6

Semisimple Algebras

1 Semisimple Algebras

1.1 Semisimple Representations

One of the main themes of our theory will be related to completely reducible representations. It is thus important to establish these notions in full detail and generality.

Definition 1. Let S be a set of operators acting on a vector space U.

(i) We say that the vector space U is *irreducible* or *simple* under the given set S of operators if the only subspaces of U which are stable under S are 0 and U.
(ii) We say that the vector space U is *completely reducible* or *semisimple* under the given set S of operators if U decomposes as a direct sum of S-stable irreducible subspaces.
(iii) We say that the vector space U is *indecomposable* under the given set S of operators if the space U cannot be decomposed in the direct sum of two nontrivial S-stable subspaces.

A space is irreducible if and only if it is completely reducible and indecomposable.

The previous notions are essentially notions of the theory of modules. In fact, let S be a set of linear operators acting on a vector space U. From S, taking linear combinations and products, we can construct an algebra $\mathcal{E}(S)$[41] of linear operators on U. U is then an $\mathcal{E}(S)$-module. It is clear that a subspace $W \subset U$ is stable under S if and only if it is stable under the algebra $\mathcal{E}(S)$, so the notions introduced for S are equivalent to the same notions for $\mathcal{E}(S)$.

A typical example of completely reducible sets of operators is the following. Let $U = \mathbb{C}^n$ and let S be a set of matrices. For a matrix A let $A^* = \overline{A}^t$ be its adjoint (Chapter 5, 3.8). For a set S of matrices we denote by S^* the set of elements A^*, $A \in S$.

Lemma 1. *If a subspace M of $\mathbb{C}^n$ is stable under A, then $M^{\perp}$ (the orthogonal under the Hermitian product) is stable under A^*.*

[41] This is sometimes called the *envelope* of S.

Proof. If $m \in M, u \in M^{\perp}$, we have $(m, A^*u) = (Am, u) = 0$ since M is A stable. Thus $A^*u \in M^{\perp}$. □

Proposition 1. *If $S = S^*$, then $\mathbb{C}^n$ is the orthogonal sum of irreducible submodules, in particular it is semisimple.*

Proof. Take an S-stable subspace M of $\mathbb{C}^n$ of minimal dimension. It is then necessarily irreducible. Consider its orthogonal complement $M^{\perp}$. By adjunction and the previous lemma we get that $M^{\perp}$ is S stable and $\mathbb{C}^n = M \oplus M^{\perp}$.

We then proceed in the same way on $M^{\perp}$. □

A special case is when S is a group of unitary operators. More generally, we say that S is *unitarizable* if there is a Hermitian product for which the operators of S are unitary. If we consider a matrix mapping the standard basis of $\mathbb{C}^n$ to a basis orthonormal for some given Hermitian product we see

Lemma 2. *A set of matrices is unitarizable if and only if it is conjugate to a set of unitary matrices.*

These ideas have an important consequence.

Theorem 1. *A finite group G of linear operators on a finite-dimensional complex space U is unitarizable and hence the module is semisimple.*

Proof. We fix an arbitrary positive Hermitian product (u, v) on U. Define a new Hermitian product as

$$\langle u, v\rangle := \frac{1}{|G|}\sum_{g\in G}(gu, gv). \tag{1.1.1}$$

Then $\langle hu, hv\rangle = \frac{1}{|G|}\sum_{g\in G}(ghu, ghv) = \frac{1}{|G|}\sum_{g\in G}(gu, gv) = \langle u, v\rangle$ and G is unitary for this new product. If G was already unitary the new product coincides with the initial one. □

The previous theorem has a far-reaching generalization, by replacing the average given by the sum with an integral, as we will see in Chapter 8 where we prove among other things:

Theorem 3. *A compact group G of linear operators on a finite-dimensional complex space U is unitarizable and hence the module is semisimple.*

1.2 Self-Adjoint Groups

For noncompact groups there is an important class that we have already introduced for which similar results are valid. These are the self-adjoint subgroups of $GL(n, \mathbb{C})$, i.e., the subgroups H such that $A \in H$ implies $A^* \in H$.

For a self-adjoint group on a given (finite-dimensional) Hilbert space U the orthogonal of every invariant subspace is also invariant; thus any subspace or quotient module of U is completely reducible.

Take a self-adjoint group G and consider its induced action on the tensor algebra. The tensor powers of $U = \mathbb{C}^n$ have an induced canonical Hermitian form for which

$$\langle u_1 \otimes u_2 \otimes \cdots \otimes u_n | v_1 \otimes v_2 \otimes \cdots \otimes v_n \rangle = \langle u_1 | v_1 \rangle \langle u_2 | v_2 \rangle \cdots \langle u_n | v_n \rangle.$$

It is clear that this is a positive Hermitian form for which the tensor power of an orthonormal basis is also an orthonormal basis.

The map $g \to g^{\otimes n}$ is compatible with adjunction, i.e., $(g^*)^{\otimes n} = (g^{\otimes n})^*$:

$$(g^{\otimes m}(v_1 \otimes v_2 \otimes \cdots \otimes v_m) | w_1 \otimes W_2 \otimes \cdots \otimes w_m) := \prod_{i=1}^{m} (g v_i | w_i)$$

$$= \prod_{i=1}^{m} (v_i | g^* w_i) = (v_1 \otimes v_2 \otimes \cdots \otimes v_m | (g^*)^{\otimes m}(w_1 \otimes w_2 \otimes \cdots \otimes w_m)).$$

Thus:

Proposition. *If G is self-adjoint, the action of G on $T(U)$ is self-adjoint, hence all tensor powers of U are completely reducible under G.*

Corollary. *The action of G on the polynomial ring $\mathcal{P}(U)$ is completely reducible.*

Proof. The action of G on U^* is self-adjoint, so it is also self-adjoint on $T(U^*)$, and $\mathcal{P}(U)$ is a graded quotient of $T(U^*)$. □

1.3 Centralizers

It is usually more convenient to use the language of modules since the irreducibility or complete reducibility of a space U under a set S of operators is clearly equivalent to the same property under the subalgebra of operators generated by S.

Let us recall that in Chaper 1, §3.2, given a group G, one can form its *group algebra* $F[G]$. Every linear representation of G extends by linearity to an $F[G]$-module, and conversely. A map between $F[G]$ modules is a (module) homomorphism if and only if it is G-equivariant. Thus from the point of view of representation theory it is equivalent to studying the category of G representations or that of $F[G]$ modules.

We thus consider a ring R and its modules, using the same definitions for reducible, irreducible modules. We define $R^\vee$ to be the set of (isomorphism classes) of irreducible modules of R. We may call it the *spectrum* of R.

Given an irreducible module N we will say that it is of *type* α if $\alpha \in R^\vee$ is its isomorphism class.

