Introduction to representation theory?

Shrivathsa Pandelu

September 19, 2021

Contents

1 About

I was reading Amritanshu Prasad's book on Representation Theory, and the first chapter was too terse for me. I wanted more explanations and a more general theory. So I set out to write these notes in order to collect my thoughts on the subject and develop it in a general context. I have tried to keep the rings as general as possible in the sense that they are mostly non commutative. In the beginning I have made sure to take rings without unity, but near the end, especially after Artin-Wedderburn Theory, it is hopeless to consider rings without unity. Therefore, the most general rings considered here are non commutative rings that may or may not have unity. I have also made sure to avoid the use of finite dimensionality as much as possible. However, I was not bold enough to work with non associative rings.

Of course, when it comes to a subject like this, there is no point in trying to be original because all of the subject matter here has been covered by hundreds of authors in many ways, regurgitated over and over for the better part of the last century. Of course, I have shamelessly borrowed most of the material from different books, websites and papers that I have not kept track of. Of all the resources, three stand out and have been listed.

In the end, I suppose some parts are original, at least in the presentation because this is the way my thoughts flowed on the subject. Certain topics make an appearance out of necessity than as a part of a larger theory, but I guess this is a good thing because it points out a motivation for the existence of said topic. I would confidently say that some of the proofs are original in the sense that I thought of them on my own. Of course, if anyone searches for them, they might find the exact proof (may be in an even more general/exotic setting) in no time. But I wanted to find these proofs on my own, with some hints here and there in case I got stuck, and that is exactly what I have done, at least for most of the text.

So, perhaps this is nothing but glorified accounting. I wasted about two weeks' time in collecting these results from varius resources and painstakingly LaTeXing them just to feel like I am doing something useful. In fact, all of the material here can be found in T. Y. Lam's book on Noncommutative Ring Theory. But unfortunately, I discovered that book about half way through my efforts on this, and by then it was too late to stop writing this. Basically, this is an abridged version of the first few chapters of that book. It doesn't even convey that much and contains only what I thought was interesting making it all the more worthless, just like all the time I spent on this. Having said that, dear reader, do enjoy this absolute horseshit.

2 Preliminary results

Let R be a ring and M an abelian group. M is a (left) R module if there is a ring homomorphism $\rho\colon R \to \mathrm{End}(M)$ where $\mathrm{End}(M)$ is the ring of group homomorphisms $M \to M$. We denote the R-module M by (M, ρ). If R has a 1, we require 1 to map to the identity homomorphism. There is a notion of right R-module and this is when we reverse the order of multiplication in $\mathrm{End}_R(M)$. Basically, this comes from the two possible ways to make $\mathrm{End}_R(M)$ a ring. We shall only deal with left modules where the multiplication of $T_1, T_2 \in \mathrm{End}_R(M)$ is the map $T_1 \circ T_2$. Given $r \in R, m \in M$, we write rm to mean $\rho(r)(m)$.

A submodule of a module M is a subgroup of M that is closed under the action of R, i.e. closed under $\rho(r)\,\forall\, r \in R$. Given a subset $S \subseteq M$, the submodule generated by S is the smallest submodule $\langle S\rangle$ containing S, in other words it is the intersection of all submodules (including M) containing S. When R contains a 1, it is easily seen to be $\langle S\rangle = \{\sum_{\text{finite}} r_i s_i | r_i \in R, s_i \in S\}$. However, when R doesn't contain a unity, this is still a submodule, but may not contain S.

For example, take $R = 2\mathbb{Z}$ and $S = \{2\}$. Then the submodule above is $4\mathbb{Z}$ and doesn't contain 2. In order to contain S, we may proceed as follows. First take the subgroup S' generated by S in M. Then consider the set $S'' = \cup_{r\in R} rS'$. Now S'' is closed under the action of R, but need not be a subgroup. Now, take S''' to be the subgroup generated by S''. This is closed under the action of R and is a subgroup. Therefore, $\langle S\rangle = S'''$. It can also be thought of as $\langle S\rangle = \{\sum_{\text{finite}} r_r s_i | s_i \in S, r_i \in \mathbb{Z} \sqcup R\}$ using the $\mathbb{Z}$-module structure on M.

Definition. *An R-module is Artinian (Noetherian) if it satisfies the descending (ascending) chain condition on left submodules.*

Let $(M, \rho_1), (N, \rho_2)$ be R-modules. A group homomorphism $T\colon M \to N$ is said to be R-linear, or an R-module homomorphism, if

$$\begin{tikzcd} M \arrow[r, "T"] \arrow[d, "\rho_1(r)"'] & N \arrow[d, "\rho_2(r)"] \\ M \arrow[r, "T"'] & N \end{tikzcd}$$

commutes for every $r \in R$.

The center $Z(R)$ of a ring R is the set $\{x \in R | xy = yx \forall y \in R\}$. It is easy to see that $Z(R)$ is a commutative subring of R. Given a commutative ring R and a ring S, both having a unity, S is an algebra over R if there is a ring homomorphism $f\colon R \to S$ such that $f(1_R) = 1_S$ and $f(R) \subseteq Z(S)$. When R does not have a unity, we just mean that there is a homomorphism that takes R into $Z(S)$.

When S is an R-algebra, it is an R module with multiplication $r \cdot x = f(r)x \,\forall\, r \in R, x \in S$. When S, T are R-algebras, and R-algebra homomorphism between them is simply a ring homomorphism that is also R-linear.

Given R-modules M, N, the additive group all R-module homomorphisms forms a $Z(R)$-module $\mathrm{Hom}_R(M, N)$ with

$$\begin{aligned} \tilde{\rho} \colon Z(R) &\to \mathrm{Hom}(\mathrm{Hom}_R(M, N)) \\ r &\mapsto \{T \mapsto \rho_2(r) \circ T\} \end{aligned}$$

When $M = N$, we write $\mathrm{Hom}_R(M, M) = \mathrm{End}_R(M)$. Because of the R-linearity, it is easy to see that $\mathrm{End}_R(M)$ is actually a $Z(R)$-algebra. If we do not look for R-linearity, then the additive group of group homomorphisms $\mathrm{Hom}(M, N)$ is an R-module with the obvious action.

