SEMISIMPLE MODULES AND ALGEBRAS.

ANDREI YAFAEV

We start with some definitions.

Definition 0.1. *A* **ring** *is a set R endowed with two operations : addition, denoted $+$ and multiplication, denoted $\cdot$ that satisfy the following conditions*

- $a + b = b + a$ *(+ is commutative)*
- $a + (b + c) = (b + a) + c$ *(+ is distributive)*
- $(ab)c = a(bc)$ *($\cdot$ is distributive)*
- $a(b + c) = ab + ac$
- $(b + c)a = ba + ca$

In addition, there is an element $0 \in R$ satisfying $a + 0 = 0 + a = a$. For each $a \in R$, there is an element $-a$ such that $a + (-a) = 0$ (note that this implies that $(R, +)$ is an abelian group).

There is an element 1 in R such that $1 \cdot a = a \cdot 1 = a$.

Examples of rings include $\mathbb{Z}$, F (field), $F[X]$, $\mathbb{Z}/n\mathbb{Z}$, $F[X]/I$ where $I \subset F[X]$ is an ideal. These rings are commutative (i.e. multiplication is commutative).

In this course we will be mainly concerned with some non-commutative rings. An example of this is $M_n(F)$ (matrices over a field F). Another example is the set of upper triangular matrices. More generally, for any ring R, the set $M_n(R)$ of matrices with entries in R is a ring.

A ring D is called a **division ring** if any $a \in D$, $a \neq 0$ has a two sided inverse i.e. there exists an $a^{-1} \in D$ such that $aa^{-1} = a^{-1}a = 1$.

A field is of course a division ring.

We now define modules over rings.

Definition 0.2. *A (left) module M over a ring R is an* abelian group *M with a map ϕ from $R \times M$ to M satisfying the following properties (we write rm for $\phi(r, m)$):*

- $1m = m$ *for all* $m \in M$
- $r(m + n) = rm + rn$ *for all* $r \in R$ *and* $m, n \in M$
- $(r + s)m = rm + sm$ *for all* $r, s \in R$ *and* $m \in M$
- $r(sm) = (rs)m$ *for all* $r, s \in R$ *and* $m \in M$

We define the notion of *right* R-module in an exactly analogous way with multiplication by elements of R on the right.

Take *any* abelian group, then it is naturally a $\mathbb{Z}$-module.

Let R be a field F. An F-module is a vector space over F.

Let R be a commutative ring. An ideal in R is an R-module.

Take any ring R and $a \in R$. Then the set Ra is a left R-module and aR a right R-module.

$M_n(F)$ is a module over both F (in which case it is simply viewed as a vector space of dimension n^2) and the ring $M_n(F)$.

Let R be a ring, then $R[X]$ is a module over R.

A module M is called *finitely generated* if there is a finite subset of M such that any element of M is a linear combination of elements of this set.

For example $M_n(F)$ is finitely generated over F while $F[X]$ is not.

In this course we will mainly deal with finitely generated modules. Unless explicitly stated otherwise, the modules are assumed to be finitely generated.

Definition 0.3. *Let M be an R-module and let N be a* subgroup *of M. We say that N is a (left) R-submodule of M (often simply submodule) if N is a subgroup of $(M, +)$ and $rn \in N$ for all $r \in R$ and $n \in N$.*

If M is an R-module, $v \in M$, then

$$Rv = \{av : a \in R\}$$

is a left submodule of M.

Let R be a commutative ring. Submodules of R are exactly the ideals. If R is non-commutative, left R-submodules of R are called left ideals, right submodules are called right ideals. Subgroups that are both right and left ideals are called two-sided ideals.

Consider the ring $M_n(R)$ of $n \times n$ matrices over a ring R. Fix $1 \leq j \leq n$. Let I be the set of matrices with zeros outside the jth column. Then I is a left ideal (exercise).

Similarly, fix $1 \leq j \leq n$. The set of matrices with zeros outside of jth row is a right ideal.

Look now at two-sided ideals.