Given a set S of operators on U we set $S' := \{A \in \mathrm{End}(U) | As = sA, \forall s \in S\}$. S' is called the *centralizer* of S. Equivalently S' should be thought of as the set of all S-linear endomorphisms. One immediately verifies:

Proposition 1.

(i) S' *is an algebra.*
(ii) $S \subset S''$.
(iii) $S' = S'''$.

The centralizer of the operators induced by R in a module M is also usually indicated by $\hom_R(M, M)$ or $\mathrm{End}_R(M)$ and called the *endomorphism ring.*

Any ring R can be considered as a module on itself by left multiplication (and as a module on the opposite of R by right multiplication).

Definition 1. R considered as module over itself is called *the regular representation.*

Of course, for the regular representation, a submodule is the same as a left ideal. An irreducible submodule is also referred to as a *minimal left ideal.*

A trivial but useful fact on the regular representation is:

Proposition 2. *The ring of endomorphisms of the regular representation is the opposite of R acting by right multiplications.*

Proof. Letting $f \in \mathrm{End}_R(R)$ we have $f(a) = f(a1) = af(1)$ by linearity, thus f is the right multiplication by $f(1)$.

Given two homomorphisms f, g we have $fg(1) = f(g(1)) = g(1)f(1)$, and so the mapping $f \to f(1)$ is an isomorphism between $\mathrm{End}_R(R)$ and R^o. □

Exercise. Another action of some interest is the action of $R \otimes R^o$ on R given by $a \otimes b(c) := acb$; in this case the submodules are the two-sided ideals and the centralizer is easily seen to be the *center* of R.

One can generalize the previous considerations as follows. Let R be a ring.

Definition 2. A cyclic module is a module generated by a single element.

A cyclic module should be thought of as the linear analogue of a single orbit. The structure of cyclic modules is quite simple. If M is generated by an element m, we have the map $\varphi : R \to M$ given by $\varphi(r) = rm$ (analogue of the orbit map).

By hypothesis φ is surjective, its kernel is a left ideal J, and so M is identified with R/J. Thus a module is cyclic if and only if it is a quotient of the regular representation.

Example. Consider $M_n(F)$, the full ring of $n \times n$ matrices over a field F. As a module we take F^n and in it the basis element e_1.

Its annihilator is the left ideal I_1 of matrices with the first column 0. In this case though we have a more precise picture.

Let J_1 denote the left ideal of matrices having 0 in all columns except for the first. Then $M_n(F) = J_1 \oplus I_1$ and the map $a \to ae_1$ restricted to J_1 is an isomorphism.

In fact we can define in the same way J_i (the matrices with 0 outside the i^{th} column).

Proposition 3. *$M_n(F) = \bigoplus_{i=1}^n J_i$ is a direct sum of the algebra $M_n(F)$ into irreducible left ideals isomorphic, as modules, to the representation F^n.*

Remark. This proof, with small variations, applies to a division ring D in place of F.

Lemma. *The module D^n is irreducible. We will call it the standard module of $M_n(D)$.*

Proof. Let us consider a column vector u with its i^{th} coordinate u_i nonzero. Acting on u with a diagonal matrix which has u_i^{-1} in the i^{th} position, we transform u into a vector with i^{th} coordinate 1. Acting with elementary matrices we can make all the other coordinates 0. Finally, acting with a permutation matrix we can bring 1 into the first position. This shows that any submodule contains the vector of coordinates $(1, 0, 0, \ldots, 0)$. This vector, in turn, generates the entire space again acting on it by elementary matrices. □

Theorem. *The regular representation of $M_n(D)$ is the direct sum of n copies of the standard module.*

Proof. We decompose $M_n(D)$ as direct sum of its columns. □

Remark. In order to understand $M_n(D)$ as module endomorphisms we have to take D^n as a *right* vector space over D or as a left vector space over D^o.

As done for groups in Chapter 1, §3.1, given two cyclic modules R/J, R/I we can compute $\hom_R(R/J, R/I)$ as follows.

Letting $f : R/J \to R/I$ be a homomorphism and $\bar{1} \in R/J$ is the class of 1, set $f(\bar{1}) = \bar{x}$, $x \in R$ so that $f : r\bar{1} \to r\bar{x}$. We must have then $J\bar{x} = f(J\bar{1}) = 0$, hence $Jx \subset I$. Conversely, if $Jx \subset I$ the map $f : r\bar{1} \to r\bar{x}$ is a well-defined homomorphism.

Thus if we define the set $(I : J) := \{x \in R | Jx \subset I\}$, we have

$$I \subset (I : J), \quad \hom_R(R/J, R/I) = (I : J)/I.$$

In particular for $J = I$ we have the *idealizer,* $\mathcal{I}(I)$ of I, $\mathcal{I}(I) := \{x \in R | Ix \subset I\}$.

The idealizer is the maximal subring of R in which I is a two-sided ideal, and $\mathcal{I}(I)/I$ is the ring $\hom_R(R/I, R/I) = \mathrm{End}_R(R/I)$.

1.4 Idempotents

It is convenient in the structure theory of algebras to introduce the simple idea of idempotent elements.

Definition. An idempotent in an algebra R, is an element e, such that $e^2 = e$. Two idempotents e, f are *orthogonal* if $ef = fe = 0$; in this case $e + f$ is also an idempotent.

Exercise. In a ring R consider an idempotent e and set $f := 1 - e$. We have the decomposition

$$R = eRe \oplus eRf \oplus fRe \oplus fRf$$

which presents R as matrices:

$$R = \begin{vmatrix} eRe & eRf \\ fRe & fRf \end{vmatrix}.$$

Prove that $\mathrm{End}_R(Re) = eRe$.

1.5 Semisimple Algebras

The example of matrices suggests the following:

Definition. A ring R is *semisimple* if it is semisimple as a left module on itself.

This definition is a priori not symmetric although it will be proved to be so from the structure theorem of semisimple rings.

Remark. Let us decompose a semisimple ring R as direct sum of irreducible left ideals. Since 1 generates R and 1 is in a finite sum we see:

Proposition 1. *A semisimple ring is a direct sum of finitely many minimal left ideals.*

Corollary. *If D is a division ring then $M_n(D)$ is semisimple.*

We wish to collect some examples of semisimple rings.
First, from the results in 1.1 and 1.2 we deduce:

Maschke's Theorem. *The group algebra $\mathbb{C}[G]$ of a finite group is semisimple.*

Remark. In fact it is not difficult to generalize to an arbitrary field. We have (cf. [JBA]):

The group algebra $F[G]$ of a finite group over a field F is semisimple if and only if the characteristic of F does not divide the order of G.

Next we have the obvious fact:

Proposition 2. *The direct sum of two semisimple rings is semisimple.*

In fact we let the following simple exercise to the reader.

