

Semisimple rings and modules

The material in these notes is based upon the treatments in S. Lang, Algebra, Third Edition, chapters 17 and 18 ; J.-P. Serre, Linear representations of finite groups and N. Jacobson, Basic Algebra, II.

Section 1 Algebras

Definition 1.1 An algebra A over a field \mathcal{K} is a \mathcal{K} -vector space A together with a \mathcal{K} -bilinear map $\mu : A \times A \rightarrow A$. The map μ is the multiplication operation in A , and we shall assume that multiplication is associative. We shall assume in addition that A has a unit element 1 (i.e. $\mu(1, a) = \mu(a, 1) = a$ for all $a \in A$) and that \mathcal{K} lies in the (multiplicative) center of A .

Every algebra A is a ring with a vector space structure attached to the operation $+$.

Definition 1.2 An algebra A is called a division algebra if every nonzero element a has a multiplicative inverse b ; that is, $ab = ba = 1$.

Definition 1.3 A map f between two \mathcal{K} -algebras A and B is an algebra homomorphism if f is a \mathcal{K} -linear map of vector spaces such that $f(aa^*) = f(a) f(a^*)$ for all elements a, a^* in A .

Examples 1.4

1) Let V be a vector space over a field \mathcal{K} , and let $\text{End}_{\mathcal{K}}(V)$ denote the set of \mathcal{K} -linear transformations of V . Clearly $\text{End}_{\mathcal{K}}(V)$ is a vector space over \mathcal{K} , and the multiplication operation in $\text{End}_{\mathcal{K}}(V)$ is given by composition.

2) Let $M_n(\mathcal{K})$ denote the collection of $n \times n$ matrices whose elements lie in a field \mathcal{K} . $M_n(\mathcal{K})$ is a vector space of dimension n^2 over \mathcal{K} in which the addition operation $+$ is the usual one and multiplication is matrix multiplication. If V is an n -dimensional vector space over \mathcal{K} , then by fixing a basis of V we obtain an algebra isomorphism between $\text{End}_{\mathcal{K}}(V)$ and $M_n(\mathcal{K})$.

3) Group algebras $\mathcal{K}[G]$

Let G be any group, not necessarily finite, and let $\mathcal{K}[G]$ denote the set of formal finite sums $\sum_{g \in G} a_g g$, where the coefficients a_g lie in \mathcal{K} . Note that $\mathcal{K} \subseteq \mathcal{K}[G]$ and $G \subseteq \mathcal{K}[G]$.

Addition is defined in the obvious way by $(\sum_{g \in G} a_g g) + (\sum_{g \in G} b_g g) = (\sum_{g \in G} (a_g + b_g) g)$. Given elements x of \mathcal{K} , h of G and $\xi = \sum_{g \in G} a_g g$ of $\mathcal{K}[G]$ we define $x\xi = \xi x = \sum_{g \in G} x a_g g$ and $h\xi = \sum_{g \in G} a_g hg$. The definition of $h\xi$ extends in the obvious way to a multiplication on $\mathcal{K}[G]$ that makes $\mathcal{K}[G]$ an algebra.

Note :

- 1) \mathcal{K} always lies in the center of $\mathcal{K}[G]$.
- 2) The elements of the group G are linearly independent in $\mathcal{K}[G]$ with respect to \mathcal{K} . Hence, if G is a finite group, then $\mathcal{K}[G]$ has finite dimension $|G|$ over \mathcal{K} . Moreover, the group algebra $\mathcal{K}[G]$ is finite dimensional over $\mathcal{K} \Leftrightarrow G$ is a finite group.

Example 1.5 Central elements in $\mathbb{C}[G]$

Let G be a finite group, and let $\{\rho_i : G \rightarrow GL(V_i), 1 \leq i \leq r\}$ be a complete set, up to equivalence, of irreducible complex finite dimensional representations of G .

a) For a class function $f : G \rightarrow \mathbb{C}$ define $e_f = \sum_{g \in G} f(g) g \in \mathbb{C}[G]$.

b) For $1 \leq i \leq r$ define $e_i \in \mathbb{C}[G]$ by $e_i = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g$, where χ_i is the

character of the representation ρ_i and d_i is the dimension of V_i .

Assertion The element e_f lies in the center of $\mathbb{C}[G]$ for each class function $f : G \rightarrow \mathbb{C}$. The elements e_i lie in the center of $\mathbb{C}[G]$ for $1 \leq i \leq r$, and are a \mathbb{C} -basis for $\{e_f, f \text{ a class function on } G\}$.

We shall see later in Proposition 6.7 that every element of the center of $\mathbb{C}[G]$ is one of the elements $e_f, f : G \rightarrow \mathbb{C}$ a class function on G .

Proof of the assertion (cf. Serre, Theorem 8, p. 34)

If f is any class function on G , then it is routine to show that e_f commutes with all elements in G and hence with all elements in $\mathbb{C}[G]$. The function $f_i(g) = \frac{d_i}{|G|} \overline{\chi_i(g)}$ is a

class function on G for each i , and hence e_i lies in the center of $\mathbb{C}[G]$ for all i . The characters $\{\chi_i : G \rightarrow \mathbb{C}, 1 \leq i \leq r\}$ are an orthonormal basis for the class functions on G

relative to the inner product $(\varphi | \psi) = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}$. If $f : G \rightarrow \mathbb{C}$ is a class

function on G , then so is \bar{f} and we may write $\bar{f} = \sum_{i=1}^r a_i \chi_i$, where $a_i \in \mathbb{C}$. Hence $e_f =$

$$\sum_{i=1}^r b_i e_i, \text{ where } b_i = (\bar{a}_i |G|) / d_i.$$

It remains only to show that the elements $\{e_1, e_2, \dots, e_n\}$ are linearly independent in $\mathbb{C}[G]$. From the definition one sees that each element e_i is nonzero since the character χ_i that defines it is a nonzero function on G and the elements of G are linearly independent in $\mathbb{C}[G]$. (Recall that $\chi_i(1) = \dim V_i$). By the corollary below, $e_i^2 = e_i$ for $1 \leq i \leq r$ and $e_i e_j = 0$ if $i \neq j$. Suppose that $0 = \sum_{i=1}^r a_i e_i$ for some elements $a_i \in \mathbb{C}$. Then $0 = e_j (\sum_{i=1}^r a_i e_i) = a_j e_j$. Hence $a_j = 0$ for each j since e_j is nonzero. \square

The elements e_i in $\mathbb{C}[G]$ also have special meaning for the decomposition of an arbitrary complex representation $\rho : G \rightarrow GL(V)$ into isotypic components.

Proposition

Let G be a finite group, and $\{\rho_i : G \rightarrow GL(V_i), 1 \leq i \leq r\}$ be a complete set, up to equivalence, of irreducible complex finite dimensional representations of G . Let $e_i = \frac{d_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g$, where χ_i is the character of the representation ρ_i and d_i is the dimension of V_i .

Let $\rho : G \rightarrow GL(V)$ be a complex representation of G . Let W_i be the direct sum of all irreducible submodules of V that are equivalent to V_i . Then

- $V = W_1 \oplus W_2 \oplus \dots \oplus W_r$
- $\rho(e_i) \in \text{End}(V)$ is the projection map $V \rightarrow W_i$ if $W_i \neq \{0\}$.
- $\rho(e_i) = 0$ if $W_i = \{0\}$.
- $\rho_j(e_i) = \delta_{ij} \cdot \text{Id}$. For any $\xi \in \mathbb{C}[G]$ $\chi_j(e_i \xi) = \chi_j(\xi e_i) = \chi_j(\xi) \delta_{ij}$.

Proof of the Proposition

The assertion in a) is obvious. To prove b) and c) we note that the map $\rho(e_i)$ commutes with $\rho(g)$ for all $g \in G$ since e_i lies in the center of $\mathbb{C}[G]$. If W is an irreducible G -submodule of V , then $\rho(e_i) = \lambda_i \cdot \text{Id}$ on W by Schur's Lemma for some $\lambda_i \in \mathbb{C}$. Taking the trace of the expression above we find that $\lambda_i = (1/d) \chi(e_i)$, where d is the dimension of W and χ is the character of ρ . Since W is equivalent to V_j as a G -module for some j , $1 \leq j \leq r$, it follows that $d = d_j$ and $\chi = \chi_j$. We compute $\chi_j(e_i) = \frac{d_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \chi_j(g) = d_i$

$(\chi_j | \chi_i) = d_i \delta_{ij}$. Hence $\lambda_i = (1/d_j) \chi_j(e_i) = (d_i/d_j) \delta_{ij}$. We conclude that $\rho(e_i) = \text{Id}$ on W if W is an irreducible G -submodule of V that is equivalent to V_i , and $\rho(e_i) = 0$ on W if W is an irreducible G -submodule of V that is equivalent to V_j for some $j \neq i$. This completes the proofs of b) and c). If one applies c) of the proposition in the case that $\rho = \rho_j$, then it follows immediately that $\rho_j(e_i) = \delta_{ij} \cdot \text{Id}$, which proves the first assertion of d). If $\xi \in \mathbb{C}[G]$ is arbitrary, then from the first part of d) and the fact that e_j is a central element

of $\mathbb{C}[G]$ we obtain $\rho_j(e_i \xi) = \rho_j(\xi e_i) = \rho_j(\xi) \rho_j(e_i) = \delta_{ij} \rho_j(\xi)$. Taking traces in the equation above completes the proof of d). \square

Corollary

Let G be a finite group, and let $\{e_1, e_2, \dots, e_r\}$ be the central elements in $\mathbb{C}[G]$ defined above. Then

- 1) $1 = e_1 + e_2 + \dots + e_r$.
- 2) $e_i^2 = e_i$ for $1 \leq i \leq r$.
- 3) $e_i e_j = 0$ if $i \neq j$.

Proof

We begin by recalling some facts about the regular representation $\text{reg} : G \rightarrow \text{GL}(\mathbb{C}^n)$, where $n = |G|$, and its character $\chi_{\text{reg}} : G \rightarrow \mathbb{C}$.