Lemma 0.1. *Every two-sided ideal of $M_n(R)$ is of the form $M_n(I)$ for a two sided ideal I of R.*

Proof. Let $J \subset M_n(R)$ be an ideal. Let $E_{i,j}$ be the matrix with 1 at the position (i, j) and zero elsewhere. Recall that matrices $E_{i,j}$ satisfy the relation:

$$E_{i,j}E_{j,k} = E_{i,k}$$

and for a matrix $A = (a_{i,j})$, we have

$$E_{m,i}AE_{j,k} = a_{i,j}E_{m,k}$$

Let

$$I = \{r \in R : rE_{1,1} \in J\}$$

This is a two sided ideal of R. Indeed, let a be in R and r in I. We have $(aE_{1,1})(rE_{1,1}) = arE_{1,1}$ hence $ar \in I$. Similarly, $ra \in I$.

For any matrix A in J we have

$$a_{i,j}E_{1,1} = E_{1,j}AE_{j,1}$$

As J is an ideal, the right-hand side belongs to J and hence $a_{i,j} \in I$. It follows that $J \subset M_n(I)$.

Furthermore, if $r \in I$, then $E_{i,1}(rE_{1,1})E_{1,j} = rE_{i,j}$. As $rE_{1,1} \subset J$ and J is a two-sided ideal, we see that $rE_{i,j} \in J$ for all $r \in I$. As any element of $M_n(I)$ is a sum of elements of the form $rE_{i,j}$, $r \in I$, we see that $M_n(I)$ is contained in J. We have shown that $J = M_n(I)$. □

A consequence of this lemma is the following. Suppose $R = F$ is a field. The only ideals of F are $\{0\}$ and F itself, hence the only two-sided ideals of $M_n(F)$ are $\{0\}$ and $M_n(F)$.

More generally, if D is a division ring, then the only two-sided ideals of $M_n(D)$ are $\{0\}$ and $M_n(D)$.

Let M be a module and N a submodule. As N is an abelian subgroup, one has a quotient M/N (as abelian groups) which is endowed with the structure of R-submodule by $r(m+N) = rm+N$ for $r \in R$ and $m + N \in M/N$.

Let N_1 and N_2 be two submodules of M. One defines the sum N_1+N_2 as

$$N_1 + N_2 = \{x + y : x \in N_1, y \in N_2\} \subset M$$

This is a submodule of M. The sum is *direct* (denoted $N_1 \oplus N_2$) if $N_1 \cap N_2 = \{0\}$.

One says that a submodule N of M is a *direct summand* if there exists a submodule N' of M such that

$$M = N \oplus N'$$

An important example of a ring is the ring $\mathbb{H}$ of quaternions. It is defined as follows :

$$\mathbb{H} = \{a \cdot 1 + b \cdot i + c \cdot j + d \cdot k : a, b, c, d \in \mathbb{R}\}$$

where $i^2 = j^2 = k^2 = -1$ and

$$ij = k, jk = i, ki = j$$

and

$$ji = -k, kj = -i, ik = -j$$

The ring $\mathbb{H}$ is an $\mathbb{R}$ module. It is also a $\mathbb{C}$ module:

$$a \cdot 1 + b \cdot i + c \cdot j + d \cdot k = a + bi + (c + ib)j(k = ij!)$$

Hence by setting $\mathbb{C} = \{a + bi \in \mathbb{H}\}$, we get $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$. Note that for $z \in \mathbb{C}$, we have $jz = \overline{z}j$! This means that the structures of left and right $\mathbb{C}$-modules on $\mathbb{H}$ differ.

The ring $\mathbb{H}$ is a division ring (exercise).

Definition 0.4. *Let M, N be two R-modules. A* homomorphism $\phi \colon M \longrightarrow N$ *is a group homomorphism satisfying*

$$\phi(rm) = r\phi(m)$$

The kernel $\ker(\phi)$ *of ϕ is the set of elements of M mapping to zero in N.*

The kernel and the image of ϕ are submodules of M and N respectively.