Exercise. Decomposing a ring A in a direct sum of two rings $A = A_1 \oplus A_2$ is equivalent to giving an element $e \in A$ such that

$$e^2 = e, \ ea = ae, \ \forall a \in A,$$

$$A_1 = Ae, A_2 = A(1-e) \qquad e \text{ is called a } \textit{central idempotent}.$$

Having a central idempotent e, every A module M decomposes canonically as the direct sum $eM \oplus (1-e)M$. Where eM is an A_1 module, $(1-e)M$ an A_2 module. Thus the module theory of $A = A_1 \oplus A_2$ reduces to the ones of A_1, A_2.

From the previous corollary, Proposition 2, and these remarks we deduce:

Theorem. *A ring $A := \bigoplus_i M_{n_i}(D_i)$, with the D_i division rings, is semisimple.*

1.6 Matrices over Division Rings

Our next task will be to show that also the converse to Theorem 1.5 is true, i.e., that every semisimple ring is a finite direct sum of rings of type $M_m(D)$, D a division ring.

For the moment we collect one further remark. Let us recall that:

Definition. A ring R is called *simple* if it does not possess any nontrivial two-sided ideals, or equivalently, if R is irreducible as a module over $R \otimes R^o$ under the left and right action $(a \otimes b)r := arb$.

This definition is slightly confusing since a simple ring is by no means semisimple, unless it satisfies further properties (the d.c.c. on left ideals [JBA]).

A classical example of an infinite-dimensional simple algebra is the algebra of differential operators $F\langle x_i, \frac{\partial}{\partial x_i}\rangle$ (F a field of characteristic 0) (cf. [Cou]).

We have:

Proposition. *If D is a division ring, $M_m(D)$ is simple.*

Proof. Let I be a nontrivial two-sided ideal, $a \in I$ a nonzero element. We write a as a linear combination of elementary matrices $a = \sum a_{ij}e_{ij}$; thus $e_{ii}ae_{jj} = a_{ij}e_{ij}$ and at least one of these elements must be nonzero. Multiplying it by a scalar matrix we can obtain an element e_{ij} in the ideal I. Then we have $e_{hk} = e_{hi}e_{ij}e_{jk}$ and we see that the ideal coincides with the full ring of matrices. □

Exercise. The same argument shows more generally that for any ring A the ideals of the ring $M_m(A)$ are all of the form $M_m(I)$ for I an ideal of A.

1.7 Schur's Lemma

We start the general theory with the following basic fact:

Theorem (Schur's lemma). *The centralizer $\Delta := \mathrm{End}_R(M)$ of an irreducible module M is a division ring.*

Proof. Let $a : M \to M$ be a nonzero R-linear endomorphism. Its kernel and image are submodules of M. Since M is irreducible and $a \neq 0$ we must have $\mathrm{Ker}(a) = 0$, $\mathrm{Im}(a) = M$, hence a is an isomorphism and so it is invertible. This means that every nonzero element in Δ is invertible. This is the definition of a division ring. □

This lemma has several variations. The same proof shows that:

Corollary. *If $a : M \to N$ is a homomorphism between two irreducible modules, then either $a = 0$ or a is an isomorphism.*

1.8 Endomorphisms

A particularly important case is when M is a finite-dimensional vector space over $\mathbb{C}$. In this case since the only division ring over $\mathbb{C}$ is $\mathbb{C}$ itself, we have that:

Theorem. *Given an irreducible set S of operators on a finite-dimensional space over $\mathbb{C}$, then its centralizer S' is formed by the scalars $\mathbb{C}$.*

Proof. Rather than applying the structure theorem of finite-dimensional division algebras one can argue that, given an element $x \in S'$ and an eigenvalue α of x, the space of eigenvectors of x for this eigenvalue is stable under S and so, by irreducibility, it is the whole space. Hence $x = \alpha$. □

Remarks. 1. If the base field is the field of real numbers, we have (according to the theorem of Frobenius (cf. [Her])) three possibilities for Δ: $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$, the algebra of quaternions.

2. It is not necessary to assume that M is finite dimensional: it is enough to assume that it is of countable dimension.

Sketch of proof of the remarks. In fact M is also a vector space over Δ and so Δ, being isomorphic to an $\mathbb{R}$-subspace of M, is also countably dimensional over $\mathbb{R}$.

This implies that every element of Δ is algebraic over $\mathbb{R}$. Otherwise Δ would contain a field isomorphic to the rational function field $\mathbb{R}(t)$ which is impossible, since this field contains the uncountably many linearly independent elements $1/(t-r)$, $r \in \mathbb{R}$.

Now one can prove that a division algebra[42] over $\mathbb{R}$ in which every element is algebraic is necessarily finite dimensional,[43] and thus the theorem of Frobenius applies. □

Our next task is to prove the converse of Theorem 1.5, that is, to prove that every semisimple algebra A is a finite direct sum of matrix algebras over division algebras (Theorem 1.9). In order to do this we start from a general remark about matrices.

Let $M = M_1 \oplus M_2 \oplus M_3 \oplus \cdots \oplus M_k$ be an R-module decomposed in a direct sum.

For each i, j, consider $A(j,i) := \hom_R(M_i, M_j)$. For three indices we have the composition map $A(k,j) \times A(j,i) \to A(k,i)$.

The groups $A(j,i)$ together with the composition maps allow us to recover the full endomorphism algebra of M as *block matrices*:

$$A = (a_{ji}), \ a_{ji} \in A(j,i).$$

(One can give a formal abstract construction starting from the associativity properties).

---

[42] When we want to stress the fact that a division ring Δ contains a field F in the center, we say that Δ is a division algebra over F.

[43] This depends on the fact that every element of Δ algebraic over $\mathbb{R}$ satisfies a quadratic polynomial.

In more concrete form let $e_i \in \mathrm{End}(M)$ be the projection on the summand M_i with kernel $\bigoplus_{j\neq i} M_j$. The elements e_i are *a complete set of orthogonal idempotents in* $\mathrm{End}(M)$, i.e., they satisfy the properties

$$e_i^2 = e_i,\ e_ie_j = e_je_i = 0,\ i \neq j, \text{ and } \sum_{i=1}^k e_i = 1.$$

When we have in a ring S such a set of idempotents we decompose S as

$$S = \left(\sum_{i=1}^k e_i\right) S \left(\sum_{i=1}^k e_i\right) = \bigoplus_{i,j} e_iSe_j.$$

This sum is direct by the orthogonality of the idempotents.

We have $e_iSe_je_jSe_k \subset e_iSe_k$, $e_iSe_je_hSe_k = 0$, when $j \neq h$. In our case $S = \mathrm{End}_R(M)$ and $e_iSe_j = \hom_R(M_j, M_i)$.

In particular assume that the M_i are all isomorphic to a module N and let $A := \mathrm{End}_R(N)$. Then

$$\mathrm{End}_R(N^{\oplus k}) = M_k(A). \tag{1.8.1}$$

Assume now that we have two modules N, P such that $\hom_R(N, P) = \hom_R(P, N) = 0$. Let $A := \mathrm{End}_R(N)$, $B := \mathrm{End}_R(P)$; then

$$\mathrm{End}_R(N^{\oplus k} \oplus P^{\oplus h}) = M_k(A) \oplus M_h(B).$$

Clearly we have a similar statement for several modules.

