Introduction to representation theory
Lecture 4

Alexei KOTOV

University of Hradec Králové
Faculty of Science

July 19, 2021, Hradec Kralove

Rings and algebras

- A ring $\mathcal{R}$ is an abelian group together with an associative multiplication respecting the group structure (the summation):

$$(a+b)(c+d) = ac + ad + bc + bd, \quad \forall a, b, c, d \in \mathcal{R}$$

- A ring is a k−algebra if, in addition, it is a vector space over a field k, such that the multiplication is a bilinear operation. There are also algebras over rings (we will define them later).
- A ring (an algebra) is unital if it has identity.
- A division ring (a division algebra) if any its non-zero element is invertible.

Examples of rings and algebras

(*) Any field is a ring, an algebra over itself and a commutative division algebra.

(*) $\mathbb{Z}$ is a ring.

(*) $\mathbb{H}$ is a non-commutative division algebra.

(*) For a ring (an algebra) $\mathcal{R}$, the set of polynomials with $\mathcal{R}-$coefficients is a ring (an algebra). It is commutative if and only if so is $\mathcal{R}$.

(*) For any set X, the space of functions on X with values in a ring (algebra) $\mathcal{R}$ is a ring (an algebra) under the pointwise product. It is commutative if and only if so is $\mathcal{R}$.

(*) For a ring (an algebra) $\mathcal{R}$, $\mathrm{Mat_n}(\mathcal{R})$ is a ring (an algebra).

(*) For any vector space V over a field k, $\mathrm{End_k}(\mathrm{V})$ is a k$-$algebra.

- A subring (a subalgebra) is a subset which is closed under both operations. It is a ring (an algebra) itself.
- Given a (possibly infinite) collection of rings (algebras), their Cartesian product and direct sum are rings (algebras).
- A left (right) ideal is a subring (a subalgebra) stable under the left (right) multiplication on all elements from the ring (algebra); if it is left and right at the same time, it is called a two-sided ideal or just an ideal.
- A morphism of rings (algebras) is a map, which preserves both the additive and the multiplicative structures.
- Rings (algebras) form a category, whose objects are ring (algebras) and arrows are the corresponding morphisms.
- The kernel of any morphism is an ideal. The image of a morphism is a subring.

- An ideal is called proper if it does not coincide with the whole ring (algebra); non-trivial if it is proper and non-zero.
- A non-zero ideal is called minimal if it does not strictly contain any other non-zero ideal.
- A non-trivial ideal which is not strictly contained in any other proper ideal is called maximal.
- A ring (an algebra) is called simple if it does not have ideals other than $\{0\}$ and itself.
- A semisimple algebra is a direct sum of simple algebras.
- An algebra is semisimple if and only if it is the direct sum of its minimal ideals. Indeed, any summand in the direct sum of simple algebras is a minimal ideal. Vice versa, for any two ideals from the above collection, their product belongs to their intersection which is zero, thus the ring is the direct sum of algebras.

Modules over rings

For any abelian group, the set of its endomorphisms is a ring with respect to the natural summation and composition of maps.

We call an abelian group $\mathcal{M}$ a module over a ring $\mathcal{R}$ if there is a morphism $\mathcal{R} \to \mathrm{End}(\mathcal{M})$, i.e. to each $a \in \mathcal{R}$ we associate a map

$$\mathcal{M} \ni x \mapsto ax \in \mathcal{M}$$

such that

$$a(x_1 + x_2) = ax_1 + ax_2, \ \ a_1(a_2x) = (a_1a_2)x$$

$$(a_1 + a_2)x = a_1x + a_2x, \ \ \forall a, a_1, a_2 \in \mathcal{R}, x, x_1, x_2 \in \mathcal{M}$$

A morphism of modules is a morphism of the corresponding abelian groups which commutes with the action of the ring.

Example. Every abelian group is a $\mathbb{Z}-$module.

A vector space over k is linear module over a ring (an algebra) $\mathcal{R}$ if there is a morphism $\mathcal{R} \to \mathrm{End}_{\mathrm{k}}(\mathrm{V})$.