Every module has at least two submodules, namely $\{0\}$ and M itself. We now introduce a very important notion :

Definition 0.5. *A non-sero module M is called simple (one also says irreducible) if the only submodules of M are 0 and M.*

Lemma 0.2. *Any simple R-module M is generated by any of its non-zero vectors i.e. for any $v \in M$, $v \neq 0$, $M = Rv$.*

Proof. Let $v \in M$ be a non-zero vector, then Rv is a non-zero submodule of M. As M is simple, $Rv = M$. □

A field F is simple, viewed as a module over itself.

The F-module F^n for $n > 1$ is not simple, indeed any non-zero proper vector subspace is a non-trivial submodule.

It is *not* simple as F-module, indeed, as an F-module, it is isomorphic to to F^n.

We prove the following important result.

Lemma 0.3 (Shur's lemma)**.** *Any non-zero homomorphism between simple R-modules is an isomorphism.*

Proof. Let M and N be simple R-modules and let $\phi \colon M \longrightarrow N$ be an R-module homomorphism. As $\ker(\phi)$ is a submodule of M and different from M (because $\phi \neq 0$!), one has $\ker(\phi) = \{0\}$.

Similarly, $\mathrm{im}(\phi)$ is a non-zero submodule of M hence $\mathrm{im}(\phi) = M$.

This shows that ϕ is an isomorphism. □

Let D be a division ring. The module $M_n(F)$ is not simple as a left or a right module. Indeed, consider the subset C_j of $M_n(D)$ consisting of matrices which are zero everywhere outside of jth column. This is a left $M_n(D)$ submodule of $M_n(D)$. This is easily checked by matrix multiplication. This module is in fact simple as $M_n(D)$-module. Let M be a non-trivial left submodule of C_j. It has a non-zero vector v. The vector v (viewed as a matrix in $M_n(D)$) is of the form

$$v = \sum_{l=1}^{n} c_l E_{l,j}$$

One of the c_ls, say c_k is not zero. We have

$$c_k^{-1} E_{i,k} v = E_{i,j} \in M$$

And this for any i! As the $E_{i,j}$ generate C_j, we conclude that $M = C_j$. Notice that we used in an essential way that the matrices are over a *division ring* (we had to invert c_k).

It is clear that all C_js are isomorphic as $M_n(D)$-modules. In fact they are all isomorphic to the following module: consider D^n as the set of column vectors with entries in D. This is naturally a left $M_n(D)$ module (multiplying a column vector on the left by a matrix).

This module is isomorphic to any of the C_j. More generally:

Lemma 0.4. *Any simple $M_n(D)$ module is isomorphic to the module D^n.*

Proof. Let M be a simple $M_n(D)$ module. Then by 0.2, $M = M_n(D)v$ for a non-zero vector $v \in M$. We also have $D^n = M_n(D)e_1$ where e_1 is the first vector of the standard basis. The R-module homomorphism $M \longrightarrow D^n$ sending v to e_1 is non-zero hence is an isomorphism. □

We will now give an alternative version of this lemma. To do this, one need to introduce yet another definition. Consider a module M. An R-module homomorphism $M \longrightarrow M$ is called an *endomorphism*. The set of all endomorphisms, denoted $\mathrm{End}_R(M)$ is a ring. This is an exercise: the multiplication being the composition of endomorphisms and the identity is naturally the identity endomorphism, sending $x \in M$ to x.

Lemma 0.5 (Shur, version 2)**.** *Let M be a simple module, then* $\mathrm{End}(M)$ *is a division ring.*

If F is a field viewed as a module over itself, then $\mathrm{End}_F(F) = F$.

Consider the module F^n viewed as a left $M_n(F)$-module. Then

$$\mathrm{End}_{M_n(F)}(F^n) = \{f \in \mathrm{End}_F(F^n) = M_n(F) : f(\alpha x) = \alpha f(x), \forall \alpha \in M_n(F), x \in F^n\}$$
$$= \{A \in M_n(F) : AB = BA, \forall B \in M_n(F)\} = \{\lambda I_n : \lambda \in F\} \cong F$$

Hence we find that $\mathrm{End}_{M_n(F)}(F^n)$ is a division ring.