We can add together all these remarks in the case in which a module M is a finite direct sum of irreducibles.

Assume $N_1, N_2, \dots, N_k$ are the distinct irreducible which appear with multiplicities $h_1, h_2, \dots, h_k$ in M. Let $D_i = \mathrm{End}_R(N_i)$ (a division ring). Then

$$\mathrm{End}_R\left(\bigoplus_{i=1}^k N_i^{h_i}\right) = \bigoplus_{i=1}^k M_{h_i}(D_i). \tag{1.8.2}$$

1.9 Structure Theorem

We are now ready to characterize semisimple rings. If R is semisimple we have that $R = \bigoplus_{i=1}^k N_i^{m_i}$ (as in the previous section) as a left R module; then

$$R^o = \mathrm{End}_R(R) = \mathrm{End}_R(\bigoplus_{i\in I} N_i^{m_i}) = \bigoplus_{i\in I} M_{m_i}(\Delta_i).$$

We deduce that $R = R^{oo} = \bigoplus_{i\in I} M_{m_i}(\Delta_i)^o$.

The opposite of the matrix ring over a ring A is the matrices over the opposite ring (use transposition) and so we deduce finally:

Theorem. *A semisimple ring is isomorphic to the direct sum of matrix rings R_i over division rings.*

Some comments are in order.

1. We have seen that the various blocks of this sum are simple rings. They are thus distinct irreducible representations of the ring $R \otimes R^o$ acting by the left and right action.

   We deduce that the matrix blocks are minimal two-sided ideals. From the theory of isotypic components which we will discuss presently, it follows that the only ideals of R are direct sums of these minimal ideals.
2. We have now the left-right symmetry: if R is semisimple, so is R^o.

Since any irreducible module N is cyclic, there is a surjective map $R \to N$. This map restricted to one of the N_i must be nonzero, hence:

Corollary 1. *Each irreducible R module is isomorphic to one of the N_i (appearing in the regular representation).*

Let us draw another consequence, a very weak form of a more general theorem.

Corollary 2. *For a field F every automorphism ϕ of the F-algebra $M_n(F)$ is inner.*

Proof. Recall that an inner automorphism is an automorphism of the form $X \mapsto AXA^{-1}$. Given ϕ we define a new module structure F^n_ϕ on the standard module F^n by setting $X \circ_\phi v := \phi(X)v$. Clearly F^n_ϕ is still irreducible and so it is isomorphic to F^n. We have thus an isomorphism (given by an invertible matrix A) between F^n and F^n_ϕ. By definition then, for every $X \in M_n(F)$ and every vector $v \in F^n$ we must have $\phi(X)Av = AXv$, hence $\phi(X)A = AX$ or $\phi(X) = AXA^{-1}$. □

A very general statement by Skolem–Noether is discussed in [Jac-BA2], Theorem 4.9.

2 Isotypic Components

2.1 Semisimple Modules

We will complete the theory with some general remarks:

Lemma 1. *Given a module M and two submodules A, B such that A is irreducible, either $A \subset B$ or $A \cap B = 0$.*

Proof. Trivial since $A \cap B$ is a submodule of A and A is irreducible. □

Lemma 2. *Given a module M a submodule N and an element $m \notin N$ there exists a maximal submodule $N_0 \supset N$ such that $m \notin N_0$. M/N_0 is indecomposable.*

Proof. Consider the set of all submodules containing N and which do not contain m. This has a maximal element since it satisfies the hypotheses of Zorn's lemma; call this maximal element N_0. Suppose we could decompose M/N_0. Since the class of m cannot be contained in both summands we could find a larger submodule not containing m. □

The basic fact on semisimple modules is the following:

Theorem. *For a module M the following conditions are equivalent:*

(i) M is a sum of irreducible submodules.
(ii) Every submodule N of M admits a complement, i.e., a submodule P such that $M = N \oplus P$.
(iii) M is completely reducible.

Proof. This is a rather abstract theorem and the proof is correspondingly abstract.

Clearly (iii) implies (i), so we prove (i) implies (ii) implies (iii).

(i) implies (ii). Assume (i) holds and write $M = \sum_{i \in I} N_i$ where I is some set of indices.

For a subset A of I set $N_A := \sum_{i \in A} N_i$. Let N be a given submodule and consider all subsets A such that $N \cap N_A = 0$. It is clear that these subsets satisfy the conditions of Zorn's lemma and so we can find a maximal set among them; let this be A_0. We have then the submodule $N \oplus N_{A_0}$ and claim that $M = N \oplus N_{A_0}$.

For every $i \in I$ consider $(N \oplus N_{A_0}) \cap N_i$. If $(N \oplus N_{A_0}) \cap N_i = 0$ we have that $i \notin A_0$. We can add i to A_0 getting a contradiction to the maximality.

Hence by the first lemma $N_i \subset (N \oplus N_{A_0})$, and since i is arbitrary, $M = \sum_{i \in I} N_i \subset (N \oplus N_{A_0})$ as desired.

(ii) implies (iii). Assume (ii) and consider the set J of all irreducible submodules of M (at this point we do not even know that J is not empty!).

Consider all the subsets A of J for which the modules in A form a direct sum. This clearly satisfies the hypotheses of Zorn's lemma, and so we can find a maximal set adding to a submodule N.

We must prove that $N = M$. Otherwise we can find an element $m \notin N$ and a maximal submodule $N_0 \supset N$ such that $m \notin N$. By hypothesis there is a direct summand P of N_0.

We claim that P is irreducible. Otherwise let T be a nontrivial submodule of P and consider a complement Q to $N_0 \oplus T$. We have thus that M/N_0 is isomorphic to $T \oplus Q$ and so is decomposable, against the conclusions of Lemma 2.

P irreducible is also a contradiction since P and N form a direct sum, and this contradicts the maximal choice of N as direct sum of irreducibles. □

Comment. If the reader is confused by the transfinite induction he should easily realize that all these inductions, in the case where M is a finite-dimensional vector space, can be replaced with ordinary inductions on the dimensions of the various submodules constructed.

Corollary 1. *Let $M = \sum_{i \in I} N_i$ be a semisimple module, presented as a sum of irreducible submodules. We can extract from this sum a direct sum decomposing M.*

Proof. We consider a maximal direct sum out of the given one. Then any other irreducible module N_i must be in the sum, and so this sum gives M. □

Corollary 2. *Let $M = \bigoplus_{i \in I} N_i$ be a semisimple module, presented as a direct sum of irreducible submodules. Let N be an irreducible submodule of M. Then the projection to one of the N_i, restricted to N, is an isomorphism.*

2.2 Submodules and Quotients

Proposition.