A morphism of linear modules is a k−linear map which commutes with the action of the ring (the algebra).

Modules and linear modules over a ring (an algebra) is a category, the objects of which are modules and the morphisms are the corresponding morphisms.

- (*) A vector space V over a field k is a k−module.
- (*) V is also a module over $\mathrm{End}_{\mathrm{k}}(\mathrm{V})$ as well as over any subring $\mathcal{R} \subset \mathrm{End}_{\mathrm{k}}(\mathrm{V})$.
- (*) In general, for any morphism of rings $\mathcal{R}_1 \to \mathcal{R}_2$, if V is an $\mathcal{R}_2$−module, then it is automatically an $\mathcal{R}_1$−module.
- (*) Hereafter, by a module over a group or a k−algebra we will mean a linear module (unless otherwise specified).

- (*) Simple modules and irreducible representations for rings (algebras) are defined in the same way as for groups.
- (*) The Schur's Lemma is true, i.e. morphisms between two simple modules are either isomorphisms or equal to zero.
- (*) In particular, for an irreducible representation of a ring $\mathcal{R}$ on V, its commutant $\mathcal{R}' = \mathrm{End}_{\mathcal{R}}(\mathrm{V})$, i.e. the set of linear operators commuting with the action of $\mathcal{R}$, is a division k−algebra. In general, $\mathcal{R}' = \mathrm{End}_{\mathcal{R}}(\mathrm{V})$ is just a k−algebra.
- (*) Given an indexed, possibly infinite, collection of rings (algebras) and their modules $\{(\mathcal{R}_\mathrm{i}, \mathrm{V}_\mathrm{i})\}_{\mathrm{i}\in\mathrm{I}}$, the Cartesian product $\mathrm{V}_\mathrm{I} = \prod_{\mathrm{i}\in\mathrm{I}} \mathrm{V}_\mathrm{i}$ and the direct sum $\bigoplus_{\mathrm{i}\in\mathrm{I}} \mathrm{V}_\mathrm{i}$ are modules over $\mathcal{R}_\mathrm{I}$, where $\mathcal{R}_\mathrm{I} = \prod_{\imath\in\mathrm{I}} \mathcal{R}_\mathrm{i}$.

(*) In particular, if $\mathcal{R}_i = \mathcal{R}$ for all $i \in I$, then V_I and $\bigoplus_{i \in I} V_i$ are modules over $\mathcal{R}_I$, the product of I copies of $\mathcal{R}$.

(*) The diagonal embedding $\mathcal{R} \to \mathcal{R}_I$ is a morphism of rings (algebras), thus V_I and $\bigoplus_{i \in I} V_i$ are also $\mathcal{R}-$modules.

(*) Besides, given any $k \in I$, there is a monomorphism $\mathcal{R} \hookrightarrow \mathcal{R}_I$, which associates to any $a \in \mathcal{R}$ a function on I

$$I \ni i \mapsto \begin{cases} a, & i = k \\ 0, & i \neq k \end{cases}$$

When I is finite, it is

$$\mathcal{R} \ni a \mapsto (0, \dots, \overset{i}{a}, \dots, 0) \in \mathcal{R}_I$$

Therefore the direct product and the direct sum of a collection of $\mathcal{R}-$modules indexed by I, can be endowed with an $\mathcal{R}-$module structure in I possible ways.

Geometrical point of view.

The direct product of an I−family of rings (algebras) and modules $(\mathcal{R}_i, V_i)$ can be viewed as the space of sections of the following "bundles":

$$\coprod_{i\in I} \mathcal{R}_i \to I, \quad \mathcal{R}_i \ni a_i \mapsto i \in I$$

$$\coprod_{i\in I} V_i \to I, \quad V_i \ni v_i \mapsto i \in I$$

The diagonal embedding corresponds to constant sections, while the embedding on the k−th position to "delta functions".

There are obvious topological (smooth) counterparts in the category of topological spaces (smooth manifolds).