The converse does not hold:

Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. It is certainly not simple. Indeed it contains $\mathbb{Z}$ as a proper submodule. However, $\mathrm{End}_{\mathbb{Z}}(\mathbb{Q}) = \mathbb{Q}$.

Indeed, let f be an endomorphism of the $\mathbb{Z}$-module $\mathbb{Q}$. Then, for any $n \in \mathbb{Z}$, $f(n) = nf(1)$ and for $n \neq 0$,

$$f(1) = f(n\frac{1}{n}) = nf(\frac{1}{n})$$

hence $f(\frac{1}{n}) = \frac{1}{n}f(1)$. It follows that $f(a) = af(1)$ for all $a \in \mathbb{Q}$.

The map $\mathrm{End}(\mathbb{Q}) \longrightarrow \mathbb{Q}$ sending f to $f(1)$ is an isomorphism.

Let's look at a few more examples of $\mathbb{Z}$-modules:

Every simple $\mathbb{Z}$ module is finite. Indeed, let M be an simple $\mathbb{Z}$-module. Let $v \in M$ be a non-zero vector. The map $\phi\colon n \mapsto nv$ from $\mathbb{Z}$ to M is a non-zero morphism of modules. As $M$is simple, ϕ surjective. The kernel of ϕ is a proper submodule of $\mathbb{Z}$ (it is not zero as otherwise $\mathbb{Z} \cong M$ and $\mathbb{Z}$ is not semi-simple, it is not $\mathbb{Z}$ because ϕ is non-zero). The kernel is $n\mathbb{Z}$ and M is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ hence finite.

We claim that n has to be a prime number. If not, then two cases occur.

Case 1:

$n = n_1 n_2$ with n_1, n_1 coprime and $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ hence not simple.

Case 2:

n is a power of a prime number, say $n = p^n$ with $n > 1$. Then $\mathbb{Z}/p^n\mathbb{Z}$ contains a non-trivial submodule $\mathbb{Z}/p\mathbb{Z}$ hence is not simple.

The only simple $\mathbb{Z}$-modules are the $\mathbb{Z}/p\mathbb{Z}$ where p is a prime

Ex. Show that simple modules over $F[x]$ are the $F[x]/I$ where I is a prime ideal.

Definition 0.6. *A module is called* semisimple *if it is a direct sum of simple modules.*

Consider the example of $M_n(F)$ viewed as a left module. This module is *not* simple. Indeed, we have seen that it contains submodules C_j (column) vectors. The modules C_j *are* simple and quite clearly

$$M_n(F) = \oplus_{j=1}^{n} C_j$$

The module $M_n(F)$ is thus semi-simple. Recall from what preceeded that the *ring* $M_n(F)$ is simple.

We now prove the following characterisation of semisimple modules (at least the finitely generated ones):

Proposition 0.6. *Let M be a* finitely generated *R-module. The following properties are equivalent.*

(1) *Any submodule of M is a direct summand i.e, if $W \subset M$ is a submodule, then there exists a submodule W' such that $= W \oplus W'$.*
(2) *M is a finite sum of simple submodules.*

Proof. Let us first show that (2) implies (1).

We suppose that M is semisimple. By definition,

$$M = \oplus_{i \in I} M_i$$

where I is a certain finite set of integers and M_i are simple submodules of M.

Let W be a submodule of M. We can assume that $W \neq M$ and that $W \neq 0$ as otherwise there is nothing to prove.

Let J be the subset of I consisting of all is such that $W \cap M_i = \{0\}$.

Notice that the complement of J in I consists of all is such that $M_i \subset W$. Indeed, if $i \notin J$, then $W \cap M_i$ is a non-zero submodule of M_i which is simple hence $W \cap M_i = M_i$ i.e. $M_i \subset W$.

The sum $W^* = W + \oplus_{i \in J} M_i$ is direct by definition of J.

Let us show that $W^* = M$ which is equivalent to showing that $M_i \subset W^*$ for any $i \in I$.

Let $i \in I$.