(i) *Submodules and quotients of a semisimple module are semisimple, as well as direct sums of semisimple modules.*
(ii) *R is semisimple if and only if every R module is semisimple. In this case its spectrum is finite and consists of the irreducible modules appearing in the regular representation.*
(iii) *If R has a faithful semisimple module M, then R is semisimple.*

Proof. (i) Since the quotient of a sum of irreducible modules is again a sum of irreducibles the statement is clear for quotients. But every submodule has a complement and so it is isomorphic to a quotient. For direct sums the statement is clear.

(ii) If every module is semisimple clearly R is also semisimple. Conversely, let R be semisimple. Since every R-module is a quotient of a free module, we get from (i) that every module is semisimple. Proposition 1.4 implies that R is a finite direct sum of irreducibles and Corollary 1, §1.9 implies that these are the only irreducibles.

(iii) For each element m of M take a copy M_m of M and form the direct sum $M := \bigoplus_{m \in M} M_m$. M is a semisimple module.

Map $R \to \bigoplus_{m \in M} M_m$ by $r \mapsto (rm)_{m \in M}$. This map is clearly injective so R, as a submodule of a semisimple module, is semisimple. □

2.3 Isotypic Components

An essential notion in the theory of semisimple modules is that of *isotypic component.*

Definition. Given an isomorphism class of irreducible representations, i.e., a point of the spectrum $\alpha \in R^\vee$ and a module M, we set M^α to be the sum of all the irreducible submodules of M of type α. This submodule is called *the isotypic component of type α.*

Let us also use the notation M_α to be the sum of all the irreducible submodules of M which are *not* of type α.

Theorem. *The isotypic components of M decompose M into a direct sum.*

Proof. We must only prove that given an isomorphism class α, $M^\alpha \cap M_\alpha = 0$.

M^α can be presented as a direct sum of irreducibles of type α, while M_α can be presented as a direct sum of irreducibles of type different from α.

Thus every irreducible submodule in their intersection must be 0; otherwise by Corollary 2 of 2.1, it is at the same time of type α and of type different from α. From Proposition 2.2 (i), any submodule is semisimple, and so this implies that the intersection is 0. □

Proposition 1. *Given any homomorphism $f : M \to N$ between semisimple modules it induces a morphism $f_\alpha : M^\alpha \to N^\alpha$ for every α and f is the direct sum of the f_α. Conversely,*

$$\hom_R(M, N) = \prod_\alpha \hom(M^\alpha, N^\alpha). \tag{2.3.1}$$

Proof. The image under a homomorphism of an irreducible module of type α is either 0 or of the same type, since the isotypic component is the sum of all the submodules of a given type the claim follows. □

Now that we have the canonical decomposition $M = \bigoplus_{\alpha \in R^\vee} M^\alpha$, we can consider the projection $\pi^\alpha : M \to M^\alpha$ with kernel M_α. We have:

Proposition 2. *Given any homomorphism $f : M \to N$ between semisimple modules we have a commutative diagram, for each $\alpha \in R^\vee$:*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi^\alpha"'] & N \arrow[d, "\pi^\alpha"'] \\ M^\alpha \arrow[r, "f"] & N^\alpha \end{tikzcd} \tag{2.3.2}$$

Proof. This is an immediate consequence of the previous proposition. □

2.4 Reynold's Operator

This rather formal analysis has an important implication. Let us assume that we have a group G acting as automorphisms on an algebra A. Let us furthermore assume that A is semisimple as a G-module. Thus the subalgebra of invariants A^G is the isotypic component of the trivial representation.

Let us denote by A_G the sum of all the other irreducible representations, so that $A = A^G \oplus A_G$.

Definition. The canonical projection $\pi^G : A \to A^G$ is usually indicated by the symbol R and called *the Reynold's operator.*

Let us now consider an element $a \in A^G$; since, by hypothesis, G acts as algebra automorphisms, both left and right multiplication by a are G equivariant. We thus have the commutative diagram 2.3.2, for $\pi_\alpha = R$ and f equal to the left or right multiplication by a, and deduce the so-called *Reynold's identities.*

Proposition.

$$R(ab) = aR(b), \;\; R(ba) = R(b)a, \;\; \forall b \in A, \; a \in A^G.$$

We have stated these identities since they are the main tool to develop the theory of Hilbert on invariants of forms (and its generalizations) (see [DL], [SP1]) and Chapter 14.

2.5 Double Centralizer Theorem

Although the theory could be pursued in the generality of Artinian rings (cf. [JBA]), let us revert to finite-dimensional representations.

Let $R = \bigoplus_{i\in I} R_i = \bigoplus_{i\in I} M_{m_i}(\Delta_i)$ be a finite-dimensional semisimple algebra over a field F. In particular, now all the division algebras Δ_i will be finite dimensional over F. In the case of the complex numbers (or of an algebraically closed field) they will coincide with F. For the real numbers we have the three possibilities already discussed.

If we consider any finite-dimensional module M over R we have seen that M is isomorphic to a finite sum

$$M = \bigoplus_i M_i = \bigoplus_{i\in I} N_i^{p_i},$$

where M_i is the isotypic component relative to the block R_i and $N_i = \Delta_i^{m_i}$.

We have also from 1.8.2:

$$S := \mathrm{End}_R(M) = \bigoplus_{i\in I} \mathrm{End}_R(M_i) = \bigoplus_{i\in I} \mathrm{End}_R(N_i^{p_i}) = \bigoplus_{i\in I} M_{p_i}(\Delta_i{}^o)$$
$$:= \bigoplus_{i\in I} S_i.$$

The block S_i acts on $N_i^{p_i}$ as m_i copies of its standard representation, and as zero on the other isotypic components. In fact by definition $S_i = \mathrm{End}_R(N_i^{p_i})$ acts as 0 on all isotypic components different from the i^{th} one.

As for the action on this component we may identify $N_i := \Delta_i^{m_i}$ and thus view the space $N_i^{p_i}$ as the set $M_{m_i,p_i}(\Delta_i)$ of $m_i \times p_i$ matrices. Multiplication on the right by a $p_i \times p_i$ matrix with entries in Δ_i induces a typical endomorphism in S_i. The algebra of such endomorphisms is isomorphic to $M_{p_i}(\Delta_i^o)$, acting by multiplication on the right, and the m_i subspaces of $M_{m_i,p_i}(\Delta_i)$ formed by the rows decompose this space into irreducible representations of S_i isomorphic to the standard representation $(\Delta_i^o)^{p_i}$. Summarizing:

Theorem.

(i) Given a finite-dimensional semisimple R module M the centralizer S of R is semisimple.

(ii) The isotypic components of R and S coincide.

(iii) The multiplicities and the dimensions (relative to the corresponding division ring) of the irreducibles appearing in an isotypic component are exchanged, passing from R to S.

