C}$.

Also, since $H \in \mathcal{C}$, $A(H,K)$ is semi-simple and by Bourbaki (8, p.93, Cor.4),

$$J\left[A(G,K) \otimes_K A(H,K)\right] = (0)$$

i.e. $J(G \times H,K) = (0)$.

i.e. $G \times H \in \mathcal{C}$

(ii) If K is a field of characteristic p, then G has no p-elements. Then by Theorems 5.1, 5.2 for $p = 0$ and $p \neq 0$

$$U(G,K) = (0).$$

Now $A(G \times G_0,K) \cong A(G_0,A(G,K))$. By Lemma 6.2, since $U(G,K) = (0)$, $A(G_0,A(G,K))$ is semi-simple. Hence $A(G \times G_0,K)$ is semi-simple.

and $G \times G_0 \in \mathcal{C}$

(Corollary 6.6 could be deduced from (ii) above).

REFERENCES

1. Amitsur, S.A.: The identities of PI rings.
(Proc. American Math. Soc. 4 (1953) 27-34).

2. ____________: A general theory of radicals II.
(American J. Math. 76 (1954) 100-125).

3. ____________: Algebras over infinite fields.
(Proc. American Math. Soc. 7 (1956) 35-46).

4. ____________: The radical of field extensions.
(Bull. Research Council of Israel, 7F (1957) 1-10).

5. ____________: A Generalisation of Hilbert's Nullstellensatz.
(Proc. American Math. Soc. 8 (1957) 649-656).

6. ____________: On the semi-simplicity of group algebras.
(Michigan Math. J. 6 (1959) 251-254).

7. Baer, R.: Radical ideals.
(American J. Math. 65 (1943) 537-567).

8. Bourbaki, N: Algèbre, Chapitre 8. (Hermann, Paris, 1958).

9. Connell, I. G.: On the group ring.
(Canadian J. Math. 15 (1963) 650-685).

10. Curtis, C.W. and Reiner, I.: Representation Theory of
Finite Groups and Linear Associative Algebras. (Wiley, 1962).

11. Jacobson, N.: Theory of Rings.
(American Math. Soc. 1943).

12. ____________: The radical and semi-simplicity for arbitrary rings
(American J. Math. 67 (1945) 300-319).

13. ______________ : Structure of Rings.

(American Math. Soc. Colloquium Publications XXXVII 1956).

14. ______________ : Lectures in Abstract Algebra Vol III, Theory of Fields, Galois Theory. (Van Nostrand, 1964).

15. Maschke, H. : Uber den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionen gruppen. (Math. Annalen 50(1898) 482-498).

16. Passman, D.S.: Nil ideals in group rings. (Michigan Math. J. 9 (1962) 375-382).

17. Rickart, C. : The uniqueness of norm problem in Banach algebras (Annals of Math. 51 (1950)).

18. van der Waerden, B.L. : Moderne Algebra (Erster Teil) (Springer, 1930).