When $M = N$, then $\rho_1(R) \subseteq \mathrm{End}(M)$, however, it is easy to see that $\rho_1(r)$ is $Z(R)$-linear for every $r \in R$, therefore, $\rho_1(R) \subseteq \mathrm{End}_{Z(R)}(M)$. In particular, when R is a K-algebra, $\rho_1(r)$ is a K-vector space transformation. We shall see later that under some specific conditions, $\rho_1(R) = \mathrm{End}_K(M)$.

Suppose $\{V_i\}_{i\in I}$ is a collection of R-modules over some indexing set I. The direct product of this collection is the module structure on the cartesian product $\prod_{i\in I} V_i$. The direct sum is the module $\oplus_{i\in I} V_i$ with underlying set the formal sums of terms from V_i with all but finitely many being zero. It can be thought of as the collection of functions from $I \to \prod_{i\in I} V_i$ that are zero at all but finitely many points in I.

If $\{V_i\}_{i\in I}$ is a collection of submodules of a module V, then we form the internal direct sum $\oplus V_i$ if every element in $\sum V_i$ has a unique representation. That is, there is exactly one way to write the elements of $\sum V_i$ as a (finite) sum of elements from V_i. The internal direct sum is the image of the external direct sum in V (take the external sum $v_{i_1} \oplus \cdots \oplus v_{i_k} \mapsto v_{i_1} + \cdots + v_{i_k}, i_1, \ldots, i_k \in I$).

If I is an indexing set and V an R-module, then we write $V^I = \prod_{i\in I} V, V^{(I)} = \oplus_{i\in I} V$. When I is finite, the two notions are equivalent and we use the notations interchangeably.

Let K be a field and suppose R has a unity and is a finite dimensional K-algebra. By the K-algebra structure on R, and the fact that R has a unity make every R module a K-vector space. For a general ring, we define the following.

Definition. *An R-module M is simple (or irreducible) if it has no nontrivial submodule. The module M is semisimple (or completely reducible) if it can be written as a direct sum of simple modules. The ring R is semisimple if every R module is semisimple.*

Let G be a finite group, a representation of G is a finite dimensional K-vector space V with a group homomorphism $\rho \colon G \to \mathrm{GL}(V)$. If we form the ring $K[G]$ which is a finite dimensional K-algebra, then V is a $K[G]$ module. Two representations of G are isomorphic if they are isomorphic as $K[G]$-modules.

Examples:

- If R is a K-algebra, then we have a non zero ring homomorphism $K \to R$. Since K is a field, this homomorphism should be injective, therefore R contains a copy of K in its center.
- Suppose $R = K[G]$, then the elements of $K[G]$ can be thought of as functions $G \to K$. An element $f \in K[G]$ is in the center if and only if $gfg^{-1} = f \,\forall\, g \in G$. This means that f is constant on conjugacy classes. Such a function is called a class function on G. Therefore, $Z(K[G])$ is the set of all class functions on G.

Theorem 1. *Let M be an R-module and N a submodule. Then M is Artinian (Noetherian) if and only if $N, M/N$ are Artinian (Noetherian).*

Proof. We prove the Artinian case, Noetherian is similar. Suppose M is Artinian. Then any descending chain in N is a descending chain in M, hence stabilises. Similarly, any descending chain in M/N corresponds to a descending chain of submodules in M containing N, therefore stabilises.

Conversely, suppose $N, M/N$ are submodules. Let $M_1 \supseteq M_2 \supseteq \ldots$ be a descending chain of submodules. Form the chains $(M_i \cap N)_{i\geq 1}, ((M_i + N)/N)_{i\geq 1}$. Both of these chains stabilize after some stage. So, there is an N such that

$$M_n \cap N = M_{n+1} \cap N, (M_n + N)/N = (M_{n+1} + N)/N \,\forall\, n \geq N.$$

For $n \geq N$, we know $M_n \supseteq M_{n+1}$. Given $x \in M_n$, we know that $x + N \in (M_{n+1} + N)/N$, so there is a $y \in M_{n+1}$ such that $x - y \in N$. Therefore, $x - y \in M_n \cap N = M_{n+1} \cap N \Rightarrow x \in M_{n+1}$. Therefore, $M_n = M_{n+1} \, \forall \, n \geq N$ and M is Artinian. □

Corollary. *A finite direct sum of Artinian (Noetherian) R-modules is Artinian (Noetherian).*

Proof. We proceed by induction. Suppose $M_1, \ldots, M_n$ are Artinian modules and $M = M_1 \oplus \cdots \oplus M_n$. Then $M/M_1 \cong M_2 \oplus \cdots \oplus M_n$. If the corollary is true for $n-1$, then by the theorem it is true for n. Therefore, by induction it is true for every finite direct sum. □

Lemma 1. *Suppose M is an R-module for some ring R, then M is semisimple if and only if it is a sum of simple submodules.*

Proof. Suppose $\phi \colon \oplus M_i \to \oplus M$ is an isomorphism where M_i (over some indexing set) are simple modules. The images $\phi(M_i)$ are isomorphic to M_i and are simple. Moreover, $\phi(M_i) \cap \phi(M_j) = \{0\}$ for $i \neq j$ as if $\phi(x) = \phi(y)$ for some $x \in M_i, y \in M_j$, then $\phi(x - y) = 0$, but $x - y \neq 0$ in $\oplus M_i$. It follows that $M = \oplus \phi(M_i)$ is a (internal direct) sum of simple submodules.

Conversely, suppose $M = \sum_{i \in I} M_i$ is a sum of simple submodules. Given M_i, M_j, either $M_i = M_j$ or $M_i \cap M_j = \{0\}$ by simplicity.

Consider $M_1, \ldots, M_k$. If there are two ways to write some element in $\sum_{j=1}^k M_j$, then there are elements $x_j \in M_j$ such that $x_1 + \cdots + x_k = 0 \in M$. Suppose $x_k \neq 0$, then $x_k \in M_1 + \ldots M_{k-1}$, therefore, $M_k \subseteq M_1 + \cdots + M_{k-1}$ by simplicity of M_k. This means that $M_1 + \cdots + M_k = M_1 + \cdots + M_{k-1}$. If k is minimal in the sense that no fewer M_i add up to $\sum M_i$, then it follows that the sum is actually an internal direct sum.