If $M_i \cap W = \{0\}$ then $i \in J$ and $M_i \subset W^*$. If $M_i \cap W \neq \{0\}$ then, because M_i is simple, $W \cap M_i = M_i$ i.e. $M_i \subset W$. Again $M_i \subset W^*$.

Hence $W^* = M$. We take $W' = \oplus_{i \in J} M_i$. This finishes the proof of (2) implies (1).

Remark 0.7. *Notice that as a subproduct of this proof we proved that a submodule and a quotient of a semisimple module is semisimple.*

Indeed, let M be a semisimple module, $M = \oplus_{i \in I} M_i$. Let W be a submodule and $J \subset I$ as in the proof. We showed that

$$M = W \oplus W'$$

where $W = \oplus_{i:M_i \subset W} M_i$ hence W is semisimple. We also showed that $W' = \oplus_{i:M_i \cap W = \{0\}} M_i$. As $M/W \cong W'$, it is semisimple.

Let us do (1) implies (2). We suppose that every submodule of M admits a direct summand.

We need an intermediate lemma:

Lemma 0.8. *Every non-zero module satisfying the assumtion (1) contains a simple module.*

Proof. Before giving a proof, let us introduce the following definitions.

Definition 0.7. *A submodule $N \subset M$ is called* maximal *if for any submodule $K \subset M$ such that $N \subset K \subset M$, then either $K = N$ or $K = M$.*

In particular a (left) ideal in R is called maximal *if and only if $A \neq R$ and for any left ideal B with $A \subset B \subset R$, either $A = B$ or $B = R$.*

Clearly a submodule $N \subset M$ is maximal if and only if M/N is simple.

We use without proof the following proposition:

Proposition 0.9. *Any proper submodule of a finitely generated module is contained in a maximal submodule.*

Let V be a non-zero R-module satisfying the assumption (1). Let $v \in V$ a non-zero element. Consider the submodule Rv and a homomorphism $\phi\colon R \longrightarrow Rv$. The kernel L of ϕ is a left ideal in R, different from R. It is contained in a maximal ideal $M \neq R$. Then M/L is a *maximal* submodule of R/L. It follows that Mv is a maximal submodule of Rv (recall that $R/\ker(\phi) = R/L$ is isomorphic to $\mathrm{im}(\phi) = Rv$), hence M/L is isomorphic to Mv. As V satisfies the assumption (1), we have

$$V = Mv \oplus M'$$

for some submodule M'. When we intersect with Rv, we get

$$Rv = Mv \oplus (M' \cap Rv)$$

(simply write that any element of $x \in Rv$ decomposes uniquely as $x = \alpha v + x'$ with $x' \in M'$). The module $M' \cap Rv$ is simple as it is isomorphic to Rv/Mv which is simple because Mv is maximal. □

Now, let $M_0 \subset M$ be the sum of all simple submodules of M. If $M_0 \neq M$, then we write

$$M = M_0 \oplus W$$

with $W \neq \{0\}$. As W is not zero, there exists a simple submodule of W, thus contradicting the definition of M_0. Therefore $W = \{0\}$ and M is the sum of all its disctinct simple submodules M_i. This sum is automatically direct, as for $i \neq j$, $M_i \cap M_j$ is either $\{0\}$ or M_i. In the latter case, $M_i = M_j$ contradicting the fact that the M_i are distinct. We obtain that M is direct sum of simple submodules. The sum is finite because M is finitely generated. □

This proposition for example shows that $\mathbb{Z}$ is not semisimple as a $\mathbb{Z}$-module. We have seen that the only simple $\mathbb{Z}$-modules are the $\mathbb{Z}/p\mathbb{Z}$ with p prime and $\mathbb{Z}$ is clearly not a sum of a finite number of such modules: $\mathbb{Z}$ is torsion free while such a sum certainly isn't.

By Chinese remainder theorem, semisimple $\mathbb{Z}$-modules are precisely the $\mathbb{Z}/n\mathbb{Z}$ where n is a square-free integer.

If F is a field, then F^n is certainly semisimple as an F-module. In fact any semisimple F-module is isomorphic to F^n for some n i.e. it is a finite dimensional vector space.

