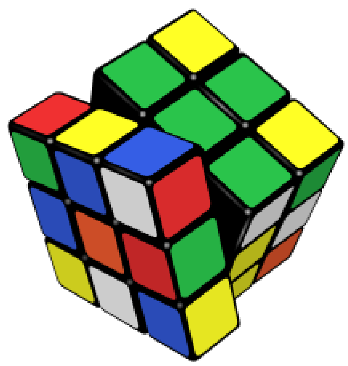
Representation Theory

2012



Contents

CHAPTER 1

Introduction

1. Algebraic Structures

Definition 1.1. **[Group, Monoid, Semigroup]** Let G be a set and let $\cdot$ be any binary operation on G:

$$\begin{array}{rccc} \cdot: & G \times G & \longrightarrow & G \\ & (g_1, g_2) & \longmapsto & g_1 \cdot g_2 \end{array}$$

Instead of writing $g_1 \cdot g_2$ we will omit the operation symbol and we will write $g_1 g_2$. We will say that $(G, \cdot)$ is a **group** if the following properties hold:

1) Associativity of $\cdot$. For all $g_1, g_2, g_3 \in G$, $(g_1 g_2) g_3 = g_1 (g_2 g_3)$.
2) Existence of a **neutrum element**. There exists some $e \in G$ such that for all $g \in G$ it holds: $ge = eg = g$. If such element exists it must be unique.

   Remark 1.2. Assuming the existence of two neutrum elements e and e' we get: $e' = e'e = e$. Therefore, such element is unique. Moreover, we will use indistinctly the notations 1, e or 1_G to denote this element.

3) Existence of an **inverse element**. For each $g \in G$, there exists an element $g' \in G$ such that $gg' = g'g = e$. If such element exists it must be unique.

   Remark 1.3. Assuming the existence of two inverse elements g' and g'' for g we get: $g' = g'gg'' = g''$. Therefore, such element is unique. We will denote this element by g^{-1}.

Given a group $(G, \cdot)$, we will say that it is **abelian** if for each $g_1, g_2 \in G$ it holds that $g_1 g_2 = g_2 g_1$.

We say that $(G, \cdot)$ is a **monoid** if properties 1) and 2) hold. We say that it is a **semigroup** if property 1) hold.

Definition 1.4. **[Subgroup]** Let $(G, \cdot)$ be a group and consider $H \subseteq G$ a subset of G. We say that H is a **subgroup of G** and we will denote it by $H \leq G$ if it is closed under the operation $\cdot$ and closed under taking inverses. That is to say:

- For all $h_1, h_2 \in H$, $h_1 h_2 \in H$.
- For all $h \in H$, $h^{-1} \in H$.

Definition 1.5. **[Ring]** Let R be a set and let $+$ and $\cdot$ be two binary operations on R:

$$\begin{array}{rccc} +: & R \times R & \longrightarrow & R \\ & (r_1, r_2) & \longmapsto & r_1 + r_2 \end{array} \qquad \begin{array}{rccc} \cdot: & R \times R & \longrightarrow & R \\ & (r_1, r_2) & \longmapsto & r_1 \cdot r_2 \end{array}$$

As before, we will use $r_1 r_2$ instead of $r_1 \cdot r_2$.

We will say that $(R, +, \cdot)$ is a **ring** if the following properties hold:

1) $(R, +)$ is an abelian group.

Remark 1.6. We will use additive notation for $(R,+)$. Therefore, for each $r \in R$ we will denote its inverse by $-r$ and we will use 0 or 0_R to denote the neutrum element.

2) $(R,\cdot)$ is a semigroup.
3) **Ditributivity** of $\cdot$ among $+$. That is, for all $r_1, r_2, r_3 \in R$ it holds:

$$r_1(r_2+r_3) = r_1r_2 + r_1r_3 \qquad (r_1+r_2)r_3 = r_1r_3 + r_2r_3$$

Remark 1.7. Under the last property we can prove that for each $r \in R$, $0r = r0 = 0$. Just notice that $r0 = r(r-r) = rr - rr = 0$.

We will say that the ring $(R,+,\cdot)$ is a **unit ring** if $(R,\cdot)$ is a monoid. We will denote its neutrum element by 1 or 1_R. We will say that it is **commutative** if for each $r_1, r_2 \in R$ it holds $r_1r_2 = r_2r_1$.

Let $S \subseteq R$ be any subset of R. We will say that it is a **subring of R** and we will denote it by $S \leq R$, if $(S,+) \leq (R,+)$ and it is closed under the operation $\cdot$, i.e., for all $s_1, s_2 \in S$ it holds that $s_1s_2 \in S$.

Definition 1.8. **[Ideal]** Let $(R,+,\cdot)$ be a ring and let $I \subseteq R$ be any subset of R. We say that it is a **right-ideal [left-ideal]** of R if the following properties hold:

1) $(I,+) \leq (R,+)$
2) For all $r \in R$ and for all $x \in I$ it holds $xr \in I$ $[rx \in I]$.

We say that I is a **bilateral ideal** of R, or just **ideal** of R, it is both left and right-ideal.

Proposition 1.9. *Let $(R,+,\cdot)$ be a ring and let $X = \{x_1, \cdots, x_t\} \subseteq R$ be any finite subset of R, it holds:*

- $(X)_R = (x_1, \cdots, x_t)_R = \{\sum_{i=1}^t x_ir_i : \ r_i \in R \ \ 1 \leq i \leq t\}$ *is a right-ideal.*
- $(X)_L = (x_1, \cdots, x_t)_L = \{\sum_{i=1}^t r_ix_i : \ r_i \in R \ \ 1 \leq i \leq t\}$ *is a left-ideal.*

Proof. We will just check the first statement. The second one is quite analogous. Clearly, $((X)_R,+)$ is a additive subgroup of $(R,+)$. Let now $x \in (X)_R$ be an arbitrary element and $r \in R$. By definition of $(X)_R$, there must exist $r_i \in R$ for $1 \leq i \leq t$ such that $x = \sum_{i=1}^t x_ir_i$. Now considering the product xr we get:

$$\begin{aligned} xr &= (\textstyle\sum_{i=1}^t x_ir_i)r \\ &= \textstyle\sum_{i=1}^t (x_ir_i)r \\ &= \textstyle\sum_{i=1}^t x_i(r_ir) \end{aligned}$$

Since $r_ir \in R$ for all $1 \leq i \leq t$, it holds that $xr \in (X)_R$. $\square$

Definition 1.10. **[Finitely Generated Ideals]** Let $(R,+,\cdot)$ be a ring. A right-ideal I of R is said to be **finitely generated** if there exists a finite subset $X \subseteq R$ such that $I = (X)_R$. Analogously we obtain the definition for finitely generated left-ideals. We will say that an ideal I of R is **finitely generated** if it is so as right or left-ideal.

Definition 1.11. **[ID, PID, Division Ring, Field]** A ring $(R,+,\cdot)$ is called **integral domain**, or **ID** if it holds:

ID) For each $r_1, r_2 \in R$, if $r_1r_2 = 0$ then must hold $r_1 = 0$ or $r_2 = 0$.

We will say that $(R,+,\cdot)$ is a **principal ideal domain**, or **PID** if it holds:

PID) For each I ideal of R, there exists an element $r_I \in R$ such that $I = (r_I)$

Let $(R, +, \cdot)$ be a unit ring, we define the **right-units** of R, $U_R(R)$, and the **left-units** of R, $U_L(R)$ to be the following sets:

$U_R(R) = \{r \in R : \exists s \in R \ (rs = 1)\}$
$U_L(R) = \{r \in R : \exists s \in R \ (sr = 1)\}$

$(R, +, \cdot)$ is said to be a **ring division** if:

RD) $U_R(R) = U_L(R) = R \setminus \{0\}$

Finally, $(R, +, \cdot)$ is a **field** if:

F1) $(R, +, \cdot)$ is a commutative unit ring.
F2) $(R, +, \cdot)$ is a division ring.

Remark 1.12. We will refer to fields as $(K, +, \cdot)$ instead of $(R, +, \cdot)$. Notice that in a field it holds $U(K) = U_R(K) = U_L(K) = K \setminus \{0\}$, where:

$$U(K) = \{r \in K : \exists s \in K \ (rs = sr = 1)\}$$

Definition 1.13. **[Vector Space over a Field K]** Let $(K, +, \cdot)$ be a field and let V be a set with a binary operation $+$ and a **scalar product**:

$$\begin{array}{rccc} + : & V \times V & \longrightarrow & V \\ & (v_1, v_2) & \longmapsto & v_1 + v_2 \end{array} \qquad \begin{array}{rccc} \cdot : & K \times V & \longrightarrow & V \\ & (\lambda, v) & \longmapsto & \lambda v \end{array}$$

We will say that V is **vector space over the field K**, or **K-vector space** if it satisfies the following properties:

V1) $(R, +)$ is an abelian group.
V2) For all $\alpha, \beta \in K$ and $v \in V$, $\alpha(\beta v) = (\alpha\beta)v$.
V3) For all $\alpha, \beta \in K$ and $v \in V$, $(\alpha + \beta)v = (\alpha v) + (\beta v)$.
V3) For all $\alpha \in K$ and $v, w \in V$, $\alpha(v + w) = (\alpha v) + (\alpha w)$.

Let $W \subseteq V$ be any subset of V. It is called a **vector subspace** of V if it is an additive subgroup of $(V, +)$ and it is closed under scalar product, i.e., for all $w \in W$ and $\lambda \in K$, it holds that $\lambda w \in W$.

Definition 1.14. **[K-algebra]** Let $(K, +, \cdot)$ be a field and let $(A, +, \cdot)$ be a ring with a scalar product:

$$\begin{array}{rccc} \cdot : & K \times A & \longrightarrow & A \\ & (\lambda, a) & \longmapsto & \lambda a \end{array}$$

We say that A is a **K-algebra** if the following properties hold:

A1) A is a K-vector space.
A2) For all $\alpha \in K$ and $a, b \in A$, $\alpha(ab) = (\alpha a)b$.

A subset $B \subseteq A$ is called a **subalgebra** of A if $(B, +, \cdot)$ is a subring of $(A, +, \cdot)$ and B is a vector subspace of A.

A subset $I \subseteq A$ is a **[right, left] ideal** if I is a [right,left] ideal of $(A, +, \cdot)$ and I is a vector subspace of A.

Definition 1.15. **[Module over a K-algebra]** Let $(K, +, \cdot)$ be a field, let $(A, +, \cdot)$ be a K-algebra and let V be any set together with three operations:

$$\begin{array}{rccc} + : & V \times V & \longrightarrow & V \\ & (v_1, v_2) & \longmapsto & v_1 + v_2 \end{array} \qquad \begin{array}{rccc} \cdot : & K \times V & \longrightarrow & V \\ & (\lambda, v) & \longmapsto & \lambda v \end{array}$$

$$\begin{array}{rccc} * : & V \times A & \longrightarrow & V \\ & (v, a) & \longmapsto & v * a \end{array}$$

V is said to be an **A-module** if the following properties hold:

M1) $(V, +, \cdot)$ is a K-vector space.
M2) For all $\alpha \in K$, $a \in A$ and $v \in V$, $\alpha(v * a) = (\alpha v) * a = v * (\alpha a)$.
M3) For all $a, b \in A$ and $v \in V$, $v * (a + b) = v * a + v * b$.
M4) For all $a \in A$ and $v, w \in V$, $(v + w) * a = v * a + w * a$.

If $(A, +, \cdot)$ is a unit K-algebra we demand also the following property on V:

M5) For all $v \in V$, $v * 1 = 1 * v = v$.

A subset $W \subseteq V$ is called a **submodule** of V, written $W \leq_A V$, if $(W, +, \cdot)$ is a vector subspace of $(V, +, \cdot)$ and for each $w \in W$ and for each $a \in A$ it holds $w * a \in W$.

Definition 1.16. [Regular Module] Let $(K, +, \cdot)$ be a field and let $(A, +, \cdot)$ be a K-algebra. Let us set $V = A$ with the operation $* = \cdot$. It is straightforward to see that A is an A-module. We call that module the **regular A-module**.

Definition 1.17. [Simple Module] Let $(K, +, \cdot)$ be a field and let $(A, +, \cdot)$ be a K-algebra. An A-module V is called **simple** if every $W \leq_A V$ submodule of V is either the trivial module $\{0\}$ or the greatest one, V.

Definition 1.18. [Semisimple Module] Let $(K, +, \cdot)$ be a field and let $(A, +, \cdot)$ be a K-algebra. An A-module V is called **semisimple** or **completely reducible** if there exists a finite family of simple submodules $V_i \leq_A V$ such that $V = \bigoplus_{i=1}^{s} V_i$ as direct sum of vector spaces, i.e.:

- $V = \sum_{i=1}^{s} V_i$
- For each $i \in \{1, \cdots, s\}$,

$$V_i \cap \left(\sum_{j=1, j \neq i}^{s} V_j \right) = \{0\}$$

2. Morphisms over Structures

Definition 1.19. [Group Homomorphism] Let $(G_1, \cdot)$ and $(G_2, \cdot)$ be two groups. A mapping $f : G_1 \to G_2$ is called a **group homomorphism** if it verifies the following equation for each $g, h \in G_1$:

$$f(gh) = f(g)f(h)$$

We denote the set of all group homomorphisms between G_1 and G_2 by $Hom(G_1, G_2)$. We will say that a group homomorphism f is a **monomorphism** if it is an injective mapping, f is a **epimorphism** if it is a surjective and finally, f is a **isomorphism** if it is a bijection.

Definition 1.20. [Ring Homomorphism] Let $(R_1, +, \cdot)$ and $(R_2, +, \cdot)$ be two rings. A mapping $f : R_1 \to R_2$ is called a **ring homomorphism** if it verifies:

- $f : (R_1, +) \to (R_2, +)$ is a group homomorphism.
- For each $r, s \in R_1$ it holds:

$$f(rs) = f(r)f(s)$$

Definition 1.21. **[Linear Map]** Let $(K, +, \cdot)$ be a field and let V, W be two K-vector spaces. A mapping $f : V \to W$ is said to be **linear** if for each $v_1, v_2 \in V$ and $\alpha, \beta \in K$ it satisfies:

$$f(\alpha v_1 + \beta v_2) = \alpha f(v_1) + \beta f(v_2)$$

We denote by $Hom_k(V, W) = \{f : V \to W : \ f \text{ is linear}\}$ to the set of all linear mappings. For the case $W = V$, we will write $End_k(V)$ instead of $Hom_K(V, V)$. Finally, we define the set of all isomorphisms from V to V as $GL_K(V)$.

Definition 1.22. **[Algebra Homomorphism]** Let $(K, +, \cdot)$ be a field and let A, B be two K-algebras. A mapping $f : A \to B$ is said to be an **algebra homomorphism** if it is linear (considering A and B as vector spaces) and moreover, for each $a_1, a_2 \in A$ it holds that $f(ab) = f(a)f(b)$. Furthermore, if A and B are unit K-algebras, it must hold that $f(1_A) = 1_B$. We also define, in an analogous way , the sets $Hom_K(A, B)$ and $End_K(A)$.

Definition 1.23. **[Homomorphism between Modules]** Let $(K, +, \cdot)$ be a field,let A be a K-algebras and let V, W be two A-modules. A mapping $f : V \to W$ is said to be an **homomorphism between A-modules** if it is linear (considering V and W as vector spaces) and moreover, for each $a \in A$ and $v \in V$ it holds that $f(va) = f(v)a$. We also define, in an analogous way , the sets $Hom_A(V, W)$ and $End_A(V)$.