- a) $\chi_{\text{reg}} = \sum_{i=1}^r d_i \chi_i$, where $d_i = \dim V_i$. Equivalently, the irreducible module V_i has multiplicity d_i in the regular representation.
- b) $\chi_{\text{reg}}(g) = 0$ if $g \neq 1$, and $\chi_{\text{reg}}(1) = |G|$.
- c) $\text{reg} : G \rightarrow \text{GL}(\mathbb{C}^n)$ is injective.

From the definition of the elements $\{e_i\}$ and the facts above we compute $e_1 + e_2 + \dots + e_r = (1/|G|) \sum_{g \in G} \{ \sum_{i=1}^r d_i \overline{\chi_i(g)} \} g = (1/|G|) \sum_{g \in G} \overline{\chi_{\text{reg}}(g)} g = 1$. This proves 1). Now let $\mathbb{C}^n = W_1 \oplus W_2 \oplus \dots \oplus W_r$ be the decomposition of the regular representation into isotypic components as in the proposition above. Since each irreducible submodule V_i appears with positive multiplicity for $\rho = \text{reg}$ it follows from b) of the proposition that $\rho(e_i)$ is the projection of V onto W_i for $1 \leq i \leq r$. Hence $\rho(e_i^2) = \rho(e_i)^2 = \rho(e_i)$ for all i and $\rho(e_i e_j) = \rho(e_i) \rho(e_j) = 0$ if $i \neq j$ by the properties of projection maps. The assertions 2) and 3) of the corollary now follow since ρ is injective. \square

1.6 Finite dimensional division algebras

For an arbitrary field \mathcal{K} there may, in general, be an infinite number of \mathcal{K} -division algebras that are finite dimensional over \mathcal{K} . For example, let $\mathcal{K} = \mathbb{Q}$, the field of rational numbers, and let $a \in \mathbb{C}$ be a root of an irreducible polynomial $f(x)$ of degree n in $\mathbb{Q}[x]$. We shall see that \mathbb{Q} and a are contained in subfield $\mathbb{Q}(a)$ of \mathbb{C} such that $\mathbb{Q}(a)$ is an n -dimensional vector space over \mathbb{Q} .

If $\mathcal{K} = \mathbb{R}$, then one has the following striking result of Frobenius (proof omitted).

Theorem (Frobenius)

Let A be a finite dimensional division algebra over \mathbb{R} . Then A is isomorphic to one of the following algebras :

- 1) $A = \mathbb{R}$ (1-dimensional over \mathbb{R})
- 2) $A = \mathbb{C}$ (2-dimensional over \mathbb{R})
- 3) $A = \mathbb{H}$ (4-dimensional over \mathbb{R} , the quaternions)

The first two examples are fields, but the quaternions are not commutative with respect to multiplication.

1.7 A-modules are vector spaces

Let $(M,+)$ be an abelian group, and let $\text{Hom}(M)$ denote the additive abelian group of homomorphisms of $(M,+)$. $\text{Hom}(M)$ becomes a ring with the identity map Id as unit if composition is taken as the multiplicative operation. If R is a ring, then an R -module is an abelian group $(M,+)$ together with a ring homomorphism $\rho : R \rightarrow \text{Hom}(M)$.

Now let A be an algebra over a field \mathcal{K} , and let M be a nontrivial A -module. We assert that the homomorphism $\rho : A \rightarrow \text{Hom}(M)$ is injective on \mathcal{K} with $\rho(1)(m) = m$ for all $m \in M$. Identifying \mathcal{K} with $\rho(\mathcal{K})$ we then obtain a \mathcal{K} -vector space structure on M .

If $\rho(z^*) = 0$ for some nonzero element z^* of \mathcal{K} , then $\rho(1) = \rho((1/z^*) \cdot (z^*)) = \rho(1/z^*) \circ \rho(z^*) = 0$. For any element z of \mathcal{K} we then have $\rho(z) = \rho(z \cdot 1) = \rho(z) \circ \rho(1) = 0$. This contradicts the hypothesis that ρ is a nonzero homomorphism. Therefore $\rho : \mathcal{K} \rightarrow \text{Hom}(M)$ is injective. A similar argument shows that $\rho(1) = \text{Id}$ on M .

The next observation is useful in the discussion of group algebras $\mathcal{K}[G]$, where G is a finite group.

Proposition

Let A be a finite dimensional algebra over a field \mathcal{K} , and let M be a nontrivial A -module. Then M is finitely generated as an A -module $\Leftrightarrow A$ is finite dimensional as a \mathcal{K} -vector space.

Proof

If M is finite dimensional as a vector space over \mathcal{K} , then any finite \mathcal{K} -basis \mathfrak{B} for M is also a finite generating set for M as an A -module since $\mathcal{K} \subseteq A$. Conversely, suppose that M is a finitely generated A -module, and let $\{x_1, x_2, \dots, x_n\}$ be a finite generating set. Let $\{a_1, a_2, \dots, a_N\}$ be a \mathcal{K} -basis of A . If $\mathfrak{B} = \{a_i(x_j) : 1 \leq i \leq n, 1 \leq j \leq N\}$, then it is easy to

check that \mathfrak{B} is a (finite) \mathcal{K} -spanning set for M . Hence \mathfrak{B} contains a finite \mathcal{K} -basis for M . \square

Section 2 Structure of $\text{End}_{\mathbf{R}}(M)$

In this section let R be a ring with 1. Let M be an R -module, and let $f : R \rightarrow \text{Hom}(M)$ be the homomorphism that defines the action of R on M . A ring R is a division ring if every nonzero element of R has an inverse.

Commutants and bicommutants

Definition 2.1 $\text{End}_{\mathbf{R}}(M) = \{ \varphi \in \text{Hom}(M) : \varphi \text{ commutes with } f(r) \text{ for all } r \in R \}$.

Equivalently, we may let r denote $f(r)$ and define $\text{End}_{\mathbf{R}}(M) = \{ \varphi \in \text{Hom}(M) : \varphi(rm) = r\varphi(m) \text{ for all } r \in R \text{ and all } m \in M \}$.

Note that $R' = \text{End}_{\mathbf{R}}(M)$ is a subring of $\text{Hom}(M)$, and M becomes a module over R' . The ring R' is called the commutant of R .

If $R'' = \text{End}_{R'}(M) = \{ \varphi \in \text{Hom}(M) : \varphi \text{ commutes with all } r' \in R' \}$, then R'' is called the bicommutant of R . If r is an element of R , then $f(r)$ commutes with the elements of R' and hence is an element of R'' . The map $f : R \rightarrow \text{Hom}(M)$ therefore has image in R'' , and we obtain by restriction a ring homomorphism $f : R \rightarrow R''$. The Jacobson Density Theorem in section 4 says that the image $f(R)$ is a "large" subset of R'' if M is semisimple over R .

In the sequel we will typically suppress the notation $f(r)$ and just use r as is customary. The ring R then becomes a subring of R'' .

Simple R -modules

Definition 2.2 An R -module M is simple if the only R -submodules are $\{0\}$ and M .

Proposition 2.3

Let M be a simple R -module, and let $D = \text{End}_{\mathbf{R}}(M)$. Then D is a division ring. If R is an algebra over a field \mathcal{K} , then D is a division algebra over \mathcal{K} .

Proof

Let T be any nonzero element of $\text{End}_{\mathbf{R}}(M)$. It follows immediately from the definition of $\text{End}_{\mathbf{R}}(M)$ that $N = \text{Ker}(T)$ and $N^* = \text{Im}(T)$ are both R -submodules of M . Since M is simple and T is nonzero it follows that $\text{Ker}(T) = \{0\}$ and $\text{Im}(T) = M$. Hence T is invertible.

If R is an algebra over a field \mathcal{K} , then it is easy to see that $D = \text{End}_{\mathbf{R}}(M)$ is an algebra over \mathcal{K} . \square

The case that R is an algebra over a field \mathcal{K}

We observed in section 1 that if R is an algebra over a field \mathcal{K} , then an R -module is also a vector space over \mathcal{K} . Regarding \mathcal{K} as an algebra, then the algebra of \mathcal{K} -linear transformations of M is precisely $\text{End}_{\mathcal{K}}(M) = \{T \in \text{Hom}(M) : T \text{ commutes with } x \text{ for all } x \in \mathcal{K}\}$. In this context it is useful to observe the following

Proposition 2.4

Let R be an algebra over a field \mathcal{K} , and let M be an R -module. Then R , $R' = \text{End}_R(M)$ and $R'' = \text{End}_{R'}(M)$ are all subalgebras of $\text{End}_{\mathcal{K}}(M)$.

Proof

Since \mathcal{K} lies in the center of R it follows immediately that $R \subseteq \text{End}_{\mathcal{K}}(M)$. Next, observe that $R' = \text{End}_R(M) \subseteq \text{End}_{\mathcal{K}}(M)$ since $\mathcal{K} \subseteq R$. Finally, $\mathcal{K} \subseteq R'$ since $\mathcal{K} \subseteq Z(R)$, the center of R , and hence $R'' = \text{End}_{R'}(M) \subseteq \text{End}_{\mathcal{K}}(M)$. \square

Examples

If R is a finite dimensional algebra over a field \mathcal{K} , then any simple R -module M is a finite dimensional vector space over \mathcal{K} by the discussion in section 1.7 ; if m is any nonzero element of M , then Rm is a nonzero R -submodule of M and hence equal to M . In this case we can often add to the statement of Proposition 2.3 that $D = \text{End}_R(M)$ is a division algebra.

Proposition 2.5

Let R be a finite dimensional algebra over a field \mathcal{K} and let M be a simple R -module.

- 1) $\text{End}_R(M)$ is a finite dimensional algebra over \mathcal{K} .
- 2) If \mathcal{K} is algebraically closed, then $\text{End}_R(M) = \{\lambda \text{Id} : \lambda \in \mathcal{K}\} \cong \mathcal{K}$.
- 3) If $\mathcal{K} = \mathbb{R}$, then $\text{End}_R(M) \cong \mathbb{R}, \mathbb{C}$ or \mathbb{H} .

Proof

1) By Proposition 2.4 and the discussion above M is a finite dimensional vector space over \mathcal{K} , and $\text{End}_R(M)$ is a subalgebra of $\text{End}_{\mathcal{K}}(M)$, whose k -dimension is finite.

