CHAPTER X
LINEAR ASSOCIATIVE ALGEBRAS

10.01 **Fields and algebras.** A set of elements which are subject to the laws of ordinary rational algebra is called a *field*. We may make this idea more precise as follows. Let \( a, b, \ldots \) be a set of entities, \( F \), which are subject to two operations, addition and multiplication; this set is called a field if it satisfies the following postulates:

1. \( a + b \) is a uniquely determined element of \( F \).
2. \( a + b = b + a \).
3. \( (a + b) + c = a + (b + c) \).
4. There is a unique element 0 in \( F \) such that \( a + 0 = a \) for every element \( a \) in \( F \).
5. For every element \( a \) in \( F \) there exists a unique element \( b \) in \( F \) such that \( a + b = 0 \).

M1. \( ab \) is a unique element of \( F \).
M2. \( ab = ba \).
M3. \( ab \cdot c = a \cdot bc \).
M4. There is a unique element 1 in \( F \) such that \( a1 = a \) for every \( a \) in \( F \).
M5. For every element \( a \neq 0 \) in \( F \) there exists a unique element \( b \) in \( F \) such that \( ab = 1 \).

AM. \( a(b + c) = ab + ac, (b + c)a = ba + ca \).

R. If \( m \) is a whole number and \( ma \) denotes the element which results from adding together \( m \) a’s, then \( ma \neq 0 \) for any \( m > 0 \) provided that \( a \neq 0 \).

If M2 is omitted the resulting set is said to be a *division algebra*. This does not imply that M2 does not hold, only that it is not presupposed; if it does hold, the algebra is said to be commutative. If M2, 4, 5 are all omitted, the corresponding set is called an *associative algebra*. If the algebra contains an identity, that is, an element satisfying the condition laid down in M4 for 1, this element is called the *principal unit* of the algebra. Postulate R is included merely as a matter of convenience; its effect is to exclude modular fields. In consequence of R every field which we shall consider contains the field of rational numbers as a subset.

As an example of a field we may take the field of rational numbers extended by a cube root of unity, \( \omega = (-1 + \sqrt{-3})/2 \). Every number of this field can be put in the form

\[ a = \alpha + \beta \omega = \alpha 1 + \beta \omega \]

1 These postulates are not independent; they are formed so as to show the principal properties of the set. In place of M5 it is often convenient to take: M5' If \( a \neq 0 \), \( ax = 0 \) implies \( x = 0 \).

2 Strictly speaking, we should say that the field contains a subset simply isomorphic with the field \( R \) of rational numbers. This subset is then used in place of \( R \) in the same way as scalars are replaced by scalar matrices in §1.04.
where $\alpha$ and $\beta$ are rational numbers; the form of $a$ is unique since $\alpha + \beta \omega = \gamma + \delta \omega$ gives $(\beta - \delta) \omega = \gamma - \alpha$ and, since $\omega$ is not rational, this is impossible unless $\beta - \delta = 0 = \gamma - \alpha$. We say that $1, \omega$ is a basis of $F$ relative to the field $R$ of rational numbers, and $F$ is said to be a field of order $2$ over $R$.

As an example of an associative algebra we may take the algebra of matrices with rational coordinates. Here any element $a$ of the algebra can be put uniquely in the form $a = \sum a_{ij} e_{ij}$, where the $a_{ij}$ are rational numbers; and $e_{ij}(i, j = 1, 2, \ldots, n)$ form a basis of the algebra, which is of order $n^2$. We also have an algebra if the coordinates $a_{ij}$ are taken to be any elements of the field $F = (1, \omega)$ described above. This algebra is one of order $n^2$ over $F$. Instead of regarding it as an algebra over $F$ we may clearly look on it as an algebra of order $2n^2$ over $R$ the basis being $e_{ij}, \omega e_{ij}$ ($i, j = 1, 2, \ldots, n$).

10.02 Algebras which have a finite basis. Let $A$ be a set of elements which form an associative algebra and $G$ a subset which is also an algebra. We shall say that $a_1, a_2, \ldots, a_n$ form a basis of $A$ relatively to $G$ if (i) each $a_i$ lies in $A$, (ii) if every element of $A$ can be put uniquely in the form

$$a = \gamma_1 a_1 + \gamma_2 a_2 + \cdots + \gamma_n a_n$$

where the $\gamma$'s belong to $G$. Though it is not altogether necessary to do so, we shall restrict ourselves to the case in which $G$ is a field which contains the rational field, that is, we assume as a postulate:

BR. For every algebra $A$ under consideration there exists a non-modular field $F$ and a subset of elements $a_1, a_2, \ldots, a_n$ such that (i) every element of $A$ can be put uniquely in the form

$$a = \sum_{i=1}^{n} \gamma_i a_i$$

$(\gamma_i$ in $F)$

and (ii) every element of this form belongs to $A$; and further the elements of $F$ are commutative with $a_1, a_2, \ldots, a_n$.

Since the product of any two elements of $A$ is also an element of $A$ and can therefore be expressed in the form (1), we have

$$a_i a_j = \sum_k \gamma_{ij} a_k$$

$(i, j = 1, 2, \ldots, n)$

where $\gamma_{ij}$ are elements of $F$. Since the law of combination of the elements of $F$ is supposed known, (2) defines the product of any two elements of $A$; for

$$\sum a_i a_i \sum \beta a_j a_j = \sum \gamma_{ij} a_k.$$
that \( a_i a_j a_k = a_i a_j a_k \) for all the elements of the basis. This gives immediately the ‘associativity’ condition

\[
\sum_a \gamma_{ija} \gamma_{ial} = \sum_a \gamma_{ijl} \gamma_{akl} \quad (i, j, k, l = 1, 2, \ldots, n).
\]

10.03 The matrix representation of an algebra. If we set

\[
A_i = \sum_{p,q=1}^{n} \gamma_{ipq} e_{pq} \quad (i = 1, 2, \ldots, n),
\]

the law of multiplication for matrices gives

\[
A_i A_j = \Sigma \gamma_{ipq} \gamma_{jqr} e_{pq}
\]

and therefore from (4)

\[
A_i A_j = \Sigma \gamma_{ija} \gamma_{ipq} e_{pq} = \Sigma \gamma_{ija} A_i.
\]

Hence the set of matrices of the form \( \Sigma \alpha_i A_i \) is isomorphic with the given algebra in regard to both addition and multiplication. Further, if the algebra contains the identity, the isomorphism is simple; for, if there exist elements \( \alpha_i \) of the field such that \( \Sigma \alpha_i A_i = 0 \), it follows that

\[
(\Sigma \alpha_i a_i) x = 0
\]

for every element \( x \) of the algebra, and putting \( x = 1 \) we get \( \Sigma \alpha_i a_i = 0 \).

If the algebra does not have a principal unit, all that is necessary is to replace (5) by

\[
A_i = \sum_{p,q=1}^{n+1} \gamma_{ipq} e_{pq}
\]

where \( \gamma_{i,j,n+1} = 0 \ (i, j \leq n) \) and \( \gamma_{n+1,i,j} = \delta_{ij} = \gamma_{i,j,n+1} \) for all \( i \) and \( j \).

The importance of this representation is that it enables us to carry over the theory of the characteristic and reduced equations from the theory of matrices. The main theorem is as follows.

**Theorem 1.** The general element \( x = \Sigma \xi_i a_i \) satisfies an equation of the form

\[
\lambda^m + b_1 \lambda^{m-1} + \cdots + b_m = 0
\]

where \( b_p \) is a rational homogeneous polynomial in the \( \xi \)'s of degree \( p \); and if the variable coordinates \( \xi_p \) are given particular values in \( F \), there exists a rational polynomial

\[
\varphi(\lambda) = \lambda^n + \beta_1 \lambda^{n-1} + \cdots + \beta_n
\]

such that (i) \( \varphi(x) = 0 \), (ii) if \( \psi(\lambda) \) is any polynomial with coefficients in \( F \) such that \( \psi(x) = 0 \), then \( \varphi(\lambda) \) is a factor of \( \psi(\lambda) \).
This theorem follows immediately from the theory of the reduced equation as given in §2.05 and from the fact that the equation which is satisfied by the general element must clearly be homogeneous in the coordinates of that element.

As in the theory of matrices, \(-b_1\) is called the trace of \(x\) and is written \(\text{tr}(x)\). The trace is linear and homogeneous in the coordinates and hence \(\text{tr}(x + y) = \text{tr}(x) + \text{tr}(y)\).