Example 1.24. Let $(K, +, \cdot)$ be a field and let V be a K-vector space. Take $A = End_K(V)$. It is a K-algebra with the operations:

$$\begin{array}{rccc} + : & A \times A & \longrightarrow & A \\ & (f, g) & \longmapsto & f + g \end{array} \quad \text{where,} \quad \begin{array}{rccc} f + g : & V \times V & \longrightarrow & V \\ & (v_1, v_2) & \longmapsto & vf + vg \end{array}$$

$$\begin{array}{rccc} \cdot : & A \times A & \longrightarrow & A \\ & (f, g) & \longmapsto & g \circ f \end{array} \quad \text{where,} \quad \begin{array}{rccc} fg : & V \times V & \longrightarrow & V \\ & (v_1, v_2) & \longmapsto & (vf)g \end{array}$$

$$\begin{array}{rccc} : & K \times A & \longrightarrow & A \\ & (\lambda, f) & \longmapsto & \lambda f \end{array} \quad \text{where,} \quad \begin{array}{rccc} \lambda f : & V \times V & \longrightarrow & V \\ & (v_1, v_2) & \longmapsto & \lambda(vf) \end{array}$$

Example 1.25. Let $(K, +, \cdot)$ be a field and let G be a group. We define $KG = \{\sum_{g \in G} t_g g : \ \forall g \in G \ (t_g \in K)\}$ to be the set of all linear combinations of elements of G. Let us consider the following three operations; For $a, b \in KG$ with $a = \sum_{g \in G} t_g g$ and $b = \sum_{h \in G} u_h h$ and $\lambda \in K$, we define:

$$a + b = \textstyle\sum_{g \in G}(t_g + u_g)g \qquad ab = \textstyle\sum_{g,h \in G}(t_g + u_h)(gh) \qquad \lambda a = \textstyle\sum_{g \in G}(\lambda t_g)g$$

With these three operations, KG is a K-algebra.

CHAPTER 2

Representations

1. Basic Definitions

Definition 2.1. **[Representation]** Let $(G, \cdot)$ be a finite group. Let $(K, +, \cdot)$ be a field and let V be a K-vector space of finite dimension. Let us consider the group $(GL(V), \cdot)$ of linear bijections from V to V together with the composition of mappings, i.e., for $f, g \in GL(V)$, $fg = g \circ f$. Any group homomorphism from G to $GL(V)$ is called a **representation** of G.

$$\begin{array}{rccccccc} D: & G & \longrightarrow & GL(V) & & & \\ & g & \longmapsto & D_g: & V & \longrightarrow & V \\ & & & & v & \longmapsto & (v)D_g \end{array}$$

We will refer to $n = dim_K(V)$ as the **degree** of the representation D.

Remark 2.2. Notice that $GL(V) \cong GL(n, K)$ (by fixing a basis in V and sending any linear bijection to the representative matrix in the fixed basis). Therefore, using the existence of such isomorphism $\varphi : GL(V) \to GL(n, K)$, given any representation D of G, it can be seen as a group homomorphism $D : G \to GL(n, K)$. In this case we will say that D is a **matrix representation** of G over K.

Remark 2.3. Definition 2.1 can be generalised in the following way; Let $(S, \cdot)$ be a semigroup. Let $(K, +, \cdot)$ be any ring and let V be a free K-module. Let us consider the semigroup $(End_K(V), \cdot)$ of endomorphisms on V as K-module. Any semigroup homomorphism from S to $End_K(V)$ is called a representation **representation** of S. For the case of $(M, \cdot)$ being a monoid we will demand $(K, +, \cdot)$ to be a unit ring. Any monoid homomorphism from M to $End_K(V)$ is called a **representation** of M. Notice that each representation must send 1 to id_V. There also exists the notion of **matrix representation**. Just notice that $End_K(V) \cong Mat_n(K)$.

Example 2.4. Let us present some examples of representations.

a) Let $(G, \cdot)$ be any finite group. Let $(K, +, \cdot)$ be any field and let V be any K-vector space of finite dimension. The **trivial representation**, R, is defined for each $g \in G$ as $R(g) = id_V$.

b) Consider the field $(\mathbb{R}, +, \cdot)$ of real numbers and the group $G = \{1, -1\} \subseteq \mathbb{R}$. Let V be any $\mathbb{R}$-vector space of finite dimension n. We define the following representation:

$$\begin{array}{rccccccc} D: & G & \longrightarrow & GL(V) & & & \\ & 1 & \longmapsto & D_1: & V & \longrightarrow & V \\ & & & & v & \longmapsto & v \\ & & & & & & \\ & -1 & \longmapsto & D_{-1}: & V & \longrightarrow & V \\ & & & & v & \longmapsto & -v \end{array}$$

In matrix form, $D_1 = I_n$ and $D_{-1} = -I_n$.

c) Let G be the finite group with presentation

$$G = \langle x, y \mid x^2 = y^3 = 1,\ y^x = y^{-1} \rangle$$

Notice that $G = [C_3]C_2 \cong \Sigma_3$. Let $(K, +, \cdot)$ be a field containing a cubic root of the unit, i.e., $\exists \omega \in K$ such that $\omega^3 = 1$. We define D as the matrix representation, $D : G \to GL(2, K)$, given by:

$$D_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad D_y = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$$

In order to check that D is a matrix representation, we just need to check that it is order-preserving and check that the relator conditions hold.

$$D_x^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

$$D_y^3 = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}^3 = \begin{bmatrix} \omega^3 & 0 \\ 0 & \omega^6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

$$D_y D_x = D_x D_y^2$$

Thus, D is a group homomorphism and therefore we can conclude that it is a matrix representation of G with degree 2.

Given any K-vector space with $dim_K(V) = 2$, let us fix any basis $\{v_1, v_2\}$ of V. According to the matrix representation of D, the representation associated to this basis is given by:

$$\begin{array}{rcccccc} D: & G & \longrightarrow & GL(V) & & & \\ & x & \longmapsto & D_x: & V & \longrightarrow & V \\ & & & & v_i & \longmapsto & v_{3-i} \\ & & & & & & \\ & y & \longmapsto & D_y: & V & \longrightarrow & V \\ & & & & v_i & \longmapsto & \omega^i v_i \end{array}$$

for $i \in \{1, 2\}$.

d) Let $G = C_n = \langle g \rangle$ be the cyclic group or order n. Let $(K, +, \cdot)$ be a field containing ξ, an n-th root of the unit. We define R as the matrix representation given by:

$$\begin{array}{rccc} R: & G & \longrightarrow & GL(1, K) \cong K \\ & g^s & \longmapsto & R_{g^s} = \xi^s \end{array}$$

R is a matrix representation of G of degree 1.

Definition 2.5. **[Linear Representation of K-algebras]** Let $(K, +, \cdot)$ be a field. Let A be a K-algebra and let V be any K-vector space of finite dimension. Let us consider $(End_K(V), +, \cdot)$ as a K-algebra (taking the product as the composition of linear mappings). Any K-algebra homomorphism D from A to $End_K(V)$ is called a **linear representation** of the K-algebra A.

$$\begin{array}{rcccccc} D: & A & \longrightarrow & End_K(V) & & & \\ & a & \longmapsto & D_a: & V & \longrightarrow & V \\ & & & & v & \longmapsto & (v)D_a \end{array}$$

Notice that in the case of unit K-algebras, $D(1) = Id_V$. We will refer to $n = dim_K(V)$ as the **degree** of the representation D and to V as the **representation space**.

Example 2.6. Let us consider the following examples:

a) Let $(K, +, \cdot)$ be a field. Let A be a K-algebra and take $V = A$. The **regular linear representation**, R, is defined as:

$$\begin{array}{rccccc} R: & A & \longrightarrow & End_K(A) & & \\ & a & \longmapsto & D_a: & A & \longrightarrow & A \\ & & & & b & \longmapsto & (b)R_a = ba \end{array}$$

1. Let us check that R is well-defined, i.e., $R_a \in End_K(A)$.
   Let us consider $a \in A$, $b, c \in A$ and $\alpha, \beta \in K$. It holds:
   $$\begin{array}{rcccccc} (\alpha b + \beta c)R_a & = & (\alpha b + \beta c)a & = & (\alpha b)a + (\beta c)a & = \\ & = & \alpha(ba) + \beta(ca) & = & \alpha(b)R_a + \beta(c)R_a & \end{array}$$
2. Let us now check that R is a K-algebra homomorphism.

2.1 Take $a, b \in A$, $c \in A$ and $\alpha, \beta \in K$. It holds:
$$\begin{array}{rcccccc} (c)R_{\alpha a + \beta b} & = & c(\alpha a + \beta b) & = & c(\alpha a) + c(\beta b) & = \\ & = & \alpha(ca) + \beta(cb) & = & \alpha(c)R_a + \beta(c)R_b & = \\ & = & (c)(\alpha R_a + \beta R_b) & & & \end{array}$$

2.2 Take $a, b \in A$, $c \in A$. It holds:
$$\begin{array}{rcccccc} (c)R_{ab} & = & c(ab) & = & [(c)R_a]b & = \\ & = & [(c)R_a]R_b & = & (c)R_a R_b & \end{array}$$

(3.) Moreover, for the case of A being a unit K-algebra, it holds:
$$\begin{array}{rccccc} R: & A & \longrightarrow & End_K(A) & & \\ & 1 & \longmapsto & D_1: & A & \longrightarrow & A \\ & & & & b & \longmapsto & b1 \end{array}$$

Thus $R_1 = Id_A$

Hence, R is a K-algebra homomorphism and we conclude that R is a linear representation of A.

b) Last example can be generalised as follows; Let $(K, +, \cdot)$ be a field. Let A be a K-algebra and consider any A-module M. Consider the following linear representation θ

$$\begin{array}{rccccc} \theta: & A & \longrightarrow & End_K(M) & & \\ & a & \longmapsto & \theta_a: & M & \longrightarrow & M \\ & & & & m & \longmapsto & (m)\theta_a = ma \end{array}$$

It is straightforward to see that θ_a is well-defined for each $a \in A$ and that θ is an homomorphism between K-algebras, thus θ is a linear representation of A.

2. Basic Properties

Proposition 2.7. *Let $(G, \cdot)$ be any finite group and let $(K, +, \cdot)$ be a field. Every representation of G can be extended to a linear representation of the K-algebra KG (from Example 1.25). Conversely, every linear representation of KG induces a representation of G.*

Proof. Let V be any K-vector space and let $R : G \to GL(V)$ be a representation of G. Let us define $\overline{R}$ as follows:

$$\begin{array}{llllll} \overline{R}: & KG & \longrightarrow & End_K(V) & & \\ & a=\sum_{g\in G} t_g g & \longmapsto & R_a: & V & \longrightarrow & V \\ & & & & v & \longmapsto & (v)R_a=(v)\sum_{g\in G} t_g R_g \end{array}$$

For each $a \in KG$, R_a is clearly well-defined. Let us check that it is a homomorphism between K-algebras:

1. Take $a, b \in KG$ and $\alpha, \beta \in K$. Assume $a = \sum_{g\in G} t_g g$ and $b = \sum_{g\in G} u_g g$ It holds:

$$\begin{aligned} \overline{R}(\alpha a+\beta b) &= \overline{R}(\alpha \sum_{g\in G} t_g g + \beta \sum_{g\in G} u_g g) = \\ \overline{R}(\sum_{g\in G}(\alpha t_g)g + \sum_{g\in G}(\beta u_g)g) &= \overline{R}(\sum_{g\in G}(\alpha t_g+\beta u_g)g) = \\ \sum_{g\in G}(\alpha t_g+\beta u_g)R_g &= \alpha\sum_{g\in G} t_g R_g + \beta\sum_{g\in G} u_g R_g = \\ \alpha\overline{R}(\sum_{g\in G} t_g g) + \beta\overline{R}(\sum_{g\in G} u_g g) &= \alpha\overline{R}(a)+\beta\overline{R}(b). \end{aligned}$$

2. Take $a, b \in A$. It holds:

$$\begin{aligned} \overline{R}(ab) &= \overline{R}((\sum_{g\in G} t_g g)(\sum_{h\in G} u_h h)) \\ &= \overline{R}(\sum_{g,h\in G} t_g u_h gh) \end{aligned}$$

Fixed any $x \in G$, it holds $gh = x \Leftrightarrow h = g^{-1}x$. Therefore:

$$\begin{aligned} \overline{R}(\sum_{x\in G}(\sum_{g\in G} t_g u_{(g^{-1}x)} x)) &= \sum_{x\in G}(\sum_{g\in G} t_g u_{(g^{-1}x)} R(x)) = \\ \sum_{g,h\in G} t_g u_h R(gh) &= \sum_{g,h\in G} t_g u_h R(g)R(h) = \\ (\sum_{g\in G} t_g R(g))(\sum_{h\in G} u_h R(h)) &= \overline{R}(\sum_{g\in G} t_g g)\overline{R}(\sum_{h\in G} u_h h) = \\ &= \overline{R}(a)\overline{R}(b). \end{aligned}$$

Thus $\overline{R}$ is a linear representation of KG.

For the converse, let $\overline{R} : KG \to End_K(V)$ be any linear representation of KG. We define $R = \overline{R}_{|G}$, $R : G \to End_K(V)$. Let us check that it is a representation of G.

1. R is a group homomorphism. Take $g, h \in G$. It holds:

$$R(gh) = \overline{R}(gh) = \overline{R}(g)\overline{R}(h) = R(g)R(h)$$

2. Moreover, for each $g \in G$, $R(g)$ is a bijective endomorphism on V. Just notice that $R(g)$ has as inverse homomorphism $R(g^{-1})$.

$$R(g)R(g^{-1}) = R(g^{-1})R(g) = R(1) = Id_V$$

We conclude that R is a representation of G.

□

Remark 2.8. Last Proposition stablishes the correspondence between the representations of G and the linear representations of KG. Nevertheless, it is important to consider them as independent objects since each representations have quite different invariants. Consider the following examples; Let $\overline{\theta}$ be a linear representation of KG. We can consider its associated θ from Proposition 2.7. It holds that $Ker\overline{\theta}$ is an ideal of KG while $Ker\theta \trianglelefteq G$. This leads, in the case of the trivial representation, to the equations $Ker\overline{\theta} = KG$, but $Ker\theta = G$, which are clearly different structures. In order to avoid confusions we will write $Ker_\theta(G \text{ over } V)$ instead of $Ker\theta$.

Proposition 2.9. *There exists a duality between linear representations and modules. This duality is expressed in the following statements:*

a) *Let $(K, +, \cdot)$ be a field and let A be any K-algebra. Let R be a linear representation with representation space V. Then V has structure of A-module with the internal law:*

$$\begin{array}{cccc} * : & V \times A & \longrightarrow & V \\ & (v, a) & \longmapsto & (v)R_a \end{array}$$

b) *Let $(K, +, \cdot)$ be a field, let A be a K-algebra and let V be any A-module. We define R as follows:*

$$\begin{array}{cccccccc} R : & A & \longrightarrow & End_K(V) & & & & \\ & a & \longmapsto & R_a : & & V & \longrightarrow & V \\ & & & & & v & \longmapsto & va \end{array}$$

Then R is a linear representation of A.

Proof. Let us check the two statements:

a) Consider V together with the operation $*$. Notice that the operation $*$ is well-defined since $R_a \in End_K(V)$ for each $a \in A$. Therefore we must check that the conditions of V being an A-module (Definition 1.15) hold:

M1) V was already a K-vector space.

M2) Let $\alpha \in K$, $a \in A$ and $v \in V$ it holds:

$$\alpha(v * a) = \alpha((v)R_a) = (\alpha v)R_a = (\alpha v) * a$$

M3) Let $a, b \in A$ and $v \in V$ it holds:

$$v * (a + b) = (v)R_{a+b} = (v)(R_a + R_b) = (v)R_a + (v)R_b = v * a + v * b$$

M4) Analogous to M3).