2) If T is any element of $\text{End}_R(M)$, then T has an eigenvalue in \mathcal{K} since \mathcal{K} is algebraically closed. By definition R leaves invariant the eigenspace V_{λ} of T , and hence $V_{\lambda} = V$ since V is R -simple. We conclude that $T = \lambda \text{Id}$, which proves 1).

3) Since $D = \text{End}_R(M)$ is a division algebra by Proposition 2.3 and is finite dimensional over \mathbb{R} by 1) the result follows from the Frobenius theorem in section 1.6.

Examples of finite dimensional algebras over \mathbb{R}

1) Let $R = \mathbb{C}$ and $M = \mathbb{C}$. Then R may be regarded as a 2-dimensional algebra over \mathbb{R} , and M is a simple R -module since R acts transitively on $M = R$. In this case $\text{End}_R(M) = \text{End}_{\mathbb{C}}(\mathbb{C}) \cong \mathbb{C}$.

2) Let $R = \mathbb{H}$ and $M = \mathbb{H}$. Then R is a 4-dimensional algebra over \mathbb{R} , and M is a simple R -module relative to left multiplication since R acts transitively on M . Let \mathbb{H} denote the 4-dimensional subalgebra of $\text{End}_{\mathbb{R}}(M)$ obtained from the left multiplication of \mathbb{H} on M . Let \mathbb{H}^{OP} denote the 4-dimensional subalgebra of $\text{End}_{\mathbb{R}}(M)$ obtained from the right multiplication of \mathbb{H} on M . Since \mathbb{H} and \mathbb{H}^{OP} commute it follows that $\mathbb{H}^{\text{OP}} \subseteq \text{End}_{\mathbb{R}}(M)$ and equality holds since $4 = \dim_{\mathbb{R}} \mathbb{H}^{\text{OP}} \leq \dim_{\mathbb{R}} \text{End}_{\mathbb{R}}(M) \leq 4$ by the Frobenius theorem. (One may also prove equality by a tedious direct calculation). It follows that $\text{End}_{\mathbb{R}}(M) \cong \mathbb{H}$.

Opposite rings and $\text{End}_{\mathbb{R}}(R)$

If $M = R$ and R acts on itself on the left, then one has a simple and explicit description of $\text{End}_{\mathbb{R}}(R)$ in terms of the opposite ring R^{OP} . We define $R^{\text{OP}} = R$ as a set, the addition in R and R^{OP} is the same but the multiplication $\#$ of R^{OP} is defined by $x\#y = y \cdot x$, where \cdot is the given multiplication operation in R .

Proposition 2.6

- 1) For every element x of R the map $f(x) : R \rightarrow R$ given by $f(x)(r) = rx$ is an element of $\text{End}_{\mathbb{R}}(R)$.
- 2) The map $f : R \rightarrow \text{End}_{\mathbb{R}}(R)$ is a bijection that satisfies $f(xy) = f(y) \circ f(x)$ and $f(x+y) = f(x) + f(y)$ for all x, y in R .
- 3) If $I : R^{\text{OP}} \rightarrow R$ is the identity map, then $g = f \circ I : R^{\text{OP}} \rightarrow \text{End}_{\mathbb{R}}(R)$ is a ring isomorphism.

Proof

The proof of 1) is routine since right and left multiplication maps always commute. Assertion 3) follows immediately from 2). We prove 2). The assertions $f(x+y) = f(x) + f(y)$ and $f(xy) = f(y) \circ f(x)$ for all x, y in R are obvious. If $f(x) = f(y)$ for x, y in R , then $x = f(x)(1) = f(y)(1) = y$. If φ is any element of $\text{End}_{\mathbb{R}}(R)$ and $x = \varphi(1)$, then $\varphi = f(x)$ since $\varphi(r) = \varphi(r \cdot 1) = r\varphi(1) = rx = f(x)(r)$ for all $r \in R$. \square

The next elementary result is basic for the structure theory of semisimple rings that we discuss next.

Proposition 2.7

Let M be an R -module and n a positive integer. Let M^n denote the direct sum of n copies of M . Then $\text{End}_{\mathbb{R}}(M^n)$ is ring isomorphic to $M_n(R')$, the collection of $n \times n$ matrices with elements in $R' = \text{End}_{\mathbb{R}}(M)$.

Proof

For $1 \leq i \leq n$ let $\pi_i : M^n \rightarrow M$ denote projection onto the i^{th} factor and define

$I_i : M \rightarrow M^n$ by $I_i(m) = (0, \dots, 0, m, 0, \dots, 0)$, where m sits in the i^{th} position. It is easy to check that π_i and I_j commute with the R -action on M and M^n for all i and j . Hence if φ is any element of $\text{End}_R(M^n)$, then $A_{ij}(\varphi) = \pi_i \circ \varphi \circ I_j$ is an element of $R' = \text{End}_R(M)$ for all $1 \leq i, j \leq n$. Let $A(\varphi)$ denote the $n \times n$ matrix in $M_n(R')$ determined by an element φ of $\text{End}_R(M^n)$. If we regard the elements (m_1, m_2, \dots, m_n) of M^n as "column vectors" then it is easy to check that $\varphi(m_1, m_2, \dots, m_n) = A(\varphi) \cdot (m_1, m_2, \dots, m_n)$ ("matrix multiplication") for all elements (m_1, m_2, \dots, m_n) of M^n and elements φ of $\text{End}_R(M^n)$; that is, $\varphi(m_1, m_2, \dots, m_n) = (y_1, y_2, \dots, y_n)$, where $y_i = \sum_{j=1}^n A_{ij}(\varphi) m_j$. Hence the map $\varphi \rightarrow A(\varphi)$ is an injective ring homomorphism of $\text{End}_R(M^n)$ into $M_n(R')$. Conversely, given an element B of $M_n(R')$ we define a map φ in $\text{Hom}(M^n)$ by $\varphi(m_1, m_2, \dots, m_n) = B(m_1, m_2, \dots, m_n)$ (matrix multiplication). It follows that φ commutes with the R -action on M^n since the entries of B lie in $R' = \text{End}_R(M)$. This proves that $\varphi \in \text{End}_R(M^n)$ and $B = A(\varphi)$. Hence $\varphi \rightarrow A(\varphi)$ is a ring isomorphism of $\text{End}_R(M^n)$ onto $M_n(R')$. \square

Section 3 Basic structure of semisimple rings and modules

The basic structure theorem for semisimple rings, due to Wedderburn, says that every semisimple ring R is a direct product $R_1 \times R_2 \times \dots \times R_n$ of finitely many simple rings. Moreover, a simple ring R is isomorphic to a matrix algebra $M_n(D)$, where D is a division algebra and n is a positive integer that depend on R . The nature of this dependence will be made precise later. If $R = \mathbb{C}[G]$, where G is a finite group, then the simple rings R_i that are factors of R are precisely the simple algebras $\text{End}_{\mathbb{C}}(V_i)$, where $\{V_1, V_2, \dots, V_r\}$ is a complete list (up to equivalence) of the complex irreducible G -modules.

In this section we discuss definitions and basic properties of semisimple rings and modules.

Proposition 3.1

The following are equivalent for a ring R with 1 and an R -module M .

- 1) For every R -submodule N there exists an R -module N' such that $N \oplus N' = M$.
- 2) M is a direct sum of finitely many simple R -submodules.

Proof

See Lang, Algebra, pp. 645-646.

Definition 3.2

- a) An R -module M is said to be semisimple if either the conditions of Proposition 3.1 hold.
- b) A ring R with 1 is said to be semisimple if it is semisimple as an R -module, where R acts on itself by left multiplication.
- c) A left ideal J of a ring R is said to be simple if J contains no proper left ideals I of R .
- d) A ring R with 1 is simple if $R = L_1 \oplus L_2 \oplus \dots \oplus L_n$, where $\{L_i\}$ are simple left ideals of R that are all isomorphic. (In particular any simple ring is semisimple.)

Proposition 3.3

If R is a semisimple ring, then every R -module M is semisimple.

Proof

See Lang, Algebra, p. 651.

Lemma 3.4

Let L be a simple ideal of an arbitrary ring R with 1, and let M be a simple R -module. Then either L is isomorphic to M as an R -module or $LM = \{0\}$.

Proof

Suppose that $LM \neq \{0\}$, and let m be a nonzero element of M such that $N = Lm \neq \{0\}$. Note that $RN = R(Lm) = Lm = N$ since L is a left ideal of R . Hence N is a nonzero submodule of M and must equal M . The map $f : L \rightarrow M$ given by $f(r) = rm$ is a surjective homomorphism of R -modules. It follows that $\text{Ker}(f) = \{0\}$ and f is an isomorphism since $\text{Ker}(f)$ is an R -submodule of the simple R -module L .

Corollary 3.5

Let R be a semisimple ring, and let M be a simple R -module. Then

- 1) M is isomorphic as an R -module to some simple left ideal of R .
- 2) If R is a simple ring, then any two simple R -modules are isomorphic.
- 3) If R is a simple ring, then any two simple left ideals are isomorphic.

Proof

By the definition of a semisimple ring we can find simple left ideals L_1, L_2, \dots, L_n of R such that $R = L_1 \oplus L_2 \oplus \dots \oplus L_n$. If M is not isomorphic to L_i for any i , then by the lemma above $L_i M = \{0\}$ for every i . We conclude that $RM = \{0\}$, which contradicts the fact that R contains 1. This proves 1). If R is a simple ring, then the simple left ideals $\{L_i\}$ above can be chosen to be all isomorphic. Assertion 2) now follows from the proof of 1). Assertion 3) follows from 2) since simple left ideals are simple R -modules. \square

Examples 3.6

1) We begin with an example of a simple ring R , which will turn out to be the only example.