We now define the notion of an Algebra over a field.

Definition 0.8. *Let F be a field. An* algebra *A over F is a ring which has a structure of a F-vector space which is compatible with the ring multiplication in the following sense:*

$$(\lambda a)b = \lambda(ab) = a(\lambda b)$$

for all $\lambda \in F$ and $a, b \in A$.

An algebra is finite dimensional (one also says of finite rank) if its dimension as F-vector space is finite.

A homomorphism of algebras is naturally a ring homomorphism which is also a linear transformation.

For example : F, $F[X]$, $F[X]/I$ (I ideal), $M_n(F)$ are all algebras...

The algebra $F[X]$ is not finite dimensional.

In what follows we will implicitly assume that our algebras are finite dimensional.

The quaternion algebra is an algebra over the reals, however it is not an algebra over the complexes (recall that $zj = j\overline{z}$!).

As an algebra is a ring, we can look at modules over it, which will be automatically endowed with the structure of an F-vector space. In particular :

Definition 0.9. *An algebra A is called* semisimple *if all non-zero A-modules are semisimple.*

And we immediately prove the following result which characterises semisimple algebras:

Proposition 0.10. *An algebra A is semisimple if and only if the A-module A is semisimple.*

Proof. Suppose A to be semisimple as A-module. Let M be an A-module and choose a set $\{m_1, \ldots, m_r\}$ of generators for M. Let A^r be the direct sum of r copies of A. This is clearly a semisimple A-module (write $A = \oplus A_i$ with A_i simple A-modules, then $A^r = \oplus A_i^r \ldots$). Define a map

$$\phi \colon A^r \longrightarrow M$$

Clearly ϕ is a surjective morphism hence M is isomorphic to a quotient of a semisimple module A^r. From the previous proposition, it follows that M is semi-simple.

The converse is trivial. □

Proposition 0.11. *Let A be a semisimple algebra. Suppose that, as an A-module, A is a sum*

$$A = A_1 \oplus \cdots \oplus A_r$$

of simple A-modules A_i.

Then any *simple A-module is isomorphic to one of the A_i.*

Proof. Let S be a simple A-module and fix $s \in S$, $s \neq 0$. Then As is a submodule of S and consider the epimorphism

$$\phi \colon A \longrightarrow As$$

sending a to as. As S is simple, we have $As = S$. Let ϕ_i be the restriction of ϕ to A_i. If $\phi_i = 0$ for all i, then $\phi = 0$ which is not the case, hence there exists an i such that $\phi_i \neq 0$. By **Shur's lemma**, ϕ_i is an isomorphism. □

Proposition 0.12. *Suppose that A is semisimple algebra and let A_i be the collection of simple distinct A-submodules of A.*

Let M be an A-module (automatically semisimple). There is a unique *set of integers n_i such that*

$$M = A_1^{n_1} \oplus \cdots \oplus A_r^{n_r}$$

Only the uniqueness needs proving. This will follow from the definition and a theorem stated below.

Definition 0.10. *Let M be a module over a ring R. A composition series of M is a finite sequence of submodules $N_i \subset M$ such that*

$$M = N_r \supset N_{r-1} \supset \cdots \supset N_0 = \{0\}$$

and

$$N_i/N_{i-1}$$

is a simple module.

A module may or may not have a composition series. For example, $\mathbb{Z}$ viewed as a module over itself does not have a composition series. Indeed, if there was one, then $N_1 = n\mathbb{Z}$ for some integer $n \neq 0$, but then $N_1/N_0 = n\mathbb{Z}$ which is not a simple $\mathbb{Z}$-module (we have seen that simple $\mathbb{Z}$-modules are finite).

A semisimple module always has a composition series: if $M = M_1 \oplus \cdots\cdots M_r$ with M_is simple, one can set $N_i = N_1 \oplus \cdots \oplus M_i$.

Two somposition series N_i $(i = 0, \ldots, r)$ and N_i' $(i = 0, \ldots, s)$ are equivalent if $r = s$ and after permutation $N_i/N_{i-1} \cong N_i'/N_{i-1}'$.