In the case of A being a unit K-algebra it holds:

m5) Let $v \in V$, it holds:

$$v * 1 = (v)R_1 = (v)Id_V = v$$

Finally, we can conclude that V has structure of A-module.

b) See Example 2.6.

□

Remark 2.10. Proposition 2.7 states the equivalency between the study of the representations of a given group G over a field K and the study of linear representations of KG. Moreover, last Proposition 2.9 states the duality between linear representations of KG and KG-modules. In a few words, we will use the following three equivalent tools:

$$\begin{array}{ccccc} \text{Representations} & & \text{Linear Representations} & & \text{Modules} \\ D: G \to GL(V) & \Leftrightarrow & \overline{D}: KG \to End_K(V) & \Leftrightarrow & V \text{ as } KG\text{-module} \end{array}$$

Example 2.11. We present some instances of Proposition 2.9.

1) Let R be the trivial representation from Example 2.4, then $V = K$ is the KG-module associated to R with the law:
$$\begin{array}{cccc} *: & K \times KG & \longrightarrow & V \\ & (\alpha, a) & \longmapsto & \alpha \end{array}$$
2) Let A be any K-algebra, then the module $V = A^0$ is the regular A-module with the law $v * a = va$, associated to regular linear representation of Example 2.6.
3) The trivial KG-module with the law $\alpha g = \alpha$, $\forall \alpha \in K\ \forall g \in G$ is associated to the trivial representation of degree 1 over K called **1-representation**.
4) Let A be a K-algebra. The regular A-module is associated to the regular representation. For the case $A = KG$, the associated regular representationis called **regular representation of G** and works this way:

   Assuming that $G = \{1, g_2, \cdots, g_n\}$,
$$\begin{array}{cccc} R: & G & \longrightarrow & GL(KG) \quad (\cong M(n, K)) \\ & g & \longmapsto & R_g \end{array}$$
   $(g_i)R_g = g_i g = g_j \in G$. If we take G as K-basis of KG, in matrix form:
$$R(g) = \begin{array}{cc} & \begin{array}{ccccccc} & & g & & g_j & & \\ & & \downarrow & & \downarrow & & \end{array} \\ \begin{array}{c} 1 \rightarrow \\ \\ g_i \rightarrow \\ \\ \end{array} & \left[\begin{array}{ccccccc} 0 & \cdots & 1 & \cdots & 0 & \cdots \\ \vdots & & \vdots & & \vdots & \\ 0 & \cdots & 0 & \cdots & 1 & \cdots \\ \vdots & & \vdots & & \vdots & \end{array}\right] \end{array}$$
   They are, therefore, permutation matrices.

Definition 2.12. **[Equivalent Representations]** Let $R_i : KG \to GL(V_i)$ for $i = 1, 2$, be two representations of G over K. Let V_i, $i = 1, 2$, be the corresponding representation spaces of G. We will say that R_1 and R_2 are **equivalent** if there exists a bijective $P \in Hom_K(V_1, V_2)$ such that for each $g \in G$, $(R_1 g)P = P(R_2 g)$ hold. That is to say that the following diagram commutes:

$$\begin{tikzcd} V_1 \arrow[r, "P"] \arrow[d, "R_1 g"'] & V_2 \arrow[d, "R_2 g"] \\ V_1 \arrow[r, "P"'] & V_2 \end{tikzcd}$$

Last property can be expressed in terms of matrices. Assume $n = dim_K(V_i)$, for $i = 1, 2$. We must fix a basis of V_1 and V_2 and consider the corresponding matrix representations $\tilde{R}_i : KG \to Mat(n, K)$, for $i = 1, 2$. We say that the matrix representations are equivalent if there exists some $P \in GL(n, K)$ such that for each $g \in G$, $(\tilde{R}_1 g)P = P(\tilde{R}_2 g)$ hold.

Proposition 2.13. *Let R_i, for $i = 1, 2$, be two representations of G over K. Let us consider V_i, for $i = 1, 2$, as the corresponding KG-modules. Then R_1 and R_2 are equivalent if and only if $\overline{V}_1$ and $\overline{V}_2$ are isomorphic KG-modules.*

PROOF. Let us check the two implications:

$\gg$ Assume that R_1 and R_2 are equivalent, thus we can find some bijective $P \in Hom_k(V_1, V_2)$ with $(R_1 g)P = P(R_2 g)$ for all $g \in G$. Let us consider the associated linear representations $\overline{R_i} : KG \to End_K(V_i)$, for $i = 1, 2$. We will check that there exists some $\overline{P} : \overline{V_1} \to \overline{V_2}$ which is a KG-isomorphism. Notice that $\overline{V_i}$ was defined as V_i with the law $v * z = (v)(\overline{R_i} z)$ for $v \in V_i$ and $z \in KG$.

As a candidate for $\overline{P}$, we consider P itself. Let us check that P can act, in fact, as a KG-homomorphism. Consider $v \in V_1$ and $\sum_{g\in G} a_g g \in KG$, it holds:

$$\begin{array}{rlclcl} & \left[v * \sum\limits_{g\in G} a_g g \right] P & = & \left[(v) \left(\overline{R_1} (\sum\limits_{g\in G} a_g g) \right) \right] P & = \\ = & \left[\sum\limits_{g\in G} a_g (v)(R_1 g) \right] P & = & \sum\limits_{g\in G} a_g \left[(v) R_1 g \right] P & = \\ = & \sum\limits_{g\in G} a_g (v) \left[R_1 g P \right] & = & \sum\limits_{g\in G} a_g (v) \left[P R_2 g \right] & = \\ = & \sum\limits_{g\in G} a_g \left[(v) P \right] R_2 g & = & \left[(v) P \right] \left(\sum\limits_{g\in G} a_g R_2 g \right) & = \\ = & \left[(v) P \right] \overline{R_2} \left(\sum\limits_{g\in G} a_g g \right) & = & \left[(v) P \right] * \left(\sum\limits_{g\in G} a_g g \right) & \end{array}$$

That means that P is KG-linear. Moreover it is a KG-isomorphism since P was bijective.

$\ll$ Conversely, suppose that $\overline{V_1} \cong_K \overline{V_2}$, i.e., there exists some KG-isomorphism $\overline{P} : \overline{V_1} \to \overline{V_2}$. Notice that, as sets, $\overline{V_i} = V_i$ for $i = 1, 2$, therefore for $v \in V_1$ it holds:

$$\begin{array}{rclclc} (v)[R_1(g)P] & = & (v * g)P & = & (vP) * g & = \\ & = & (vP)R_2(g) & = & (v)[PR_2(g)] & \end{array}$$

Hence, for all $v \in V_1$ and for all $g \in G$, it holds $R_1(g)P = PR_2(g)$.

□

Corollary 2.14. *If $M \cong_{KG} N$ then $Ker(G \text{ over } M) = Ker(G \text{ over } N)$.*

PROOF. In fact, if $R_1 : G \to GL(M)$ and $R_2 : G \to GL(N)$ are representations of G with $M \cong_{KG} N$, using previous Proposition, there exists some bijective $P \in Hom(M, N)$ with the property $R_1(g)P = PR_2(g)$ for each $g \in G$. Therefore it holds:

$$\begin{array}{lclclc} g \in Ker(G \text{ over } M) & \Leftrightarrow & R_1(g) = 0_M & \Leftrightarrow & (v)R_1(g) = 0 & \Leftrightarrow \\ & \Leftrightarrow & [(v)R_1(g)]P = 0 & \Leftrightarrow & (v)[R_1(g)P] = 0 & \Leftrightarrow \\ & \Leftrightarrow & (v)[PR_2(g)] = 0 & \Leftrightarrow & [(v)P]R_2(g) = 0 & \Leftrightarrow^\star \\ & \Leftrightarrow^\star & (w)R_2(g) = 0 & \Leftrightarrow & R_2(g) = 0_N & \Leftrightarrow \\ & & & \Leftrightarrow & g \in Ker(G \text{ over } N) & \end{array}$$

In the proof we have considered that $v \in M$, $w \in N$ are arbitrary elements. Notice that in $\star$ we have used that P is a bijection. □

Definition 2.15. [**Faithful Representation**] Let R be a representation of G over K. We will say that R is a **faithful** if $KerR = 1$.

Remark 2.16. Let R be a representation of G over K with degree n and representation space V, then $KerR \trianglelefteq G$ and using the 1st Isomorphism Theorem, it holds that:

$$G/KerR \tilde{\leq} GL(V) \cong GL(n, K)$$

Example 2.17. The regular representation of G is a faithful representation.

$$\begin{array}{cccccc} R: & G & \longrightarrow & GL(KG) & & \\ & g & \longmapsto & R_g: & KG & \longrightarrow & KG \\ & & & & \sum_{x\in G} a_x x & \longmapsto & \sum_{x\in G} a_x (xg) \end{array}$$

Definition 2.18. [**Irreducible, Semisimple**] Let R be a representation of G over K with associated module V. Then:

a) We will say that R is **irreducible** if V is an irreducible KG-module. Otherwise, we will say that R is **reducible**.
b) R is said to be **completely reducible** or **semisimple** if so is V as KG-module.

There exist, up to equivalency, a finite number of irreducible representations. This fact motivates the study of Characters.

Example 2.19. Let us consider the following examples:

a) If $G \neq 1$ then the regular representation of G is not irreducible, since the associated module (the regular KG-module) has always a KG-submodule of dimension 1: the one generated by $\sum_{g\in G} g$. Since $|G| > 1$, we get:

$$0 \neq \langle \sum_{g\in G} g \rangle_K \lneq KG$$

This submodule is isomorphic to the trivial module K.

b) Consider the group $G \cong \Sigma_3$ and the representation defined in Example 2.4 c). For the case $K = \mathbb{C}$ the representation is irreducible. Let us prove this statement:

Proof. Let V be the KG-module of dimension 2 associated to the representation D. It will be enough to check that V is irreducible, which is equivalent to check that V has no submodule of dimension 1. Notice that each submodule will also be a vector subspace, and any 1-dimensional submodule of V will have the form $\mathbb{C}v$ for some $v \in V$. First, notice that $\mathbb{C}v_1$ and $\mathbb{C}v_2$ are not submodules since they are not fixed by x. Now, assume that $\mathbb{C}(v_1 + \lambda v_2)$ is a submodule of V with $\lambda \in \mathbb{C}$. Then applying x and y respectively we obtain:

- $(v_1 + \lambda v_2)x = v_1 x + \lambda v_2 x = v_2 + \lambda v_1 \in \mathbb{C}(v_1 + \lambda v_2)$
  We can deduce that there exists some $\alpha \in \mathbb{C}$ such that
  $$v_2 + \lambda v_1 = \alpha(v_1 + \lambda v_2)$$
  Frome this equation we deduce that $\lambda = \pm 1$. But in both cases the submodule is not closed under the action of y:

+1) $(v_1 + v_2)y = v_1y + v_2y = \omega v_1 + \omega^2 v_2$

Which necessarily does not belong to $\mathbb{C}(v_1 + v_2)$ since $\omega \neq \omega^2$.

−1) Analogous.

Thus, $\mathbb{C}(v_1 + \lambda v_2)$ is not a submodule of V. We have already checked all possibilities since $\{v_1, v_2\}$ forms a basis of V. Then V has no submodule of dimension 1 and V is irreducible. □

Theorem 2.20. *Let K be a field having characteristic $p > 0$ and let M be an irreducible KG-module. It holds:*

a) *If G is a p-group, then $M = KG$ is the trivial module.*
b) *More generally, it holds $O_p(G) \leq Ker(G \text{ over } M)$.*

Proof. FALTA! □

CHAPTER 3

Jacobson's Radical

Definition 3.1. **[Jacobson's Radical, Annihilator]** Let K be a field and let A be a K-algebra. We define the **Jacobson's radical** as the set:

$$J(A) = \{a \in A : \; Va = \{0\} \text{ for each irreducible } A\text{-module } V\}$$

Let V be an A-module, we define its **annihilator** in A as the set:

$$ann_A(V) = \{a \in A : \; Va = \{0\}\}$$

It follows from the definitions that:

$$J(A) = \bigcap_{\substack{V \text{ irreducible} \\ A\text{-module}}} ann_A(V)$$

Thus, by the considerations of the previous chapter (the correspondance between A-modules and the representations of A), it follows that $J(A)$ is the intersection of all the kernels of the irreducible representations of A.

Remark 3.2. $J(A)$ is an ideal of A.

Proof. It holds that $(J(A), +) \leq (A, +)$. Given $x, y \in J(A)$ and any irreducible A-module V, we get that $V(x-y) = Vx - Vy = \{0\}$. Now let $x \in J(A)$, $a \in A$ and let V be an irreducible A-module, it holds:

$$V(xa) = \{v(xa) : \; v \in V\} = \{0_V a : \; v \in V\} = \{0\}$$

$$V(ax) = \{v(ax) : \; v \in V\} = \{wx : \; w \in Va\} = (Va)x = \{0\}$$

In the last equation we have used that $Va \subseteq V$. Therefore we can conclude that $xa, ax \in J(A)$, thus $J(A)$ is an ideal. $\square$

Theorem 3.3. *Let A be a K-algebra and let $x \in A$. The following statements are equivalent:*

a) The element x belongs to every maximal right-ideal of A
b) For each $a \in A$, the element $1 - xa$ is invertible.
c) $x \in J(A)$.

Proof. We will check all the implications:

$a) \gg b)$ Let a be an arbitrary element of A. It is straightforward to see that $(1-xa)A$ is a right-ideal of A. If $(1-xa)A = A$, since $1 \in A$ we can easily conclude that there exists an element $b \in A$ such that $(1-xa)b = 1$, i.e., $(1-xa)$ is invertible. Assume now that $(1-xa)A \subsetneq A$, then there exists a maximal right-ideal U of A containing $(1-xa)A$. In particular, $(1-xa) \in U$. By assumption $x \in U$ and thus xa also belongs to U, therefore $(1 - xa) + xa = 1 \in U$ which contradicts the fact that U is a maximal ideal.

$b) \gg c)$ For each $a \in A$, the element $(1 - xa)$ is invertible, let us see that this implies $x \in J(A)$. Let V be an irreducible A-module and assume that $Vx \neq 0$, therefore there exists some $v \in V$ for which $vx \neq 0$ hold. Hence $(vx)A \neq 0$. It also holds that $0 \neq (vx)A \leq_A V$, since V is irreducible we can say that $V = (vx)A$. Since $v \in V$, there exists some $a \in A$ such that $vxa = v$, i.e., $v(1 - xa) = 0$, since $(1 - xa)$ is invertible, it follows that $v = 0$ and we arrive to a contradiction.

$c) \gg a)$ Let $x \in J(A)$ and consider any maximal right-ideal W of A. Notice that $A_{|W}$ is an irreducible A-module (Given $a+W \in A_{|W}$ and $b \in A$, we define the law $(a + W) * b = (a + b) + W)$. Hence, $(A_{|W})x = 0$, which means that for each $a \in A$

$$(a + W)x = ax + W = 0 + W$$

Thus, $ax \in W$ for each $a \in A$, in particular for $a = 1$ we conclude that $x \in W$.

□

Corollary 3.4. *$J(A)$ is the intersection of all the maximal right-ideals of A.*

Remark 3.5. It can be analogously proved that $J(A)$ is the intersection of all the maximal left-ideals of A. Latest Theorem is also valid by changing right by left and $1 - xa$ by $1 - ax$.