Let D be a division ring, and let $M_n(D)$ denote the algebra of $n \times n$ matrices with entries in D . Let D^n denote the space of n -tuples (d_1, d_2, \dots, d_n) , $d_i \in D$. Let $M_n(D)$ act on D^n on the left by matrix multiplication, regarding the elements of D^n as column vectors. For $1 \leq i \leq n$ let L_i denote the matrices in $M_n(D)$ whose j^{th} column is zero for all $j \neq i$. Equivalently, $L_i = \{X \in M_n(D) : X(e_j) = \{0\} \text{ for all } j \neq i\}$, where $\{e_1, e_2, \dots, e_n\}$ denotes the usual natural basis of D^n . It is clear from the second description that each L_i is a left ideal of $M_n(D)$, and it is not difficult to show that each L_i is simple. Clearly, $M_n(D) = L_1 \oplus L_2 \oplus \dots \oplus L_n$.

If L is a left ideal of $M_n(D)$, then LX is a left ideal isomorphic to L for any invertible element X of $M_n(D)$. Moreover, L is simple $\Leftrightarrow LX$ is simple. Let P_{ij} be the permutation matrix in $M_n(D)$ such that $P_{ij} e_k = e_k$ if $k \notin \{i, j\}$, $P_{ij} e_i = e_j$ and $P_{ij} e_j = e_i$. It is easy to see that $L_i P_{ij} = L_j$ and $P_{ij}^2 = \text{Id}$. It follows that the simple left ideals $\{L_i\}$ are all isomorphic, and hence $M_n(D)$ is a simple ring.

2) Let G be a finite group and let $R = \mathcal{K}[G]$, the group algebra over a field \mathcal{K} whose characteristic does not divide $|G|$, the order of G . Then R is a semisimple algebra (cf. Lang). We have already seen this in the case that $\mathcal{K} = \mathbb{C}$. For a proof in the general case see Lang.

3) Clifford algebras

These are semisimple algebras that are finite dimensional over \mathbb{R} or \mathbb{C} , and they play an important role in geometry and physics. We describe briefly one classical example over \mathbb{R} . For further discussion see Lang pp. 749-758, Fulton and Harris, Representation Theory a First Course, Springer, GTM # 129, 1991, pp. 299-307 or Lawson and Michelsohn, Spin Geometry, Princeton University Press, 1989, Chapter 1.

Start with \mathbb{R}^n equipped with some inner product \langle, \rangle , say the standard dot product. Let $\{e_1, e_2, \dots, e_n\}$ be an orthonormal basis of \mathbb{R}^n relative to \langle, \rangle , say the standard basis relative to the dot product. The choice of inner product and orthonormal basis doesn't matter since the resulting algebras will all be equivalent and of dimension 2^n over \mathbb{R} .

Let $C^{\mathbb{Q}}(n)$ denote the set of finite formal sums $\sum r_{i_1 i_2 \dots i_j} e_{i_1 i_2 \dots i_j}$, where the $r_{i_1 i_2 \dots i_j}$ are real numbers. Multiplication of the expressions $e_{i_1 i_2 \dots i_j}$ and $e_{m_1 m_2 \dots m_k}$ is defined by $(e_{i_1 i_2 \dots i_j})(e_{m_1 m_2 \dots m_k}) = e_{i_1 i_2 \dots i_j m_1 m_2 \dots m_k}$, subject to the rules $e_i e_j =$

$-e_j e_i$ if $i \neq j$, and $e_i^2 = -1$. By expanding vectors v and w of \mathbb{R}^n in terms of the orthonormal basis $\{e_1, e_2, \dots, e_n\}$ and using the multiplication rules above we obtain the important relations

$$(*) \quad \begin{aligned} vw + wv &= -2 \langle v, w \rangle && \text{for all vectors } v \text{ and } w \text{ in } \mathbb{R}^n \\ v^2 &= -|v|^2 \in \mathbb{R} && \text{for all vectors } v \text{ in } \mathbb{R}^n \end{aligned}$$

The second relation in (*) follows from the first by setting $v = w$. The relations (*) also show that multiplication does not depend on the choice of orthonormal basis in \mathbb{R}^n .

By definition $C\ell(n)$ contains the real numbers \mathbb{R} and also \mathbb{R}^n , corresponding to the expressions $\sum r_i e_i$. By inspection any expression $e_{i_1 i_2 \dots i_j}$, where $j > n$, contains at least two equal indices and can be reduced by the multiplication rules to an expression $e_{m_1 m_2 \dots m_k}$, where $k \leq n$ and $m_r \leq m_{r+1}$ for all r , $1 \leq r \leq k$. For each integer $1 \leq k \leq n$ let V_k denote the vector space of all real linear combinations of elements of the form $e_{m_1 m_2 \dots m_k}$, where $\{m_1, m_2, \dots, m_k\}$ is any subset of k elements in $\{1, 2, \dots, n\}$ such that $m_r \leq m_{r+1}$ for all r , $1 \leq r \leq k$. Hence $C\ell(n) = V_0 \oplus V_1 \oplus \dots \oplus V_n$, where $V_0 = \mathbb{R}$, $V_1 = \mathbb{R}^n$ and V_k has dimension $\binom{n}{k} = (n!) / (k! (n-k)!)$ for every k . Note that V_n has dimension 1 and consists of all real multiples of the element $e_1 e_2 \dots e_n$. Adding up the dimensions of the $\{V_i\}$ we see (by induction on n) that $\dim C\ell(n) = 2^n$ for every n . The multiplication defined above is associative, and $C\ell(n)$ becomes an algebra over \mathbb{R} .

We sketch a proof that $C\ell(n)$ is a semisimple algebra for every n . The relations (*) above show that left multiplication on $C\ell(n)$ by a nonzero element v of \mathbb{R}^n is an invertible linear transformation of $C\ell(n)$. Let $\text{Pin}(n)$ denote the subgroup of $\text{GL}(C\ell(n))$ generated by all left multiplications by unit vectors v in \mathbb{R}^n . One can show that $\text{Pin}(n)$ is a compact subgroup of $\text{GL}(C\ell(n))$.

Now let $\rho : C\ell(n) \rightarrow \text{GL}(U)$ be any algebra homomorphism (i.e. a representation of $C\ell(n)$), where U is a finite dimensional real vector space. Then ρ is continuous and $\rho(\text{Pin}(n))$ is a compact subgroup of $\text{GL}(U)$. The compactness of $\rho(\text{Pin}(n))$ implies, by a standard averaging process similar in spirit to that used for finite subgroups of $\text{GL}(\mathbb{R}^k)$, that there exists an inner product $\langle \cdot, \cdot \rangle$ on U such that $\rho(\text{Pin}(n))$ is a subgroup of the orthogonal group of $\{U, \langle \cdot, \cdot \rangle\}$. This means that $\langle \rho(g)u, \rho(g)u^* \rangle = \langle u, u^* \rangle$ for all vectors u, u^* in U and all elements g in $\text{Pin}(n)$.

Let $\rho : C\ell(n) \rightarrow \text{GL}(U)$ be any algebra homomorphism and let $\langle \cdot, \cdot \rangle$ be an invariant inner product for $\rho(\text{Pin}(n))$ on U as above. If v is a unit vector in \mathbb{R}^n , then $\rho(v)^2 = -\text{Id}$ since $v^2 = -1$ by the relations (*) above. The fact that $\rho(v)^2 = -\text{Id}$ means that $-\rho(v) = \rho(v)^{-1} = \rho(v)^t$. We conclude that $\rho(v)$ is skew symmetric as well as orthogonal relative to $\langle \cdot, \cdot \rangle$ if v is a unit vector in \mathbb{R}^n . It follows immediately that $\rho(v)$ is skew symmetric relative to $\langle \cdot, \cdot \rangle$ for all v in \mathbb{R}^n since $\rho(\lambda v) = \lambda \rho(v)$ for all v in \mathbb{R}^n and all real numbers λ .

Summary : Any algebra homomorphism $\rho : C\ell(n) \rightarrow GL(U)$ admits an inner product $\langle \cdot, \cdot \rangle$ on U such that the transformations in $\rho(\mathbb{R}^n)$ are all skew symmetric relative to $\langle \cdot, \cdot \rangle$. If W is a subspace of U invariant under $\rho(C\ell(n))$, then W^\perp is invariant under $\rho(\mathbb{R}^n)$, where W^\perp denotes the orthogonal complement of W in U relative to $\langle \cdot, \cdot \rangle$. The algebra $\rho(C\ell(n))$ is generated by $\rho(\mathbb{R}^n)$ since the algebra $C\ell(n)$ is generated by \mathbb{R}^n . Hence W^\perp is invariant under $\rho(C\ell(n))$ if W is invariant under $\rho(C\ell(n))$. This means that every finite dimensional real $C\ell(n)$ -module U is semisimple. Apply this fact now in the case that $U = C\ell(n)$ and $\rho : C\ell(n) \rightarrow \text{End}(C\ell(n))$ is the homomorphism given by $\rho(g) =$ left multiplication by g . We conclude that $C\ell(n)$ is a semisimple algebra.

Example $C\ell(2) \cong \mathbb{H}$

Let $\{e_1, e_2\}$ be the standard orthonormal basis for \mathbb{R}^2 . From the description above $C\ell(2) = \mathbb{R} \oplus \mathbb{R}(e_1) \oplus \mathbb{R}(e_2) \oplus \mathbb{R}(e_1e_2)$, and the multiplication rules are $e_1e_2 = -e_2e_1$ and $e_1^2 = e_2^2 = -1$. If we define $I = e_1, J = e_2$ and $K = e_1e_2$, then the multiplication rules for $C\ell(2)$ show that $I^2 = J^2 = K^2 = -1$; $IJ = -JI = K$; $JK = -KJ = I$ and $KI = -IK = J$. This shows that $C\ell(2)$ is isomorphic to the quaternions \mathbb{H} .

Section 4 The Jacobson Density Theorem and applications

Fix a ring R with 1 and an R -module M . Let $f : R \rightarrow \text{Hom}(M)$ be the homomorphism that defines the action of R on M . We recall from section 2 that the ring $R' = \text{End}_R(M)$ is called the commutant of R , and $R'' = \text{End}_{R'}(M)$ is called the bicommutant of R . Moreover, we observed that $f(R) \subseteq R''$ or simply $R \subseteq R'' \subseteq \text{Hom}(M)$ if we suppress the notation f as is customary. If R is semisimple, then we can say much more.