10.04 The calculus of complexes. If \(x_1, x_2, \ldots, x_r\) are any elements of an algebra \(A\) in a field \(F\), the set \(B\) of all elements of the form \(\sum \xi_i x_i\) (\(\xi\) in \(F\)) is called a complex\(^3\) or linear set. Any subset \(B\) of \(A\) which has the property that, when \(x, y\) are any two of its elements, then \(\xi x + \eta y\) is also an element of the set is a complex. This follows readily from the theory of linear dependence and the existence of a finite basis for \(A\); it is also easily shown that any subcomplex of \(A\) has a finite basis; the order of this basis is called the order of the complex.

We shall write \(B = (x_1, x_2, \ldots, x_r)\); this does not imply that the \(x_i\)'s are necessarily linearly independent. If \(C = (y_1, y_2, \ldots, y_s)\) is a second complex, the sum of \(B\) and \(C\) is defined by

\[B + C = (x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s),\]

that is, \(B + C\) is the set of all elements of the form \(x + y\) where \(x\) lies in \(B\) and \(y\) in \(C\). Similarly the product is defined by

\[BC = (x_i y_j; i = 1, 2, \ldots, r; j = 1, 2, \ldots, s).\]

The set of elements common to \(B\) and \(C\) forms a complex called the intersection of \(B\) and \(C\); it is denoted by \(B \cap C\). If \(B\) and \(C\) have no common element, we write \(B \cap C = 0\). If every element of \(C\) lies in \(B\) but not every element of \(B\) in \(C\), we shall write \(C < B\); in this case \(B + C = B\). A complex of order 1 is defined by a single element, say \(x_1\), and for most purposes it is convenient to denote the complex \((x_1)\) simply by \(x_1\); \(x_1 < B\) then means that \(x_1\) is an element of \(B\).

If a complex \(B\) is an algebra, the product of any two of its elements lies in \(B\) and hence \(B^2 \subseteq B\); conversely, if this condition is satisfied, the definition of the product \(BB = B^2\) shows that \(B\) is an algebra.

We add a summary of the properties of the symbols introduced in this section.

\[
\begin{align*}
B + C &= C + B, & (B + C) + D &= B + (C + D), & BC \cdot D &= B \cdot CD, \\
B \cap C &= C \cap B, & (B \cap C) \cap D &= B \cap (C \cap D), \\
B(C + D) &= BC + BD, & (C + D)B &= CB + DB, \\
B + (C \cap D) &\leq (B + C) \cap (B + D), & B(C \cap D) &\leq BC \cap BD.
\end{align*}
\]

\(^3\) The term ‘complex,’ which was introduced by Frobenius in the theory of groups, is more convenient than ‘linear set’ and no confusion is likely to arise between this meaning of the term and the one used in geometry.

\(^4\) To avoid circumlocution we say the complexes have ‘no element in common’ in place of the more correct phrase ‘no element in common except 0.’
If $B \leq C$, then $B + C = C$, and conversely.
If $B < C$, there exists $D < C$ such that $C = B + D, B \sim D = 0$.
If $B = C + D$ and $C \sim D = 0$, we shall say that $B$ is congruent to $C$ modulo $D$, or

\[ B = C \pmod{D}; \]

and if $b, c, d$ are elements of $B, C, D$, respectively, such that $b = c + d$, then

\[ b = c \pmod{D}, \quad c = b \pmod{D}. \]

10.05 **The direct sum and product.** If $A = (a_1, a_2, \cdots, a_n)$ and $B = (b_1, b_2, \cdots, b_\beta)$ are associative algebras of orders $\alpha, \beta$, respectively, over the same field $F$, we can define a new algebra in terms of them as follows. Let $C$ be the set of all pairs of elements $(a, b)$ where $a < A$ and $b < B$ and two pairs $(a, b)$, $(a', b')$ are regarded as equal if, and only if, $a = a', b = b'$. If we define addition and multiplication by

\[
(a, b) + (a', b') = (a + a', b + b')
\]

\[
(a, b) (a', b') = (aa', bb')
\]

\[ \xi(a, b) = (\xi a, \xi b) \quad (\xi \text{ in } F), \]

it is readily shown that the set $C$ forms an associative algebra. This algebra is called the **direct sum** of $A$ and $B$ and is denoted by $A \oplus B$; its order is $\alpha + \beta$.

The set $\mathfrak{A}$ of all elements of the form $(a, 0)$ forms an algebra which is simply isomorphic with $A$, and the set $\mathfrak{B}$ of elements $(0, b)$ forms an algebra which is simply isomorphic with $B$; also

\[ C = \mathfrak{A} + \mathfrak{B}, \quad \mathfrak{A} \mathfrak{B} = 0 = \mathfrak{B} \mathfrak{A}, \quad \mathfrak{A} \mathfrak{A} = 0. \]

In consequence of this it is generally convenient to say that $C$ is the direct sum of $\mathfrak{A}$ and $\mathfrak{B}$.

If we replace (9) by

\[
\xi(a, b) = (\xi a, b) = (a, \xi b) \quad (\xi \text{ in } F)
\]

\[ (a, b) (a', b') = (aa', bb'), \]

we get another type of algebra of order $\alpha \beta$ which is called the **direct product** of $A$ and $B$ and is denoted by $A \otimes B$ or by $A \times B$ when there is no chance of confusion. If both $A$ and $B$ contain the identity, the set $\mathfrak{A}$ of elements of the form $(a, 1)$ forms an algebra simply isomorphic with $A$ and the set $\mathfrak{B}$ of elements $(1, b)$ is an algebra simply isomorphic with $B$; also

\[ C = \mathfrak{A} \mathfrak{B} = \mathfrak{B} \mathfrak{A}, \quad \mathfrak{A} \mathfrak{B} = (1, 1) = 1, \]

and the order of $C$ is the product of the orders of $\mathfrak{A}$ and $\mathfrak{B}$. As in the case of the direct sum it is convenient to say that $A$ is the direct product of $\mathfrak{A}$ and $\mathfrak{B}$ and to indicate this by writing $C = \mathfrak{A} \times \mathfrak{B}$.

\* Strictly speaking we should use different symbols here for the identity elements of the separate algebras.
The following theorem gives an instance of the direct product which we shall require later.

**Theorem 2.** If an algebra $A$, which contains the identity, contains also the matrix algebra $M \langle e_{ij}; i, j = 1, 2, \ldots, n \rangle$, the identity being the same for $A$ and $M$, then $A$ can be expressed as the direct product of $M$ and another algebra $B$.

Let $B$ be the set of elements of $A$ which are commutative with every element of $M$; these elements form an algebra since, if $b_i e_{pq} = e_{pq} b_i (i = 1, 2, \ldots)$, then also

$$(b_i + b_j) e_{pq} = e_{pq} (b_i + b_j), \quad b_i b_j e_{pq} = e_{pq} b_i b_j.$$ Further $B \sim M$ is the field $F$, since scalars are the only elements of $M$ which are commutative with every element of $M$.

If $x$ is any element of $A$ and

$$x_{pq} = \sum_i e_{ip} x e_{qi},$$

then

$$x_{pq} e_{rs} = \sum_i e_{ip} x e_{qi} e_{rs} = e_{rp} x e_{qs} = e_{rs} \sum_i e_{ip} x e_{qi} = e_{rs} x_{pq},$$

so that $x_{pq}$ belongs to $B$. Also

$$\sum_{pq} x_{pq} e_{pq} = \sum_{pq} e_{ip} x e_{qi} e_{pq} = \sum_{pq} e_{pp} x e_{qq} = x,$$

so that $A = BM$, which proves the theorem.

**10.06 Invariant subalgebras.** If $B$ is a subalgebra of $A$ such that

$$(10) \quad AB \leq B, \quad BA \leq B,$$

then $B$ is called an invariant subalgebra of $A$. If we set

$$A = B + C, \quad B \sim C = 0,$$

the product of any two elements $c_i, c_j$ of $C$ lies in $A$ and hence

$$c_i c_j = c_{ij} + b_{ij}, \quad c_{ij} < C, \quad b_{ij} < B.$$

If we now introduce a new operation $\times$ defined by

$$(11) \quad c_i \times c_j = c_{ij},$$

then the operations $+$ and $\times$, when used to combine elements of $C$, satisfy all the postulates for an associative algebra. To prove this we need only consider the associativity postulate M3 since the proofs of the others are immediate. If $c_1, c_2, c_3$ are any elements of $C$, then both $c_1 \times (c_2 \times c_3)$ and $(c_1 \times c_2) \times c_3$ differ by an element of $B$ from $c_1 c_2 c_3$; their difference is therefore an element of both $B$ and $C$ and hence is 0.