Let $\mathcal{R}$ be a ring, $\{V_i\}_{i \in I}$ and W be $\mathcal{R}-$modules. A multilinear map $\phi\colon \prod_{i \in I} V_i \to W$ is called $\mathcal{R}-$multilinear if it commutes with the $\mathcal{R}-$action on each argument.

Eg. for a finite index set $I = \{1, \dots, m\}$, this implies that for all $a \in \mathcal{R}$, $v_j \in V_j$, $j = 1, \dots, m$ one has

$$\phi(v_1, \dots, av_i, \dots, v_m) = a\phi(v_1, \dots, v_i, \dots, v_m)$$

A ring $\mathcal{A}$ is called an $\mathcal{R}-$algebra, if it is an $\mathcal{R}-$module and the multiplication $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$ is $\mathcal{R}-$bilinear.

- (*) $\mathcal{R}[t]$, the ring of polynomials with coefficients in $\mathcal{R}$ is an $\mathcal{R}-$algebra.
- (*) If $\mathcal{R}$ is commutative, then $M_n(\mathcal{R})$ is an $\mathcal{R}-$algebra.
- (*) If $\mathcal{R}$ is a unital ring, i.e. it has a unit, then any $\mathcal{R}-$algebra is a k$-$algebra.
- (*) In general, for any morphism of rings $\mathcal{R}_1 \to \mathcal{R}_2$, if $\mathcal{A}$ is an $\mathcal{R}_2-$algebra, then it is an $\mathcal{R}_1-$algebra.

General problems in representation theory

Given a group (semigroup, ring, algebra, ...), it is natural to address the problem of classification of its linear representations.

Isomorphic object possesses the same properties $\Longrightarrow$

Two isomorphic objects are viewed as the same $\Longrightarrow$

The problem is to classify representations up to isomorphisms

Example

Linear representations of the algebra of polynomials $k[x]$ on a $k-$vector space V are in on-to-one correspondence with linear operators A, so that $x \mapsto A \in \mathrm{End}(V)$ and

$$k[x] \ni p(x) \mapsto p(A) \in \mathrm{End}(V)$$

The problem: classify normal forms of linear operators with respect to the conjugation $A \mapsto CAC^{-1}$, $C \in GL(V)$.

For a finite-dimensional V over $\mathbb{C}$, the answer is known as the Jordan canonical (or normal) form. Eg.

$$A = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_2 & 1 & 0 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_3 & 1 & 0 \\ 0 & 0 & 0 & 0 & \lambda_3 & 1 \\ 0 & 0 & 0 & 0 & 0 & \lambda_3 \end{pmatrix}, \quad \lambda_1, \lambda_2, \lambda_3 \in \mathbb{C}$$

Remark that A decomposes into 3 blocks, corresponding to the decomposition $V = V_1 \oplus V_2 \oplus V_3$, where $V = \mathbb{C}^6$, $V_1 = \mathbb{C}^1$, $V_2 = \mathbb{C}^2$ and $V_3 = \mathbb{C}^3$, such that $A_i \in \mathrm{End}(V_i)$ for $i = 1, 2, 3$:

$$A = \begin{pmatrix} A_1 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & A_3 \end{pmatrix}$$

Decomposition of modules

Given a linear module, another problem is to find its decomposition into the direct sum of submodules, as elementary as possible.

The simplest possible "bricks" are simple modules, which correspond to irreducible representations. If a module decomposes in a direct sum of simple submodules, it is called semisimple, and so is the decomposition.

In the previous example (representation of $\mathbb{C}[x]$ in $V = \mathbb{C}^3$), $V_1 = \mathbb{C}^1$ is a simple module, while the other two are not. For instance, for (V_3, A_3) there is a chain of submodules

$$\{0\} \subset \mathbb{C}^1 \subset \mathbb{C}^2 \subset \mathbb{C}^3 = V_3$$

such that A_3 acts on $\mathbb{C}^1$ by multiplication on λ_3 and on $\mathbb{C}^2$ as

$$\begin{pmatrix} \lambda_3 & 1 \\ 0 & \lambda_3 \end{pmatrix}$$

Notice that both quotient modules $\mathbb{C}^2/\mathbb{C}^1$ and $\mathbb{C}^3/\mathbb{C}^2$ are isomorphic to $(\mathbb{C}^1, \lambda_3)$. Therefore there exist exact short sequences of linear modules