Theorem 4.1 (Jacobson Density Theorem)

Let M be a semisimple R -module over a ring R with 1. Let $R' = \text{End}_R(M)$ and let $R'' = \text{End}_{R'}(M)$. Let X be any finite subset of M and let r'' be any element of R'' . Then there exists an element r of R such that $rx = r''x$ for every x in X .

Lemma 4.2

If N is any R -submodule of M , then N is also an R'' -submodule of M .

Proof of Lemma 4.2

Let N be any R -submodule of M . Since M is semisimple over R there is an R -submodule N' such that $M = N \oplus N'$. If $\pi : M \rightarrow N$ is the projection map, then π is R -linear since N and N' are R -submodules, or equivalently, π is an element of R' . Any

element r'' in R'' commutes with π , and hence $r''N = (r'' \circ \pi)(M) = (\pi \circ r'')(M) \subseteq \pi(M) = N$. \square

Proof of Theorem 4.1 (following Bourbaki)

We first consider the case that X is a single element $\{x\}$ of M . The set $N = Rx$ is an R -submodule of M and hence also an R'' -submodule by the lemma above. The element x lies in N since R contains 1. If $r'' \in R''$ is any element, then $r''x \in N = Rx$, and hence there exists $r \in R$ such that $rx = r''x$.

Now let $X = \{x_1, x_2, \dots, x_n\}$ be any subset of M with n elements, and let $M^n = M \oplus M \oplus \dots \oplus M$ (n times). Note that M^n is an R -module, where the R -action on M^n is the diagonal action given by $r(m_1, m_2, \dots, m_n) = (rm_1, rm_2, \dots, rm_n)$ for $r \in R$ and $(m_1, m_2, \dots, m_n) \in M^n$. Moreover, M^n is semisimple over R since M is semisimple over R . Let $R'(n)$ denote $\text{End}_R(M^n)$ and let $R''(n)$ denote $\text{End}_{R''(n)}(M^n)$. Let R' and R'' act on M^n by the diagonal action $\xi(m_1, m_2, \dots, m_n) = (\xi m_1, \xi m_2, \dots, \xi m_n)$.

If $\varphi \in R'(n)$, then by Proposition 2.6 there exists a matrix $A = A(\varphi) \in M_n(R')$ such that for all $(m_1, m_2, \dots, m_n) \in M^n$ we have (*) $\varphi(m_1, m_2, \dots, m_n) = A(m_1, m_2, \dots, m_n) = (y_1, y_2, \dots, y_n)$, where $y_i = \sum_{j=1}^n A_{ij} m_j$. If $r'' \in R''$ is any element, then r'' commutes on M with the elements $\{A_{ij}\} \subseteq R'$, and it follows immediately from (*) that r'' commutes on M^n with all elements φ of $R'(n)$. This proves that $R'' \subseteq R''(n)$. By the case $n = 1$ above applied to the element $x = (x_1, x_2, \dots, x_n) \in M^n$ we know that for every element $r'' \in R'' \subseteq R''(n)$ there exists an element $r \in R$ such that $(rx_1, rx_2, \dots, rx_n) = rx = r''x = (r''x_1, r''x_2, \dots, r''x_n)$. Hence $rx_i = r''x_i$ for $1 \leq i \leq n$. \square

Applications of the Density Theorem

Proposition 4.3

Let A be a semisimple algebra that is finite dimensional over a field \mathcal{K} . Let M be a finitely generated A -module, and let $R = \rho(A)$, where $\rho : A \rightarrow \text{Hom}(M)$ is the ring homomorphism that defines the action of A . Let $R' = \text{End}_R(M)$ and $R'' = \text{End}_{R'}(M)$.

Then

- 1) $R = R'' \subseteq \text{End}_{\mathcal{K}}(M)$.
- 2) If M is a simple A -module and \mathcal{K} is algebraically closed, then $R = \text{End}_{\mathcal{K}}(M)$.

Proof

1) We showed in Proposition 2.4 that R, R' and R'' are all subalgebras of $\text{End}_{\mathcal{K}}(M)$. Note that R is a finite dimensional algebra over \mathcal{K} since A has this property. Hence M is a finite dimensional vector space over \mathcal{K} by the discussion in section 1.7. Let \mathcal{B} be a \mathcal{K} -basis of M , and let $r'' \in R''$ be given. By the density theorem there exists an element $r \in R$ such that $rx = r''x$ for all $x \in \mathcal{B}$. Since r and r'' are elements of $\text{End}_{\mathcal{K}}(M)$

with the same values on a basis it follows that $r = r''$. Hence $R'' \subseteq R$ and we observed earlier that the reverse inequality holds for any ring R .

2) Let M be a simple A -module, or equivalently a simple R -module, and let T be an element of R' . The elements of R commute with T and hence leave invariant every eigenspace of T . Since M is R -simple it follows that $T = c \text{Id}$ for some $c \in \mathcal{K}$. Hence $R' = \mathcal{K} \text{Id}$, and from 1) we conclude that $R = R'' = \text{End}_{R'}(M) = \text{End}_{\mathcal{K}}(M)$.

Corollary 4.4

Let G be a finite group, and let $\rho : G \rightarrow \text{GL}(V)$ be an irreducible representation of G on a finite dimensional complex vector space V . Then $\rho(\mathbb{C}[G]) = \text{End}_{\mathbb{C}}(V)$.

Proof

The group algebra $\mathbb{C}[G]$ is a semisimple algebra, and V is a simple $\mathbb{C}[G]$ -module. Now apply 2) of Proposition 4.3. \square

Corollary 4.5

Let G be a finite group, and let $\{\rho_i : G \rightarrow \text{GL}(V_i), 1 \leq i \leq r\}$ be a complete set, up to equivalence, of irreducible complex finite dimensional representations of G . Let $V = V_1 \oplus V_2 \oplus \dots \oplus V_r$, and let $\rho = \rho_1 + \rho_2 + \dots + \rho_r : G \rightarrow \text{GL}(V)$ denote the corresponding representation. Let $W = \text{End}_{\mathbb{C}}(V_1) \times \text{End}_{\mathbb{C}}(V_2) \times \dots \times \text{End}_{\mathbb{C}}(V_r) \subseteq \text{End}_{\mathbb{C}}(V)$. Then

- 1) If $R = \rho(\mathbb{C}[G])$, then $R' = \{T \in W : T = \lambda_i \text{Id on each } V_i \text{ for some } \lambda_i \in \mathbb{C}\}$.
- 2) $\rho : \mathbb{C}[G] \rightarrow W$ is an algebra isomorphism.

Proof

1) We note that $R' \subseteq \text{End}_{\mathbb{C}}(V)$ since $\mathbb{C} \subseteq R$. The subspaces $\{V_i : 1 \leq i \leq r\}$ are the isotypic components of V since the representations $\{\rho_i : G \rightarrow \text{GL}(V_i), 1 \leq i \leq r\}$ are inequivalent. By the Proposition in section 1.5 the projections $\pi_i : V \rightarrow V_i$ are elements of $R = \rho(\mathbb{C}[G])$; specifically, $\pi_i = \frac{d_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \rho(g)$, where χ_i is the character of the representation ρ_i and d_i is the dimension of V_i . Hence the elements of R' leave invariant each subspace V_i since they commute with the projections $\{\pi_i : V \rightarrow V_i, 1 \leq i \leq r\}$. This means that $R' \subseteq W$ by the definition of W . On V_i the elements of R' must be multiples of the identity since they commute with $\rho_i(G)$ and each V_i is an irreducible G -module. This completes the proof of 1)

2) It is evident that $\rho : \mathbb{C}[G] \rightarrow W$ is an algebra homomorphism. If d_i is the dimension of V_i , then $\dim_{\mathbb{C}} \text{End}_{\mathbb{C}}(V_i) = d_i^2$ for all i . As vector spaces over \mathbb{C} both $\mathbb{C}[G]$ and W have dimension $|G| = \sum_{i=1}^r d_i^2$. It suffices to prove that $\rho : \mathbb{C}[G] \rightarrow W$ is

surjective. Let $R = \rho(\mathbb{C}[G])$. Then $R = R'' \subseteq \text{End}_{\mathbb{C}}(V)$ by Proposition 4.3, and $R \subseteq W$ by the definitions of R and ρ . By 1) it follows that $R'' = W$. \square

Remark

In Proposition 6.10 below we shall obtain an explicit formula for the inverse of the isomorphism $\rho : \mathbb{C}[G] \rightarrow W$.

Section 5 Structure of simple rings

We begin this section with a useful basic result.

Proposition 5.1

Let R be a simple ring with 1.

- 1) If L and L' are simple left ideals, then $L' = La$ for some element a of R .
- 2) $LR = R$ for any left ideal L of R .
- 3) R has no proper 2-sided ideals.

Proof

We regard R as an R -module by letting R act on itself on the left. The R -submodules are then precisely the left ideals of R .

1) By Corollary 3.5 there exists an R -module isomorphism $\varphi : L \rightarrow L'$. Since R is semisimple there exists a left ideal M of R such that $R = L \oplus M$. The projection $\pi : R \rightarrow L$ lies in $\text{End}_R(R)$ as does the composition $\varphi \circ \pi : R \rightarrow L' \subseteq R$. By Proposition 2.6 there exists an element $a \in R$ such that $(\varphi \circ \pi)(x) = xa$ for all $x \in R$. In particular, $L' = (\varphi \circ \pi)(L) = La$.

2) If L is a left ideal of R , then $R = L_1 \oplus L_2 \dots \oplus L_k$, where each L_i is a left ideal isomorphic to L . By 1) we can find elements x_1, x_2, \dots, x_k in R such that $L_i = Lx_i$ for all i . Hence $L_i \subseteq LR$ for all i , and it follows that $LR \subseteq R = L_1 \oplus L_2 \dots \oplus L_k \subseteq LR$.