The elements of $C$ therefore form an associative algebra relatively to the
operations $+$ and $\times$. When this algebra is considered abstractly, the operation $\times$ may be called multiplication; the resulting algebra is called the difference algebra of $A$ and $B$ and is denoted by $(A - B)$.

The difference algebra may also be defined as follows. Let $b_1, b_2, \cdots, b_9$ be a basis of $B$ and $c_1, c_2, \cdots, c_7$ a basis of $C$, so that $b_1, b_2, \cdots, b_9, c_1, \cdots, c_7$ is a basis of $A$. Since $A$ is an algebra, the product $c_i c_j$ can be expressed in terms of this basis and we may therefore set

$$c_i c_j = \Sigma \gamma_{ij} c_k + \Sigma \delta_{ij} b_k.$$  
(12)

The argument used above then shows that

$$d_i d_j = \Sigma \gamma_{ij} d_k$$  
(13)

defines an associative algebra when $B$ is invariant.

It is readily seen that the form of the difference algebra is independent of the particular complex $C$ which is used to supplement $B$ in $A$. For if $A = B + P$, $B \sim P = 0$, it follows that to an element $p$ of $P$ there corresponds an element $c$ of $C$ such that $p - c < B$; and we may therefore choose a basis for $P$ for which

$$p_i = c_i + q_i \quad (q_i < B; i = 1, 2, \cdots, \gamma).$$

Equation (12) then gives

$$p_i p_j = \Sigma \gamma_{ij} p_k + b_{ij}$$

where

$$b_{ij} = g_{ij} + q c_j + c q_i + \Sigma \delta_{ij} b_k - \Sigma \gamma_{ij} b_k < B,$$

and the algebra derived from this in the same way as (13) is from (12) is abstractly the same as before.

If the algebra $A$ does not contain the identity, it may happen that $A^2 < A$, $A^3 < A^2$, and so on. Since the basis of $A$ is finite, we must however have at some stage

$$A^m < A^{m-1}, \quad A^{m+1} = A^m;$$

the integer $m$ is then called the index of $A$. The most interesting case is when $A^m = 0$; the algebra is then said to be nilpotent.

When $N_1$ and $N_2$ are nilpotent subalgebras of $A$ which are also invariant, then $N_1 + N_2$ is a nilpotent invariant subalgebra of $A$. This is shown as follows. Let $m_1, m_2$ be the indices of $N_1$ and $N_2$ respectively; $N_3 = N_1 \sim N_2$ is nilpotent and, since $N_3^m \leq N_1^m = 0$, its index $m_3$ is not greater than $m_1$. Now

$$(N_1 + N_2)^2 = N_1^2 + N_2^2 + N_1 N_2 + N_2 N_1$$
$$\leq N_1^2 + N_2^2 + N_3 \leq N_1 + N_2$$

since it follows from the invariance of $N_1$ and $N_2$ that $N_1 N_2$ and $N_2 N_1$ are contained in both $N_1$ and $N_2$ and therefore in $N_3$. Similarly

$$(N_1 + N_2)^r \leq N_1^r + N_2^r + N_3$$
so that, if \( m \) is the greater of \( m_1 \) and \( m_2 \),

\[
(N_1 + N_2)^m \leq N_1^m + N_2^m + N_3 = N_3
\]

and hence \( N_1 + N_2 \) is a nilpotent subalgebra. Further

\[
A(N_1 + N_2) = AN_1 + AN_2 \leq N_1 + N_2
\]

\[
(N_1 + N_2)A = N_1A + N_2A \leq N_1 + N_2
\]

so that \( N_1 + N_2 \) is invariant. It follows that the totality of all nilpotent invariant subalgebras is itself a nilpotent invariant subalgebra; this algebra is called the maximal nilpotent invariant subalgebra or radical of \( A \).

An algebra \( A \) which is not nilpotent and which has no radical is said to be \textit{semi-simple}; if in addition it has no invariant subalgebra, it is said to be \textit{simple}.

We have then the following theorem whose proof we leave to the reader.

**Theorem 3.** If \( N \) is the radical of a non-nilpotent algebra \( A \), then \( (A - N) \) is semi-simple.

10.07 Idempotent elements. In the preceding section we defined a nilpotent algebra of index \( m \) as one for which \( A^m = 0, A^{m-1} \neq 0 \). An immediate consequence of this definition is that every element of a nilpotent algebra is nilpotent; we shall now prove the converse by showing that, if \( A \) is not nilpotent, it contains an idempotent element.

**Theorem 4.** Every algebra which is not nilpotent contains an idempotent element.

Let \( A = (a_1, a_2, \ldots, a_n) \) be an algebra of order \( \alpha \). If \( aA = A \) for some element \( a \) in \( A \), then \( ax = 0 \) only when \( x = 0 \); for \( aA = A \) implies that \( aa_i, aa_2, \ldots, aa_n \) is a basis, which means that there is no relation of the form

\[
0 = \Sigma \xi_i a_i = a \Sigma \xi_i a_i
\]

except when every \( \xi_i = 0 \). Also, if \( aA = A \), there must be an element \( e \) in \( A \) such that \( ae = a \); this gives \( ae^2 = ae \) or \( a(e^2 - e) = 0 \) and hence \( e^2 = e \).

The theorem is true for algebras of order 1; assume it true for algebras of order less than \( \alpha \). If \( a_iA = A \) for some \( a_i \), the theorem has just been shown to hold. If \( a_iA < A \) for every \( a_i \) in the basis of \( A \), then, since \( (a_iA)^2 = a_iAa_iA \leq a_iA \), either \( a_iA \) contains an idempotent element or, being of order less than \( \alpha \), it is nilpotent. Now \( (Aa_iA)^r \leq A(a_iA)^r \) and therefore \( Aa_iA \) is also nilpotent; but

\[
A \cdot Aa_iA \leq Aa_iA, \quad Aa_iA \cdot A \leq Aa_iA
\]

so that \( Aa_iA \) is invariant and being nilpotent is contained in the radical \( N \) of \( A \). Hence

\[
A^3 = \sum_i Aa_iA \leq N
\]

*Simple algebras are usually excluded from the class of semi-simple algebras; it seems more convenient however to include them.

The statement that \( A \) is not nilpotent is made in order to exclude the algebra of order 1 defined by a single element whose square is 0.
so that $A^3$, and therefore also $A$, is nilpotent, contrary to the hypothesis of the theorem. It follows that some $a_eA$ is not nilpotent and being of lower order than $A$ contains an idempotent element by assumption. The theorem is therefore proved.

The following lemma is an immediate consequence of Theorem 4.

**Lemma 1.** A non-nilpotent algebra cannot have a basis every element of which is nilpotent, nor a basis for which the trace of every element is 0.

For, if every element of the basis is nilpotent, the trace of every element of the algebra is 0 whereas the trace of an idempotent element is not 0 since the only roots of its characteristic equation are 0 and 1.

If $e$ is the only idempotent element in $eAe$, it is said to be primitive. An algebra which is not nilpotent contains at least one primitive idempotent element. For, if $eAe$ contains an idempotent element $e_1 \neq e$, then $e_1(e - e_1) = 0$ so that $e_1eAe_1$ does not contain $e - e_1$ and is therefore of lower order than $eAe$; since the order of $eAe$ is finite, a succession of such steps must lead to a primitive idempotent element.

**Theorem 4.5.** A simple algebra has a principal unit.

If $A$ is not nilpotent, it contains an idempotent element $e$. If $a$ is any element of $A$, we may set $a = a_1 + a_2$ where

$$a_1 = ea + ae - eae < eA + Ae, \quad a_2 = a - a_1, \quad ea_2 = 0 = a_2e.$$ 

We can therefore find a complex $A_1$ such that

$$A = eA + Ae + A_1, \quad eA + Ae \sim A_1 = 0, \quad eA_1 = 0 = A_1e.$$ 

If $A_1$ is not nilpotent, it contains an idempotent element $e'$ and $e + e'$ is also idempotent since $ee' = 0 = e'e$. We can therefore take $e + e'$ in place of $e$ so reducing the order of $A_1$, and after a finite number of such steps we arrive at a stage at which $A_1$ contains no idempotent element and is therefore nilpotent; we shall now assume that $e$ was chosen at the start so that $A_1$ is nilpotent; we shall also assume that $e$ is not an identity for $A$ and there is no real loss of generality in assuming in addition that it is not a left-hand identity.