Consider all possible direct sums $\oplus_{i \in J} M_i$ where $J \subseteq I$. In essence, this is all collections of M_i such that their sum is an internal direct sum. Order this collection by saying that a direct sum over J_1 is less than that over J_2 if $J_1 \subseteq J_2$. Zorn's lemma applies to give us a maximal direct sum $V = \oplus_{i \in J} M_i$. Now, given any M_i, by simplicity, either $M_i \subseteq W$ or $M_i \cap W = \{0\}$. In the second case, $W \oplus M_i$ is a strictly larger direct sum contradicting maximality of W. Therefore, each M_i is in W, so $M = \oplus_{i \in J} M_i = W$ is semisimple. Note that removing redundancies from the original collection would still require Axiom of Choice. □

3 New representations from old

Suppose (V, ρ) is a representation of G, and G_1 is a subgroup of G, then V is also a G_1 representation given by the restriction of ρ to G_1. More generally, if R is a K-algebra, and V is an R-module, and S is a subalgebra, then V is also an S-module.

Suppose G, H are finite groups and (V, ρ) is a representation of G, and (W, σ) a representation of H. Then the space $\mathrm{Hom}_K(V, W)$ is a $G \times H$ representation as follows. Given $(g, h) \in G \times H, T \in \mathrm{Hom}_K(V, W)$, we want

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "\rho(g)"'] & W \arrow[d, "\sigma(h)"] \\ V \arrow[r, "(g,h)\cdot T"'] & W \end{tikzcd}$$

to commute. So we define $(g, h) \cdot T = \sigma(h) \circ T \circ \rho(g)^{-1}$. This gives a group homomorphism $G \times H \to \mathrm{GL}(\mathrm{Hom}_K(V, W))$.

There is another $G \times H$ representation that we can form from V, W. This is the external tensor product denoted by $V \boxtimes W$, which is the vector space $V \otimes_K W$ with group action

$$\begin{aligned} \rho \boxtimes \sigma \colon G \times H &\to \mathrm{GL}(V \otimes W) \\ (g, h) &\mapsto \rho(g) \otimes \sigma(h) \end{aligned}$$

More generally, if R, S are K-algebras, and V is an R-module, and W an S-module, then we can similarly form $V \boxtimes W$ which is an $R \otimes_K S$ module. In the case of group representations, we have

$K[G]\otimes_K K[H] \cong K[G\times H]$, so the external tensor product becomes a $G\times H$ representation. However, unlike group representations, it is not always possible to make $\mathrm{Hom}_K(V, W)$ an $R \otimes_K S$-module.

The reason it is called an external tensor product is the obvious fact that there is an internal tensor product. If V, W were representations of G, then $V \otimes W$ is also a representation of G, given by $g \mapsto \rho(g) \otimes \sigma(g)$. Observe that this representation is the restriction of the $G \times G$ representation $V \boxtimes W$ to the diagonal subgroup $G \leq G \times G$.

The K-vector space K is a representation of the trivial group 1. Given a G representation (V, ρ), we can make $V^* = \mathrm{Hom}_K(V, K)$ a $G \times 1 = G$ representation.

Theorem 2. *For finite dimensional K-vector spaces V, W, we have $V \cong V^*$ and $Hom_K(V, W) \cong V^* \otimes_K W$ as K-vector spaces.*

Proof. Fix a basis $\{e_1, \dots, e_n\}$ of V. We have the corresponding dual basis $\{f_1, \dots, f_n\}$ of V^* defined by

$$\begin{aligned} f_i \colon V &\to K \\ \sum_{j=1}^{n} a_j e_j &\mapsto a_i \end{aligned}$$

Note that because $\{e_1, \dots, e_n\}$ is a basis, $f_1, \dots, f_n$ are well defined linear functionals on V. Given any $f \in V^*$, if we set $a_i = f(e_i) \in K$, then it is easy to see that $f, a_1 f_1 + \dots a_n f_n$ agree on $\{e_1, \dots, e_n\}$, and hence on V by linearity. It is easy to see that the set $\{f_1, \dots, f_n\}$ is linearly independent in V^*, and therefore form a basis of V^*. Therefore $e_i \mapsto f_i$ is an isomorphism.

We have the K-bilinear map

$$\begin{aligned} V^* \times W &\to \mathrm{Hom}_K(V, W) \\ (f, w) &\mapsto \{v \mapsto f(v)w\} \end{aligned}$$

which induces a vector space homomorphism

$$\begin{aligned} T_1 \colon V^* \otimes W &\to \mathrm{Hom}_K(V, W) \\ f \otimes w &\mapsto \{v \mapsto f(v)w\} \end{aligned}$$

Now, fix a basis $\{e_1, \dots, e_n\}$ of V, and let $f_i = e_i^*$ be the dual of e_i. Define

$$\begin{aligned} T_2 \colon \mathrm{Hom}_K(V, W) &\to V^* \otimes W \\ T &\mapsto \sum_{i=1}^{n} f_i \otimes T(e_i) \end{aligned}$$

It is clear that T_2 is a K-vector space homomorphism. Now, $T_1 \circ T_2(T)(e_j) = T_1(\sum_{i=1}^n f_i \otimes T(e_i))(e_j) = T(e_j)$, and therefore, $T_1 \circ T_2 = Id_{\mathrm{Hom}_K(V,W)}$. Now, given $f \otimes w \in V^* \otimes W$, writing $f = a_1 f_1 + \dots + a_n f_n$, we can rewrite $f = f_1 \otimes w_1 + \dots f_n \otimes w_n$ for some $w_1, \dots, w_n$. This means that each $f \otimes w$ is of the form $T_2(T)$ for some T (in this case $T \colon e_i \to w_i$), so T_2 is surjective. Thus, $T_2 \circ T_1 = Id_{V^* \otimes W}$. Hence, T_1 is an isomorphism with inverse T_2. $\square$

Remark. In the proof above, we did not require W to be finite dimensional. Moreover, we can define a dual set even when V is not finite dimensional, and the resulting set is going to be linearly independent. The definition of T_1 doesn't require V or W to be finite dimensional.