$$\{0\} \subset \mathbb{C}^1 \hookrightarrow \mathbb{C}^2 \twoheadrightarrow \mathbb{C}^1 \to \{0\}$$

$$\{0\} \subset \mathbb{C}^2 \hookrightarrow \mathbb{C}^3 \twoheadrightarrow \mathbb{C}^1 \to \{0\}$$

which we can not split in the category of modules: the matrix corresponding to the direct sum of two copies of the representation $(\mathbb{C}^1, \lambda_3)$ would be the operator of multiplication on λ_3 in $\mathbb{C}^2$, which is clearly not conjugated to

$$\begin{pmatrix} \lambda_3 & 1 \\ 0 & \lambda_3 \end{pmatrix}$$

Semisimple decomposition

For a module W, denote

$$\mathrm{rW} = \underbrace{\mathrm{W} \oplus \ldots \oplus \mathrm{W}}_{\mathrm{r}}$$

Let V be a module. Assume V is semisimple, i.e. it splits in a direct sum of simple submodules

$$\mathrm{V} = \bigoplus_{\rho} \mathrm{r}_\rho \mathrm{V}_\rho$$

such that V_{ρ_1} and V_{ρ_2} are isomorphic if and only if $\rho_1 = \rho_2$.

Proposition (for a finite semisimple decomposition).

The collection of simple modules $\{\mathrm{V}_\rho\}$ and the multiplicities $\{\mathrm{r}_\rho\}$ are uniquely determined by V (up to an isomorphism).

Proof.

Assume that V decomposes in a different way:

$$\mathrm{V} = \bigoplus_{\rho'} \mathrm{r}_{\rho'} \mathrm{V}_{\rho'}$$

Let

$$\{\lambda_\mathrm{i}\} = \{\underbrace{\rho_1, \dots, \rho_1}_{\mathrm{r}_1}, \underbrace{\rho_2, \dots, \rho_2}_{\mathrm{r}_2}, \dots\}$$

$$\{\lambda'_\mathrm{i}\} = \{\underbrace{\rho'_1, \dots, \rho'_1}_{\mathrm{r}'_1}, \underbrace{\rho'_2, \dots, \rho'_2}_{\mathrm{r}'_2}, \dots\}$$

be the sets of all indices written in a row.
Take V_{λ_1} and $\mathrm{V}_{\lambda'_1}$ and consider the following composition of morphisms

$$\mathrm{V}_{\lambda_1} \hookrightarrow \mathrm{V} \xrightarrow{\pi'_1} \mathrm{V}_{\lambda'_1}$$

where π'_1 is the projection of V onto $\mathrm{V}_{\lambda'_1}$.

There are two possibilities:

(i) V_{λ_1} and $V_{\lambda'_1}$ are not isomorphic. Then $\pi'_1(V_{\lambda_1}) = \{0\}$ and

$$V_{\lambda_1} \subset \bigoplus_{\lambda' \neq \lambda'_1} V_{\lambda'} = \operatorname{Ker} \pi'_1$$

Finally we will find another index λ', such that $V_{\lambda_1} \simeq V_{\lambda'}$.

(ii) $V_{\lambda_1} \simeq V_{\lambda'_1}$. Then there is an isomorphism of modules

$$\bigoplus_{\lambda \neq \lambda_1} V_{\lambda} \simeq \bigoplus_{\lambda' \neq \lambda'_1} V_{\lambda'}$$

determined by $\bar{\pi}'_1 = \mathrm{id} - \pi'_1$ and we proceed by induction.

Proposition (equivalent definitions of a semisimple module).

Let V be a module over a ring $\mathcal{R}$. The following properties are equivalent.

(i) V is a sum of simple submodules.

(ii) V is a direct sum of simple submodules.

(iii) Every submodule $W \subset V$ is a direct summand, i.e. there exists a submodule $\bar{W}$, such that $V = W \oplus \bar{W}$.