Let $r$ be the index of $A_1$. If $r > 1$ and $x \neq 0$ is any element of $A_1^{r-1}$ then $xA_1 = 0 = A_1x$, $ex = 0$; if $r = 1$, then $A_1 = 0$ and since $e$ is not a left-hand identity, $e \leq eA < A$ so that there is an $x \neq 0$ such that $ex = 0$; we have therefore in both cases

$$xA_1 = 0 = A_1x, \quad ex = 0.$$ 

We now have $Ax = eAx, AxA = eAxA$; hence $Ax < A, AxA < A$ and $AxA$ is therefore an invariant subalgebra of $A$; if $AxA = 0$, then $Ax$ is invariant and not equal to $A$; if $Ax = 0$, then $xA$ is a proper invariant subalgebra unless it is 0 in which case $X = \{ x \}$ is a non-zero invariant subalgebra of $A$. In the case of a simple algebra it follows that $e$ is an identity.
Corollary. An algebra without a principal unit is not semi-simple. For 
\((Ax)^2 = AxAx = AxeAx = 0\) if \(A_1 \neq 0\).

10.08 Matric subalgebras. Let \(A\) be an algebra which contains the identity and let \(e_1\) be a primitive idempotent element; then \(e_\alpha = 1 - e_1\) is also idempotent and, if \(e_\alpha A e_\alpha\) is denoted by \(A_{\alpha\alpha}\), then

\[
A = (e_1 + e_\alpha)A(e_1 + e_\alpha) = A_{11} + A_{1\alpha} + A_{\alpha1} + A_{\alpha\alpha}.
\]

Suppose in the first place that \(A_{\alpha1}A_{1\alpha}\) is not nilpotent; there is then some \(a_{12} < A_{1\alpha}\) such that \(A_{\alpha1}a_{12}\), which is an algebra, is not nilpotent since otherwise \(A_{\alpha1}A_{1\alpha}\) would have a basis of nilpotent elements, which is impossible by Lemma 1; hence some such \(A_{\alpha1}a_{12}\) contains an idempotent element, say \(e_2 = a_{21}a_{12}\). If \(e_2\) is not primitive in \(A\), say \(e_2 = e' + e''\), \(e'e'' = 0 = e''e'\), where \(e'\) is primitive in \(A\), then \(a_{12}e' \neq 0\) since otherwise

\[
e' = e_2e' = a_{21}a_{12}e' = 0;
\]

also \(e' < A_{\alpha\alpha}\) since \(0 = e_1e_2 = e_1e' + e_1e''\), so that \(e_1e'' = -e_1e'\) and therefore

\[
e_1e' = -e_1e''e' = 0
\]

and similarly \(e'e_1 = 0\); we may therefore take \(a_{12} = a_{12}e'\) and \(a_{21} = e'a_{21}\) in place of \(a_{12}\) and \(a_{21}\), which gives \(e'\) in place of \(e_2\). We can therefore assume \(a_{12}\) so chosen that \(e_2\) is primitive in \(A\); also, since \(e_2a_{21}a_{12}e_2 = e_2^2 = e_2\), then, replacing \(a_{21}\) by \(e_2a_{21}\), if necessary, we may assume \(e_2a_{21} = a_{21}\) and similarly \(a_{12}e_2 = a_{12}\).

The element \(a_{12}a_{21}\) is not 0 since

\[
a_{21}a_{12}a_{21}a_{12} = a_{21}a_{12}a_{21}a_{12} = e_2^2 = e_2,
\]

and it is idempotent since

\[
(a_{12}a_{21})^2 = a_{12}a_{12}a_{21}a_{21} = a_{12}e_2a_{21} = a_{12}a_{21}.
\]

But \(a_{12}a_{21} \leq A_{1\alpha}A_{\alpha1} \leq A_{11}\); and, since \(e_1\) is primitive, it follows that \(a_{12}a_{21} = e_1\).

For the sake of symmetry we now put \(a_{11} = e_1, a_{22} = e_2\), and we then have a matric subalgebra of \(A\), namely \(a_{11}, a_{12}, a_{21}, a_{22}\).

Since \(A_{\alpha1}(A_{1\alpha}A_{\alpha1})^*A_{1\alpha} = (A_{\alpha1}A_{1\alpha})^{*+1}\), it follows that \(A_{1\alpha}A_{\alpha1}\) and \(A_{\alpha1}A_{1\alpha}\) are either both nilpotent or both not nilpotent. Suppose that both are nilpotent; then, since their product is in either order is 0, their sum is nilpotent and, because

\[
(A_{1\alpha} + A_{\alpha1})^2 = A_{1\alpha}A_{\alpha1} + A_{\alpha1}A_{1\alpha},
\]

it follows that

\[
N_1 = A_{1\alpha} + A_{\alpha1} + A_{1\alpha}A_{\alpha1} + A_{\alpha1}A_{1\alpha}
\]

is nilpotent. Now

\[
AN_1 = (A_{11} + A_{1\alpha} + A_{\alpha1} + A_{\alpha\alpha})(A_{1\alpha} + A_{\alpha1} + A_{1\alpha}A_{\alpha1} + A_{\alpha1}A_{1\alpha})
\]

\[
= A_{11}A_{1\alpha} + A_{11}A_{\alpha1}A_{\alpha1} + A_{1\alpha}A_{\alpha1} + A_{1\alpha}A_{\alpha1}A_{1\alpha} + A_{\alpha1}A_{\alpha\alpha}A_{\alpha1} + A_{\alpha1}A_{\alpha\alpha}A_{1\alpha}
\]

\[
\leq N_1
\]

since \(A_{1\alpha}A_{\alpha\alpha} = 0\) (\(p \neq j\), \(A_{ij}A_{ij} \leq A_{ij}\)). Similarly \(N_iA \leq N_1\). Hence \(N_1\) lies in the radical of \(A\).
Suppose that we have found a matric subalgebra $a_{ij}$ ($i, j = 1, 2, \cdots, r - 1$) such that $e_i = a_{ii}$ ($i = 1, 2, \cdots, r - 1$) are primitive idempotent elements of $A$; let $e_{i_0} = 1 - \sum_{i=1}^{r-1} e_i$ and set $A_{i_0} = e_i A e_j$ as before. Suppose further that $A_{a_{ii}} A_{i_0}$ is not nilpotent for some $i$; we may then take $i = 1$ without loss of generality. By the argument used above there then exists a primitive idempotent element $e_r = a_{rr} < A_{a_{ii}} A_{1a}$ and elements $a_{r1} < A_{a_{ii}}, a_{ir} < A_{1a}$ such that

$$a_{r1} a_{ir} = a_{r1}, \quad a_{ir} a_{r1} = a_{r1},\quad a_{r1} a_{1r} = a_{r1},\quad a_{1r} a_{r1} = a_{1r}.$$ 

If we set

$$a_{ir} = a_{1r} a_{i1}, \quad a_{ri} = a_{1r} a_{i1} \quad (i = 1, 2, \cdots, r - 1),$$

then $a_{ir} \neq 0$ since $a_{1i} a_{ri} = a_{1r}$ and $a_{ij} (i, j = 1, 2, \cdots, r)$ form a matric algebra of higher order than before.

Again, if every $A_{a_{ii}} A_{a_{ii}}$ is nilpotent, it follows as above that each $A_{i_0} A_{a_{ii}}$ is also nilpotent and hence

$$N_{r-1} = \sum_{i, j=1}^{r-1} (A_{i_0} + A_{a_{ii}} + A_{a_{ij}} A_{a_{ij}} + A_{a_{ii}} A_{i_0}),$$

having a nilpotent basis, is itself nilpotent; and it is readily seen as before that it is invariant and therefore belongs to the radical of $A$.