Theorem 3. *The isomorphisms T_1, T_2 above are $G \times H$ linear.*

Proof. For a vector v, group element g, denote by $g\cdot v$ the action of g on v. We just need to show that T_1, T_2 are $K[G \times H]$ linear, in particular it suffices to show linearity for $(g, h) \in G \times H$. Fix $(g, h) \in G \times H$, for any $x \in V$

$$T_1((g, h)\cdot f \otimes w)(x) = T_1(g\cdot f \otimes h\cdot w)(x) = (g\cdot f)(x) h\cdot w = f(g^{-1}\cdot x) h\cdot w$$

and

$$(g,h).T_1(f\otimes w)(x) = h\cdot T_1(f\otimes w)(g^{-1}\cdot x) = h\cdot (f(g^{-1}\cdot x)w) = f(g^{-1}\cdot x)h\cdot w.$$

Therefore, T_1 is $G\times H$-linear. Since T_2 is the inverse of T_1, it is bijective, and it follows that T_2 is also $G\times H$-linear because T_1 is. Therefore, $V^*\boxtimes W \cong \mathrm{Hom}_K(V,W)$ as $G\times H$ representations. □

4 Complete reducibility

In this section we will be dealing with generic modules over generic rings. Given a ring R, the additive group of R is an R-module with the homomorphism

$$\begin{aligned} R &\to \mathrm{End}(R) \\ r &\mapsto \{x\mapsto rx\} \end{aligned}$$

This module is called the (left) regular module ${}_RR$. The submodules of ${}_RR$ are the left ideals of R. Multiplication on the right is not going to give us a ring homomorphism because of the way composition is defined in $\mathrm{End}(R)$. However, if we reverse the order of multiplication on the left R, then we have a new ring called the opposite ring, and the right ideals of R are submodules of the right regular module R_R.

If an R module V is not simple, then we would like to decompose it into a direct sum of submodules. Ideally, given a submodule W of V, we would like a submodule W' such that $V = W\oplus W'$. Such a W' is called an invariant complement of W.

Lemma 2. *Let V be an R-module with W a submodule. If every submodule of V has an invariant complement, then every submodule of W has an invariant complement in W, and every submodule of V/W has an invariant complement in V/W.*

Proof. Suppose $V = W\oplus W'$, and U is a submodule of W. Then U is a submodule of V, and there is a U' such that $V = U\oplus U'$. Look at $U'\cap W$. This is a submodule in W, and it is easy to see that $W = U\oplus (U'\cap W)$.

Suppose $\tilde{U}$ is a submodule of V/W, then $\tilde{U} = U/W$ for some submodule $W\subseteq U\subseteq V$. There is a submodule U' such that $V = U\oplus U'$. Look at $(U'+W)/W$ which is a submodule of V/W, and we have $V/W = U/W\oplus (U'+W)/W$. □

Lemma 3. *(Krull's theorem) Suppose V is a finitely generated R-module, then V has a maximal submodule, i.e. a submodule $W\subsetneq V$ such that if $W\subseteq V'\subseteq V$, then either $v' = W$ or $V' = V$.*

Proof. Let $\mathcal{S}$ be the collection of all proper submodules of V partially ordered by inclusion. Suppose $\mathcal{C}$ is a chain in $\mathcal{S}$, then take $W = \cup_{U\in\mathcal{C}}U$. It is clear that W is a submodule of V.

Now, assume V is generated by some $e_1,\ldots,e_n\in V$. If $W = V$, then $e_1,\ldots,e_n\in W$. This means that there are $U_1,\ldots,U_n\in\mathcal{C}$ such that $e_i\in U_i, 1\le i\le n$. Because $\mathcal{C}$ is a chain, one of the U_i, say U_n, is largest, and therefore contains each e_i. Therefore, $U_n = V$ which is a contradiction as $U_n\in\mathcal{S}$. Therefore, $W\in\mathcal{S}$ is an upper bound for $\mathcal{C}$. By Zorn's lemma, $\mathcal{S}$ has a maximal element which is a maximal submodule of V. □

Remark. The proof can be adjusted so that the maximal submodule contains a fixed submodule V_1. Moreover, the exact same proof works for rings with 1, where submodules are left/right ideals.

Lemma 4. *An R-module V is completely reducible if and only if every invariant submodule has an invariant complement.*

Proof. Suppose V is completely reducible, say $V = \oplus_{i\in I}V_i$ where I is some indexing set, and V_i are simple. Let W be a submodule of V. Let $\mathcal{S}$ be the collection of submodules U of V such that $U\cap W = \{0\}$. Since $\mathcal{S}$ contains the zero ideal, it is non empty. Partially order $\mathcal{S}$ by inclusion, then given an chain $\mathcal{C}$ in $\mathcal{S}$, then union of elements of $\mathcal{C}$ is a submodule of V and has trivial intersection with W, and therefore an upper bound of $\mathcal{C}$. By Zorn's lemma, $\mathcal{S}$ has a maximal element, say U.

Suppose $U + W \neq V$, then for some $i \in I$, we must have $V_i \neq V_i \cap (U + W)$. Since V_i is simple, $V_i \cap (U + W) = \{0\}$. Then $(V_i + U) \cap W = \{0\}$ because any element of $V_i + U$ is of the form $v + u$, for $v \in V_i, u \in U$. This contradicts the maximality of U because $V_i + U \in \mathcal{S}$, and $V_i \not\subseteq U$ because $V_i \cap (U + W) = \{0\}$. Therefore, $U \oplus W = V$, and U is the invariant complement of W.

Conversely, suppose every submodule of V has an invariant complement. First we establish that V has at least one simple submodule. Take a non zero $v \in V$ and look at the submodule Rv. This is a finitely generated submodule, so by Krull's theorem it has a maximal proper submodule, say $W \subsetneq Rv$. Now, W has an invariant complement $W' \neq 0$ in Rv, so $Rv = W \oplus W'$. By maximality, W' is a simple submodule in Rv, hence in V. The same argument shows that every non zero submodule of V contains a simple submodule.

Let $\mathcal{S}$ be the collection of all simple submodules. Set $W_1 = \sum_{W \in \mathcal{S}} W \subseteq V$. If this is a proper submodule, then it has an invariant complement W_2. Let $0 \neq W_3 \subseteq W_2$ be a simple submodule, then $W_3 \in \mathcal{S}$ and $0 \neq W_3 = W_3 \cap W_1 \subseteq W_2 \cap W_1$ which is a contradiction. Therefore, $W_1 = V$ is a sum of simple submodules. It follows that V is completely reducible. □

Corollary. *Suppose V is completely reducible, then submodules and quotients of V are also completely reducible.*

Lemma 5. *Suppose the left regular module ${}_RR$ of a unital ring R is completely reducible, then every R-module is completely reducible.*

Proof. Since ${}_RR$ is completely reducible, so is every direct sum $\oplus_{i \in I} {}_RR = {}_RR^{(I)}$ (with indexing set $I \times J$ where J is the indexing set for ${}_RR$). Let V be an R-module and pick any $v \in V$. Then the map ${}_RR \to V$ sending $r \mapsto rv$ is an R-module homomorphism. Going through each $v \in V$, we get an R-module homomorphism ${}_RR^{(V)} \to V$. Because R has a unity, this map is surjective. So, V is a quotient of a completely reducible R module ${}_RR^{(V)}$, hence V is completely reducible. □

Remark. So the notion of ${}_RR$ being completely reducible and R being a semisimple ring are equivalent when R has a unity.