Proof.

(i) $\longrightarrow$ (ii)

Let $V = \sum_{i \in I} V_i$ be the sum of all simple submodules.

Take a maximal $J \subset I$, such that the sum $V' = \sum_{j \in J} V_j$ is direct.

To make our life easier, we assume that I is finite and V is a finite-dimensional vector space.

However, this finiteness restriction can be avoided by use of the Zorn's lemma to prove the existence of a maximal J and (at least one) simple submodule of any submodule.

For any V_k, $k \notin J$, either:

(a) $V_k \cap V' = \{0\}$, but then the sum of V_k and V' is direct, which is not possible as J is minimal,

(b) $V_k \subset V'$.

Finally, $V_k \subset V'$ for all $k \in I$ and thus $V = V'$ and

$$V = \bigoplus_{j \in J} V_j$$

is the desired semisimple decomposition of V.

(ii) $\longrightarrow$ (iii)

Let J be a maximal subset of I, such that the sum of W and $V' = \bigoplus_{j \in J} V_j$ is direct (here $V = \bigoplus_{i \in I} V_j$). The collection of those subsets is not empty as, if $W \neq V$ then at least one simple submodule has zero intersection with W. Now we use the same trick as before by proving that every "new" simple submodule must belong to the direct sum of W and V′.

Thus $V = W \oplus V'$ and $\bar{W} = V'$.

(iii) $\longrightarrow$ (i)

Consider the sum V_0 of all simple submodules of V. There exists at least one simple submodule (by the finiteness assumption or by Zorn's Lemma).

V_0 a semisimple submodule of V. There exists V′, such that $V_0 \oplus V' = V$. If V′ is non-zero, there must be at least one simple submodule of V′. But then, by definition, it is in V_0, thus $V' = \{0\}$ and $V = V_0$.

Proposition.

Any submodule of a semisimple module is semisimple.

Proof.

Let $W \subset V$ be a submodule of a semisimple module.

Consider W_0, the sum of all simple submodules of W.

By property (iii) there exists $\bar{W}_0$, such that

$$V = W_0 \oplus \bar{W}_0$$

Every $w \in W$ uniquely decomposes into the sum $w_0 + \bar{w}_0$, $w_0 \in W_0$ and $\bar{w}_0 \in \bar{W}_0$. Now $\bar{w} = w - w_0 \in W$ and hence

$$W = W_0 \oplus (\bar{W}_0 \cap W)$$

But $\bar{W}_0 \cap W = \{0\}$, otherwise it will contain at least one simple submodule of W. We obtain $W = W_0$.

Corollary (of the two previous propositions).

Notations as above (the index set is finite).

(i) There exists a subset $\mathrm{I}' = \{\lambda'\} \subset \mathrm{I}$, such that

$$\mathrm{W} = \bigoplus_{\lambda' \in \mathrm{I}'} \mathrm{W}_{\lambda'}, \quad \bar{\mathrm{W}} = \bigoplus_{\mu \in \mathrm{I} \setminus \mathrm{I}'} \bar{\mathrm{W}}_{\mu}$$

with $\mathrm{W}_{\lambda'} \simeq \mathrm{V}_{\lambda'}$ and $\bar{\mathrm{W}}_{\mu} \simeq \mathrm{V}_{\mu}$ for all $\lambda' \in \mathrm{I}'$, $\mu \in \mathrm{I} \setminus \mathrm{I}'$.

(ii) In particular, if

$$\mathrm{V} = \mathrm{r}\mathrm{V}_{\rho},$$

then

$$\mathrm{W} = \mathrm{k}\mathrm{V}_{\rho}, \quad \bar{\mathrm{W}} = \mathrm{l}\mathrm{V}_{\rho}$$

for some non-negative integers k, l, such that $\mathrm{k} + \mathrm{l} = \mathrm{r}$.

Lemma.

Let V be a semisimple $\mathcal{R}-$module, $\mathcal{R}'$ be the commutant. Then for any $\mathrm{f} \in \mathrm{End}_{\mathcal{R}'}(\mathrm{V}), \mathrm{v} \in \mathrm{V}$, there exists $\mathrm{a} \in \mathcal{R}$, such that $\mathrm{av} = \mathrm{f}(\mathrm{v})$.