We can now treat $A_{a_{ii}}$ in the same way as $A$, and by doing so we derive a set of matric algebras $M_p(a_{ii}; i, j = 1, 2, \cdots, r_p)$ with the identity elements

$$a_p = \sum_{i=1}^{r_p} a_{ii},$$

such that $\Sigma a_p = 1$; also

$$N' = \sum_{p \neq q} (a_p A a_q + a_p A a_q A a_p)$$

is contained in the radical $N$ of $A$. We have therefore the following Lemma.

**Lemma 2.** If $A$ is an algebra with an identity, there exists a set of matric subalgebras $M_p = (a_{ij}^p; i, j = 1, 2, \cdots, r_p)$ with the principal units

$$a_p = \sum_{i=1}^{r_p} a_{ii}^p \quad (p = 1, 2, \cdots, k)$$

such that $a_p a_q = 0$ ($p \neq q$) and $\Sigma a_p = 1$, and such that

$$N' = \sum_{p \neq q} (a_p A a_q + a_p A a_q A a_p)$$

lies in the radical $N$ of $A$. Further each $a_{ii}^p$ is a primitive idempotent element of $A$. 
Corollary. $B_k = a_kAa_k + N'$ is an invariant subalgebra of $A$. For

$$AB_k = \Sigma a_qA(a_kAa_k + \sum_{p \neq q} a_pAa_q + a_pAa_qAa_p)$$

$$= a_kAa_k + N' = B_k.$$

10.09 We shall now consider the properties of the algebras $a_pAa_p$ where $a_p$ ($p = 1, 2, \ldots, k$) are the idempotent elements defined in Lemma 2.

**Lemma 3.** $a_pAa_p$ is the direct product of $M_p$, and an algebra $B_p$ in which the principal unit is the only idempotent element.

The first part of this lemma is merely a particular case of Theorem 2. That $B_p$ contains only one idempotent element is seen as follows. If $e$ is a primitive idempotent element of $B_p$, then $a^p_1e$ and $a^p_1(a_p - e)$ are distinct and, if not zero, are idempotent and lie in $a^p_1Aa^p_1$; but this algebra contains only one idempotent element since $a^p_1$ is primitive; hence $a^p_1(a_p - e) = 0$, and therefore $e = a_p$ is the only idempotent element in $B_p$.

**Lemma 4.** If $B$ is an algebra whose principal unit $1$ is its only idempotent element, any element of $B$ which is singular is nilpotent; and the totality of such elements forms the radical of $B$.

The proof of the first statement is immediate; for, if $a$ is singular, the algebra $\{a\}$ generated by $a$ does not contain the principal unit and, since $B$ contains no other idempotent element, $a$ is nilpotent by Theorem 4. To prove the second part, let $x$ and $y$ be nilpotent but $z = x + y$ non-singular; then $1 = z^{-1}x + z^{-1}y = x_1 + y_1$. Here $x_1$ and $y_1$ are singular and therefore nilpotent. If $m$ is the index of $x_1$, then

$$(1 - x_1)(1 + x_1 + x_1^2 + \cdots + x_1^{m-1}) = 1$$

and this is impossible since $y_1 = 1 - x_1$ is nilpotent. Hence $z$ is also nilpotent and the totality of nilpotent elements forms an algebra; and this algebra is invariant since the product of any element of $B$ into a nilpotent element is singular and therefore nilpotent. It follows that $B$ is a division algebra whenever it has no radical, that is, when it is semi-simple.

10.10 **The classification of algebras.** We shall now prove the main theorem regarding the classification of algebras in a given field $F$.

**Theorem 5.** (i) Any algebra which contains an identity can be expressed in the form

$$A = S + N$$

7 An element of $B$ is singular in $B$ if it does not have an inverse relatively to the principal idempotent element of $B$. 
where $N$ is the radical of $A$ and $S$ is a semi-simple subalgebra; $S$ is not necessarily unique but any two determinations of it are simply isomorphic.

(ii) A semi-simple algebra can be expressed uniquely as the direct sum of simple algebras.

(iii) A simple algebra can be expressed as the direct product of a division algebra $D$ and a simple matric algebra $M$; these are not necessarily unique but, if $D_1, M_1, D_2, M_2$ are any two determinations of $D$ and $M$, then $D_1 \sim D_2, M_1 \sim M_2$.

We have seen in Lemma 2 that $A = \Sigma a_p A a_p + N'$, where $N' \leq N$, and also in Lemmas 3, 4 that $a_p A a_p = M_p \times B_p$, where $M_p$ is a simple matric algebra. The first part of the theorem therefore follows for $A$ when it is proved for any algebra like $B_p$ and when it is shown that the direct product of $M_p$ by a division algebra is simple; for, if $B_p = D_p + N_p$, then $D_p$ is a division algebra and

$$a_p A a_p = M_p \times D_p + M_p \times N_p, \quad M_p N_p \leq N.$$ 

If the field $F$ is one in which every equation has a root, the field itself is clearly the only division algebra and hence $M_p D_p = M_p$; in this case part (i) is already proved. Further, the theorem is trivial for algebras of order 1; we may, therefore, as a basis for a proof by induction assume it is true for algebras of order less than the order $\alpha$ of $A$.

If the field $F$ is extended to $F(\xi)$ by the adjunction of an algebraic irrationality $\xi$ of degree $\rho + 1$, we get in place of $A$ an algebra $A' = A(\xi)$ which has the same basis as $A$ but which contains elements whose coordinates lie in $F(\xi)$ but not necessarily in $F$; all elements of $A$ are also elements of $A'$. Regarding $A'$ we have the following important lemma.

**Lemma 5.** If $N$ is the radical of $A$, the radical of $A' = A(\xi)$ is $N' = N(\xi)$.

Let $A = C + N$, $C \cap N = 0$, and let the radical of $A'$ be $N''$; then clearly $N'' \geq N'$. If $N'' > N'$, there is an element of $N''$ of the form

$$c'' = c_0 + c_1 \xi + \cdots + c_\rho \xi^\rho,$$ 

$(c_1 < c, c_0 \neq 0)$.

Since $c''$ is nilpotent,

$$0 = \text{tr}(c'') = \text{tr}(c_0) + \xi \text{tr}(c_1) + \cdots$$

and since $\text{tr}(c_0), \text{tr}(c_1), \cdots$ are rational in $F$, each is separately 0. But, if $a_1, a_2$ are arbitrary elements in $A$,

$$a_1 c'' a_2 = a_1 c_0 a_2 + a_1 c_1 a_2 \xi + \cdots$$

lies in $N''$ and, since each $a_1 c_0 a_2$ is rational in $F$, the trace of each is 0 as above. Hence the trace of every element in $Ac_0 A$ is 0 from which it follows by Lemma 1 that $Ac_0 A$ is nilpotent and being invariant and also rational it must lie in $N$ (cf. §10.06). But $Ac_0 A$ contains $c_0$ since $A$ contains 1 whereas $C \cap N = 0$; hence no elements of $N''$ such as $c''$ exist and the lemma is therefore true.

We may also note that, if $B, C$ are complexes for which $B \cap C = 0$, and $B', C'$ the corresponding complexes in $A'$, then also $B' \cap C' = 0$. 


Suppose now that the identity is the only idempotent element of \( A \) and that the first part of the theorem is true for algebras of order less than \( \alpha \). Let \( a \neq 1 \) be an element of \( A \) corresponding to an element \( \bar{a} \) of \((A - N)\) and let \( f(\lambda) \) be the reduced characteristic function of \( \bar{a} \); \( f(\lambda) \) is irreducible in \( F \) since \((A - N)\) is a division algebra. Since \( f(\bar{a}) = 0 \), it follows that \( f(a) < N \) and hence, if \( \tau \) is the index of \( f(a) \), the reduced characteristic function of \( a \) is \([f(\lambda)]^\tau \). If we adjoin to \( F \) a root \( \xi \) of \( f(\lambda) \), this polynomial becomes reducible so that in \( A' = A(\xi) \) the difference algebra \((A' - N')\) is no longer a division algebra though by Lemma 5 it is still semi-simple. If we now carry out in \( F(\xi) \) the reduction given in Lemma 2, say

\[
A' = \Sigma e_p A'e_p + N^*,
\]
either the algebras \( e_p A'e_p \) are all of lower order than \( \alpha \), or, if \( A' = e_1 A'e_1 \), then it contains a matric algebra \( M' \) of order \( n^2 \) \((n > 1)\) and if we set \( A' = M'B' \), as previously, \( B' \) is of lower order than \( \alpha \). In all cases, therefore, part (i) of the theorem follows for algebras in \( F(\xi) \) of order \( \alpha \) when it is true for algebras of order less than \( \alpha \), and its truth in that case is assumed under the hypothesis of the induction.