We use the following

Theorem 0.13 (Jordan-Holder)**.** *Let M be a finitely generated R module having a composition series. Any two composition series are equivalent.*

The uniqueness of the n_is follows immediately from this theorem.

Recall that our aim is to classify semisimple algebras. We now start working towards it.

Let D be a finite-dimensional F-algebra. For any n, let $M_n(D)$ be set of $n \times n$-matrices with entries in D. This is an F-algebra of dimension $n^2 \dim_F(D)$.

We say that D is a **division algebra** if D is a division ring - any non-zero element has a multiplicative inverse. For example any field is a division algebra, $\mathbb{H}$ is a division algebra...

The algebra $M_n(F)$ is not a division algebra if $n > 1$, a product $D_1 \times D_2$ of division algebras is not a division algebra (it contains non-zero elements such as $(a, 0)$).

The following theorem of Frobenius classifies all finite dimensional division algebras over the reals:

Theorem 0.14. *The only finite dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.*

They have dimensions one, two and four respectively.

The aim of this part of the course is to show that any semisimple algebra is isomorphic to a direct sum of algebras of the form $M_n(D)$ where D is a division algebra.

We define the notion of *opposite algebra.* Let B be an algebra. The algebra B^{op} is the set B with the same addition and scalar multiplication but with multiplication befined as

$$a * b = ba$$

The following properties are obvious:

(1) $B^{op^{op}} = B$
(2) B is a division algebra if and only if B^{op} is
(3) $(B_1 \oplus B_2)^{op} = B_1^{op} \oplus B_2^{op}$

We also have:

Lemma 0.15. *Let B an algebra. Then $M_n(B)^{op} \cong M_n(B^{op})$ for any n.*

Proof. Define
$$\psi\colon M_n(B)^{op} \longrightarrow M_n(B^{op})$$
by setting $\psi(X) = X^t$. Obviously it is bijective. It is an exercise in matrix multiplication to show that
$$\psi(X * Y) = \psi(X)\psi(Y)$$
□

We prove the following:

Lemma 0.16. *Let B an algebra. Then*
$$B^{op} \cong \mathrm{End}_B(B)$$

Proof. Let $\phi \in \mathrm{End}_B(B)$ and let $a = \phi(1)$. Then for any b in B, we have
$$\phi(b) = b\phi(1) = ba$$
Hence $\phi = \rho_a$, endomorphism given by right multiplication by a. Therefore
$$\mathrm{End}_B(B) = \{\rho_a : a \in B\}$$
hence ther is a bijection between B and $\mathrm{End}_B(B)$. We need to show that
$$\rho_a\rho_b = \rho_{a*b}$$
Let $a, b, x \in B$. We have
$$(\rho_a\rho_b)(x) = xba = \rho_{ba}(x) = \rho_{a*b}(x)$$
□

Lemma 0.17. *If S is a simple A-module, then for any n, we have*
$$\mathrm{End}_A(S^n) = M_n(\mathrm{End}(S))$$

Proof. Regard elements of S^n as column vectors. Let $A = (a_{ij}) \in M_n(\mathrm{End}(S))$ and define $\Gamma(A)\colon S^n \longrightarrow S^n$ by
$$\Gamma(A)\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{nn} \end{pmatrix}\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$$
One sees that
$$\Gamma(A)(as + t) = a\Gamma(A)s + \Gamma(A)t$$
(because a_{ij} are A-module homomorphisms). It follows that $\Gamma(A) \in \mathrm{End}(S^n)$.

Ex. Check that $\Gamma\colon M_n(\mathrm{End}(S)) \longrightarrow \mathrm{End}(S^n)$ is an algebra monomorphism.