Proof.

Consider the submodule $\mathcal{R}\mathrm{v} = \{\mathrm{bv} \,|\, \mathrm{b} \in \mathcal{R}\}$.

Since V is semisimple, there is a complement W, so that

$$\mathrm{V} = \mathcal{R}\mathrm{v} \oplus \mathrm{W}$$

The projector $\pi\colon \mathrm{V} \to \mathcal{R}\mathrm{v}$ commutes with $\mathcal{R}$, thus it belongs to $\mathcal{R}'$ and, by the property of f, π commutes with f. Hence

$$\pi(\mathrm{f}(\mathrm{v})) = \mathrm{f}(\pi(\mathrm{v})) = \mathrm{f}(\mathrm{v})$$

which means $\mathrm{f}(\mathrm{v}) \in \mathcal{R}\mathrm{v}$, i.e. $\exists\, \mathrm{a} \in \mathcal{R}$, such that $\mathrm{f}(\mathrm{v}) = \mathrm{av}$.

Let V be a module over $\mathcal{R}$, $\mathcal{R}' = \mathrm{End}_{\mathcal{R}}(V)$ be the commutant. Consider the direct sum of n copies of V

$$V^n = nV = \underbrace{V \oplus \ldots \oplus V}_{n}$$

It is an $\mathcal{R}$−module with the action

$$a(v_1, \ldots, v_n) = (av_1, \ldots, av_1), \quad a \in \mathcal{R},\ v_1, \ldots, v_n \in V$$

Lemma

$\mathcal{R}'_n = \mathrm{End}_{\mathcal{R}}(V^n)$ is the ring of matrices with coefficients in $\mathcal{R}'$.

Explanation.

This means that $T \in \mathcal{R}'_n$ is in one-two-one correspondence with an $n \times n$ matrix (t_{ij}), whose elements belong to $\mathcal{R}'$, such that

$$T(v_1, \ldots, v_n) = \sum_{j=1}^{n} (t_{1j}(v_j), \ldots, t_{nj}(v_j)), \quad v_1, \ldots, v_n \in V$$

Proof.

Notice that for a general $T \in \mathrm{End}_k(V^n)$, the entries of the corresponding matrix (t_{ij}) consist of arbitrary linear operators acting on V. We have to prove that they belong to $\mathcal{R}'$.

Indeed, if $T \in \mathcal{R}'_n = \mathrm{End}_{\mathcal{R}}(V^n)$, then $\forall a \in \mathcal{R}, v_1, \ldots, v_n \in V$

$$aT(v_1, \ldots, v_n) = \sum_{j=1}^{n} (at_{1j}(v_j), \ldots, at_{nj}(v_j))$$

$$T(av_1, \ldots, av_n) = \sum_{j=1}^{n} (t_{1j}(av_j), \ldots, t_{nj}(av_j))$$

Clearly, this holds if all entries t_{ij} are in $\mathcal{R}'$, i.e. $at_{ij} = t_{ij}a$. To prove the converse, it is sufficient to consider vectors of the form

$$(0, \ldots, \overset{i}{v}, \ldots, 0)$$

for all $v \in V$ and $i = 1, \ldots, n$.

Theorem (Jacobson)

Let V be a semisimple module over $\mathcal{R}$ and $\mathcal{R}'$ be the commutant. Let $f \in \mathrm{End}_{\mathcal{R}'}(V)$, $v_1, \ldots v_n \in V$. Then there exists $a \in \mathcal{R}$, such that $av_i = f(v_i)$ for all $i = 1, \ldots, n$.

Proof.

The direct sum V^n is again a semisimple module over $\mathcal{R}$. Let $f^n : V^n \to V^n$,

$$f^n(v_1, \ldots, v_n) = (f(v_1), \ldots, f(v_n)), \quad v_1, \ldots, v_n \in V$$

Let $\mathcal{R}'_n = \mathrm{End}_{\mathcal{R}}(V^n)$; it is the ring of matrices with coefficients in $\mathcal{R}'$.