Corollary 3.6. *It holds:*

$$J\left(A/J(A)\right) = 0$$

Proof. Just notice that:

$$J\left(A/J(A)\right) = \bigcap_{\substack{W,\text{ maximal} \\ \text{right-ideal} \\ \text{of } A/J(A)}} W = \bigcap_{\substack{M,\text{ maximal} \\ \text{right-ideal} \\ \text{of } A, \\ J(A) \subseteq M}} M/J(A) = J(A)/J(A) = \{0_{J(A)}\}$$

□

Definition 3.7. **[Nilideal, Nilpotent]** Let N be an ideal of A. It is said to be **nilideal** if for each $x \in N$, there exists $n_x \in \mathbb{N}$ such that $x^{n_x} = 0$. We will say that N is **nilpotent** if there exists some $n \in \mathbb{N}$ with $N^n = 0$, which is equivalent to say that for all $x_1, \cdots x_n \in N$, it holds:

$$x_1 \cdots x_n = 0$$

Corollary 3.8. *Every nilpotent ideal is nilideal.*

Remark 3.9. We introduce here some notation. Let N be a subset of a given A-module M and let $B \subseteq A$. NB will denote the additive subgroup of M generated by $\{nb : n \in N, b \in B\}$.

Proposition 3.10. *Let N be a right-nilideal [left] of A, then $N \subseteq J(A)$.*

Proof. Let $x \in N$ and let $a \in A$, it suffices to prove that $1 - xa$ is invertible. Since N is right-ideal, we get that $xa \in N$, since it is nilideal, we can find some $k \in \mathbb{N}$ such that $(xa)^k = 0$. It follows that $1 - (xa)^k = 1$, i.e.,

$$(1 - xa)(1 + xa + \cdots + (xa)^{k-1}) = 1$$

Which means $1 - xa$ is invertible. □

Remark 3.11. The Jacobson's radical can be defined for arbitrary rings. Moreover, the preceding results can be applied to unit rings. Nevertheless, the following result is only valid for those rings in which the minimum condition for right-ideal [left] holds (here we are going to use the fact that A has finite dimension).

Theorem 3.12. *Let A be a K-algebra, then $J(A)$ is nilpotent, thus every nilideal of A is nilpotent, moreover $J(A)$ is the unique maximal nilpotent ideal of A.*

Proof. Let us consider a decomposition serie of A as A-module:

$$A = A_0 \geq A_1 \geq \cdots A_r = 0$$

that is, with the property A_i/A_{i+1} is an irreducible A-module for $0 \leq i \leq r-1$. Therefore for each $x \in J(A)$ we get $(A_i/A_{i+1})\, x = 0$ which is equivalent to say that $\forall x \in J(A)$, $A_i x \in A_{i+1}$, therefore $A_i J(A) \leq A_{i+1}$. In particular:

$$AJ(A)^r = A_0 J(A)^r \leq A_1 J(A)^{r-1} \leq \cdots \leq A_{r-1} J(A) \leq A_r = 0$$

Notice that $AJ(A)^r = J(A)^r = 0$, hence $J(A)$ is nilpotent. Notice that if N is a nilpotent ideal, then N is nilideal and hence, by the previous Proposition, $N \subseteq J(A)$. □

Given an A-module V we are going to determine two associated irreducible A-modules; an A-submodule and a quotient one. This very useful construction is closely related to the Jacobson's ideal and it will be used in many future results.

Lemma 3.13. *Let V be an A-module with submodules $W_1, \cdots W_t$ with the property that for each $i = 1, \cdots t$, V/W_i is semisimple. Then $V/\cap W_i$ is semisimple as well.*

Proof. First of all, let us remember some useful properties on semisimple modules:

$$\begin{array}{lcl} U \text{ is semisimple} & \Leftrightarrow & U = \bigoplus_{i=1}^{k} W_i \text{ , for } W_i \text{ simple, } i = 1, \cdots t \\ & \Leftrightarrow & U = \sum_{i \in I} W_i \text{ , for } W_i \text{ simple, } i \in I \\ & \Leftrightarrow & \forall W \leq_A U, \exists Z \leq_A U \text{ with } U = W \oplus Z. \end{array}$$

It also holds that if U is semisimple and $W \leq_A U$, then U/W is also semisimple.

We will prove it by induction on t. The statement is trivial for $t = 1$. Assume it holds for a number of of submodules strictly less than t. Let us check it holds for exactly t submodules. Let $\{W_1, \cdots W_t\}$ be a family of t submodules of V with the property that for each $i = 1, \cdots t$, V/W_i is semisimple. Let us consider $\tilde{W}_1 = W_1$ and $\tilde{W}_2 = \cap_{i=2}^{t} W_i$. By induction, $V/\tilde{W}_j$ is semisimple for $j = 1, 2$.

Let us define now $W_0 = \tilde{W}_1 \cap \tilde{W}_2$ and let $U_j = \tilde{W}_j / W_0$ for $j = 1, 2$. We want to prove that $V/W_0 = V/\cap_{i=1}^{t} W_i$ is semisimple. We define $U = U_1 \oplus U_2$ (it is well defined because $U_1 \cap U_2 = 0$). It holds:

$$U_1 \cong U/U_2 \qquad U_2 \cong U/U_1 \qquad \star$$

Notice that for $j = 1, 2$, we get:

$$U/U_j = (U_1 \oplus U_2)/U_j \cong \frac{(\tilde{W}_1 + \tilde{W}_2)/W_0}{\tilde{W}_j/W_0} \leq V/\tilde{W}_j$$

Since V/W_j is semisimple, we conclude that U/U_J is also semisimple, for $j = 1, 2$. It follows $(\star)$ that U_j for $j = 1, 2$ and finally we conclude that $U = U_1 \oplus U_2$ is semisimple.

We will end the proof by checking that $U = V/W_0$. Notice that:

$$\frac{V/W_0}{U_2} = \frac{V/W_0}{\tilde{W}_2/W_0} \cong V/\tilde{W}_2$$

which is semisimple. Hence, there exists some $Z/U_2 \leq_A \frac{V/W_0}{U_2}$ such that:

$$\frac{V/W_0}{U_2} = \frac{U}{U_2} \oplus \frac{Z}{U_2}$$

This implies that $U + Z = V/W_0$ and $(U/U_2) \cap (Z/U_2) = U_2/U_2 = 0$ which means that $U \cap Z = U_2$. Let us check that $V/W_0 = U_1 + Z$. In fact, we have:

$$\left.\begin{array}{rcl} U & = & U_1 \oplus U_2 \\ V/W_0 & = & U + Z \\ U \cap Z & = & U_2 \end{array}\right| = \left|\begin{array}{rcl} U & = & U_1 + U_2 \\ U_1 \cap U_2 & = & 0 \\ V/W_0 & = & U + Z \\ U \cap Z & = & U_2 \end{array}\right.$$

Therefore, $U_1 \cap Z = (U_1 \cap U) \cap Z = U_1 \cap (U \cap Z) = U_1 \cap U_2 = 0$.

Now, let $vinV/W_0 = U + Z$, there exists some $u \in U$ and $z \in Z$ with $v = u + z$. Since $U = U_1 \oplus U_2$ we can find some elements $u_j \in U_j$ for $j = 1, 2$ with $u = u_1 + u_2$. Hence, $v = (u_1 + u_2) + z = u_1 + (u_2 + z)$ with $u_1 \in U_1$ and $u_2 + z \in Z$, this means that $V/W_0 = U_1 \oplus Z$. Notice that:

$$Z \cong \frac{V/W_0}{U_1} = \frac{V/W_0}{\tilde{W}_1/W_0} \cong V/\tilde{W}_1$$

This leads to Z being semisimple and finally V/W_0 is also semisimple. □

Definition 3.14. **[Socle, Radical, Head]** Let V be an A-module. We define the **Socle** of V, denoted by $Soc(V)$, to the sum of every irreducible submodule of V. The **Radical** of V, denoted by $Rad(V)$, is defined to be the intersection of every maximal submodule of V. And finally the **Head** of V, denoted by $H(V)$ is the quotient $V/Rad(V)$.

Remark 3.15. The dimension of V is finite, therefore $Rad(V)$ is the intersection of a finite family of maximal submodules of V. In fact, consider the family of all the finite intersections of maximal submodules of V:

$$\mathcal{F} = \{\bigcap_{i=1}^{t} M_i : \ M_i \text{ is a maximal submodule of } V, \ i = 1, \cdots t\}$$

Since $dim_K(V) \leq \infty$ it holds that $\mathcal{F}$ has some minimal element $U = \bigcap_{i=1}^{t} M_i$. Which means that U is included in every finite intersection of maximal ideals. Let us see that $U = Rad(V)$. It is straightforward to see that $Rad(V) \subseteq U$. Assume that $Rad(V) \neq U$. Assume also that for each maximal submodule $M \leq_A V$ the condition $U \cap M = U$, then $U \subseteq M$, i.e.,

$$U \subseteq \bigcap_{\substack{M \leq_A V, \\ \text{maximal}}} M = Rad(V)$$

which contradicts the assumption $Rad(V) \neq U$, therefore we can find some maximal submodule $M \leq_A V$ with $U \cap M < U$. It means that $U \cap M$ is minimal, contradicing the election of U, and we get a contradiction. Finally, $U = Rad(V)$.

Remark 3.16. For the case $V = A$, we get $J(A) = Rad(A)$, because the maximal submodules of the regular A-module are precisely the maximal right-ideals of the correspondent algebra.

Lemma 3.17. *If V is a completely reducible A-module then $Rad(V) = 0$.*

Proof. Since V is completely reducible, we can write it as $V = \bigoplus_{i=1}^{k} W_i$. Notice that each maximal submodule must have the form W^i for $i = 1, \cdots k$, where:

$$W^i = W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_n$$

Therefore $Rad(V) \subseteq \bigcap_{i=1}^{t} W^i = 0$. □

Proposition 3.18. *Let V be an A-module. It holds:*

i) *$Soc(V)$ is the greatest semisimple submodule of V.*

ii) *$H(V)$ is the greates semisimple quotient of V, i.e., $Rad(V)$ is the smallest A-submodule of V that produces a semisimple module by taking its quotient.*

Proof. We will check the two statements:

i) By definition, $Soc(V)$ is the sum of every irreducible submodule of V. In particular, it is semisimple and also contains all the others semisimple modules.

ii) By the previous Remark, $Rad(V)$ is the intersection of a finite family $\{M_1, \cdots M_t\}$ of maximal right-ideals of V.Notice that for each $i = 1, \cdots t$, V/M_i is a irreducible A-module, in particular these quotients are completely reducible, then using Lemma 3.13, $V/Rad(V)$ is semisimple. Let us finally check that $H(V)$ is the greatest semisimple quotient of V. Let $U \leq_A V$ be such that V/U is semisimple, therefore we can write it as:

$$V/U = \bigoplus_{i=1}^{n} V_i/U$$

with V_i/U irreducible for $i = 1, \cdots, n$. Let us define for each $i = 1, \cdots t$ the module V^i as:

$$V^i = V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_n$$

It is straightforward to see that V^i is a maximal submodule of V because $V/V^i \cong V_i$. Moreover, it holds:

$$U \subseteq \bigcap_{i=1}^{n} V^i \subseteq V^1 \cap \left(\bigoplus_{i=2}^{n} V^i \right) = U$$

Therefore, $\bigcap_{i=1}^{n} V^i = U$. Since each V^i was maximal for $i = 1, \cdots, n$, we conclude that $Rad(V) \subseteq U$.

Remark 3.19. Last statement is equivalent to check that $Rad(V)$ is the smallest A-submodule of V that produces a semisimple module by taking its quotient. Let N be a module of V with the property that V/N is completely reducible, then by Lemma 3.17, $Rad(V/N) = 0$, hence:

$$Rad(V) = \bigcap_{\substack{M \leq_A V, \\ \text{maximal}}} M \subseteq \bigcap_{\substack{M \leq_A V, \\ \text{maximal} \\ N \subseteq M}} M) = N$$

Therefore, $Rad(V) \subseteq N$.

□

Corollary 3.20. *$A/J(A)$ is the greatest completely reducible quotient of A. That is, $J(A)$ is the smallest ideal of A that produces a completely reducible module by taking its quotient.*

Corollary 3.21. *V is a completely reducible A-module if and only if $Rad(V) = 0$.*

Definition 3.22. **[Semisimple Algebras]** Let K be a field and let A be a K-algebra. A is said to be **semisimple** if $J(A) = 0$.

The main interest in studying the Jacobson's Radical for our purposes clearly appear in the following result:

Corollary 3.23. *Let A be a K-algebra. The following statements are equivalent:*

1) *A is semisimple.*
2) *The regular A-module is completely reducible.*
3) *Every A-module is completely reducible.*

Proof. We will check the following implications:

$1) \gg 2)$ Assume that A is semisimple, then $J(A) = 0$. Let us consider the regular A-module $V = A^0$, then $Rad(V) = J(A) = 0$. Hence V is completely reducible.

$2) \gg 3)$ Let V be an A-module with basis $\{v_1, \cdots, v_n\}$. Let $v \in V$ be an arbitrary but fixed element of V and let us define the following A-module homomorphism:

$$\begin{array}{rccc} \varphi_v : & A & \longrightarrow & V \\ & a & \longmapsto & va \end{array}$$

Notice that $\langle v \rangle \leq Im\varphi_v \leq V$. In particular, taking as $v = v_i$ for $i = 1, \cdots n$, we obtain that $V = \sum_{i=1}^{n} Im\varphi_{v_i} = V$. Notice that for each $i = 1, \cdots, n$, $Im\varphi_{v_i} \cong A/Ker\varphi_{v_i}$ which is completely reducible by assumption, and hence so is V.

$3) \gg 1)$ As a particular case, if we consider the regular A-module $V = A^0$, we obtain that $0 = Rad(V) = J(A)$.

□

Proposition 3.24. *It holds:*

i) *V is an irreducible A module $\Leftrightarrow$ V is an irreducible $A/J(A)$-module.*

ii) *V is a semisimple A module $\Leftrightarrow$ V is a semisimple $A/J(A)$-module.*

PROOF. We firstly prove the statement i):

- $\gg$ Assume that V is an irreducible A-module, then it can be seen as a $A/J(A)$-module with the law $(a + J(A))v = va$ for each $a \in A$. It is well defined because $VJ(A) = 0$. Moreover, the $A/J(A)$-submodules of V are also A-submodules of V. Thus, V is an irreducible $A/J(A)$-module.
- $\ll$ Conversely, if V is an $A/J(A)$-module, it can be seen as an A-module with the law $va = v(a + J(A))$ for each $a \in A$ and $v \in V$. Notice that the submodules coincide. Hence if V is irreducible as $A/J(A)$-module it is so as A-module.

For the second statement, if we suppose that V is a semisimple A-module, then we can write it as $V = \bigoplus_{i=1}^{n} V_i$ with $V_i \leq_A V$ irreducible submodules for $i = 1, \cdots, n$. Notice that V is also an $A/J(A)$-module because $V_i J(A) = 0$ for each $i = 1, \cdots, n$ and therefore $VJ(A) = 0$. We reason the rest of the proof analogously. □

Proposition 3.25. *Let V be an A-module, then:*

i) $VJ(A) = Rad(V)$.

ii) $Soc(V) = ann_V(J(A)) = \{v \in V : \ vJ(A) = 0\}$

PROOF. We will check the two statements:

i) We denote by $A_0 = A/J(A)$ and $V_0 = V/VJ(A)$. THence, the law $(v + VJ(A))(a + J(A)) = va + VJ(A)$ is well defined and therefore V_0 can be seen as an A_0-module in such a way that the A_0-submodules and the A-submodules of V coincide. Since A_0 is semisimple, we get that V_0 is completely reducible as A_0-module and hence as A-module. Therefore, $Rad(V) \subseteq VJ(A)$. Moreover, since $H(V) = V/Rad(V)$ is completely reducible, we obtain:

$$(V/Rad(V))J(A) = 0 \ \Rightarrow \ VJ(A)/Rad(V) = 0 \ \Rightarrow \ VJ(A) = Rad(V)$$

ii) It is straightforawrd to see the inclusion $Soc(V) \subseteq ann_V(J(A))$. On the other hand, the set $\{v \in V : \ vJ(A) = 0\}$ is an A_0-submodule of V. Since A_0 is semisimple, then V is completely reducible as A_0-submodule and also as A-module, this leads to $V \subseteq Soc(V)$ and finally, $Soc(V) = ann_V(J(A))$.