(iv) If for a given i, $M_i \neq 0$, then the centralizer of S on M_i is R_i (or rather the ring of operators induced by R_i on M_i). In particular if R acts faithfully on M we have $R = S' = R''$ (Double Centralizer Theorem).

All the statements are implicit in our previous analysis.

We wish to restate this in case $F = \mathbb{C}$ for a semisimple algebra of operators as follows:

Given two sequences of positive integers $m_1, m_2, \ldots, m_k$ and $p_1, p_2, \ldots, p_k$ we form the two semisimple algebras $A = \bigoplus_{i=1}^k M_{m_i}(\mathbb{C})$ and $B = \bigoplus_{i=1}^k M_{p_i}(\mathbb{C})$.

We form the vector space $W = \bigoplus_{i=1}^k \mathbb{C}^{m_i} \otimes \mathbb{C}^{p_i}$ and consider A, B as commuting algebras of operators on W in the obvious way, i.e., $(a_1, a_2, \ldots, a_k) \sum u_i \otimes v_i = \sum a_i u_i \otimes v_i$ for A and $(b_1, b_2, \ldots, b_k) \sum u_i \otimes v_i = \sum u_i \otimes b_i v_i$ for B. Then:

Corollary. *Given a semisimple algebra R of operators on a finite-dimensional vector space M over $\mathbb{C}$ and calling $S = R'$ its centralizer, there exist two sequences of integers $m_1, m_2, \ldots, m_k$ and $p_1, p_2, \ldots, p_k$ and an isomorphism of M with $W = \bigoplus_{i=1}^k \mathbb{C}^{m_i} \otimes \mathbb{C}^{p_i}$ under which the algebras R, S are identified with the algebras A, B.*

This corollary gives very precise information on the nature of the two algebras since it claims that on each isotypic component we can find a basis indexed by pairs of indices such that, if we order the pairs by setting first all the pairs which *end* with 1, then all that *end* with 2 and so on, the matrices of R appear as diagonal block matrices.

We get a similar result for the matrices of S if we order the indices by setting first all the pairs which *begin* with 1 then all that *begin* with 2 and so on.

Let us continue a moment with the same hypotheses as in the previous section. Choose a semisimple algebra $A = \bigoplus_{i=1}^k M_{m_i}(\mathbb{C})$ and two representations:

$$W_1 = \bigoplus_{i=1}^k \mathbb{C}^{m_i} \otimes \mathbb{C}^{p_i}, \quad \text{and } W_2 = \bigoplus_{i=1}^k \mathbb{C}^{m_i} \otimes \mathbb{C}^{q_i}$$

which we have presented as decomposed into isotypic components. According to 1.8.1 we can compute as follows:

$$\begin{aligned} \hom_A(W_1, W_2) &= \bigoplus_{i=1}^k \hom_A(\mathbb{C}^{m_i} \otimes \mathbb{C}^{p_i}, \mathbb{C}^{m_i} \otimes \mathbb{C}^{q_i}) \\ &= \bigoplus_{i=1}^k \hom_{\mathbb{C}}(\mathbb{C}^{p_i}, \mathbb{C}^{q_i}). \end{aligned} \tag{2.5.1}$$

We will need this computation for the theory of invariants.

2.6 Products

We want to deduce an important application. Let H, K be two groups (not necessarily finite) and let us choose two finite-dimensional irreducible representations U, V of these two groups over $\mathbb{C}$.

Proposition 1. *$U \otimes V$ is an irreducible representation of $H \times K$, and any finite-dimensional irreducible representation of $H \times K$ is of this form.*

Proof. The maps $\mathbb{C}[H] \to \mathrm{End}(U)$, $\mathbb{C}[K] \to \mathrm{End}(V)$ are surjective, hence the map $\mathbb{C}[H \times K] \to \mathrm{End}(U) \otimes \mathrm{End}(V) = \mathrm{End}(U \otimes V)$ is also surjective, and so $U \otimes V$ is irreducible.

Conversely, assume that we are given an irreducible representation W of $H \times K$ so that the image of the algebra $\mathbb{C}[H \times K]$ is the whole algebra $\mathrm{End}(W)$.

Let W' be the sum of all irreducible H-submodules of a given type appearing in W. Since K commutes with H we have that W' is K stable. Since W is irreducible we have $W = W'$. So W is a semisimple $\mathbb{C}[H]$-module with a unique isotypic component.

The algebra of operators induced by H is isomorphic to the full matrix algebra $M_n(\mathbb{C})$, and its centralizer is isomorphic to $M_m(\mathbb{C})$ for some m, n. W is nm-dimensional and $M_n(\mathbb{C}) \otimes M_m(\mathbb{C})$ is isomorphic to $\mathrm{End}(W)$.

The image R of $\mathbb{C}[K]$ is contained in the centralizer $M_m(\mathbb{C})$. Since the operators from $H \times K$ span $\mathrm{End}(W)$ the algebra R must coincide with $M_m(\mathbb{C})$, and the theorem follows. □

This theorem has an important application to matrix coefficients.

Let $\rho : G \to GL(U)$ be a finite-dimensional representation of G. Then we have a mapping $i_U : U^* \otimes U \to \mathbb{C}[G]$ to the functions on G defined by (cf. Chapter 5, §1.5.4):

$$(2.6.1) \qquad i_U(\phi \otimes u)(g) := \langle \phi \mid gu \rangle = \mathrm{tr}(\rho(g) \circ u \otimes \phi).$$

Proposition 2. *i_U is $G \times G$ equivariant. The image of i_U is called the* ***space of matrix coefficients of*** U.

Proof. We have $i_U(h\phi \otimes ku)(g) = \langle h\phi \mid gku \rangle = \langle \phi \mid h^{-1}gku \rangle = {}^h i_U(\phi \otimes u)^k$. □

In the last part of 2.6.1 we are using the identification of $U^* \otimes U$ with $U \otimes U^* = \mathrm{End}(U)$. Under this identification the map i_U becomes $X \mapsto \mathrm{tr}(X\rho(g))$, for $X \in \mathrm{End}(U)$.

Theorem.

(i) If U is irreducible, the map $i_U : U^* \otimes U \to \mathbb{C}[G]$ is injective.
(ii) Its image equals the isotypic component of type U in $\mathbb{C}[G]$ under the right action and equals the isotypic component of type U^* in $\mathbb{C}[G]$ under the left action.

Proof. (i) $U^* \otimes U$ is an irreducible $G \times G$ module, and i_U is clearly nonzero, then i_U is injective.

(ii) We do it for the right action; the left is similar.

Let us consider a G-equivariant embedding $j : U \to \mathbb{C}[G]$ where $\mathbb{C}[G]$ is considered as a G-module under right action. We must show that its image is in $i_U(U^* \otimes U)$.