5 Maschke's theorem

Let K be a field and G a finite group. Suppose (V, ρ) is a $K[G]$-module and W a submodule. Given any representation of G, we would like to decompose it into simple representations. Maschke's theorem tells us when a representation of G is completely reducible.

The idea is that we find an invariant complement for W. If we can do that, then it follows that V is completely reducible. Given any K-subspace W, we have the map $\pi_W : V \to V$ projecting V onto W. It satisfies $\pi_W^2 = \pi_W$ and is a diagonalisable operator. Let U be a complement of W in V, so that $V = W \oplus U$. Let π_U be the corresponding projection map. Note that $\pi_W + \pi_U = I$. With the shorthand $gv = \rho(g)(v)$ for $g \in G, v \in V$, we have the following.

Lemma 6. *π_W, π_U are G-linear if and only if W, U are G-invariant.*

Proof. Because I is G-linear, it suffices to check that π_W or π_U is G-linear. Given any $v \in V$, it can be written uniquely as $v = v_W + v_U$ where $v_W \in W, v_U \in U$. For $g \in G, gv = gv_W + gv_U$. If both W, U are G-invariant, then $gv_W \in W, gv_U \in U$, and $\pi_W(gv) = gv_W = g\pi_W(v)$, so π_W and π_U are G-linear. If π_W is G-linear, then

$$gv_w = \pi_W(gv) \Rightarrow \pi_W(gv_U) = 0 \Rightarrow gv_U \in U$$

so U is G-invariant. Similarly W is G invariant. □

Suppose W is G-invariant. It is not guaranteed that π_W is G-linear. For it to be G-linear, we need $\rho(g) \circ \pi_W = \pi_W \circ \rho(g) \, \forall \, g \in G$. In other words, π_W should be a fixed point of the conjugation by elements $\rho(g) \in \mathrm{End}_R(V), g \in G$. In order to maintain that, we average the conjugates of π_W over G, i.e. we look at

$$\frac{1}{|G|} \sum_{g \in G} \rho(g) \circ \pi_W \circ \rho(g)^{-1}.$$

However, we will need $|G| \neq 0$ in K for this to make any sense.

Theorem 4. *When char$(K) \nmid |G|$, every G-representation V is completely reducible.*

Proof. Let W be a G-invariant subspace of V and π_W be the correponding projection map. Let U be the complement subspace of W in V. Consider

$$T = \frac{1}{|G|} \sum_{g \in G} \rho(g) \pi_W \rho(g)^{-1} \colon V \to V.$$

Because $\mathrm{char}(K) \nmid |G|, T$ is well-defined.

Given $v \in V, g \in G$ we have $\pi_W \rho(g^{-1}) v \in W$, so $\rho(g)\pi_W \rho(g^{-1}) v \in W \Rightarrow Tv \in W$. Furthermore, for any $w \in W$,

$$\rho(g) \circ \pi_W \circ \rho(g^{-1}) w = \rho(g)\rho(g^{-1}) w = w \Rightarrow Tw = w.$$

Next, given $v \in V, h \in G$, we have

$$\begin{aligned}
|G| Thv &= \sum_{g \in G} g \pi_W g^{-1}(hv) \\
&= \sum_{g \in G} h(h^{-1}g) \pi_W (h^{-1}g)^{-1} v \\
&= h \sum_{g \in G} g \pi_W g^{-1} v
\end{aligned}$$

Therefore, $T(hv) = h(Tv)$ and T is G-linear.

Lastly, we show that $T^2 = T$, so that T is a projection map. Keep in mind that $\pi_W \circ T = T$ because the image of T lies in W.

$$\begin{aligned}
T^2 &= \frac{1}{|G|^2} \sum_g g \pi_W g^{-1} (\sum_h h \pi_W h^{-1}) \\
&= \frac{1}{|G|^2} \sum_g g \pi_W (\sum_h (g^{-1}h) \pi_W (g^{-1}h)^{-1} g^{-1}) \\
&= \frac{1}{|G|^2} \sum_g g \circ \pi_W \circ (|G| \cdot T) \circ g^{-1} \\
&= \frac{1}{|G|} \sum_g g \circ T \circ g^{-1} \\
&= \frac{1}{|G|} \sum_g T = T
\end{aligned}$$

In the last line we used the fact that T is G-linear. So, $T^2 = T$ which gives $(I - T)^2 = (I - T)$. We have $W = T(V)$, set $U = (I - T)(V)$. Now, if $Tx = (I - T)y$ for some $x, y \in V$, then

$$Tx = T^2 x = T(I - T)y = (T - T)y = 0.$$

Furthermore, every $v \in V$ can be written as $v = Tv + (I - T)v$. Therefore, $W \cap U = \{0\}$ and $V = W \oplus U$. Lastly, for any $g \in G$, we have $g(I - T)x = (I - T)gx$, so U is G-invariant. It follows that V is completely reducible. $\square$

We can extend the theorem by taking any unital ring R in place of K and consider the group ring $R[G]$ and its modules. We need R to contain a unity, so we can talk about $|G| \in R$. Moreover $|G| \cdot 1$ must be a unit in R, so we can invert it. If we can find a substitute for π_W, then the proof above holds without any changes. To obtain π_W would mean that W is a direct summand of V. Since W is arbitrary (not entirely as it is G-invariant, but we suppose it can be arbitrary), this is equivalent to V being semisimple. Since V is arbitrary, this means that R should be semisimple.

The converse of the theorem is also true. Suppose $R[G]$ is semisimple for a ring R. There is the augmentation map $\epsilon\colon R[G] \to R$ that sends every element to the sum of coordinates, i.e. is identity on R and $\epsilon(G) = 1$. This homomorphism allows us to extend any R-module M to an $R[G]$-module. Semisimplicity of M as an $R[G]$-module is the same as that as an R-module because the action of G is trivial.