□

Theorem 3.26. *$A/J(A)$ is the greatest completely reducible quotient A-module of A. In particular every irreducible A-module is isomorphic to a composition factor of $A/J(A)$.*

PROOF. Consider the regular A-module $V = A^0$, we have that $V/Rad(V)$ is the greatest completely reducible A-module of V. Notice that $Rad(V) = Rad(A) = J(A)$, which concludes the first part of the proof.

Assume now that V is an irreducible A-module. Let $v \in V$ arbitrary but fixed nonzero element of V and consider the following A-module homomorphism:

$$\begin{array}{rccc} \varphi_v : & A & \longrightarrow & V \\ & a & \longmapsto & va \end{array}$$

It holds that $\varphi_V(1) = v \neq 0$, thus $0 < Im\varphi_v \leq V$. Since V is irreducible, we get that $Im\varphi_V = V$. Using 1st Isomorphism Theorem, we get that $A/Ker\varphi_v \cong Im\varphi_v = V$. Since $Ker\varphi_V$ is a maximal right-ideal of A, we get that $J(A) \subseteq Ker\varphi_V$. This means that V is isomorphic to a composition factor of $A/J(A)$. □

Corollary 3.27. *Proposition 3.24 appears as a direct corollary of the last Theorem.*

The following Lemma provides a sufficient condition on semisimplicity and it will be used in the proof of Maschke's Theorem.

Lemma 3.28. *Let A be a K-algebra and let $\{a_1, \cdots, a_n\}$ be a K-basis of A and let R be a representation of A with representation space V. Let us denote by $b_{ij} = trR(a_i a_j)$ the trace of $R(a_i a_j)$. If for each $1 \leq i, j \leq n$, $det(b_{ij}) \neq 0$, then A is semisimple.*

Theorem 3.29. [Maschke] *Let G be a group and let K be a field, it holds:*

$$KG \textit{ is semisimple} \quad \Leftrightarrow \left| \begin{array}{l} carK = 0 \textit{ or} \\ carK = p \textit{ with } p \nmid |G|. \end{array} \right.$$

Proof. We will check the two implications:

$\ll$ Let R be the regular representation of KG and let $n = |KG|$. Take as basis the elements of G, $\{g_1, \cdots, g_n\}$. If $g \neq 1$, then it holds that $trR(g) = 0$, because $R(g)$ is a nontrivial permutation matrix. For the unit case, we get that $trR(1) = n$. It means that for each pair $1 \leq i, j \leq n$:

$$trR(g_i g_j) = \left\{ \begin{array}{ccc} 0 & \text{if} & g_i g_j \neq 1 \\ n & \text{if} & g_i g_j = 1 \end{array} \right\} \Rightarrow det(trR(g_i g_j)) = det(b_{ij}) = \pm n^n$$

Since $carK = 0$ or $carK \nmid n = |G|$ and G is notempty, then $\pm n^n \neq 0$. Applying last Lemma, we conclude that KG is semisimple.

$\gg$ Assum now that $carK = p||G|$ and consider the nonzero element $i = \sum_{g \in G} g$. Let $h \in G$, since G is a basis of KG, then $ih = i = hi$. Thus, for each $\alpha \in KG$ we get that $i\alpha = \alpha i$, which implies that $i \in Z(KG)$. Moreover:

$$i^2 = \left(\sum_{g \in G} g \right)^2 = \left(\sum_{g \in G} g \right) \left(\sum_{h \in G} h \right) = \left(\sum_{g \in G} |G| g \right) = |G| \sum_{g \in G} g = 0$$

Therefore $i^2 = 0$ and $0 \neq i \in J(KG)$ which implies that KG is not semisimple.

□

CHAPTER 4

Completely Reducible Modules and Semisimple Algebras

1. Decompositions

As we have already seen in the preceding Chapter, an algebra is semisimple iff the associated regular A-module is completely reducible, which is equivalent to affirm that every A-module is completely reducible. Our aim in this chapter is to study in depth the properties of these structures.

Definition 4.1. **[Homogeneous component, W-homogeneuos]** Let A be a K-algebra, let V be an A-module and let W be an irreducible A-module we define:

$$H_W(V) \quad = \left| \begin{array}{ll} 0 & \text{if there is no } U \leq_A V \text{ with } U \cong W \\ \sum\limits_{U \in \mathcal{U}} U & \text{where } \mathcal{U} = \{U : \ U \leq_A V, \ U \cong W\}. \end{array} \right.$$

We will call this submodule the **homogeneous component** of V associated to W. By definition, $H_W(V)$ is completely reducible. If $V = H_W(V)$ then we will say that V is **W-homogeneous**.

Remark 4.2. Let $V = \bigoplus_{i=1}^n V_i$ be a completely reducible A-module where V_i is an irreducible component of V for $i = 1, \cdots, n$. Notice that the irreducible components are, at first sight, not uniquely determined by V, that is there exists the possibility of finding some alternative decomposition into irreducible factors. Nevertheless, it holds that the sum of all the V_i isomorphic to some given irreducible A-module W need to be independent of the considered decomposition and hence it will be uniquely determined by V, as it shows the following result:

Theorem 4.3. *Let $V = \bigoplus_{i=1}^n V_i$ be a completely reducible A-module where V_i is an irreducible component of V for $i = 1, \cdots, n$. Let W be an irreducible A-module. Then $H_W(V) = \bigoplus_{V_i \cong W} V_i$ and thus, $V = \bigoplus_W H_W(V)$ where W belongs to a family of representatives of the classes of isomorphy of irreducible A-modules (specifically, irreducible submodules of V).*

Proof. Let W be an irreducible A-module, we define $T = \bigoplus_{V_i \cong W} V_i$. It is straightforward to see that $T \leq H_W(V)$. For the other inclusion let $U \leq_A V$ with $U \cong W$ and assume towards a contradiction that $U \not\leq T$. Hence, $0 \leq_A U \cap T \lneq_A U$ and using that U is irreducible we get that $U \cap T = 0$. Thus:

$$(U + T)/T = (U \oplus T)/T \cong_A U \cong_A W$$

It also holds that:

$$V/T = \frac{\bigoplus\limits_{i=1}^{n} V_i}{\bigoplus\limits_{V_i \cong W} V_i} \cong \bigoplus_{V_j \ncong W} V_j$$

Since $(U+T)/T \leq_A V/T$ and $(U+T)/T \cong W$ it happens that $W \tilde{\leq} \bigoplus_{V_j \not\cong W} V_j$ which contradicts the Jordan-Hölder Theorem. Hence $U \leq T$ and finally, $U = T$. $\square$

Proposition 4.4. *Let M be an A-module and let $M = M_1 \oplus \cdots \oplus M_t$ be a decomposition of M in its homogeneous components M_i for $1 \leq i \leq t$. Let $U \leq_A M$ be any submodule of M, then:*

$$U = (U \cap M_1) \oplus \cdots \oplus (U \cap M_t)$$

Moreover, the homogeneous components of U are precisely $\{U \cap M_i : \ 1 \leq i \leq t\}$.

Proof. Assume that for each $i = 1, \cdots, t$, M_i is N_i-homogeneous, that is:

$$M_i = \sum_{\substack{X \leq_A M_i \\ X \cong N_i}} X$$

We define for each $i = 1, \cdots, t$, U_i to be the N_i-homogeneous component of U, $U_i = H_{N_i}(U)$. Since $U \leq_A V$ it follows that $U_i \subseteq M_i$ and trivially $U_i \subseteq (U \cap M_i)$. Moreover, $U \cap M_i \subseteq M_i$, thus $U \cap M_i$ is also a sum of irreducible A-submodules of U isomorphic to N_i, therefore $U \cap M_i \subseteq U_i$. $\square$

The following results show that every direct decomposition of a given K-algebra A is determined by a decomposition of the unit element of A in a sum of ortogonal idempotent elements in such a way that, associated to each primitive idempotent element we find an indecomposable ideal. Moreover those ideals will coincide with the irreducible ones when the algebra is semisimple. Therefore, these results are very useful for the study of unit algebras.

Definition 4.5. **[Idempotent, ortogonal, primitive, decomposable]** Let A be a K-algebra. An element $0 \neq e \in A$ is **idempotent** if $e^2 = e$ holds. Two idempotent elements $e_1, e_2 \in A$ are **ortogonal** if $e_1 e_2 = e_2 e_1 = 0$. An element is said to be **primitive** if it can not be written as the sum of two ortogonal idempotent elements. An A-module M is **decomposable** if there exists two non-trivial submodules M_1 and M_2 with $M = M_1 \oplus M_2$, otherwise we will say that M **indecomposable**.

Lemma 4.6. *Let $e \in A$ be an idempotent element, the following statements are equivalent:*

i) *eA is indecomposable.*
ii) *e is a primitive element.*

Proof. Let us check the two implications.

$\ll$ Assume that $eA = A_1 \oplus A_2$ with $A_i \neq 0$ for $i = 1, 2$. Since $e = e1 \in eA$, there exists some $e_i \in A_i$ for $i = 1, 2$ such that $e = e_1 + e_2$. From the fact that $e_i \in A_i \subseteq eA$, there exists also $a_i \in A$ such that $e_i = ea_i$ for $i = 1, 2$. Therefore:

$$e_1 = ea_1 = (e_1 + e_2)a_1 = e_1 a_1 + e_2 a_1$$

with $e_1 a_1 \in A_1$ and $e_2 a_1 \in A_2$. It follows that $e_1 - e_1 a_1 = e_2 a_1 \in A_1 \cap A_2 = 0$ because the sum is direct, therefore $0 = e_2 a_1$ and $e_1 = e_1 a_1$. Notice that:

$$e_1 = ea_1 = e^2 a_1 = (e_1 + e_2)^2 a_1 = (e_1^2 + e_1 e_2 + e_2 e_1 + e_2^2) a_1 =$$
$$= e_1^2 a_1 + e_2(e_1 a_1) + e_1(e_2 a_1) = e_2^2 + a_1 = e_1^2 a_1 + e_2 e_1$$

with $e_1^2a_1 \in A_1$ and $e_2a_1 \in A_2$. As before, it follows that $e_1^2a_1 = e_1$ and $e_2e_1 = 0$. We can reproduce the preceding argument to justify that also $e_1e_2 = 0$. Moreover, since e was idempotent it implies also the idempotency of e_1 and e_2 (because they are otogonal). Finally, we have written e as the sum of two ortogonal idempotent elements which contradicts e being primitive.

$\gg$ Conversely, assume that e is not primitive, then we can express e as $e = e_1 + e_2$ with $e_1^2 = e_1$, $e_2^2 = e_2$ and $e_1e_2 = e_2e_1 = 0$. Then it is straightforward to see that $eA = e_1A + e_2A$. Let $z \in e_1A_1 \cap e_2A$, then $z = e_1a_1 = e_2a_2$ for some $a_i \in A$, $i = 1, 2$. Notice that $e_1z = e_1^2a_1 = e_1a_1 = z$. Then, $e_1z = e_1(e_2a_2) = (e_1e_2)a_2 = 0$ and we conclude that $z = 0$. Therefore $eA = e_1A \oplus e_2A$, since $e_i \neq 0$ we can conclude that eA is decomposable.

$\square$

Theorem 4.7. *Let A be a K-algebra. It holds:*

a) *Assume that $A = \bigoplus_{i=1}^n A_i$ with A_i a right-ideal of A for $i = 1, \cdots, n$. Let the unit of A be decomposed as $1 = \sum_{i=1}^n e_i$ with $e_i \in A_i$. Then, the elements e_i for $i = 1, \cdots, n$ are idempotent and ortogonal to each other moreover $A_i = e_iA$.*

b) *Conversely, if we can decompose the unit element $1 = \sum_{i=1}^n e_i$ with e_i idempotent and ortogonal to each other, $i = 1, \cdots, n$, then:*

$$A = \bigoplus_{i=1}^n e_iA = \bigoplus_{i=1}^n Ae_i$$

c) *On the two previous items, the decomposition on ideals is associated with the decomposition of the unit element in central idempotent ortogonal to each other elements.*

d) *If $e \neq 1$ is an idempotent element of A, then $\{e, 1 - e\}$ is a pair of idempotent ortogonal elements for which $A = Ae \oplus A(1 - e)$ holds.*

Proof. Let us prove each statement:

a) Consider the decomposition $1 = \sum_{i=1}^n e_i$ with $e_i \in A_i$ for $i = 1, \cdots, n$. Then,for $j = 1, \cdots, n$, $e_j = e_j1_A = e_j(\sum_{i=1}^n e_i) = \sum_{i=1}^n e_je_i$. Notice that for all $i = 1, \cdots, n$, $e_je_i \in A_i$. Since the sum is a direct one, we can conclude that $e_ie_j = 0$ for $i \neq j$ and also that $e_j^2 = e_j$. Then, the elements e_i for $i = 1, \cdots, n$ are idempotent and ortogonal to each other. For the second part of the statement, notice that for all $i = 1, \cdots, n$, $e_i \in A_i$ and A_i is a right-ideal of A, thus $e_iA \subseteq A_i$. For the other inclusion, notice that any $x \in A_i$ can be decomposed as before:

$$x = 1_Ax = (\sum_{j=1}^n e_j)x = \sum_{j=1}^n e_jx = e_ix$$

This ends the proof since $e_ix = x \in e_iA$.

b) Assum now that we can decompose the unit element $1 = \sum_{i=1}^n e_i$ with e_i idempotent and ortogonal to each other, $i = 1, \cdots, n$, then let us check that $A = \bigoplus_{i=1}^n Ae_i$. Let $x \in A$, as before,$x = 1_Ax = (\sum_{i=1}^n e_i)x = \sum_{i=1}^n e_ix$ with $e_ix \in e_iA$ for each $i = 1, \cdots, n$. Thus, $A = \sum_{i=1}^n Ae_i$. Let us check that this in fact a direct sum. Assume that $\sum_{i=1}^{n} e_i a_i = 0$ and fix some $i_0 \in \{1, \cdots n\}$, then:

$$0 = e_{i_0} 0 = e_{i_0}(\sum_{i=1}^{n} e_i a_i) = \sum_{i=1}^{n} (e_{i_0} e_i) a_i = e_{i_0}^2 a_{i_0} = e_{i_0} a_i$$

Thus $a_i = 0$ for each $i = 1, \cdots, n$. Therefore $A = \bigoplus_{i=1}^{n} Ae_i$. There is an analogous proof to check that $A = \bigoplus_{i=1}^{n} e_i A$.

c) Assume that $A = \bigoplus_{i=1}^{n} A_i$ with A_i ideal of A for $i = 1, \cdots, n$. We have already seen in the item a) that we can find $\{e_1, \cdots, e_n\}$, a decomposition of 1_A, in idempotent and ortogonal elements, moreover $A_i = e_i A$. We must see that also each e_i for $i = 1, \cdots, n$ is central. Let $x \in A$, it holds:

$$x = 1_A x = (\sum_{j=1}^{n} e_j) x = \sum_{j=1}^{n} e_j x$$

$$x = x 1_A = x(\sum_{j=1}^{n} e_j) = \sum_{j=1}^{n} x e_j$$

Therefore, since the sum is direct, $xe_i = e_i x$ for each $i = 1, \cdots, n$, which means that e_i is central.

d) Let $e \in A$ be an idempotent element with $e \neq 1_A$. Let us check that $(1 - e)$ is idempotent:

$$(1-e)(1-e) = 1 - e - e + e^2 = 1 - e - e + e = 1 - e$$

Moreover, it also holds that $e(1-e) = e - e^2 = e - e = 0$ and $1 = e + (1-e)$. Therefore, since we have a decomposition of 1 in idempotent and ortogonal elements, applying b) we get that $A = Ae \oplus A(1-e)$.