Let $\phi \in U^*$ be defined by

$$\langle \phi | u \rangle := j(u)(1).$$

Then

$$(2.6.2) \qquad j(u)(g) = j(u)(1g) = j(gu)(1) = \langle \phi | gu \rangle = i_U(\phi \otimes u)(g).$$

Thus $j(u) = i_U(\phi \otimes u)$. □

Remark. The theorem proved is completely general and refers to any group. It will be possible to apply it also to continuous representations of topological groups and to rational representations of algebraic groups.

Notice that, for a finite group G, since the group algebra is semisimple, we have:

Corollary.

$$\mathbb{C}[G] = \bigoplus_i U_i^* \otimes U_i \tag{2.6.3}$$

where U_i runs over all the irreducible representations.

$\mathbb{C}[G]$ *is isomorphic as an algebra to* $\bigoplus_i \mathrm{End}(U_i)$.

Proof. By definition, for each i we have a homomorphism of $\mathbb{C}[G]$ to $\mathrm{End}(U_i)$, given by the module structure. Since it is clear that restricted to the corresponding matrix coefficients this is a linear isomorphism, the claim follows. □

Important Remark. This basic decomposition will be the guiding principle throughout all of our presentation. It will reappear in other contexts: In Chapter 7. §3.1.1 for linearly reductive algebraic groups, in Chapter 8, §3.2 as the Peter–Weyl theorem for compact groups and as a tool to pass from compact to linearly reductive groups; finally, in Chapter 10, §6.1.1 as a statement on Lie algebras, to establish the relation between semisimple Lie algebras and semisimple simply connected algebraic groups. We will see that it is also related to Cauchy's formula of Chapter 2 and the theory of Schur's functions, in Chapter 9, §6.

2.7 Jacobson Density Theorem

We discuss now the Jacobson density theorem. This is a generalization of Wedderburn's theorem which we will discuss presently.

Theorem. *Let N be an irreducible R-module, Δ its centralizer,*

$$u_1, u_2, \dots, u_n \in N$$

elements which are linearly independent relative to Δ and

$$v_1, v_2, \dots, v_n \in N$$

arbitrary. Then there exists an element $r \in R$ such that $ru_i = v_i$, $\forall i$.

Proof. The theorem states that the module N^n is generated over R by the element $a := (u_1, u_2, \dots, u_n)$.

Since N^n is completely reducible, N^n decomposes as $Ra \oplus P$. Let $\pi \in \mathrm{End}_R(N^n)$ be the projection to P vanishing on the submodule Ra.

By 1.8.1 this operator is given by an $n \times n$ matrix d_{ij} in Δ and so we have $\sum_j d_{ij}u_j = 0$, $\forall i$ since these are the components of $\pi(a)$.

By hypothesis the elements $u_1, u_2, \dots, u_n \in N$ are linearly independent over Δ; thus the elements d_{ij} must be 0 and so $\pi = 0$ and $P = 0$ as desired. □

The term "density" comes from the fact that one can define a topology (of finite approximations) on the ring $\mathrm{End}_\Delta(N)$ so that R is dense in it (cf. [JBA]).

2.8 Wedderburn's Theorem

Again let N be an irreducible R-module, and Δ its centralizer. Assume that N is a finite-dimensional vector space over Δ of dimension n.

There are a few formal difficulties in the noncommutative case to be discussed.

If we choose a basis $u_1, u_2, \dots, u_n$ of N we identify N with Δ^n. Given the set of n-tuples of elements of a ring A thought of as column vectors, we can act on the left with the algebra $M_n(A)$ of $n \times n$ matrices. This action clearly commutes with the multiplication *on the right* by elements of A.

If we want to think of operators as always acting on the left, then we have to think of left multiplication for the *opposite* ring A^o.

We thus have dually the general fact that the endomorphism ring of a free module of rank n on a ring A is the ring of $n \times n$ matrices over A^o. We return now to modules.

Theorem 1 (Wedderburn). *R induces on N the full ring $\mathrm{End}_\Delta(N)$ isomorphic to the ring of $m \times m$ matrices $M_m(\Delta^o)$.*

Proof. Immediate consequence of the density theorem, taking a basis $u_1, u_2, \dots, u_n$ of N. □

We end our abstract discussion with another generality on characters.

Let R be an algebra over $\mathbb{C}$ (we make no assumption of finite dimensionality). Let M be a finite-dimensional semisimple representation. The homomorphism $\rho_M : R \to \mathrm{End}(M)$ allows us to define a *character* on R setting $t_M(a) := \mathrm{tr}(\rho_M(a))$.

Theorem 2. *Two finite-dimensional semisimple modules M, N are isomorphic if and only if they have the same character.*

Proof. It is clear that if the two modules are isomorphic the traces are the same. Conversely, let I_M, I_N be the kernels respectively of ρ_M, ρ_N.

By the theory of semisimple algebras we know that R/I_M is isomorphic to a direct sum $\bigoplus_i M_{n_i}(\mathbb{C})$ of matrix algebras and similarly for R/I_N.

Assume that M decomposes under $\bigoplus_{i=1}^k M_{n_i}(\mathbb{C})$ with multiplicity $p_i > 0$ for the i^{th} isotypic component. Then the trace of an element $r = (a_1, a_2, \dots, a_k)$ as operator on M is $\sum_{i=1}^k p_i \,\mathrm{Tr}(a_i)$ where $\mathrm{Tr}(a_i)$ is the ordinary trace as an $n_i \times n_i$ matrix.

We deduce that the bilinear form $\mathrm{tr}(ab)$ is nondegenerate on R/I_M and so I_M is the kernel of the form induced by this trace on R. Similarly for R/I_N.

If the two traces are the same we deduce that the kernel is also the same and so $I_M = I_N$, and $R/I_M = \bigoplus_i M_{n_i}(\mathbb{C}) = R/I_N$. In order to prove that the representations are the same we check that the isotypic components have the same multiplicities. This is clear since p_i is the trace of e_i, a central unit of $M_{n_i}(\mathbb{C})$. □

3 Primitive Idempotents

3.1 Primitive Idempotents

Definition. An idempotent is called *primitive* if it cannot be decomposed as a sum $e = e_1 + e_2$ of two nonzero orthogonal idempotents.

If $R = M_k(F)$ is a matrix algebra over a field F, an idempotent $e \in M_k(F)$ is a projection to some subspace $W := eF^k \subset F^k$. It is then easily verified that a primitive idempotent is a projection to a 1-dimensional subspace, i.e., an idempotent matrix of rank 1 which, in a suitable basis, can be identified with the elementary matrix $e_{1,1}$.

When $e = e_{1,1}$, the left ideal Re is formed by all matrices with 0 on the columns different from the first one. As an R-module it is irreducible and isomorphic to F^k. Finally $eRe = Fe$.

More generally the same analysis holds for matrices over a division ring D, thought of as endomorphisms of the *right* vector space D^n. In this case, again if e is primitive, one can identify $eRe = D$.