3) Let I be a nonzero 2-sided ideal of R . By Proposition 3.3, I is a semisimple R -module, and hence I contains a simple R -submodule L , which is a simple left ideal of R . Hence $R = LR \subseteq IR \subseteq I$ by 2), and we conclude that $I = R$. \square

We now prove the main result of this section

Theorem 5.2

Let R be a simple ring. Let L be a simple left ideal of R , and let $D = \text{End}_R(L)$, where L is regarded as a simple R -module with R acting on the left. Let n denote the number of simple left ideals in a direct sum decomposition of R . Then D is a division ring and R is ring isomorphic to $M_n(D^{\text{op}})$, where D^{op} denotes the division ring opposite to D .

Remark

Any two left ideals of a simple ring R are isomorphic to each other by Corollary 3.6 or Proposition 5.1. Hence D is uniquely determined up to isomorphism, and D is a division ring by Proposition 2.3. D -modules have no nonzero torsion elements since the nonzero elements of D are invertible. Hence any finitely generated D -module M is a free D -module whose rank depends only on M . Assuming the theorem above, the simple ring R is a free D -module of rank n^2 . This will prove that the number n of simple left ideals of R in a direct sum decomposition of R is independent of the decomposition.

From the theorem above, Proposition 2.5 and the fact that D^{op} is isomorphic to D for $D = \mathbb{R}, \mathbb{C}$ or \mathbb{H} we obtain

Corollary 5.3

Let R be a simple, finite dimensional algebra over a field \mathcal{K} .

- 1) If \mathcal{K} is algebraically closed, then R is isomorphic as an algebra to $M_n(\mathcal{K})$ for some positive integer n .
- 2) If $\mathcal{K} = \mathbb{R}$, then R is isomorphic as an algebra to $M_n(D)$ for some positive integer n , where $D = \mathbb{R}, \mathbb{C}$ or \mathbb{H} .

Proof of the theorem

Let L be a simple left ideal of R . Since R is a direct sum of simple left ideals, all of which are R -isomorphic to L by Corollary 3.5, we conclude that R is isomorphic to L^n , the direct sum of n copies of L for some positive integer n . By Propositions 2.3, 2.6 and 2.7 we obtain $R^{\text{op}} \cong \text{End}_R(R) \cong \text{End}_R(L^n) \cong M_n(D)$, where $D = \text{End}_R(L)$ is a division algebra. Here \cong means ring isomorphism.

If $\varphi : (R, \cdot) \rightarrow (S, \cdot)$ is an isomorphism of rings, then it is easy to check that $\varphi : (R, \#) \rightarrow (S, \#)$ is an isomorphism of rings, where $x\#y = y \cdot x$ in both R and S . Hence $R = (R^{\text{op}})^{\text{op}} \cong M_n(D)^{\text{op}}$ by the previous paragraph. The theorem will follow immediately from the next result.

Lemma

Let R be a ring with 1. Then $M_n(R)^{\text{op}}$ is ring isomorphic to $M_n(R^{\text{op}})$.

Proof

The proof is elementary, but one must be careful since four different multiplication operations are involved, two for R and R^{op} and two matrix multiplications for $M_n(R)$ and $M_n(R)^{\text{op}}$.

Recall that S and S^{op} are equal as sets and have the same additive operation $+$ for any ring S . Here if \cdot denotes the multiplication operation in R , then the multiplication

operation $\#$ in R^{op} is defined by $x\#y = y \cdot x$. If \circ denotes the usual matrix multiplication, then $(A \circ B)_{ij} = \sum_{k=1}^n A_{ik} \cdot B_{kj}$ for $A, B \in M_n(R)$, and $(C \circ D)_{ij} = \sum_{k=1}^n C_{ik} \# D_{kj}$ for $C, D \in M_n(R^{\text{op}})$. Let $*$ denote the opposite matrix multiplication in $M_n(R)^{\text{op}}$ given by $A * B = B \circ A$ for $A, B \in M_n(R)$.

Given a matrix A in $M_n(R)^{\text{op}}$ we let $\psi(A)$ be that matrix in $M_n(R^{\text{op}})$ such that $[\psi(A)]_{ij} = A_{ji}$ for all i, j .

Assertion The map $\psi : (M_n(R)^{\text{op}}, *) \rightarrow (M_n(R^{\text{op}}), \circ)$ is an isomorphism of rings.

Let A and $B \in M_n(R)^{\text{op}}$ be given. It is routine to show that $\psi(A+B) = \psi(A) + \psi(B)$, and we omit the details. For any integers $1 \leq i, j \leq n$ we have $[\psi(A * B)]_{ij} = [\psi(B \circ A)]_{ij} = (B \circ A)_{ji} = \sum_{k=1}^n B_{jk} \cdot A_{ki}$ since the entries of A and B lie in R . Since the entries of $\psi(A)$ and $\psi(B)$ lie in R^{op} we have $[\psi(A) \circ \psi(B)]_{ij} = \sum_{k=1}^n [\psi(A)]_{ik} \# [\psi(B)]_{kj} = \sum_{k=1}^n A_{ki} \# B_{jk} = \sum_{k=1}^n B_{jk} \cdot A_{ki} = [\psi(A * B)]_{ij}$. Hence $\psi(A * B) = \psi(A) \circ \psi(B)$ for all A, B in $M_n(R)^{\text{op}}$, which proves the lemma since ψ is a bijection. \square

As another corollary to Theorem 5.2 we obtain a description of the multiplicative center of a simple ring.

Corollary 5.4

Let R be a simple ring, and let $Z(R)$ denote the multiplicative center of R . Then $Z(R)$ is isomorphic to $Z(D)$, the center of the division ring $D = \text{End}_R(L)$, where L is a simple left ideal of R . In particular, $Z(R)$ is a field.

Examples

If $D = \mathbb{R}$ or \mathbb{C} , then $Z(D) = D$, while if $D = \mathbb{H}$, then $Z(D) \cong \mathbb{R}$. From Corollaries 5.3 and 5.4 we obtain immediately

Corollary 5.5

Let R be a simple, finite dimensional algebra over a field \mathcal{K} .

- 1) If \mathcal{K} is algebraically closed, then $Z(R)$ is isomorphic as an algebra to \mathcal{K} .
- 2) If $\mathcal{K} = \mathbb{R}$, then R is isomorphic as an algebra to either \mathbb{R} or \mathbb{C} .

Proof of Corollary 5.4

By Theorem 5.2 we know that R is ring isomorphic to $M_n(D^{\text{op}})$ for some positive integer n . Since $Z(D^{\text{op}}) = Z(D)$ it suffices to prove the following

Lemma

Let D be a division ring, and $R = M_n(D)$ denote the ring of $n \times n$ matrices with coefficients in D . Then $Z(R) = \{\lambda \text{ Id} : \lambda \in Z(D)\}$, where Id denotes the identity matrix and $Z(D)$ denotes the multiplicative center of D .

Proof of the Lemma

Clearly, if $\lambda \in Z(D)$, then $A = \lambda \text{ Id}$ lies in the center of R . Conversely, let $A = (A_{ij})$ be an element in the center of R .

We show first that $A_{ij} \in Z(D)$ for all i, j . Let $x \in D$ be given, and let $B = x \text{ Id}$. Then $A_{ij}x = (AB)_{ij} = (BA)_{ij} = xA_{ij}$ for all i, j . Hence $A_{ij} \in Z(D)$ for all i, j since $x \in D$ was arbitrary.

Next we assert that $A_{ij} = 0$ if $i \neq j$. Let i and j be distinct with $1 \leq i, j \leq n$. Let $B = \text{diag}(x_1, x_2, \dots, x_n)$ be a diagonal matrix such that x_i and x_j are distinct nonzero elements of D . Then $A_{ij}x_j = (AB)_{ij} = (BA)_{ij} = x_i A_{ij} = A_{ij}x_i$ since $A_{ij} \in Z(D)$. Hence $A_{ij} = 0$ since D is a division ring and x_i, x_j are distinct nonzero elements in D .

We have proved that if $A \in Z(D)$, then A is a diagonal matrix $\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$, where $\lambda_i \in Z(D)$ for all i . We show that entries $\{\lambda_i\}$ are all equal, which will conclude the proof. Given integers $i \neq j$ let $B \in M_n(D)$ be a matrix such that $B_{ij} \neq 0$. Then $\lambda_i B_{ij} = (AB)_{ij} = (BA)_{ij} = B_{ij} \lambda_j = \lambda_j B_{ij}$ since $\{\lambda_k\} \subseteq Z(D)$. Hence $\lambda_i = \lambda_j$ since $B_{ij} \neq 0$. \square

Section 6 Structure of semisimple rings

By definition a semisimple ring R is the direct sum of finitely many simple left ideals $\{L_\alpha\}$. By the proof of Corollary 3.5 any simple left ideal of R is isomorphic to one of the ideals $\{L_\alpha\}$. Hence there exists a finite collection $\{L_1, L_2, \dots, L_n\}$ of nonisomorphic simple left ideals such that any simple left ideal L is isomorphic to exactly one of the $\{L_i\}$.

For $1 \leq i \leq n$ let R_i denote the sum of all simple left ideals isomorphic to L_i . By definition an element of R_i is a finite sum $\sum_{\beta \in A} x_\beta$, where each x_β lies in a simple left ideal L isomorphic to L_i . Hence R_i is also a left ideal of R for $1 \leq i \leq n$.

Theorem 6.1

- 1) Each R_i is a simple ring and a two sided ideal in R for $1 \leq i \leq n$.
- 2) $R_i R_j = 0$ for $i \neq j$.
- 3) There exist elements $e_i \in R_i$, $1 \leq i \leq n$, such that

$$a) 1 = \sum_{i=1}^n e_i$$

$$b) e_i y_i = y_i e_i \text{ for every element } y_i \text{ in } R_i, 1 \leq i \leq n.$$

- 4) $R = R_1 \oplus R_2 \oplus \dots \oplus R_n$. Moreover, the map $r_1 + r_2 + \dots + r_n \rightarrow (r_1, r_2, \dots, r_n)$ is a ring isomorphism of R onto the direct product

$$R_1 \times R_2 \times \dots \times R_n .$$

- 5) The decomposition of R in 4) is unique up to the order of the factors ; that is, if $R = R_1^* \oplus R_2^* \oplus \dots \oplus R_m^*$ is a direct sum of commuting simple subrings, then $m = n$ and after reordering, $R_i^* = e_i R = R e_i$ for all i , where $\{e_1, e_2, \dots, e_n\}$ are the elements from 3).