Since f commutes with elements of $\mathcal{R}'$, $f^n \in \mathrm{End}_{\mathcal{R}'_n}(V^n)$.

By the above Lemma, there exists $a \in \mathcal{R}$, such that $(av_1, \ldots, av_n) = (f(v_1), \ldots, f(v_n))$.

An $\mathcal{R}$−module V is called faithful, if $\mathcal{R} \to \mathrm{End_k(V)}$ is injective.

Theorem (Wedderburn)

Let V be a simple faithful module over $\mathcal{R}$, D be the commutant. Then $\mathcal{R} = \mathrm{End_D(V)}$.

Proof.

Let $\{e_i\}$ be a basis of V over D, $A \in \mathrm{End_D(V)}$.

By Jacobson theorem, there exists $a \in \mathcal{R}$, such that

$$ae_i = Ae_i \quad \text{for all } i = 1, \ldots, \dim V$$

Therefore $av = Av$ for any $v \in V$, which implies that $\mathcal{R} \to \mathrm{End_D(V)}$ is surjective.

But it is also injective as the module V is faithful.

Thus $\mathcal{R} = \mathrm{End_D(V)}$.

Corollary of the previous statements

(i) Every simple finite-dimensional $k-$algebra $\mathcal{A}$ is isomorphic to a matrix algebra over some division $k-$algebra.

(ii) In particular, if k is algebraically closed then $\mathcal{A}$ is isomorphic to $M_n(k)$ for some n.

Proof.

First we should verify that $M_n(D)$ is simple for any division ring D and $n \in \mathbb{N}$. Let $I \subset M_n(D)$ be a non-zero ideal. We have to show that $I = M_n(D)$.

Indeed, take the following basis $\{e_i\}_{i=1}^n$, where

$$e_i = (0, \ldots, \overset{i}{1}, \ldots, 0) \in D^n = \underbrace{D \oplus \ldots \oplus D}_{n}$$

It is sufficient to prove that I contains all elementary matrices

$$E_{ij}\colon D^n \to D^n, \quad E_{ij}(e_k) = \begin{cases} e_i, & j = k \\ 0, & j \neq k \end{cases}, \quad i, j, k = 1, \ldots, n$$

Let A be a non-zero element of I, such that $A(v) = w$ for some $v, w \in D^n \setminus \{0\}$. Choose B and C in $M_n(D)$, such that $B(w) = e_i$ and $C(e_i) = v$. Then $BAC = E_{ij}$.

Remark

While C is uniquely determined, there is an ambiguity with the choice of B. However, let us notice that, if the $k-$th component of w is not equal to zero then

$$\{e_1, \ldots, \overset{k}{w}, \ldots, e_n\}$$

is a new basis, so we can fix B by requiring $B(w) = e_i$ and $B(e_j) = 0$ for all $j \neq k$.

The rest of the proof is even easier. If $\mathcal{A}$ is simple:

(a) Consider any simple V over $\mathcal{A}$; one can take a minimal submodule of $\mathcal{A}$ corresponding to the left action of $\mathcal{A}$ on itself.

(b) V is a faithful module, since the kernel of $\mathcal{A} \to \mathrm{End}_{\mathrm{k}}(\mathrm{V})$ is an ideal, thus it has to be zero.

(c) By Schur's Lemma, $\mathrm{D} = \mathrm{End}_{\mathcal{A}}(\mathrm{V})$ is a division k−algebra.

(d) By the Wedderburn's theorem, $\mathcal{A} = \mathrm{End}_{\mathrm{D}}(\mathrm{V})$.

(e) For any choice of a basis of V over D, $\mathrm{End}_{\mathrm{D}}(\mathrm{V})$ becomes isomorphic to the matrix algebra with entries in D.

(f) If k is algebraically closed, then by Schur's Lemma, $\mathrm{D} = \mathrm{k}$.

(g) A semisimple algebra is a direct sum of simple algebras, therefore it is isomorphic to the direct sum of matrix algebras over division rings.