If an algebra $R = R_1 \oplus R_2$ is the direct sum of two algebras, then every idempotent in R is the sum $e_1 + e_2$ of two orthogonal idempotents $e_i \in R_i$. In particular the primitive idempotents in R are the primitive idempotents in R_1 and the ones in R_2.

Thus, if $R = \sum_i M_{n_i}(F)$ is semisimple, then a primitive idempotent $e \in R$ is just a primitive idempotent in one of the summands $M_{n_i}(F)$. Thus $M_{n_i}(F) = ReR$ and Re is irreducible as an R-module (and isomorphic to the module F^{n_i} for the summand $M_{n_i}(F)$).

We want a converse of this statement. We first need a lemma:

Lemma. *Let M be a semisimple module direct sum of a finite number of irreducible modules. Let P, Q be two submodules of M and $i : P \to Q$ a module isomorphism. Then i extends to an automorphism of the module M.*

Proof. We first decompose M, P, Q into isotypic components. Since every isotypic component under a homomorphism is mapped to the isotypic component of the same type we can reduce to a singe isotypic component. Let N be the irreducible module relative to this component. M is isomorphic to N^m for some m.

By isomorphism we must have P, Q both isomorphic to N^k for a given k. If we complete $M = P \oplus P'$, $M = Q \oplus Q'$ we must have that P', Q' are both isomorphic to N^{m-k}. Any choice of such an isomorphism will produce an extension of i. □

Theorem. *Let $R = \oplus R_i$ be a semisimple algebra over a field F with R_i simple and isomorphic to the algebra of matrices $M_{k_i}(D_i)$ over a division algebra D_i.*

(1) Given a primitive idempotent $e \in R$ we have that Re is a minimal left ideal, i.e., an irreducible module.
(2) All minimal left ideals of R are of the previous form.
(3) Two primitive idempotents $e, f \in R$ give isomorphic modules Re, Rf if and only if $eRf \neq 0$.
(4) Two primitive idempotents e, f give isomorphic modules Re, Rf if and only if they are conjugate, i.e., there is an invertible element $r \in R$ with $f = rer^{-1}$.
(5) A sufficient condition for an idempotent $e \in R$ to be primitive is that $\dim_F eRe = 1$. *In this case ReR is a matrix algebra over F.*

Proof. (1) We have seen that if e is primitive, then $e \in R_i$ for some i. Hence $Re = R_ie$, e is the projection on a 1-dimensional subspace and by change of basis, $R_i = M_{k_i}(D_i)$. R_ie is the *first column* isomorphic to the standard irreducible module $D_i^{k_i}$.

(2) We first decompose R as direct sum of the $R_i = M_{k_i}(D_i)$ and then each $M_{k_i}(D_i)$ as direct sum of the columns $R_i e_{i,i}$ ($e_{i,i}$ being the diagonal matrix units). A minimal left ideal is an irreducible module $N \subset R$, and it must be isomorphic to one of the columns, call this Re with e primitive. By the previous lemma, there is an isomorphism $\phi : R \to R$, such that $\phi(Re) = N$. By Proposition 2 of 1.3, we have that $\phi(a) = ar$ for some invertible r, hence $N = Rf$ with $f = r^{-1}er$.

(3) We have that each primitive idempotent lies in a given summand R_i. If Re is isomorphic to Rf, the two idempotents must lie in the same summand R_i. If they lie in different summands, then $eRf \subset R_i \cap R_j = 0$. Otherwise, $eR = eR_i$, $Rf = R_i f$ and, since R_i is a simple algebra we have $R_i = R_i e R_i = R_i f R_i$ and $R_i = R_i R_i = R_i eRf R_i \neq 0$.

(4) If $e = rfr^{-1}$ we have that multiplication on the right by r establishes an isomorphism between Re and Rf. Conversely, let Re, Rf be isomorphic. We may reduce to $R = M_k(D)$ and e, f are each a projection to a 1-dimensional subspace. In two suitable bases the two idempotents equal the matrix unit $e_{1,1}$, so the invertible matrix of base change conjugates one into the other.

(5) $eRe = \bigoplus_i eR_i e$. Hence if $\dim_F eRe = 1$, we must have that $eR_{i_0}e \neq 0$ for only one index i_0 and $e \in R_{i_0}$. If $e = a + b$ were a decomposition into orthogonal idempotents, we would have $a = aea$, $b = beb \in eRe$, a contradiction. Since e is primitive in $R_{i_0} = M_k(D_{i_0})$ in a suitable basis, it is a matrix unit and so the division algebra $eRe = D_{i_0}$ reduces to F since $\dim_F D_{i_0} = \dim_F eRe = 1$. □

Assume as before that $R = \oplus R_i$ is a semisimple algebra over a field F and $\dim_F eRe = 1$.

Proposition 1. *Given a module M over R the multiplicity of Re in its isotypic component in M is equal to* $\dim_F eM$.

Proof. Let $M_0 := \oplus^k Re$ be the isotypic component. We have $eM = eM_0 = \oplus^k eRe = F^k$. □

Proposition 2.

(1) Let R be a semisimple algebra and I an ideal; then $I^2 = I$.
(2) If $aRb = 0$, then $bRa = 0$. Furthermore $aRa = 0$ implies $a = 0$.

Proof. (1) An ideal of $\bigoplus_i R_i$ is a sum of some R_j and $R_j^2 = R_j$.

(2) In fact from $aRb = 0$ we deduce $(RbRaR)^2 = 0$. Since $RbRaR$ is an ideal, by (1) we must have $RbRaR = 0$. Hence $bRa = 0$.

Similarly, $aRa = 0$ implies $(RaR)^2 = 0$. Hence the claim. □

In particular we see that a semisimple algebra has no nonzero nilpotent ideals, or ideals I for which $I^k = 0$ for some k.

It can in fact be proved that for a finite-dimensional algebra this condition is equivalent to semisimplicity (cf. [JBA]).

3.2 Real Algebras

It is interesting to study also real semisimple algebras R and real representations. We state the basic facts leaving the proofs to the reader.

A real semisimple algebra is a direct sum of matrix algebras over the three basic division algebras $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. The representations will decompose according to these blocks. Let us analyze one single block, $M_h(\Delta)$ in the three cases. It corresponds to the irreducible module Δ^h with centralizer Δ. When we complexify the algebra and the module we have $M_h(\Delta \otimes_{\mathbb{R}} \mathbb{C})$ acting on $(\Delta \otimes_{\mathbb{R}} \mathbb{C})^h$ with centralizer $\Delta \otimes_{\mathbb{R}} \mathbb{C}$. We have

$$(3.2.1) \qquad \mathbb{R} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}, \quad \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \oplus \mathbb{C}, \quad \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} = M_2(\mathbb{C}).$$

Exercise. Deduce that the given irreducible module for R, in the three cases, remains irreducible, splits into the sum of two non-isomorphic irreducibles, splits into the sum of two isomorphic irreducibles.