Conversely, let $\psi \in \mathrm{End}(S^n)$. Define $\psi_{ij} \in \mathrm{End}(S)$ by

$$\psi \begin{pmatrix} 0 \\ \vdots \\ 0 \\ s \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \psi_{1j}(s) \\ \psi_{2j}(s) \\ \vdots \\ \psi_{jj}(s) \\ \vdots \\ \psi_{n-1,j}(s) \\ \psi_{n,j}(s) \end{pmatrix}$$

The matrix $\Psi = (\psi_{ij}) \in M_n(\mathrm{End}(S))$ is such that $\Gamma(\Psi) = \psi$ which shows that Γ is surjective. □

We also have the following:

Proposition 0.18. *Let U_1 and U_2 be two submodules of an R-module such that $U_1 \cap U_2 = \{0\}$. Then*

$$\mathrm{End}(U_1 \oplus U_2) = \mathrm{End}(U_1) \oplus \mathrm{End}(U_2)$$

Proof. Exercise □

Next we prove the following lemma which is of independent interest:

Lemma 0.19. *Let D be a finite dimensional division algebra over an* **algebraically closed** *field F. Then*

$$D \cong F$$

Proof. Let $a \in D$, $a \neq 0$. As D is finite dimensional, the powers $1, a, \dots, a^k, \dots$ are linearle dependent over F. Therefore there is a relation:

$$a^n + c_1 a^{n-1} + \cdots + c_0 = 0$$

where we choose n to be the smallest possible.

Consider $f(x) = x^n + c_1 x^{n-1} + \cdots c_0$. As F is algebraically closed, f has a root λ in F i.e

$$f(x) = (x - \lambda) g(x)$$

with $\deg(g) = \deg(f) - 1$. Evaluating at a we get

$$(a - \lambda) g(a) = 0$$

As f was chosen to be of smallest degree, $g(a) \neq 0$ hence is invertible (D is a division algebra). It follows that $a = \lambda \in F$, hence $D = F$. □

The immediate consequence of this lemma and of Shur's lemma is the following:

Lemma 0.20 (Burnside)**.** *Suppose F is algebraically closed and let S be a simple A-module. Then*

$$\mathrm{End}_A(S) = F$$

One can also give a direct proof of the last theorem as follows: Let $\phi \in \mathrm{End}_A(S)$ and view it as an F-linear map of the F-vector space S. Furthermore, ϕ is invertible (by Shur). Since F is algebraically closed, ϕ has an eigenvalue λ and we get $\phi - \lambda I \in \mathrm{End}_A(S)$ which is not invertible. By Shur, it is zero and hence $\phi = \lambda I$. The map $\phi \mapsto \lambda$ is an isomorphism $\mathrm{End}_A(S) \cong F$.

We now prove the main theorem.

Theorem 0.21 (Artin-Wedderburn)**.** *An algebra A over a field F is semisimple if and only if A is isomorphic to a direct sum of matrix algebras over division algebras i.e. there exist integers n_i and division algebras D_i such that*

$$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$$

Proof. The converse is already established.

Suppose that A is semisimple. Let A_is be the non pairwise isomorphic simple submodules of A.

Write $A = U_1 \oplus \cdots \oplus U_r$ where $U_i = A_i^{n_i}$ for some $n_i \geq 1$.

We have

$$\begin{aligned} A^{op} \cong \mathrm{End}_A(A) &\cong \mathrm{End}_A(U_1) \oplus \cdot \oplus \mathrm{End}_A(U_r) \\ &\cong \mathrm{End}(A_1^{n_1}) \oplus \cdots \oplus \mathrm{End}_A(A_r^{n_i})) \\ &\cong M_{n_1}(\mathrm{End}(A_1)) \oplus \cdots \oplus M_{n_r}(\mathrm{End}(A_r)) \end{aligned}$$

By taking opposites, we find that

$$A^{op} \cong M_{n_1}(\mathrm{End}(A_1)^{op}) \oplus \cdots \oplus M_{n_r}(\mathrm{End}(A_r)^{op})$$

By Shur all the $D_i = \mathrm{End}(A_i)$s are division algebras.

By taking the opposite we find:

$$A = A^{opop} \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$$

This finishes the proof. □

The following corollary will be relevant to representation theory:

Corollary 0.22. *Suppose that F is algebraically closed. Then any semisimple algebra is isomorphic to a direct sum of matrix algebras over F.*