We may now assume

\[
A = C + N, \quad C \cap N = 0,
\]

\[
A' = S' + N', \quad S' \cap N' = 0,
\]

where \( S' \) is an algebra simply isomorphic with \((A' - N')\); \( N' \) has a rational basis, namely that of \( N \) (cf. Lemma 5).

If \( c_1, c_2, \ldots \) is a basis of \( C \) then, since \( A \) is contained in \( A' \) we have

\[
c_i = s' + m'_i, \quad s'_i < S', \quad m'_i < N', \quad (i = 1, 2, \ldots)
\]

and, since \( C \cap N = 0 \) implies \( C' \cap N' = 0 \), it follows that \( s'_1, s'_2, \ldots \) form a basis of \( S' \), that is, we may choose a basis for \( S' \) in which the elements have the form

\[
c_i + n_{i0} + n_{ii} \xi + \cdots \quad (c_i < C, n_{ii} < N)
\]

where \( c_i, n_{i0}, \ldots \) are rational in \( F \). Moreover, since \( C \) is only determined modulo \( N \), we may suppose it modified so that \( n_{i0} \) is absorbed in \( c_i \); we then have a basis for \( S' \)

\[
s'_i = c_i + n_{i0} \xi + \cdots + n_{ik} \xi^k = c_i + n'_i.
\]

When the basis is so chosen, the law of multiplication in \( S' \), say

\[
s'_is'_j = \Sigma \sigma_{ijk}s'_k,
\]

has constants \( \sigma_{ijk} \) which are rational in \( F \); for \( s'_i = c_i \) mod \( N' \) and \( c_i \) is rational. If we now replace \( s'_i \) in (16) by its value from (15) and expand, we have

\[
c_isc_i + c_in'_i + n'_ic_i + n'_in'_i = \Sigma \sigma_{ijk}c_k + \Sigma \sigma_{ijk}n'_k,
\]
but \( n_j' n_i' < (N')^2 \) and therefore

\[ c_i c_j + c_i n_j' + n_i' c_j = \Sigma \sigma_{ijk} c_k + \Sigma \sigma_{ijk} n_k' \mod (N')^2, \]

a relation which is only possible if the coefficients of corresponding powers of \( \xi \) are also equivalent modulo \( (N')^2 \) and in particular

\[ c_i c_j = \Sigma \sigma_{ijk} c_k \mod (N')^2. \]

Consequently the algebra \( A_1 \) generated by \( c_i \) \((i = 1, 2, \ldots, \sigma)\) contains no element of \( N \) which is not also in \( N^2 \) and hence, except in the trivial case in which \( N = 0 \), the order of \( A_1 \) is less than \( \sigma \). By hypothesis we can therefore choose \( C \) rationally in such a way that \( c_i c_j = \Sigma \sigma_{ijk} c_k \), that is, such that \( C \) is an algebra; part (i) of the theorem therefore follows by induction.

10.11 For the proof of part (ii) we require the following lemmas.

**Lemma 6.** If \( A \) contains the identity \( 1 \) and if \( B \) is an invariant subalgebra which has a principal unit \( e \), then

\[ A = B \oplus (1 - e)A(1 - e). \]

Since \( e \) is the principal unit of \( B \), which is invariant, \( e A e = B \); also \( e A(1 - e) \) and \( (1 - e) A e \) are both 0 since \( A e \) and \( e A \) lie in \( B \) and, if \( b \) is any element of \( B \), then \( (1 - e) b = b - b = 0 \), \( b (1 - e) = b - b = 0 \); hence

\[ (17) \quad A = e A e + (1 - e) A (1 - e), \quad e A e \sim (1 - e) A (1 - e) = 0. \]

Further \( e A e \cdot (1 - e) A (1 - e) = 0 = (1 - e) A (1 - e) \cdot e A e \), so that the sum in (17) is a direct sum.

**Lemma 7.** Every invariant subalgebra \( B \) of a semi-simple algebra \( A \) is semi-simple and therefore contains a principal unit.

Suppose that \( B \) has a radical \( N \); then

\[ AN \leq B, \quad (AN)^2 = AN \cdot N \leq BN \leq N \]

so that \( AN \) is nilpotent. But, since \( A^2 = A \), we have \( (AN)^r = (AN)^r A \); hence \( ANA \) is a nilpotent invariant subalgebra of \( A \) which, since \( A \) contains an identity, is not 0 unless \( N = 0 \). But \( A \) has no radical; hence \( N = 0 \) and \( B \) also has no radical.

In consequence of these lemmas a simple algebra is irreducible and a semi-simple algebra which is not also simple can be expressed as the direct sum of simple algebras. Let

\[ A = B_1 \oplus B_2 \oplus \cdots \oplus B_p = C_1 \oplus C_2 \oplus \cdots \oplus C_q. \]

be two expressions of \( A \) as the direct sum of simple algebras and let the principal units of \( B_i \) and \( C_i \) be \( b_i \) and \( c_i \) respectively; then \( 1 = \Sigma b_i = \Sigma c_i \). We then have \( C_k \leq \Sigma b_i C_i b_i \leq C_k \) and therefore

\[ C_k = \Sigma b_i C_i b_i = \Sigma b_i C_i b_i. \]
since when $i \neq j$ then $b_i C_i b_j \leq B_i \bowtie B_j = 0$ and $b_i C_i b_i \cdot b_j C_j b_j = 0$. If $b_i C_i b_i \neq 0$, it is an invariant subalgebra of $C_i$ and, since the latter is simple, we have $b_i C_i b_i = C_i$ for this value of $i$ and all other $b_j C_j b_j$ equal 0, and therefore $C_i = b_i A b_i = B_i$. The second part of the theorem is therefore proved.

10.12 We shall now prove part (iii) of Theorem 5 in two stages.

**Lemma 8.** If $D$ is a division algebra and $M$ the matric algebra $(e_{ij}; i, j = 1, 2, \ldots, m)$, and if $D \times M = D M$, then $D M$ is simple.

Let $B$ be a proper invariant subalgebra of $A = D M$. If $x$ is an element of $B$, then there exists an element $y$ of $A$ such that $x y = 0$, since otherwise we should have $B \geq x A = A$, in other words, every element of $B$ is singular in $A$ and hence $B \bowtie D = 0$. But

$$x = \sum d_{ij} e_{ij}, \quad d_{ij} < D$$

and $d_{ij} = \sum e_{pi} x e_{jp}$ and is therefore contained in $B$ as well as in $D$. Since $B \bowtie D = 0$, every $d_{ij} = 0$, that is, $x = 0$ so that $B = 0$. It follows immediately from Lemma 2 that a simple algebra always has the form $D \times M$, and also that $D \cong e_{ii} A e_{ii}$.

**Lemma 9.** In a simple algebra all primitive idempotent elements are similar.

Let $e$ and $a$ be primitive idempotent elements of a simple algebra $A$. We can then find a matric algebra $M = (e_{ij})$ for which $e_{11} = e$ and such that $A = D \times M$, where $D$ is a division algebra. If $ea = 0 = ae$, we can at the same time choose $e_{22} = a$; and $e_{22} = u e_{11} u^{-1}$ where

$$u = 1 - e_{11} - e_{22} + e_{12} + e_{21} = u^{-1},$$

so that the lemma is true in this case, and we may therefore assume that, say, $ea \neq 0$.