Remark 6.2

The elements $\{e_1, e_2, \dots, e_n\}$ belong to the multiplicative center of R by 2) and 3) of the theorem.

Example 6.3

Let G be a finite group and let $R = \mathbb{C}[G]$. Let $\{\rho_i : G \rightarrow GL(V_i), 1 \leq i \leq r\}$ be a complete list, up to equivalence, of irreducible complex representations of G . In Corollary 4.5 we saw that $R = \mathbb{C}[G]$ is isomorphic to $\text{End}_{\mathbb{C}}(V_1) \times \text{End}_{\mathbb{C}}(V_2) \times \dots \times \text{End}_{\mathbb{C}}(V_r)$. Since $\text{End}_{\mathbb{C}}(V_i)$ is a simple ring for $1 \leq i \leq r$ the uniqueness assertion in 5) shows the following :

- 1) Each simple ring R_i in the decomposition of $R = \mathbb{C}[G]$ is isomorphic to $\text{End}_{\mathbb{C}}(V_i)$, where V_i is an irreducible complex G -module.
- 2) The number of simple rings in the decomposition of $R = \mathbb{C}[G]$ is the number of conjugacy classes of G .

From the discussion in section 1.5 we also conclude

- 3) $e_i = \frac{d_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g$, where χ_i is the character of the representation ρ_i and d_i is the dimension of V_i .

Example 6.4

Let R be a semisimple algebra that is finite dimensional over a field \mathcal{K} .

- 1) If \mathcal{K} is algebraically closed, then R is isomorphic to a direct product of simple rings $R_1 \times R_2 \times \dots \times R_n$, where each simple ring R_i is isomorphic to a matrix algebra $M_{n_i}(\mathcal{K})$ for some positive integers $\{n_i\}$.
- 2) If $\mathcal{K} = \mathbb{R}$, then R is isomorphic to a direct product of simple rings $R_1 \times R_2 \times \dots \times R_n$, where each simple ring R_i is isomorphic to a matrix algebra $M_{n_i}(D)$ for some positive integers $\{n_i\}$, where $D = \mathbb{R}, \mathbb{C}$ or \mathbb{H} .

Proof of example 6.4

This is an immediate consequence of Theorem 6.1 and Corollary 5.3. \square

Proof of Theorem 6.1

Let i and j be distinct integers, $1 \leq i, j \leq n$. If x_α and x_β are elements of simple left ideals L_α and L_β contained in R_i and R_j respectively, then $x_\alpha x_\beta \in L_\alpha L_\beta = \{0\}$ by Lemma 3.4. This proves

(a) $R_i R_j = \{0\}$ if $i \neq j$.

We note that

(b) $R = R_1 + R_2 + \dots + R_n$

since R is a direct sum of simple left ideals $\{L_\alpha\}$ and each L_α is contained in some R_i . For $1 \leq j \leq n$ we have $R_j \subseteq R_j R = R_j (R_1 + R_2 + \dots + R_n) = R_j$; $R_j \subseteq R_j$. The equality assertions follow from (a) and (b) while the inclusion assertions follow since R contains 1 and R_j is a left ideal. Hence all inclusions are equalities, which proves

(c) Each R_i is a two sided ideal in R .

Next, we assert

(d) $R = R_1 \oplus R_2 \oplus \dots \oplus R_n$, direct sum.

By (b) we may write (*) $1 = e_1 + e_2 + \dots + e_n$, where $e_i \in R_i$ for all i . We allow the possibility that $e_i = 0$ for some i and that the decomposition (*) is not unique. (Neither of these possibilities actually happens). It suffices to show that if $0 = \sum_{j=1}^n x_j$, where $x_j \in R_j$

for all j , then $x_j = 0$ for all j . If $x \in R_i$, then by (a) $x = 1 \cdot x = \sum_{j=1}^n e_j x = e_i x$. Hence for

any integer i we have $0 = e_i \cdot 0 = \sum_{j=1}^n e_i x_j = e_i x_i = x_i$. This proves (d). (Similarly, if $x \in$

R_i , then $x = x \cdot 1 = \sum_{j=1}^n x e_j = x e_i$.)

(e) Write (*) $1 = e_1 + e_2 + \dots + e_n$, where $e_i \in R_i$ for all i . Then

(i) The elements e_i are unique.

(ii) $e_i^2 = e_i$ for every i , and $e_i x_i = x_i = x_i e_i$ for all $x_i \in R_i$.

(iii) $e_i e_j = 0$ if $i \neq j$.

The assertion (i) follows from (d), and (iii) follows from (a). Assertion (ii) was proved in the proof of (d). The fact that the map (r_1, r_2, \dots, r_n) is a ring isomorphism of R onto the direct product $R_1 \times R_2 \times \dots \times R_n$ is an immediate consequence of (a) and (d).

It remains only to prove the uniqueness assertion (5) of the theorem. Write $R = R_1 \oplus R_2 \oplus \dots \oplus R_n$, direct sum, as in (d) above. Suppose we can write $R = R_1^* \oplus R_2^* \oplus \dots \oplus R_m^*$, direct sum, where each R_j^* is a simple ring. By the definition of simple ring each R_j^* is a direct sum of simple left ideals that are isomorphic to each other. By the discussion above the set $\{L_1, L_2, \dots, L_n\}$ of left ideals of R contains exactly one of each isomorphism type of left ideals. Moreover, for $1 \leq i \leq n$, the ring R_i is the sum of all left ideals isomorphic to L_i . Hence each R_j^* is contained in R_i for some unique i . It follows that $m \leq n$, and since $R = R_1 \oplus R_2 \oplus \dots \oplus R_n = R_1^* \oplus R_2^* \oplus \dots \oplus R_m^*$ we conclude that $m = n$ and $R_j^* = R_{\sigma j}$ for all j , where σ is some permutation of

$\{1, 2, \dots, n\}$. Finally, from (a), (d) and (e) above we have $e_i R = R e_i = R_i$ for every i . This completes the proof of the theorem. \square

Centers of semisimple rings

Proposition 6.5

Let R be a semisimple ring with 1, and let $R = R_1 \oplus R_2 \oplus \dots \oplus R_n$ be its decomposition into simple rings R_i , where $R_i R_j = \{0\}$ if $i \neq j$. Let $Z(R)$ denote the multiplicative center of R . Then $Z(R) = Z(R_1) \oplus Z(R_2) \oplus \dots \oplus Z(R_n)$, where $Z(R_i)$ is a field F_i for each i .

Proof

Let $z \in Z(R)$ and write $z = \sum_{i=1}^n z_i$, where $z_i \in R_i$ for every i . If $x_j \in R_j$, then $x_j z_j = \sum_{i=1}^n x_j z_i = x_j z_j = x_j (\sum_{i=1}^n z_i) = x_j z = z x_j = \sum_{i=1}^n z_i x_j = z_j x_j$. Hence $z_j \in Z(R_j)$ for all j . This proves that $Z(R) = Z(R_1) \oplus Z(R_2) \oplus \dots \oplus Z(R_n)$, which is isomorphic to the direct product $Z(R_1) \times Z(R_2) \times \dots \times Z(R_n)$. By Corollary 5.4 each ring $Z(R_i)$ is a field. \square

If R is a semisimple algebra that is finite dimensional over a field \mathcal{K} , then we can say more. Note that each simple factor R_i of R must also be a finite dimensional algebra over \mathcal{K} .

Corollary 6.6

Let R be a semisimple algebra that is finite dimensional over a field \mathcal{K} . Let $R = R_1 \oplus R_2 \oplus \dots \oplus R_n$ be its decomposition into simple finite dimensional algebras R_i over \mathcal{K} , where $R_i R_j = \{0\}$ if $i \neq j$. Then

- 1) If \mathcal{K} is algebraically closed, then $Z(R) \cong \mathcal{K} \times \mathcal{K} \times \dots \times \mathcal{K}$, n -times.
- 2) If $\mathcal{K} = \mathbb{R}$, then $Z(R) \cong F_1 \times F_2 \times \dots \times F_n$, where $F_i = \mathbb{R}$ or \mathbb{C} for each i .

Proof

Both assertions are immediate consequences of Proposition 6.5 and Corollary 5.5. \square

Centers of group algebras

Let G be a finite group and let \mathcal{K} be a field whose characteristic does not divide $|G|$. The group algebra $\mathcal{K}[G]$ is a finite dimensional algebra over \mathcal{K} , and $\mathcal{K}[G]$ is also semisimple (cf. Lang). We proved this in the case $\mathcal{K} = \mathbb{C}$ and the proof also works for the case $\mathcal{K} = \mathbb{R}$. We may sharpen the results above still further in the case $\mathcal{K} = \mathbb{C}$.

Proposition 6.7

Let G be a finite group, and let $R = \mathbb{C}[G]$. Then

- 1) $Z(R) \cong \mathbb{C} \times \mathbb{C} \times \dots \times \mathbb{C}$, r times, where r is the number of conjugacy classes of G .
- 2) The elements $\{e_1, e_2, \dots, e_r\}$ defined in example 1.5 form a basis for $Z(R)$, and these elements satisfy the relations $e_i^2 = e_i$ for $1 \leq i \leq r$ and $e_i e_j = 0$ if $i \neq j$.

Proof

1) By assertion 2) in the discussion of example 6.3 the number of simple rings R_i in the decomposition of R is precisely the number of conjugacy classes in G . Assertion 1) now follows from assertion 1) of Corollary 6.6.

2) By the discussion in example 1.5 we know that the elements $\{e_1, e_2, \dots, e_r\}$ are linearly independent in $\mathbb{C}[G]$ and \mathbb{C} -span $\{e_1, e_2, \dots, e_r\} \subseteq Z(R)$. Equality holds since $Z(R)$ has dimension r over \mathbb{C} by 1).

Further remarks on the center of $\mathbb{C}[G]$

Let G be a finite group, and let \mathcal{K} be a field whose characteristic does not divide the order of G . There is a completely different description of the multiplicative center of $\mathcal{K}[G]$, which we relate to the discussion above in the case that $\mathcal{K} = \mathbb{C}$.