□

Proposition 4.8. *Let A be a K-algebra. Then:*

a) *An element idempotent of A is primitive if and only if eA is an idecomposable A-module.*

b) *A is semisimple if and only if there exists a decomposition of 1_A in idempotent primitive ortogonal elements $\{e_1, \cdots, e_n\}$ with $A = \bigoplus_{i=1}^{n} e_i A$ and $e_i A$ an irreducible A-module.*

Proof. Notice that item a) has been proved in Lemma 4.6. For b):

$\ll$ Let 1_A be decomposed as $1_A = e_1 \cdots e_n$ where e_i, $i = 1, \cdots, n$ is a primitive ortogonal element. Then applying last Theorem, $A = \bigoplus_{i=1}^{n} e_i A$ and using Lemma 4.6, all the $e_i A$ are idecomposable since e_i is primitive. Since they are also completely reducible, we get that they are irreducible. Therefore A is semisimple.

$\gg$ Conversely, assuming that A is semisimple, we get that $A = \bigoplus_{i=1}^{n} A_i$ with A_i an irreducible A-module. Applying last Theorem item a), there must exist a family of idempotent ortogonal elements $\{e_1, \cdots, e_n\}$ with $A_i = e_i A$. Notice that, since $e_i A$ is irreducible and hence idecomposable, must hold by Lemma 4.6 that each e_i for $i = 1, \cdots, n$ must be a primitive element.

□

Theorem 4.9. **[Pierce's Decomposition]** *Let A be a semisimple K-algebra and let R be a right-ideal of A. Then there exists an idempotent element $e \in A$ such that $R = eA$ and A admits the direct decomposition $A = eA \oplus (1-e)A$.*

Proof. Since A is semisimple, the regular A-module is completely reducible and using a previous characterisation, we know that R has a complement, i.e. there exists some right-ideal S of A, such that $A = R \oplus S$. Notice that in this context, $1_A = e + e'$ with $e \in R$ and $e' \in S$. By construction $e' = 1 - e$, and $\{e, 1-e\}$ is a decomposition of 1_A in ortogonal idempotent elements. Therefore, applying Theorem 4.7 item b), we get that $A = eA \oplus (1-e)A$. Notice that since R is a right-ideal, $eA = R$. □

Definition 4.10. **[Simple]** A K-algebra A is called **simple** if there are no more ideals on A than 0 and A. Is straightforward to see that each simple algebra is also a semisimple algebra; since $1_A \notin J(A)$ and $J(A)$ is an ideal of A, must hold that $J(A) = 0$.

Theorem 4.11. *Let A be a semisimple K-algebra and let $A_1, \cdots, A_n$ the homogeneous components different from zero of the regular A-module, then:*

a) *$A = \bigoplus_{i=1}^n A_i$ with A_i an ideal of A, $i = 1, \cdots, n$, with the property that for each $j = 1, \cdots, n$, $A_i A_j = 0$ for $i \neq j$.*
b) *Every ideal of A is the sum of some A_i's. In particular, the A_i are the minimal ideals of A, for $i = 1, \cdots, n$.*
c) *If we can decompose the unit $1_A = e_i + \cdots + e_n$ with $e_i \in A_i$, then all the e_i's for $i = 1, \cdots, n$ are central idempotent ortogonal elements and moreover, e_i acts as a unit in A_i for all $i = 1, \cdots, n$. It also holds that $A_i = e_i A = A e_i$.*
d) *Every A_i for $i = 1, \cdots, n$ is a simple K-algebra.*

Proof. Let us check all the statements:

a) Let us consider $A_i = H_{\overline{W_i}}(A)$, where $\overline{W_i}$ is an irreducible A-module. Since A is semisimple and for $i = 1, \cdots, n$, $A_i \neq 0$, there exists a simple $W_i \leq_A A_i$ (minimal right-ideal of A) with $W_i \cong \overline{W_i}$. Therefore we can work with W_i as a minimal right-ideal of A. Let us consider now an arbitrary element $a \in A$ and let us consider the A-homomorphism:
$$\begin{array}{rccc} \varphi_a : & W_i & \longrightarrow & aW_i \\ & r & \longmapsto & ar \end{array}$$
It is straightforward to see that φ is an epimorphism. Since $Ker\varphi_a$ is an ideal of W_i and W_i is minimal, it follows that $Ker\varphi_a = 0$ or $Ker\varphi_a = W_i$. In both cases, we can conclude that $aW_i \subseteq A_i$. Therefore $AW_i \leq A_i$. Let W be a minimal right-ideal of A with $W \cong W_i$ with isomorphism α. By a previous Theorem, there exists some idempotent element $e_i \in A$ such that $W_i = e_i A$ and thus, $e_i W_i = e_i(e_i A) = e_i^2 A = e_i A = W_i$, and hence, $W = (W_i)\alpha = (e_i W_i)\alpha = (e_i \alpha) W_i$. It follows that $A_i \leq AW_i$ since they are the homogeneous components of A (isomorphic to a sum of W_i's). Therefore we get the other inclusion: $A_i = AW_i$ for $i = 1, \cdots, n$. Now, since $A = \bigoplus_{i=1}^n A_i$ is a direct sum of ideals, $A_i A_j \subseteq A_i \cap A_j = 0$ if $i \neq j$.
b) Let B be an ideal of A. Since A is semisimple, we get that B is completely reducible as A-module, therefore we can write it as $B = B_1 \oplus \cdots \oplus B_n$ where B_i is a minimal right-ideal of A, $i = 1, \cdots, n$. Assume now that

$B_i \cong W_i$ for all $i = 1, \cdots, n$, then applying last item we get that $A_j = AB_i \subseteq AB \subseteq B$. Thus, B can be written as the sum of some A_i's.

c) It follows from Theorem 4.7. Moreover, for each $i = 1, \cdots, n$, let $a_i \in A_i$. It holds that $a_i = a_i 1 = a_i(e_1 + \cdots + e_n) = aie_i$. Applying the unit in the left side, we also get that $a_i = e_i a_i$, and thus e_i acts as a unit for all the elements of A_i.

d) Assume that B is an ideal of A_i and let $j \neq i$, then $BA_j = 0$, because $BA_j \subseteq A_i A_j = 0$. It follows that $BA = B(\sum_{j=1}^n A_j) = BA_i = B$. Applying A in the other side, we also conclude that $AB \subseteq B$. Thus B is an ideal of A, but notice that, by b), the A_i's are the unique minimal ideals of A. Therefore $B = 0$ or $B = A_i$. Hence A_i is a simple K-algebra. □

Definition 4.12. **[Faithful]** Let A be a K-algebra and let V be an A-module. We say that V is **faithful** if for each $a \in A$, the condition $Va = 0$ implies $a = 0$.

Remark 4.13. Let R be a faithful representation of a given group G with representation space V. Then V is not necessarily a faithful KG-module.

Theorem 4.14. *Let A be a semisimple K-algebra. As we have already seen, we can write $A = \bigoplus_{i=1}^n A_i$ with $A_i = H_{W_i}(A_i)$, where W_i is a minimal right-ideal of A, $W_i \leq A_i$ and $W_i \ncong W_j$ if $j \neq i$, for each $i = 1, \cdots, n$. Then:*

a) *There exists exactly n irreducible A-modules up to isomorphy.*
b) *If V is an irreducible A-module, then there exists some $i \in \{1, \cdots, n\}$ such that $V \cong W_i$ such that $A_i = H_V(A)$. Moreover, V is a faithful A_i-module and $VA_j = 0$ if $j \neq i$.*
c) *If $V \neq 0$ is an A-module, then $V = VA_1 \oplus \cdots \oplus VA_n = Ve_1 \oplus \cdots \oplus Ve_n$ and $VA_i = H_{W_i}(V)$.*

Proof. We will prove all the items together. Let V be an irreducible A-module, then, as we already know, V is isomorphic to a composition factor of A, which are, up to isomorphy, $\{W_1, \cdots, W_n\}$. Notice that we have used that A is semisimple. Suppose now that $V \cong W_i$, therefore, $A_i = H_{W_i}(A) = H_V(A)$. Moreover, if $j \neq i$, $VA_j \cong W_i A_j = 0$. Let us see that V is faithful; Let us consider $J = \{a \in A_i : \ W_i a = 0\}$. It is straightforward to see that J is an ideal of A_i and A_i is simple (last Theorem) therefore, $J = A_i$ or $J = 0$. Notice that $J \neq A_i$ because $e_i \notin J$, thus $J = 0$ and we can conclude that W_i is a faithful A_i-module. This proves a) and b).

Let V be an arbitrary A-module. It follows from A being semisimple that V is completely reducible. Notice that all the irreducible A-submodules of V are isomorphic to some W_i, therefore we can write V as $V = \bigoplus_{i=1}^n H_{W_i}(V)$. Moreover:

$$VA_i = \bigoplus_{j=1}^n H_{W_i}(V)A_i = H_{W_i}(V)A_i = H_{W_i}(V) = H_{W_i}(V)e_i = Ve_i$$

This means that we can write V as $V = VA_1 \oplus \cdots \oplus VA_n = Ve_1 \oplus \cdots \oplus Ve_n$. □

Corollary 4.15. *Let A be a K-algebra. The following statements are equivalent:*

1) *A is simple.*
2) *The regular A-module is homogeneous.*
3) *A has a faithful irreducible A-module.*

Proof. Let us check all the statements:

1)≫2) If A is simple, then $A = H_W(A)$ for some irreducible A-module, W.

2)≫3) Apply the last Theorem for the case $n = 1$.

3)≫1) Let V be a faithful irreducible A-submodule. Since it is irreducible, then $VJ(A) = 0$ and since it is faithful, $J(A) = 0$, therefore A is semisimple and we can write it as $A = A_1 \oplus \cdots \oplus A_n$. Notice that there must exist some $i = 1, \cdots, n$ such that $V = A_i$, therefore by ortogonality, $VA_j = 0$ for all $j \neq i$, since V was faithful, $A_j = 0$ for all $j \neq i$ and we can conclude that $A = A_i$, i.e., A is simple.

□

2. Wedderburn's Theorem

In order to prove Wedderburn's Theorem we firstly need to present the Jacobson's density Lemma:

Lemma 4.16. [Jacobson] *Let A be a K-algebra and let V be an irreducible A-module. Consider $L = End_A(V)$. Notice that L can be seen as a division algebra for the composition of functions and moreover, V can be seen as an L-module with the law $v * f = (v)f$.*[1]*. Let $\{v_1, \cdots, v_n\}$ be a family of linearly L-independent elements of V and let $\{w_1, \cdots, w_n\}$ be an arbitrary family of elements of V. Then there exist some $a \in A$ such that $v_i a = w_i$ for each $i = 1, \cdots, n$.*

Proof. It suffices to show that we can find elements $a_i \in A$ for $i = 1, \cdots, n$ such that $v_j a_i = w_j$ if $j = i$ and $v_j a_i = 0$ if $i \neq j$. In this situation the desired element a, will be precisely $a = \sum_{i=1}^{n} a_i$. Let us proceed by induction on n.

For the case $n = 1$, we got that $v_1 \neq 0$ because it is linearly L-independent. Hence, $0 \neq v_1 A \leq_A V$, and V is irreducible, thus $v_1 A = V$ and given any $w_1 \in V$ we can find some $a \in A$ with $w_1 = v_1 a$.

Assume the statement hold for any family of $m \leq n$ linearly L-independent elements. Hence, applying I.H. for each $i \in \{1, \cdots, n\}$ there exists some $a \in A$ such that:

$$\langle (v_1 a, \cdots, \widehat{v_i a}, \cdots, v_n a) \rangle = \overbrace{V \oplus \cdots \oplus V}^{n-1}$$

Now, let us check that the following statement is false:

$$\forall a \in A \quad (v_1 a = \cdots = v_{i-1} a = v_{i+1} a = \cdots = v_n a = 0 \ \Rightarrow \ v_i a = 0) \quad \star$$

If we assume towards a contradiction that this is true, we can then define the following function:

$$\begin{array}{rccc} \tau : & \overbrace{V \oplus \cdots \oplus V}^{n-1} & \longrightarrow & V \\ & (v_1 a, \cdots, \widehat{v_i a}, \cdots, v_n a) & \longmapsto & v_i a \end{array}$$

Since we have assumed that the statement $\star$ holds τ is well defined, in fact if

$$(u_1 a, \cdots, \widehat{u_i a}, \cdots, u_n a) = (v_1 a, \cdots, \widehat{v_i a}, \cdots, v_n a)$$

then $(u_j - v_j)a = 0$ for all $j \neq i$ and therefore $(u_i - v_i)a = 0$, i.e., $u_i a = v_i a$. Moreover, τ is an A-homomorphism.

[1] Left to the reader

Fix now any $1 \leq k \leq n-1$ and let ε_k the natural injection of V into $\overbrace{V \oplus \cdots \oplus V}^{n-1}$ given by:

$$\begin{array}{rccl} \varepsilon_k: & V & \longrightarrow & \overbrace{V \oplus \cdots \oplus V}^{n-1} \\ & m & \longmapsto & (0, \cdots, m, \cdots, 0) \end{array}$$

where m is in the k-th position. It holds that ε_k is an A-homomorphism for each $1 \leq k \leq n-1$. Therefore, for each $1 \leq k \leq n-1$ let us define $\tau_k = \varepsilon_k \tau$, $\tau_k \in Hom(V, V)$ and for each $i = 1, \cdots, n$ it holds:

$$v_i = (v_1, \cdots, \widehat{v_i}, \cdots, v_n)\tau = \sum_{k=1,\ k \neq i}^{n} (0, \cdots, \widehat{v_i}, \cdots, v_k, \cdots, 0)\tau = \sum_{k=1,\ k \neq i}^{n} v_k(\varepsilon_k \tau)$$

Which is a contradiction because $\{v_1, \cdots, v_n\}$ was a family of linearly L-independent elements. Therefore the statement * is false and for each $i = 1, \cdots, n$ we can find some $b_i \in A$ such that $v_j b_i = 0$ if $j \neq i$ and $v_i b_i \neq 0$.

Applying the case of $n = 1$ for the specific element $v_i b_i \neq 0$ there exists some $b'_i \in A$ such that $v_i b_i b'_i = w_i$. Now, let us define $a_i = b_i b'_i$. It holds that $v_i a_i = w_i$ and $v_j a_i = v_j(b_i b'_i) = (v_j b_i) b'_i = 0$ if $j \neq i$. This concludes the proof. $\square$

Remark 4.17. As a special case, notice that this result is a generalization of a Theorem coming from Linear Algebra about the existence of linear functions that transforms a given linear system of n-vectors into another set of n-vectors.

In fact, let us consider V, a K-vector space and let $\{v_1, \cdots, v_n\}$ be a family of n K-linear independent vectors and let $\{w_1, \cdots, w_n\}$ be an arbitrary family of vectors. Then there exists $a \in End_K(V)$ such that $v_i a = w_i$ for each $i = 1, \cdots, n$. It follows from the previous Lemma by taking $A = Hom_K(V, V)$, hence V is an irreducible A-module and $L = Hom_A(V, V)$.

Notice also that Jacobson's Lemma is also valid for any ring A.