Suppose now that $eae \neq 0$. Since $A = D \times M$, we can express $a$ in the form $\sum \alpha_{ij} e_{ij}$ ($\alpha_{ij} < D$), where $\alpha_{ii} \neq 0$ since $eae = \alpha_{11} e_{11}$. We have then

$$(e a) e = (e_1 a)^2 = (\alpha_{11} e_{11} + \alpha_{12} e_{12} + \cdots)^2 = \alpha_{11} e_{11} a$$

and hence $b = \alpha_{11}^{-1} e a$ is idempotent. We then have

$$e b = b, \quad b e = e, \quad b a = b;$$

also $a b = a b a = a b a b$ and, since $a$ is primitive, either $a b a = a$ or $a b a = 0$; but

$$e a b e = e a e \neq 0,$$

hence $a b = a$. We then have

$$b = u e u^{-1}, \quad u = 1 - b + e, \quad u^{-1} = 1 + b - e, \quad b = v^{-1} a v, \quad v = 1 - b + a, \quad v^{-1} = 1 + b - a,$$

and hence $a$ and $e$ are similar in this case also.
If $eae = 0$ but $aea \neq 0$, interchanging the roles of $e$ and $a$ leads to results similar to those just obtained; we can therefore assume $eae = 0 = aea$. If

$$u = 1 + e - ea + ae = 2(2 - e + ea - ae)^{-1},$$

then $uau^{-1} = a - ae$; we can therefore assume $ea = 0$. If

$$v = (1 + e - 2ea) = 2(2 - e + 2ea)^{-1},$$

then $vav^{-1} = a - ea$; we can therefore also assume $ea = 0$, which brings us back to the first case which we considered. The lemma is therefore proved.

Part (iii) of the theorem follows immediately. For, if $e$ and $a$ are primitive idempotent elements of $M_1$ and $M_2$ respectively, we can now find $w$ such that $a = wew^{-1}$; but $D_1 \simeq eAe$ and $D_2 \simeq aAa = weAew^{-1}$, which is similar to $eAe$ and therefore to $D_1$.

10.13 Semi-invariant subalgebras. If $B$ is a subalgebra of $A$ which is such that $AB \leq B$ ($BA \leq B$), it is called a right (left) semi-invariant subalgebra. We shall treat only the case in which $A$ is semi-simple; it has then an identity and if we restrict ourselves, as we shall, to the case of right semi-invariant subalgebras, we may assume $AB = B$.

It is clear that, if $A = A_1 \oplus A_2$, then also $B = B_1 \oplus B_2$, where $A_iB_i = B_iA_i = 0$ ($i \neq j$). It is sufficient then at first to consider only simple algebras, and in this case we have the added condition that $ABA = A$; that is, we have simultaneously

$$AB = B, \quad ABA = A.$$

If we call $B$ minimal when it contains no other semi-invariant subalgebra, we have

**Lemma 10.** A minimal right semi-invariant subalgebra of a simple algebra $A$ has the form $Au$, where $u$ is a primitive idempotent element of $A$. Conversely, if $u^2 = u$ is primitive, $Au$ is a minimal right semi-invariant subalgebra.

Let $AC = C$; if $c_1 \neq 0$ is any element of $C$, and $C_1 = Ac_1 \leq C$, then $AC_1 = C_1$. Suppose $C_1 \subset C$; then in the same way if $c_2$ is any element of $C_1$, we have $C_2 = Ac_2 \leq C_1$. If $C_2 < C_1$, we may continue this process and after a finite number of steps we shall arrive at an algebra $B \neq 0$ such that $Ab = B$ for every element $b$ of $B$ which is not 0. Since $A$ is simple, $AbA = A$ and $B^2 = B$, so that $B$ contains a primitive idempotent element $u$ and $Au = B$. If $u$ is not also primitive in $A$, let $u = u_1 + u_2$, $u_iu_j = 0$ ($i \neq j$), $u_i^2 = u_i \neq 0$. Then $u_iu = u_i$ so that $u_i$ is in $B$; hence $u$ must be primitive in $A$, if it is so in $B$.

Since $B = Au$, every $x$ in $B$ has the form $ax$ and hence $xu = x$. But also $B = Ax$ and, from the manner in which $B$ was chosen, either $Bx = 0$ or $Bx = B$. If $Bx = 0$, then $ux = 0$ and therefore

$$x^2 = xu \cdot xu = 0.$$
Also, if \( x \) is nilpotent, then \( x^2 = 0 = ux; \) for \( uAu = uBu \) is simple since, by the proof of Lemma 4, it is a division algebra, and \( ux = uxu < uBu \). If \( Bx = B \), then there is a unique \( b \) such that \( bx = x \) and, since \( b \) is then idempotent, we have \( ux = x \), that is, \( x \) lies in \( uAu \). If \( B = Au \), then \( AB = A^2u \leq B \) so that \( B \) is a right semi-invariant subalgebra of \( A \). If \( C \) is minimal, then \( B = C \) as desired.

Conversely, let \( B = Au \), \( u \) primitive; then the only idempotent quantity of \( B \) has been shown above to be \( u \) and, if \( B \) were not primitive, we should have \( B > C = Av, v \) primitive, which is impossible.

Suppose now that \( B \) is not minimal and let \( e_1, e_2, \ldots, e_r \) be a complete set of primitive supplementary idempotent elements in \( B \). Then \( B_r = Ae_1 + Ae_2 + \cdots + Ae_r \) is semi-invariant in \( A \). Let \( b \) be an element of \( B \) which is not in \( B_r \); since \( b \neq \Sigma be_i \), we may replace \( b \) by \( b - \Sigma be_i \) and so assume every \( be_i = 0 \) in which case clearly \( Ab \cap B_r = 0 \). But, if \( b \neq 0 \), then \( Ab \) contains an idempotent element \( e \) such that \( e^2 = 0 \) (\( i = 1, 2, \ldots, r \)) and \( e_{r+1} = e - \Sigma e_i \) is an idempotent element supplementary to the given complete set, which is impossible. We therefore have the following theorem.

**Theorem 6.** If \( A \) is simple and \( AB = B \) is a semi-invariant subalgebra, then

\[
B = Ae_1 + Ae_2 + \cdots + Ae_r
\]

where \( e_1, e_2, \ldots, e_r \) is a complete supplementary set of primitive idempotent elements of \( B \); and these idempotent elements are also primitive in \( A \).

We shall assume that \( A \) is semi-simple, say

\[
A = S_1 \oplus \cdots \oplus S_t,
\]

when each \( S_i \) is simple and

\[
S_i = D_i \times M_i.
\]

As previously (cf. Lemma 2) we may set \( M_i = (e_{pq}^i) \), \( p, q = 1, 2, \ldots, n_i \), where \( e_{pq}^i \) form a set of supplementary primitive idempotent elements and \( \sum_{i, p} e_{pq}^i = 1 \).

If \( B \) is any invariant subalgebra, then \( B = \sum_{i, p} Be_{pq}^i \) and \( Be_{pq}^i \) is a right semi-invariant subalgebra; if \( B \) is minimal, we have already seen that it has the form \( Bu \) where \( u \) is a primitive idempotent element, and therefore we have \( B = Be_{pq}^i = S_i e_{pq}^i \) for some \( i \) and \( p \). If set \( B_{ip} = S_i e_{pq}^i \), then

\[
B_{ip} e_{pq}^i = S_i e_{pq}^i e_{pq}^i = M_i D_i e_{pq}^i = S_i e_{qq}^i = B_{iq}.
\]

We have therefore the following theorem.

**Theorem 7.** If \( A \) is semi-simple and is given by (19), and if \( e_{pq}^i \) form a complete
set of supplementary primitive idempotent elements such that $\sum_{p=1}^{n_i} e_{p,p}^i = u_i$ is the identity of $S_i$, then every minimal right semi-invariant subalgebra has the form

\begin{equation}
B_{ip} = S_i e_{p,p}^i.
\end{equation}

Moreover, there is a number $e_{pq}^i$ in $S_i$ such that

\begin{equation}
B_{ip} e_{pq}^i = B_{iq}.
\end{equation}

10.14 The representation of a semi-simple algebra. Let $A$ be a linear associative algebra over $F$ with the identity 1, and designate elements of $A$ by $a$. A representation of $A$ is a set, $U(a)$, of matrices of order $n$ such that $a \rightarrow U(a)$ is a correspondence between the elements of $A$ and the matrices of the set in which the following conditions are satisfied

\begin{align}
U(1) &= 1, & U(a + b) &= U(a) + U(b), & U(ab) &= U(a) U(b), \\
U(\alpha a) &= \alpha U(a)
\end{align}

for every $a$ and $b$ of $A$ and every scalar $\alpha$ in $F$.