It is also true that if $R[G]$ is semisimple, then $|G| \cdot 1$ is a unit in R. For now, we prove that $|G| \cdot 1 \neq 0$ using a contradiction. Consider the left regular module ${}_{R[G]}R[G]$. This has the G-invariant submodule $R[G]_0 = \{\sum_{g\in G} a_g g | \sum a_g = 0\}$. If it has an invariant complement U, pick $v \in U$ non zero. Then $w = \sum_{g\in G} gv \in U$, but the coefficients of w are all equal.

Because $v \notin R[G]_0$, it is easy to see that $w \neq 0$ and because $|G| \cdot 1 = 0, w \in R[G]_0$. This is a contradiction and therefore, $R[G]_0$ does not have an invariant complement. This means that the ring $R[G]$ is not semisimple.

Theorem 5. *Maschke's theorem is not true for infinite groups.*

Proof. Let R be a ring with unity and G be an infinite group. Let $\epsilon\colon R[G] \to R$ be the augmentation map defined above. Observe that this map is G-invariant, i.e. $\epsilon(gx) = \epsilon(x) \,\forall\, g \in G, x \in R[G]$. So, the kernel $V = Ker(\epsilon)$ is a submodule of $R[G]$. If $R[G]$ is semisimple, then there is a submodule W such that $R[G] = V \oplus W$.

Suppose $0 \neq x = \sum_{g\in G} a_g g \in W$ where all but finitely many a_g are zero. Since W is a submodule, for any $g \in G$, we have $gx = x$ as otherwise, $x - gx \in W \cap V$ and $x - gx \neq 0$. Since gx permutes the coefficients, it follows that all a_g are equal and non zero, which is impossible as only finitely many coefficients are non zero. Therefore, V has no invariant complement and $R[G]$ is not semisimple. □

6 Schur's lemma and applications

Lemma 7. *(Schur's lemma) Suppose M, N are simple R-modules, and $\phi\colon M \to N$ is an R-module homomorphism, then either $\phi = 0$, or ϕ is an isomorphism. In particular $End_R(M)$ is a division ring.*

Proof. Since ϕ is a module homomorphism, it is clear that $Im(\phi), Ker(\phi)$ are R submodules of N, M respectively. From here, it follows that either ϕ is a bijection, or the zero map, i.e. ϕ is an isomorphism or the zero map. In particular if $\phi \in \mathrm{End}_R(M)$ is non zero, it has an inverse. It follows that $\mathrm{End}_R(M)$ is a division ring. □

Corollary. *Suppose K is algebraically closed, R a unital K-algebra. Suppose M is a simple R-module that is finite dimensional over K, and $\phi\colon M \to M$ is an R-module homomorphism, then $\phi = \lambda I$ for some $\lambda \in K$. Therefore, the division ring $End_R(M)$ is K.*

Proof. M is a finite dimensional K vector space, and ϕ is K-linear. So, we can talk about the matrix of ϕ and its eigenvalues. Since K is algebraically closed, ϕ has some eigenvalue, say $\lambda \in K$. There is a nonzero $m \in M$ such that $\phi(m) = \lambda m$ (here λ is as seen in R, i.e. the image of λ in R.) Now, $\phi - \lambda I$ is also an R-linear map (it is R-linear because K lands in the centre of R), and has non zero kernel. Therefore, by the lemma, it must be an R-isomorphism, which means that $\phi = \lambda I$. □

Corollary. *Suppose the left regular R module of a ring R with unity is completely reducible, then every simple R module is ismorphic to a submodule of ${}_RR$, i.e. left ideals of R.*

Proof. Let M be a simple R module and $m \in M, m \neq 0$. Write ${}_RR = \oplus_{i\in I} R_i$ as a direct sum of simple R-modules R_i for some indexing set I. We have the map

$$\begin{aligned}\phi_m \colon {}_RR &\to M\\ r &\mapsto rm\end{aligned}$$

Because R has a unity, ϕ_m is a non zero R-module homomorphism. For each $i \in I$, we have the composition of R-module homomorphisms $R_i \hookrightarrow {}_RR \xrightarrow{\phi_m} M$. Since $\phi_m \neq 0$, not all these maps are 0. Suppose $R_i \to M$ is non zero, then by the lemma above, this map is going to be an isomorphism. Therefore, $M \cong R_i$ is isomorphic to a submodule of R. □

Remark. Therefore, a semisimple ring is a *Kasch ring*. A left(right) Kasch ring is a ring R such that every simple left(right) R-module is isomorphic to a left(right) ideal of R (which is then necessarily minimal).

Remark. If R is a finite dimensional K-algebra, then every simple module is a K-vector space isomorphic to a subspace of R, therefore finite dimensional over K.

Lemma 8. *Suppose $\{V_i\}_{i\in I}$ is a collection of not necessarily distinct R-modules and $M = \oplus_{i\in I} V_i$ Let N be any R-module and for each $i \in I$, define $D_i = Hom_R(V_i, N)$. Then $Hom_R(M, N) \cong \prod_{i\in I} D_i$ as $Z(R)$-modules.*

Proof. Take any $\phi \in \mathrm{Hom}_R(M, N)$. Then for each $i \in I$, we have the R-module homomorphism

$$T_i(\phi)\colon V_i \hookrightarrow M \xrightarrow{\phi} N \in \mathrm{Hom}_R(V_i, N).$$

This association is a decomposition of ϕ and gives a map

$$\begin{aligned}T\colon \mathrm{Hom}_R(M, N) &\to \prod D_i\\ \phi &\mapsto (T_i(\phi))_{i\in I}\end{aligned}$$

Observe that for any fixed $i \in I$, we have $T_i(\phi_1 + \phi_2) = T_i(\phi_1) + T_i(\phi_2)$ for every $\phi_1, \phi_2 \in \mathrm{Hom}_R(M, N)$. Furthermore, given $r \in Z(R), T_i(r\phi) = rT_i(\phi)$, therefore T is a $Z(R)$-linear map.