Lemma 4.18. *Let A be any ring and let $V = \bigoplus_{i=1}^n V_i$ and $W = \bigoplus_{j=1}^m W_j$ be two A-modules. For $i = 1, \cdots, n$, let ε_i be the natural injection on V_i and for $j = 1, \cdots, m$, let π_j be the natural projection on W_j, that is:*

$$\begin{array}{rccc} \varepsilon_i: & V_i & \longrightarrow & V \\ & v & \longmapsto & v \end{array} \qquad \begin{array}{rccc} \pi_j: & W & \longrightarrow & W_j \\ & \sum_{k=1}^m v_k & \longmapsto & v_j \end{array}$$

It holds:

1) *Assume that for each pair (i, j) with $1 \leq i \leq m$ and $1 \leq j \leq n$, $\varphi_{ij} \in Hom_A(V_j, W_i)$, then we can define $\varphi \in Hom_A(V, W)$ given by:*

$$\varphi(v_1 + \cdots + v_n) = \begin{bmatrix} \varphi_{11} & \cdots & \varphi_{in} \\ \vdots & & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

2) *Conversely, if $\varphi \in Hom_A(V, V)$ we define for each pair (i, j) with $1 \leq i \leq m$ and $1 \leq j \leq n$. We define $\varphi_{ij} = \pi_i \varphi \varepsilon_j \in Hom_A(W_j, V_i)$. It also holds:*

$$\varphi(v_1 + \cdots + v_n) = \begin{bmatrix} \varphi_{11} & \cdots & \varphi_{in} \\ \vdots & & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

3) *Therefore as additive groups, we have the following isomorphism:*

$$Hom_A(V,W) \cong \begin{bmatrix} Hom_A(V_1,W_1) & \cdots & Hom_A(V_n,W_1) \\ \vdots & & \vdots \\ Hom_A(V_1,W_m) & \cdots & Hom_A(V_n,W_m) \end{bmatrix}$$

4) *In particular, if* $V^{(n)} = \overbrace{V \oplus \cdots \oplus V}^{n)}$*, then we have the following ring isomorphism:*

$$End_A(V^{(n)}) \cong Mat_n(End_A(V))$$

Proof. The proof is left to the reader. We give a hint for item b). Notice that:

$$(\varphi_i j)_i j] \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \sum_{i,j} \varphi_{ij}(v_j) = \sum_{i,j} \pi_i \varphi \varepsilon_j(v_j) = \varphi(v_1 + \cdots + v_n)$$

This happens because $\sum_i \pi_i = id_W$. □

Remark 4.19. Let D be a division ring, then D^{op} denotes the opposite division ring of D, that is D^{op} has the same underlying set and also the same addition, but we change the product that is defined as $x \cdot y := yx$. In this case, if V is a n-dimensional D-vector spacem then:

$$End_D(V) \cong Mat_n(D^{op})$$

Proof. From V being a D-vector space, we get that $V \cong \overbrace{D \oplus \cdots \oplus D}^{n)}$ as D-module. Using the previous Lemma, $End_D(V) \cong Mat_n(End_D(D))$. Therefore it is enough to show that $End_D(D) \cong D^{op}$. Let $\varphi \in End_D(D)$ and let $x \in D$ it holds $\varphi(x) = x\varphi(1)$. Therefore we define:

$$\begin{array}{rccc} \Phi: & End_D(D) & \longrightarrow & D^{op} \\ & \varphi & \longmapsto & \varphi(1) \end{array}$$

It is a well-defined, injective and surjective function. We need to see that it is also an homomorphism. Let
$varphi, \psi \in End_D(D)$ and let $x \in D$, it holds:

$$(\varphi\psi)(x) = \varphi(\psi(X)) = \varphi(x\psi(1)) = [x\psi(1)]\varphi(1) = (x)(\varphi(1)\psi(1)) = (x)[\Phi(\varphi)\Phi(\psi)]$$

Finally we get that $\Phi(\varphi\psi) = \Phi(\varphi)\Phi(\psi)$ and we can conclude that $End_D(V) \cong Mat_n(D^{op})$. □

Theorem 4.20. [Wedderburn] *The following statements hold:*

a) *Let A be a simple K-algebra and let V be an irreducible A-module. Consider $D = End_A(V)$ (which is a division algebra). Then $A \cong End_D(V) \cong Mat_n(D^{op})$ where $n = dim_D(V)$. Moreover, if K is algebraically closed (or more general, if $End_A(V) \cong K$) then A is isomorphic to a ring of matrices over K.*

b) *Let D be a division K-algebra and let V be a D-module such that $dim_D(V) = n$, then $A := End_D(V) \cong Mat_n(D^{op})$ is a simple algebra that has V as irreducible and faithful module. Moreover $D = End_A(V)$.*

c) *If D and E are two division algebras with $Mat_n(D) \cong Mat_n(E)$ then $m = n$ and $D \cong E$.*

PROOF. We will prove each statement:

a) Using some previous results, it is straightforward to see that V is, up to isomorphy, the unique irreducible A-module and notice that it is also faithful. Let us define the following function:

$$\begin{array}{rccccc} \alpha : & A & \longrightarrow & End_D(V) & & \\ & a & \longmapsto & \alpha(a): & V & \longrightarrow & V \\ & & & & v & \longmapsto & va \end{array}$$

α is well-defined. In fact, let $a \in A$, $v \in V$ and $k \in K$, it holds:

$$\alpha(a)[kv] = (kv)a = k(va) = k\alpha(a)(v) \quad \Rightarrow \quad \alpha(a) \in End_K(V)$$

moreover, for each $d \in End_A(V)$, it also holds:

$$(vd)\alpha(a) = (vd)a = (va)d = (v\alpha(a))d \quad \Rightarrow \quad \alpha(a) \in End_D(V)$$

It is left to the reader to check the fact of being α a K-algebra homomorphism as well. Now let $a \in A$. Notice the following implications: if $\alpha(a) = 0$ then for each $v \in V$, $va = 0$, therefore $Va = 0$ and using that V is faithful we conclude that $a = 0$, this means that α is a monomorphism.

Let $\{v_1, \cdots, v_n\}$ be a D-basis of V and let $f \in End_D(V)$. By Jacobson's Lemma, there exists some $a \in A$ such that $f(v_i) = v_i a$ for $i = 1, \cdots, n$, therefore $f = \alpha(a)$ and hence, α is an epimorphism. Finally, we get:

$$A \cong End_D(V) \cong Mat_n(D^{op})$$

The rest of the item follows from Schur's Lemma.

b) By construction, V is a D-module and hence it is also a faithful irreducible A-module. Let $d \in D$, $v \in V$ and $a \in A$, notice that $(va)d = (vd)a$. Therefore, D can be embed in $End_A(V)$. By a previous Corollary, it follows that A is a simple algebra. Now, let $f \in End_A(V)$ and consider any $0 \neq v \in V$ (V is a completely reducible D-module), we can write $V = vD \oplus W$ for some D-module W. Let us consider the natural projection $\pi : V \to vD$, we get that $\pi \in A$, therefore: $(v)f = (v\pi)f = (vf)\pi \in V\pi = VD$, therefore there exsits some $d \in D$ with $vf = vd$. Thus, if $w \in V$ there exists some $a \in A$ such that $w = va$ and therefore we get:

$$(w)f = (va)f = (v)fa = (vd)a = (va)d = wd$$

Last statement is valid for each $w \in V$, therefore $f = d$. As a consequence, we conclude that $End_A(V) = D$.

c) Let A be a K-algebra such that $A \cong Mat_n(D) \cong Mat_n(E)$. Applying item b), it holds that A is a simple algebra. Therefore, if V is the unique isomorphy type of the irreducible and faithful A-module then $End_A(V) \cong D^{op} \cong E^{op}$ and hence, $D \cong E$. In particular we get that $m = dim_D(V) = dim_E(V) = n$.

□

We can summarize the preceding Theorem for the case of semisimple K-algebras:

Theorem 4.21. *Let A be a semisimple K-algebra. It holds:*

a) $A = \bigoplus_{i=1}^{k} A_i$ *where* $A_i \cong Mat_{n_i}(D_i^{op})$ *are rings of matrices over a division algebra* D_i *for* $i = 1, \cdots, k$*. Moreover if* $i \neq j$*, then* $A_i A_j = 0$.

b) *A has, up to isomorphy, k irreducible A-modules that are not isomorphic to each other,* V_i *for* $i = 1, \cdots, k$ *(i.e., k irreducible representations up to equivalence). It also happens for* $i = 1, \cdots, k$ *that* V_i *is an irreducible* A_i*-module,* $\bigoplus_{j \neq i} A_i$ *annihilates* V_i *and, moreover,* $V_i A_i = V_i$*. It also occurs that* $End_{A_i}(V_i) = D_i$*, therefore, if we denote* $n_i = dim_{D_i}(V_i)$*, then* $dim_K(V_i) = n_i dim_K(D_i)$ *and therefore:*

$$dim_K(A) = \sum_{i=1}^{k} n_i^2 dim_K(D_i)$$

c) *In particular, if K is algebraically closed it holds that* $D_i \cong K$ *for* $i = 1, \cdots, k$ *and hence,* $dim_K(V_i) = n_i$ *and finally,* $dim_K(A) = \sum_{i=1}^{k} n_i^2$.

CHAPTER 5

Indecomposable Modules

Definition 5.1. **[Indecomposable]** A non-trivial A-module M is **indecomposable** if the condition $M = M_1 \oplus M_2$ implies that $M_1 = 0$ or $M_2 = 0$.

Definition 5.2. **[Local]** An algebra A is called **local** if the set of unit elements $I := \{a \in A : \ a \text{ has no inverse}\}$ is an ideal of A. Notice that in this case, I is the unique maximal right[left]-ideal of A.

Theorem 5.3. *Let A be an algebra:*

a) *If A is local, then $I = J(A)$. In particular, if $a \in A$, then it is a unit or a nilpotent element.*
b) *A is a local algebra if and only if $A/J(A)$ is a division algebra.*

Proof. For the first statement we will use the remark made on Definition 5.2; it follows that $J(A) = I$. Let $a \in A$ be a non-unit element then $a \in I = J(A)$. Let us remember that $J(A)$ is the greatest nilpotent ideal of A and therefore, a is nilpotent. For the second statement, let us check the two implications:

$\gg$ Assume that $J(A) = I$ and let $a + J(A) \in A/J(A)$ be a non-zero element of the quotient, then $a \notin J(A)$ therefore it must be a unit element, therefore there exists some $b \in A$ such that $ab = ba = 1$. Notice that $b + J(A) \neq 0$ and it is the inverse of $a + J(A)$.

$\ll$ Assume that $A/J(A)$ is a division algebra. Let us see that $I = \{a \in A : \ a \text{ has no inverse}\} = J(A)$. Consider any $a \in A$ without right-inverse therefore $aA \subsetneq A$ (because $1 \in A$). There exists some maximal right-ideal A_0 of A with $aA \subseteq A_0 \subsetneq A$. By construction of $J(A)$, we get that $J(A) \subseteq A_0$. Notice also that:

$$(aA + J(A))/J(A) \subseteq A_0/J(A) \subsetneq A/J(A)$$

but $A/J(A)$ is a division algebra that has no proper ideals, therefore $A_0/J(A) = 0$ and thus, $A_0 = J(A)$. It leads to $(aA + J(A))/J(A) = 0$ and hence, $a \in J(A)$. It means, that every element of A that has no right-inverse belongs to $J(A)$.

Assume that b has a right-inverse, i.e., there exists some $c \in A$ such that $bc = 1$. If c has no right-inverse then $c \in J(A)$, and using that $J(A)$ is an ideal of A we have that $1 = bc \in J(A)$ which is a contradiction. Therefore c has right-inverse, i.e., there exists some $d \in A$ with $cd = 1$. Therefore $b = b(cd) = (bc)d = d$. Thus, c is an inverse of b and b is a unit element. We conclude that every non-unit element belongs to $J(A)$, i.e., $I \subseteq J(A)$. But it is straightforward to see that $J(A) \subseteq I$ because every ideal of A must not contain any unit element. Thus, A is local.

□

Lemma 5.4. **[Fitting Lemma]** *Let M be an A-module and let $\alpha \in End_A(M)$ be an A-endomorphism. It holds:*

a) $\exists n_0 \in \mathbb{N}$ *such that* $M = Ker\alpha^{n_0} \oplus Im\alpha^{n_0}$.
b) α *is injective if and only if* α *is surjective.*

Proof. We will only prove the first statement. Consider the family $Im\alpha^i = \{M\alpha^i : i \in \mathbb{N}\}$ $(\alpha^0 = Id)$. M has finite dimension, therefore we can consider a minimal element $M\alpha_1^n$, for some $n_1 \in \mathbb{N}$. It follows that for every $k \geq 0$, $M\alpha^{n_1+k} = (M\alpha^k)\alpha^{n_1} \subseteq M\alpha^{n_1}$. Since $M\alpha^{n_1}$ was chosen to be minimal, we get that $M\alpha^{n_1+k} = M\alpha^{n_1}$ for each $k \geq 0$.

Now consider the family $\{Ker\alpha^i : i \in \mathbb{N}\}$ and take $Ker\alpha^{n_2}$ to be its maximal element. It holds that for each $k \geq 0$, $Ker\alpha^{n_2} \subseteq Ker\alpha n_2 + k$. Since $Ker\alpha^{n_2}$ was chosen to be maximal, we get that $Ker\alpha^{n_2} = Ker\alpha^{n_2+k}$ for each $k \geq 0$.

We set $n_0 = max(n_1, n_2)$. Let $k \geq n_0$, and $m \in Ker\alpha^k \cap Im\alpha^k$ be an arbitrary element. On one side, we can write m as $m_1\alpha$ for some $m_1 \in M$, therefore, $m\alpha^k = (m_1\alpha^k)\alpha^k = m_1\alpha^{2k}$. On the other side, since $m \in Ker\alpha^k$ then $m\alpha^k = 0$. Thus, $m_1\alpha^{2k} = 0$. Therefore $m_1 \in Ker\alpha^{2k} = Ker\alpha^k$. It means that $m = 0$ and we conclude that $Ker\alpha^k \cap Im\alpha^k = 0$.

Now let $m \in M$, it holds that $m\alpha^k \in M\alpha^k = M\alpha^{2k}$. Therefore $\exists m_1 \in M$ such that $m\alpha^k = m_1\alpha^{2k}$ and we can write m as $m = (m - m_1\alpha^k) + m_1\alpha^k$. Notice that $(m - m_1\alpha^k)\alpha^k = m\alpha^k - m_1\alpha^{2k} = m\alpha^k - m\alpha^k = 0$, thus $m - m_1\alpha^k \in Ker\alpha^k$ and it also holds that $m_1\alpha^k \in M\alpha^k = Im\alpha^k$. Therefore $M = Ker\alpha^k + Im\alpha^k$ and finally, $M = Ker\alpha^k \oplus Im\alpha^k$. □

Theorem 5.5. *Let M be an A-module and let us set $E = End_A(M)$. It holds:*

a) *M is an idecomposable A-module if and only if* 0 *and* 1 *are the only idempotent elements of E.*
b) *M is an idecomposable A-module if and only if E is a local algebra.*

Remark 5.6. We only need the condition $dim_K(A) \leq \infty$ for the left implication $(\ll)$ on item b) . The other statements hold for arbitrary dimension.

Proof. Let us firstly check the two implications of item a):

$\gg$ Assume that M is indecomposable and let $f \in E$ be an idempotent element of E. As we already know (previous Chapter), we can write $M = Mf \oplus M(1 - f)$. Notice that Mf and $M(1 - f)$ are A-submodules of M, therefore $Mf = 0$ which leads to $f = 0$ or $M(1 - f) = 0$ which implies that $f = 1$.