We can now, as in chapter I, associate with the matrices $U(a)$ a vector space $R$ with a given fundamental basis, and a change of basis corresponds to replacing $U(a)$ by $PU(a)P^{-1}$, an equivalent representation (cf. 1.08). A subspace $R_1$ of $R$ is invariant under $A$ (cf. 5.16) if every matrix $U(a)$ carries each vector of $R_1$ into a vector of $R_1$. If $R_1 \neq 0$, we may set $R = R_1 + R_2$ ($R_1 \cap R_2 = 0$); and since we are only interested in the equivalence of representations, we may suppose the basis $R$ so chosen that

\begin{equation}
U(a) = \begin{bmatrix}
U_1(a) & U_2(a) \\
0 & U_3(a)
\end{bmatrix}.
\end{equation}

The representation is said to be reducible in this case, and it is evident that both $U_1(a)$ and $U_2(a)$ give representations of $A$.

If $R$ has no proper invariant subspace, then $U(A)$ and $R$ are said to be irreducible. It is now clear that we may write

\[ R = R_1 + R_2 + \cdots + R_s \]

where $R_s = R_1 + \cdots + R_t$ is the invariant subspace of least order which contains $R_{t-1}$ ($R_0 = 0$), and in this case

\begin{equation}
U(a) = \begin{bmatrix}
U_{11}(a) & U_{12}(a) & \cdots & U_{1s}(a) \\
0 & U_{22}(a) & \cdots & U_{2s}(a) \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & U_{ss}(a)
\end{bmatrix}
\end{equation}

and the representations $U_1(a), \cdots, U_s(a)$ are irreducible. If in addition $R_s, \cdots, R_t$ are themselves invariant for some $t$, then $U_{ij}(a) = 0$ ($i \neq j; i, j = 1, 2, \cdots, t$), and we say that $U(a)$ is decomposable.
A particular case of fundamental importance arises when we take \( R \) to be \( A \) itself, that is, if \( x \) is a variable element of \( A \), then \( x' = ax \) corresponds to a linear transformation in the basis of \( R \) (or \( A \)), say
\[
x' = ax = U(a)(x),
\]
and \( U(a) \) has the property given in (23) and so is a representation of \( A \). It is obviously the representation of (6) and is one-to-one; it is called the regular representation.

The invariant subspaces of \( A \) are evidently its right semi-invariant subalgebras \( B \). If \( e_1, e_2, \ldots, e_i \) is a basis of \( B \) and
\[
\alpha e_i = \sum \alpha_{ij} e_j,
\]
then the matrices \( U(a) = \| \alpha_{ij} \| \) give a representation of \( A \) on the subspace \( B \). Suppose now that \( V(a) \) is a given representation, \( R \) the corresponding subspace, and \( B \) a right semi-invariant subalgebra of \( A \). If \( y \) is any vector of \( R \), then the set of vectors of the form \( V(b)(y) \) is an invariant subspace of \( R \), since
\[
V(a)V(b) = V(ab) = V(ba), \quad b_a < B.
\]
From (27) it is seen immediately that the set \( B' \) of elements \( b' \) in \( B \) for which \( V(b')y = 0 \) forms a right semi-invariant subalgebra of \( B \) and hence, if \( B \) is minimal, either \( B' = 0 \) or \( B' = B \). If \( B' = 0 \), then \( V(e_i)y, \ldots, V(e_i)y \) is a basis of the set \( \{V(b)(y)\} \) and
\[
V(a)V(e_i)y = V(\alpha e_i)y = \sum \alpha_{ij} V(e_j)y.
\]
But then the vectors of the form \( V(b)y \) give a representation of \( A \) equivalent to that determined by \( B \) in (26).

We shall now prove the following theorem.

**Theorem 8.** If the regular representation of an algebra is decomposable, then every representation is decomposable and its irreducible components are contained in the regular representation.

Suppose that the regular representation of \( A \) is decomposable; then \( A = B_1 + B_2 + \cdots + B_i \), where the \( B_i \) are irreducible equivalent subspaces of \( A \), that is, minimal semi-invariant subalgebras such that \( B_i \cong B_k \) for \( j \neq k \). Let \( y_1, y_2, \ldots, y_n \) be a basis of the space \( R \) of a representation of \( A \). Since \( A \) has an identity, we have
\[
R = AR = B_1R + B_2R + \cdots + B_iR
= B_1y_1 + B_2y_2 + \cdots + B_iy_i + \cdots + B_ny_n.
\]
As we have seen above, if \( B_iy_i \neq 0 \), it is a subspace of \( R \) which gives a representation equivalent to that given by \( B_i \); it follows that either \( B_iy_i = 0 \) or it is an invariant subspace of \( R \). The intersection of the invariant subspaces is also invariant so that either
$B_{y_1} \sim B_{y_2} = 0$ or $B_{y_1} = B_{y_2}$; hence we may select from the spaces $B_{y_1}$ in (28) a set of independent irreducible invariant subspaces determining $R$. This proves Theorem 8.

Consider now a semi-simple algebra

$$A = S_1 \oplus \cdots \oplus S_r$$

where $S_i$ is a simple algebra. We may write

$$1 = \sum u_{ij} \quad (i = 1, \cdots, r; \ j = 1, \cdots, n_i)$$

where the $u_{ij}$ form a complete set of supplementary primitive idempotent elements of $A$. Then

$$A = \Sigma A u_{ij} = \Sigma B_{ij}$$

where $B_{ij} = A u_{ij}$ is a minimal right invariant subalgebra of $A$. We have then decomposed $A$ into irreducible invariant subspaces and have proved the first part of the following theorem.

**Theorem 9.** The regular representation of a semi-simple algebra is decomposable, and its reducible components are those obtained by the use of the $B_{ij}$ as representation spaces. The representations given by any pair $B_{ij}$, $B_{ik}$ are equivalent while $B_{ii}$, $B_{ik}$ give inequivalent representations for $j \neq k$.

For by Theorem 7 we have $B_{ij} e_{jk} = B_{ik}$ so that the proof of Theorem 7 with $y = e_{jk}$ shows that the representation by $B_{ij}$ is equivalent to that by $B_{ip}$. In the representation by $B_{ij}$ we have

$$e_i = \sum_{j=1}^n u_{ij} \rightarrow 1_{n_i}$$

where $1_{n_i}$ is an identity matrix corresponding to the identity transformation on $B_{ij}$ since $e_i$ is the principal unit of $B_{ij}$. But in the representation by $B_{ik}$, we have $e_i \rightarrow 0$. Evidently these representations cannot be similar.

10.15 Group algebras. If $\mathfrak{G} = (g_1, g_2, \cdots, g_m)$ is a finite group, the group relation $g_i g_j = g_{ij}$ is a particular case of the associative product defined in (2) and, when it is used in conjunction with addition, we get an associative algebra $G$ of which $(g_1, g_2, \cdots, g_m)$ is a basis and $g_1$ the identity.

The representation of $\mathfrak{G}$ as a regular permutation group

$$h_i = \begin{pmatrix} g_1 & g_2 & \cdots & g_m \\ g_1 & g_2 & \cdots & g_m \end{pmatrix}$$

corresponds to the representation of $G$ as a set of matrices, the matrix $h_i$ being

$$h_i = \sum_{p=1}^m e_{ip} \quad (g_{ip} = g_{ip}).$$
Since \( i_p = p \), that is, \( g_p g_p = g_p \), only when \( g_i \) is the identity, the matrix \( h_i \) has no coordinate in the main diagonal except for \( i = 1 \) in which case \( h_1 \) is the identity matrix; hence
\[
(29) \quad \text{tr}(h_1) = m, \quad \text{tr}(h_i) = 0 \quad (i \neq 1).
\]
It follows from this that \( G \) is semi-simple. For if \( u = \Sigma \eta_i h_i \) is the matrix corresponding to some element of the radical \( N \), then \( \text{tr}(u) = 0 \) since \( u \) is nilpotent. If \( u \neq 0 \), some coordinate, say \( \eta_p \), is not 0 and in \( h_p^{-1} u \), which also corresponds to some element of \( N \), the coefficient of \( h_1 \) is not 0; we may therefore assume \( \eta_1 \neq 0 \) provided \( N \neq 0 \). But using (18) we get
\[
0 = \text{tr}(u) = \Sigma \eta_i \text{tr}(h_i) = m\eta_1;
\]

hence the assumption that \( u \neq 0 \) leads to a contradiction and therefore \( N = 0 \), that is, \( G \) is semi-simple. This gives the following theorem.

**Theorem 10.** A group algebra is semi-simple. It is therefore the direct sum of simple algebras and, if the field of the coefficients is sufficiently extended, it is the direct sum of simple matrix algebras.

The whole of the representation theory developed in the previous section can now be applied to groups.