In $\mathcal{K}[G]$ a conjugacy class is defined to be $\sum_{\sigma \in \mathcal{C}} \sigma$, the sum of all elements in a conjugacy class \mathcal{C} of G .

Proposition 6.8

If $R = \mathcal{K}[G]$, then the conjugacy classes form a basis over \mathcal{K} for $Z(R)$.

Proof

Let $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_r$ denote the conjugacy classes in G . Let $x_i \in \mathcal{K}[G]$ denote the sum of all elements in the conjugacy class \mathcal{C}_i for $1 \leq i \leq r$. We show first that the elements $\{x_1, x_2, \dots, x_r\}$ are linearly independent in $\mathcal{K}[G]$. Suppose $0 = \sum_{i=1}^r a_i x_i$ for some elements $\{a_1, a_2, \dots, a_r\}$ in \mathcal{K} . Then $0 = \sum_{i=1}^r a_i x_i = \sum_{\sigma \in \mathcal{C}} a_\sigma \sigma$, where $a_\sigma = a_i$ if $\sigma \in \mathcal{C}_i$. Since the elements of G are linearly independent in $\mathcal{K}[G]$ it follows that $a_\sigma = 0$ for all $\sigma \in G$ and hence $a_i = 0$ for all i , $1 \leq i \leq r$.

Next we show that the elements $\{x_1, x_2, \dots, x_r\}$ lie in the center of $R = \mathcal{K}[G]$. It suffices to show that $x_i \tau = \tau x_i$ for all i and all $\tau \in G$ since the elements of G generate the algebra $\mathcal{K}[G]$. We compute $x_i \tau = \sum_{\sigma \in \mathcal{C}_i} \sigma \tau = \tau \left\{ \sum_{\sigma \in \mathcal{C}_i} \tau^{-1} \sigma \right\} = \tau \left\{ \sum_{\xi \in \mathcal{C}_i} \xi \right\}$ (substituting ξ

$$= \tau^{-1} \sigma \tau) = \tau x_i.$$

Let $z \in \mathcal{K}[G]$ be an element from the center of $\mathcal{K}[G]$. We complete the proof by showing that z is a \mathcal{K} -linear combination of $\{x_1, x_2, \dots, x_r\}$. Write $z = \sum_{\sigma \in G} a_\sigma \sigma$, where $\{a_\sigma\} \subseteq \mathcal{K}$. Fix an element $\mu \in G$. Then $\mu z = \sum_{\sigma \in G} a_\sigma (\mu \sigma) = \sum_{\sigma \in G} a_\sigma (\mu \sigma \mu^{-1}) \mu = \left\{ \sum_{\xi \in G} a_{(\mu^{-1} \xi \mu)} \xi \right\} \mu$, substituting $\xi = \mu \sigma \mu^{-1}$. Since $z \mu = \left(\sum_{\xi \in G} a_\xi \xi \right) \mu$ and $z \mu = \mu z$ it follows that $\sum_{\xi \in G} a_{(\mu^{-1} \xi \mu)} \xi = \sum_{\xi \in G} a_\xi \xi$. Since G is a basis for $\mathcal{K}[G]$ this implies

$$(*) \quad a_{(\mu^{-1} \xi \mu)} = a_\xi \quad \text{for all } \xi \in G.$$

Since $\mu \in G$ was arbitrary we conclude that there exist constants $\{a_1, a_2, \dots, a_r\}$ in \mathcal{K} such that $a_\sigma = a_i$ for all $\sigma \in \mathcal{C}_i$, $1 \leq i \leq r$. Hence $z = \sum_{\sigma \in G} a_\sigma \sigma = \sum_{i=1}^r a_i x_i$. \square

In the case that $\mathcal{K} = \mathbb{C}$ we obtain an explicit description of the transition matrix between the two bases of $Z(\mathbb{C}[G])$ that we have discussed: the elements $\{e_1, e_2, \dots, e_r\}$, which were defined in section 1.5, and the conjugacy classes $\{x_1, x_2, \dots, x_r\}$ defined above.

Proposition 6.9

Let G be a finite group, and let $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_r$ be the conjugacy classes of G . For $1 \leq i \leq r$, fix an element τ_i in each conjugacy class \mathcal{C}_i , and let $x_i \in \mathbb{C}[G]$ denote the sum of the elements in the conjugacy class \mathcal{C}_i .

Let $\{\rho_i : G \rightarrow GL(V_i), 1 \leq i \leq r\}$ be a complete list, up to equivalence, of the complex irreducible representations of G , and let $\chi_i : G \rightarrow \mathbb{C}$ denote the character of ρ_i . For $1 \leq i, j \leq r$ define $A_{ij} = (d_i / |G|) \chi_i(\tau_j^{-1})$, where $d_i = \dim V_i$. For $1 \leq i \leq r$ let $e_i = \frac{d_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g$. Then

$$(*) \quad e_i = \sum_{j=1}^r A_{ij} x_j.$$

Remark

If g and h are conjugate elements in a group G , then g^{-1} and h^{-1} are also conjugate elements in G . Hence $\chi_i(\tau_j^{-1})$ does not depend on the choice of τ_j in \mathcal{C}_j since the characters $\{\chi_i\}$ are class functions.

Proof of the proposition

Let $1 \leq i \leq r$ be given. Since the elements of G form a basis of $\mathbb{C}[G]$ we can write $e_i = \sum_{\sigma \in G} a_\sigma \sigma$ for some constants $\{a_\sigma\} \subseteq \mathbb{C}$. Let $\chi_{\text{reg}} : G \rightarrow \mathbb{C}$ denote the character of the

regular representation of G . As in section 1.5 we recall that i) $\chi_{\text{reg}}(g) = 0$ if $g \neq 1$, ii) $\chi_{\text{reg}}(1) = |G|$ and iii) $\chi_{\text{reg}} = \sum_{i=1}^r d_i \chi_i$, where $d_i = \dim V_i$. From i) and ii) we compute $\chi_{\text{reg}}(e_i \tau^{-1}) = \sum_{\sigma \in G} a_{\sigma} \chi_{\text{reg}}(\sigma \tau^{-1}) = |G| a_{\tau}$ for all $\tau \in G$. From iii) and from d) of the proposition in section 1.5 we obtain $\chi_{\text{reg}}(e_i \tau^{-1}) = \sum_{j=1}^r d_j \chi_j(e_i \tau^{-1}) = d_i \chi_i(e_i \tau^{-1}) = d_i \chi_i(\tau^{-1})$. Hence $a_{\tau} = (d_i / |G|) \chi_i(\tau^{-1})$. If τ belongs to the conjugacy class \mathbb{C}_j , which contains τ_j , then $\chi_i(\tau^{-1}) = \chi_i(\tau_j^{-1})$ and $a_{\tau} = (d_i / |G|) \chi_i(\tau^{-1}) = (d_i / |G|) \chi_i(\tau_j^{-1}) = A_{ij}$. Hence $a_{\tau} = a_{\sigma} = A_{ij}$ for any two elements τ, σ in \mathbb{C}_j , which completes the proof of (*). \square

Although it is somewhat out of place logically, the next result, which describes the inverse of the algebra homomorphism in Corollary 4.5, is similar in appearance and proof to the result above.

Proposition 6.10

Let G be a finite group, and let $\{\rho_i : G \rightarrow \text{GL}(V_i), 1 \leq i \leq r\}$ be a complete set, up to equivalence, of irreducible complex finite dimensional representations of G . Let $V = V_1 \oplus V_2 \oplus \dots \oplus V_r$, and let $\rho = \rho_1 + \rho_2 + \dots + \rho_r : G \rightarrow \text{GL}(V)$ denote the corresponding representation. Let $W = \text{End}_{\mathbb{C}}(V_1) \times \text{End}_{\mathbb{C}}(V_2) \times \dots \times \text{End}_{\mathbb{C}}(V_r) \subseteq \text{End}_{\mathbb{C}}(V)$. Then $\sigma = \rho^{-1} : W \rightarrow \mathbb{C}[G]$ is given by

$$\sigma(T) = \sum_{g \in G} b_g(T) g$$

where for each element g of G , $b_g \in \text{Hom}(W, \mathbb{C})$ is given by

$$b_g(T) = \frac{1}{|G|} \sum_{i=1}^r d_i \text{Trace}_{V_i} \{\rho_i(g^{-1}) \circ T_i\},$$

with $T = (T_1, T_2, \dots, T_r)$, $T_i \in \text{End}_{\mathbb{C}}(V_i)$, an arbitrary element of W , $d_i = \dim V_i$.

Proof

Recall that $\rho : \mathbb{C}[G] \rightarrow W$ is an algebra isomorphism by Corollary 4.5. It is easy to see that b_g is a linear function on W for each element g of G . Hence $\sigma : W \rightarrow \mathbb{C}[G]$ is linear. It suffices to show that $(\sigma \circ \rho)(h) = h$ for all elements h of G since G is a basis of

$\mathbb{C}[G]$ over \mathbb{C} . For $h, g \in G$ we compute $b_g(\rho(h)) = \frac{1}{|G|} \sum_{i=1}^r d_i \text{Trace}_{V_i} \{ \rho_i(g^{-1}) \circ \rho_i(h) \} =$
 $\frac{1}{|G|} \sum_{i=1}^r d_i \text{Trace}_{V_i} \{ \rho_i(g^{-1}h) \} = \frac{1}{|G|} \sum_{i=1}^r d_i \chi_i(g^{-1}h)$. Hence $\sigma(\rho(h)) = \sum_{g \in G} b_g(\rho(h)) g =$
 $\frac{1}{|G|} \sum_{g \in G} \{ \sum_{i=1}^r d_i \chi_i(g^{-1}h) \} g = \frac{1}{|G|} \sum_{g \in G} \{ \chi_{\text{reg}}(g^{-1}h) \} g = h$ by the properties of χ_{reg} that
 were used in the proof of Proposition 6.9 and also in section 1.5. We have proved that
 $(\sigma \circ \rho)(h) = h$ for all elements h of G . \square