$\ll$ Assume that there are no more idempotent elements on E than 0 and 1. Let us prove that M is an idecomposable A-module. Assume that $M = M_1 \oplus M_2$ with $M_i \leq_A M$, $i = 1, 2$. Consider the natural projection $\pi_1 : M \to M$ on the first component. It holds that $Ker\pi_1 = M_2$ and $Im\pi_1 = M_1$. Notice that $\pi_1^2 = \pi_1$ is an idempotent element of E, therefore $\pi_1 = 0$ or $\pi_1 = 1$. For the first case, $M = Ker0 = Ker\pi_1 = M_2$, for the second one $M = ImId = Im\pi_1 = M_1$.

Let us prove the second statement:

$\ll$ Assume that E is a local algebra. Let us prove some more general result. Let T be a local K-algebra and let us see that there are no more idempotent elements on T than 0 and 1 (it will lead to the indecomposability of M by item a)). Let $e \in T$ be an idempotent element of T. It holds that e is a unit or a nilpotent element. For e being a unit element we get that $\exists f \in T$ with $ef = 1$ therefore, $1 = ef = e^2 f = e(ef) = e$. For the nilpotent case, we can find some $k \in \mathbb{N}$ with $e^k = 0$, but notice that e is idempotent, therefore, $0 = e^k = e$.

$\gg$ Assume that M is an indecomposable A-module. Using the Fitting Lemma, we can write $M = Kerf^k \oplus Imf^k$. Therefore $Kerf^k = 0$ or $Imf^k = 0$. If $Kerf^k = 0$, then f^k is a monomorphism and we conclude that f^k is an automorphism, i.e., we can find some $g \in E$ with $f^k g = gf^k = 1$. But notice that $(gf^{k-1})f = f(gf^{k-1}) = 1$, therefore f is a unit element. For the case $Imf^k = 0$, we get that $f^k = 0$ and thus, f is nilpotent. Finally, every element of E is either unit or nilpotent.

We will prove that the set of non-unit elements of E is an ideal; Let $\alpha \in E$ be a non-unit element of E and let $\beta \in E$. Notice that α is not a monomorphism because it is not a unit, therefore, aplying Fitting's Lemma, we get that $0 \neq Ker\alpha \subseteq Ker(\alpha\beta)$, therefore $\alpha\beta$ is not a monomorphism, then it is not a unit element.

Now let $\alpha_1, \alpha_2 \in E$ be two non-unit elements and let us check that also $(\alpha_1 + \alpha_2)$ is not a unit. Assume towards a contradiction, that $(\alpha_1 + \alpha_2)$ is a unit element, then there exists some $\gamma \in E$ with $(\alpha_1 + \alpha_2)\gamma = \alpha_1\gamma + \alpha_2\gamma = 1$. Let us set $\beta_i = \alpha_i\gamma$ for $i = 1, 2$. Notice that $\beta_1 + \beta_2 = 1$, thus $\beta_1 = 1 - \beta_2$, therefore:

$$\left.\begin{array}{l} \beta_1\beta_2 = (1-\beta_2)\beta_2 = \beta_2 - \beta_2^2 \\ \beta_2\beta_1 = \beta_2(1-\beta_2) = \beta_2 - \beta_2^2 \end{array}\right| \Rightarrow \ \beta_1\beta_2 = \beta_2\beta_1 \ \star$$

Using the previous result, $\beta_i = \alpha_i\gamma$ is not a unit element for $i = 1, 2$, therefore β_i is a nilpotent element for $i = 1, 2$. There exists some $n \in \mathbb{N}$ such that $\beta_1^n = \beta_2^n = 0$. Hence:

$$(\beta_1 + \beta_2)^n =^\star \sum_{i=0}^{2n} \binom{2n}{i} \beta_1^i \beta_2^{2n} = 0$$

It contradices the equation $\beta_1 + \beta_2 = 1$. Therefore, $\alpha_1 + \alpha_2$ is not a unit element.

If $\alpha \in E$ is not a unit element, it is straightforward to see that $-\alpha$ is also a non-unit element. Moreover, let $\alpha, \beta \in E$ with α being non-unit, then $\beta\alpha$ is not a unit because $Im(\beta\alpha) \subseteq Im\alpha \subsetneq M$, therefore $\beta\alpha$ is not a unit. It follows that the set $\{\alpha \in E : \ \alpha \text{ is not a unit}\}$ is an ideal of E, and we finally get that E is a local algebra.

□

Theorem 5.7. **[Krull-Schmidt]** *Let M be an A-module, then:*

a) *$M = M_1 \oplus \cdots \oplus M_n$ where M_i is an idecomposable A-module for $i = 1, \cdots, n$.*
b) *Last decomposition is unique up to index ordenation; If $M = N_1 \oplus \cdots \oplus N_k$ where N_j is an idecomposable A-module for $j = 1, \cdots, k$, then $n = k$ and $M_i \cong N_i$ up to reordenation.*

Proof. Let us prove each statement:

a) We will use induction on $dim_K(M)$. Assume that the statement is true for A-modules with dimension lower than $dim_K(M)$. If M is indecomposable we are done, take $n = 1$ and $M_i = M$. Therefore we can assume that M is not indecomposable, i.e., there are $0 \neq M_1, M_2 \leq_A M$ with $M = M_1 \oplus M_2$. Notice that $dim_k(M_i) \leq dim_K(M)$ for $i = 1, 2$ therefore, applying the inductive hypothesis, we have that $M_i = \bigoplus_{j=1}^{n_i} Mij$, for $i = 1, 2$ with M_{ij} indecomposable for $j = 1, \cdots n_i$. and we get the desired result:

$$M = M_1 \oplus M_2 = \bigoplus_{i=1}^{2} \bigoplus_{j=1}^{n_i} Mij$$

b) Assume that $M = M_1 \oplus \cdots \oplus M_n = N_1 \oplus \cdots \oplus N_k$. We will prove that, for an specific reordenation of the indices, it holds that $M_1 \cong N_1$ and it also holds that $M \cong N_1 \oplus M_2 \oplus \cdots \oplus M_n \cong N_1 \oplus \cdots \oplus N_k$. At this point, it is enough to apply an inductive step to conclude that $n = k$ and also that $M_i \cong N_i$ for $i = 1, \cdots, n$ up to reordenation.

Let us check the above affirmations; Let us set $N = \bigoplus_{j=1}^{k} N_j$. Notice that $M \cong N$, assume that they are isomorphic via φ. Let π_i be the projection of N on each M_i for $i = 1, \cdots, n$ and let ρ_j be the projection of M on each N_j for $j = 1, \cdots, k$. It holds that $1 = \sum_{j=1}^{k} \rho_j = \sum_{i=1}^{n} \pi_i$. Therefore, $\pi_1 = 1\pi_1 = (\sum_{j=1}^{k} \rho_j)\pi_1 \sum_{j=1}^{k} \rho_j\pi_1$. Let us denote $\widetilde{\rho_j\pi_1} := (\rho_j\pi_1)_{|M} \in End_A(M_1)$. Notice that $End_A(M_1)$ is a local algebra because M_1 is indecomposable, therefore for each $j \in \{1, \cdots, k\}$, $\widetilde{\rho_j\pi_1}$ is either a unit or a nilpotent element. Assume, towards a contradicition that for each $j \in \{1, \cdots, k\}$, $\widetilde{\rho_j\pi_1}$ is a nilpotent element, thus $1 = \sum_{j=1}^{k} \widetilde{\rho_j\pi_1}$ would be nilpotent, which is a contradiction. Hence, there exists some $j \in \{1, \cdots, k\}$ that we can assume, without loss of gnerality, $j = 1$, for which $\widetilde{\rho_1\pi_1}$ is a unit.

Let us denote $X := M_1\rho_1$ and $Y = N_1 \cap Ker\pi_1$ and let us check that $N_1 = X \oplus Y$. First notice that $N_1 = X + Y$; let $v \in N_1$, notice that $v\pi_1 \in M_1$, therefore one can find some $u \in M_1$ with $v\pi_1 = (u\rho_1)\pi_1$, therefore $(u\rho_1 - v)\pi_1 = 0$ which leads to affirm that $u\rho_1 - v \in Ker\pi_1 \cap N_1 = Y$. Thus, $v = u\rho_1 + (v - u\rho_1)$. Secondly let us check that $X \cap Y = 0$; let $v \in X \cap Y$ then $v = u\rho_1$ for some $u \in M_1$ and $v \in Ker\pi_1 \cap N_1$, i.e., $v\pi_1 = u\rho_1\pi_1 = 0$. This means that $u \in Ker\widetilde{\rho_1\pi_1} = 0$. It follows that $u = 0$ and hence, $v = 0$. Finally $N_1 = X \oplus Y$.

Since N_1 is indecomposable, then $X = 0$ or $Y = 0$. For $X = 0$ we get a contradiction because $M_1\rho_1\pi_1 = M_1 = 0$, therefore $Ker\pi_1 \cap N_1 = Y = 0$. It follows that $M_1\rho_1 = X = N_1$. Moreover, $(\rho_1)_{|M_1}$ is surjective and $(\pi_1)_{|N_1}$ is injective. From $\widetilde{\rho_1\pi_1}$ being an isomorphism, there exists some $g \in End_A(M_1)$ such that $\widetilde{\rho_1\pi_1}g = 1_M = (\rho_1\pi_1)_{|M}g = 1_{M_1}$, and finally we get that $(\rho_1)_{|M_1}$ is injective and we conclude that ρ_1 is an isomorphism. It leads to $M_1 \cong N_1$.

It follows from $N_1 \cap (M_2 \oplus \cdots \oplus M_n) = N_1 \cap Ker\pi_1 = Y = 0$ that $dimN_1 = dimM_1$. And we obtain our desired result:

$$M \cong N_1 \oplus M_2 \oplus \cdots \oplus M_n$$

□

CHAPTER 6

Group Algebras

In this chapter, we develop the most important example of a group algebra over a field. We will get into detail about the previous results on the group algebra KG. The fundamental result on this chapter, and one of the most important results on the whole theory is that of Maschke, already proved in Chapter 3. In this chapter, G will denote a group and K will be a field.

Theorem 6.1. [Maschke] *The group algebra is semisimple if and only if*

$$carK \nmid |G|$$

We can use the equivalence: semisimple algebra $\Leftrightarrow$ every module over the algebra is completely reducible to state last Theorem with this equivalent form

Theorem 6.2. [Maschke] *Every KG-module is completely reducible if and only if $carK \nmid |G|$.*

Theorem 6.3. *Let K be a field and let G be a finite group. Let us consider the center of KG, $Z(KG) = \{x \in KG : \ \forall y \in KG \ (xy = yx)\}$. $Z(KG)$ is a K-algebra which is a subalgebra of KG. Let $\{\mathcal{C}_i : \ i = 1, \cdots, n\}$ be the set of conjugacy classes of G and let us denote $C_i = \sum_{x\in\mathcal{C}_i} x$ for $i = 1, \cdots, n$. Then $\{C_1, \cdots, C_n\}$ is a K-basis of $Z(KG)$. In particular, $dim(Z(KG))$ is equal to the number of conjugacy classes of G.*

Proof. For each $i = 1, \cdots, n$ and $g \in G$ it holds:

$$g^{-1}C_i g = g^{-1}\left(\sum_{x\in\mathcal{C}_i} x\right) g = \sum_{x\in\mathcal{C}_i} g^{-1}xg = \sum_{x\in\mathcal{C}_i} x = C_i$$

It means that $C_i \in Z(KG)$ for each $i = 1, \cdots, n$. Moreover, the set $\{C_1, \cdots, C_n\}$ is a K-linearly independent because $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ if $i \neq j$. Let $\sum_{g\in G} a_g g$ be an arbitrary element of $Z(KG)$, then for each $h \in G$:

$$\sum_{g\in G} a_g g = h^{-1}\left(\sum_{g\in G} a_g g\right) h = \sum_{g\in G} a_g h^{-1}gh$$

this means that $a_g = a_{hgh^{-1}}$ for each $h \in G$. Then:

$$\sum_{g\in G} a_g g = \sum_{i=1}^{n} a_i \left(\sum_{g\in\mathcal{C}_i} g\right)$$

it follows that $\{C_1, \cdots, C_n\}$ is a set of generators of $Z(KG)$. $\square$

Theorem 6.4. *Let G be a finite group and let K be a field with $End_{KG}(V) \cong K$ for each irreducible KG-module V (in particular, when K is algebaically closed) and assume that $carK \nmid |G|$, then:*

$$KG \cong Mat_{n_1}(K) \oplus \cdots \oplus Mat_{n_h}(K)$$

where h is the number of conjugacy classes of G. Moreover, KG has, up to isomorphy, h irreducible representations $V_1, \cdots, V_h$. It also happens that, up to indeces reordenation, $dim_K(V_i) = n_i$ and $n_1 = 1$. Thus, $|G| = \sum_{i=1}^{h} n_i^2$ and G has, up to isomorphy, h irreducible representations.

PROOF. It is almost everything proved. By Maschke's Theorem KG is semisimple and using Wedderburn's Theorem we get that $KG \cong \bigoplus_{i=1}^{s} Mat_{n_i}(K)$ where s is the number of irreducible KG-modules and the n_i's are the respective dimensions. Moreover $Z(KG) \cong \sum_{i=1}^{s} Z(Mat_{n_i}(K))$. The dimension of each $Z(Mat_{n_i}(K))$ is 1, therefore $s = dim_K(ZG) = h$. Taking dimensions we get that

$$dim_K(KG) = |G| = \sum_{i=1}^{h} n_i^2$$

with $n_1 = 1$ (it corresponds to the trivial module and becomes associated to the conjugacy class of 1). $\square$

Remark 6.5. Let $carK = p$ for some arbitrary prime number p, then the number of isomorphic types of irreducible KG-modules is equal to the number of conjugacy classes of p'-element of G. If we avoid the hypothesis $End_{KG}(V) \cong K$ for each irreducible KG-module V, there it also exists a related result that gives the number of isomorphic types of irreducible KG-modules.

Example 6.6. Let $G \cong \Sigma_3$ be the non-abelian group of order 6. G has 3 conjugacy classes, therefore G has 3 isomorphy types of irreducible $\mathbb{C}G$-modules. In Chapter 2 we have already built the irreducible $\mathbb{C}G$-module of dimension 2. Notice that $n_1 = 1$ and $n_2 = 2$ therefore $n_3 = 1$ in order to get $6 = 1 + 2^2 + n_3^2$. Then there exists a representation $R : G \to \mathcal{C} \setminus \{0\}$. Notice that $KerR \neq G$ and it also holds that $KerR \neq \{1\}$ (otherwise, $G \cong G/\{1\} \cong G/KerR \cong \mathcal{C} \setminus \{0\}$, but $\mathcal{C} \setminus \{0\}$ is abelian). Therefore it must necessarily hold that $|KerR| = 3$ and $R(x) = -1$ and $R(y) = 1$.

Theorem 6.7. *Let G be a group and let K be a field with $carK \nmid |G|$ such that $End_{KG}(V) \cong K$ for each irreducible KG-module. With the previous notation, V_i has multiplicity n_i on the regular KG-module.*

PROOF. It holds that $KG \cong \bigoplus_{i=1}^{n} a_i$, where $A_i = Mat_{n_i}(K)$. It follows from Chapter 4 that the simple algebra A_i has exactly on irreducible and faithful module V_i with dimension n_i (up to isomorphy) for $i = 1, \cdots, n$. It also hlds that $dim_K(A_i) = n_i^2$, i.e.,

$$A_i \cong \overbrace{V_i \oplus \cdots \oplus V_i}^{n_i)}$$

which proves the theorem. $\square$