The inverse of T is given as follows. Start with $(T_i) \in \prod D_i$. Now, every element of M is a unique finite sum of elements from V_i. Suppose $v = v_{i_1} + \cdots + v_{i_k} \in M$ for $i_1, \ldots, i_k \in I$, then define

$$\phi(v) = T_{i_1}(v_{i_1}) + \cdots + T_{i_k}(v_{i_k}).$$

ϕ is well-defined and an R-module homomorphism. Thus, we have a map

$$\begin{aligned}T'\colon \prod D_i &\to \mathrm{Hom}_R(M, N)\\ (T_i) &\mapsto \phi\end{aligned}$$

It is clear that T' is also $Z(R)$-linear. Lastly, it is easy to see that T, T' are inverses of each other. Therefore, $\mathrm{Hom}_R(M, N) \cong \prod_{i\in I} D_i$ as $Z(R)$-modules. □

Next, suppose V is a simple R-module and I is some indexing set. We know that $\mathrm{End}_R(V)$ is a division ring and a $Z(R)$-algebra.

Lemma 9. *$Hom_R(V, V^{(I)}) \cong End_R(V)^{(I)}$ as $Z(R)$-modules.*

Proof. For convenience, write the ith copy of V in $V^{(I)}$ as $V_{(i)}$, so that $V^{(I)} = \oplus_{i\in I} V_{(i)}$. Given $\phi \in \mathrm{Hom}_R(V, V^{(I)})$, we have for each $i \in I$, the map $T_i\colon V \xrightarrow{\phi} V^{(I)} \to V_{(i)} \in \mathrm{End}_R(V)$. Since V is simple, T_i is either 0 or an isomorphism. Take any non zero $v \in V$, then $\phi(v) = v_{i_1} + \cdots + v_{i_k}$ for some $i_1, \ldots, i_k \in I$. This means that $T_i = 0$ for $i \neq i_1, \ldots, i_k$ as $v \in Ker(T_i)$. Therefore, only finitely many T_i are non zero. Thus, we have the map

$$\begin{aligned}T\colon \mathrm{Hom}_R(V, V^{(I)}) &\to \mathrm{End}_R(V)^{(I)}\\ \phi &\mapsto (T_i)_{i\in I}\end{aligned}$$

As before, T is a $Z(R)$-module homomorphism. We construct the inverse as follows. Given $(T_i) \in \mathrm{End}_R(V)^{(I)}$, take $T'((T_i))(v) = \sum_{i\in I} T_i(v)$. Since $T_i(v) \in V_{(i)}$ and all but finitely many of them are zero, $T'((T_i))$ is indeed a homomorphism $V \to V^{(I)}$.

It is clear that T' is $Z(R)$-linear and T, T' are inverses of each other. Therefore, as $Z(R)$-modules, $\mathrm{Hom}_R(V, V^{(I)}) \cong \mathrm{End}_R(V)^{(I)}$ is a direct sum of division rings. □

Suppose $\{V_i\}_{i\in I}$ is a collection of non-isomorphic simple R-modules and $M = \oplus_{i\in I} V_i^{(m_i)}, N = \oplus_{i\in I} V_i^{(n_i)}$ where m_i, n_i are some possibly empty indexing set. Set $D_i = \mathrm{End}_R(V_i), i \in I$.

Given $\phi \in \mathrm{Hom}_R(V_i, N)$, the only non zero projections are those that land in V_i. So, ϕ corresponds to a map $V_i \to V_i^{(n_i)}$. The inverse map is obvious. Therefore,

$$\mathrm{Hom}_R(V_i, N) = \mathrm{Hom}_R(V_i, V_i^{(n_i)}) = D_i^{(n_i)}.$$

Combining the results above, we have (as $Z(R)$-modules)

$$\mathrm{Hom}_R(M, N) = \prod_{i\in I} \mathrm{Hom}_R(V_i^{(m_i)}, N) = \prod_{i\in I} \mathrm{Hom}_R(V_i, N)^{m_i} = \prod_{i\in I} (D_i^{(n_i)})^{m_i}$$

When $M = N$, we have a similar result. First observe that as $Z(R)$-algebras, $\mathrm{Hom}_R(V_i^{(m_i)}, M) = \mathrm{End}_R(V_i^{(m_i)})$. Because restriction to $V_i^{(m_i)}$ is a ring homomorphism as well, we have

$$\mathrm{End}_R(M) = \prod_{i\in I} \mathrm{End}_R(V_i^{(m_i)}).$$

When the n_i, m_i are finite indexing sets, then $(D_i^{(n_i)})^{m_i} = D_i^{m_i n_i}$ is the space of $n_i \times m_i$ matrices over D_i and $\mathrm{Hom}_R(M, N)$ is a product of matrix rings. And as $Z(R)$-algebras, $\mathrm{End}_R(M) = \prod_{i\in I} D_i^{m_i^2}$.

Theorem 6. *Let R be a ring, V a simple module and $D = End_R(V)$. Then $V^n \cong V^m$ as R-modules if and only if $m = n$, where m, n are positive integers.*

Proof. Without loss of generality, suppose $n \geq m$ and suppose $\phi\colon V^n \to V^m$ is an R-module homomorphism. Write $V^n = V_{(1)} \oplus \cdots \oplus V_{(n)}, V^m = V'_{(1)} \oplus \cdots \oplus V'_{(m)}$ where all the $V_{(i)}, V'_{(j)}$ are V. Then ϕ induces

$$f_{ij} \colon V_{(j)} \hookrightarrow V^n \xrightarrow{\phi} V^m \to V'_{(i)} \in D.$$

Then, ϕ can be thought of as being described by the matrix $M = (f_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ and $m \times n$ matrix. Similarly, if $v = (v_1, \dots, v_n) \in V$, then we have

$$\phi(v) = \begin{bmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{m1} & f_{m2} & \dots & f_{mn} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

Now, V^n, V^m are left D-modules, and $\phi = M\colon V^n \to V^m$ is R-linear. There is no reason for ϕ to be D-linear. However, we can still apply Gaussian elimination to M. These are the row operations in linear algebra over fields. We are going to modify the rows in a reversible way. Reducing M to echelon form is the same as writing $\phi = T_k \circ \cdots \circ T_1 \circ \psi$ where $\psi\colon V^n \to V^m$ is in echelon form and $T_1, \dots, T_k$ are automorphisms of V^m corresponding to the reverse row operations.

In the echelon form, if $n > m$, then it is easy to demonstrate a non empty kernel. Therefore, for an isomorphism between V^n, V^m we must have $m = n$. The converse is obvious. □

The proof above shows that for finite n, $\mathrm{End}_R(V^n) = M_n(\mathrm{End}_R(V))$ as $Z(R)$-algebras. So, when $M = \oplus_{i\in I} V_i^{(m_i)}$ as above, and the m_i are finite indexing sets, we have $\mathrm{End}_R(M) = \prod_{i\in I} M_{m_i}(D_i)$ as $Z(R)$-algebras, in particular as rings.

Corollary. *If M is a semisimple R-module with a finite direct sum decomposition, then the decomposition is unique.*

Proof. Suppose M can be written as $V_1^{n_1}\oplus\cdots\oplus V_k^{n_k}\cong W_1^{m_1}\oplus\cdots\oplus W_t^{m_t}$ where the n_i, m_j are positive integers. The isomorphism between them gives a non zero map from each V_i to $W_1^{m_1}\oplus\cdots\oplus W_k^{m_k}$, therefore, each V_i must appear as a summand in the second decomposition. Similarly, each W_i must be a summand in the first decomposition. Therefore, we have $M = V_1^{n_1}\oplus\cdots\oplus V_k^{n_k}\cong V_1^{m_1}\oplus\cdots\oplus V_k^{m_k}$. Now we need to show that the multiplicities are the same.

The isomorphism between the two decompositions gives an isomorphism between $V_i^{n_i}, V_i^{m_i}$ therefore, $n_i = m_i$. Thus, the multiplicities are same and the decomposition is unique. □

Remark. This shows that there is at most one way to write M as a finite direct sum of simple modules, there may, however, be a way to write it as an infinite sum as well as a finite sum.

Corollary. *Let R be any semisimple ring, $V_i, i\in I$ be a collection of distinct simple modules and suppose $M=\oplus_{i\in I}V_i$. Then submodules of M are of the form $\oplus_{j\in J}V_j$ in the canonical way for some $J\subseteq I$.*

Proof. Let N be a submodule of M, then it decomposes (because R is semisimple) into a sum of simple R-modules. However, because $N\subseteq M$, these simple submodules must come from V_i.

Suppose $N\cong V_i$ for some i, then the claim is that N is the ith summand, in other words, as a set there is only one way to include V_i in M. This is because if we take any $\phi\in \mathrm{Hom}_R(V_i, M)$, then the coordinates are all zero except for the ith one. Therefore, ϕ must be an automorphism of V_i followed by the canonical embedding of V_i in M by padding with zeros. Therefore, as a set there is only one way to obtain V_i from M, hence every submodule of M must be of the form stated. □

A note on multiplicities. Suppose R is a K-algebra, where K is an algebraically closed field and $M = V_1^{n_1}\oplus\cdots\oplus V_k^{n_k}$ is an R-module with finite direct sum decomposition. Then, $\mathrm{Hom}_R(V_i, M) = \mathrm{End}_R(V)^{m_i}$ as $Z(R)$-algebras, in particular as K-vector spaces. Since R is a K-algebra, $\mathrm{End}_R(V) = K$, therefore, $m_i = \dim_K \mathrm{Hom}_R(V_i, M)$. More generally if $M=\oplus V_i^{m_i}, N=\oplus V_i^{n_i}$, then

$$\mathrm{Hom}_R(M,N) = \oplus K^{m_i n_i} \text{ and } \dim_K \mathrm{Hom}_R(M,N) = \sum m_i n_i.$$

One way to force M to have a finite direct sum decomposition is to assume that M is finitely generated as an R-module as we see in the next section.

7 Artin-Wedderburn Theory

Let R be a ring, M a finitely generated left R-module. We know that M contains maximal submodules.

Definition. *The Jacobson radical $J(M)$ of M is defined to be the intersection of all maximal submodules of M.*

Theorem 7. *M is semisimple if and only if M is Artinian and $J(M) = 0$.*

Proof. Suppose M is semisimple and $M=\oplus_{\lambda\in\Lambda}M_\lambda$ for some simple modules M_λ, indexing set Λ. Suppose M is generated by some $e_1,\dots,e_n$. Each e_i uses finitely many $\lambda\in\Lambda$, say

$$e_i = m_{i1}+\cdots+m_{in_i}, m_{ik}\in M_{\lambda_{ik}}, \lambda_{ik}\in\Lambda.$$

Together, we have $e_1,\dots,e_n\in\oplus_{\text{finite}}M_\lambda$. By unique representation of elements of M as sums of terms from the M_i, it follows that $M=\oplus_{\text{finite}}M_\lambda$, say $M = M_1\oplus\cdots\oplus M_n$. Then each M_i is Artinian as it is simple, therefore M is Artinian. Set $N_i = M_1\oplus\cdots\oplus\widehat{M_i}\oplus\cdots\oplus M_n$.

Suppose N is a submodule such that $N_i\subseteq N\subseteq M$. Now, the submodule $M_i\cap N$ is either 0 or M_i. In the first case, every term of N has ith coordinate 0, and therefore, $N = N_i$. In the second case, there is some element of N with ith coordinate non zero. Since $N_i\subseteq N$, it follows that $M_i \subseteq N$, and therefore, $N = M$. Thus, N_i is a maximal submodule of M. Consequently, $J(M) \subseteq \cap_{i=1}^n N_i = 0$.

Conversely, suppose M is Artinian and has trivial Jacobson radical. First we show that M contains simple submodules. Set $M_1 = M$. If M_n is not simple, then there is a non zero submodule $M_{n+1} \subsetneq M_n$. This way we obtain a strictly decreasing chain of submodules $M_1 \supsetneq M_2 \supsetneq \dots$ which contradicts DCC. Therefore, if the chain should stabilise, it has to be finite and hence some M_n is a simple submodule. The same proof shows that every submodule of M contains a simple submodule.

Next, we show that every simple submodule is a direct summand of M, i.e. if M_1 is a simple submodule, then there is a submodule M_2 such that $M = M_1 \oplus M_2$.

Let M_1 be a non zero simple submodule, $0 \neq x \in M_1$. Since $J(M) = 0$, there is a maximal submodule M_2 (may be 0) such that $x \notin M_2$. Since M_1 is simple and $x \notin M_2$, it follows that $M_1 \cap M_2 = 0$. Next, by maximality of M_2 we must have $M_1 + M_2 = M$. Therefore, M_2 is a complement of M_1 in M.

Finally, we show that M is a direct sum of simple submodules. Take a simple module M_1, and obtain an N_1 such that $M_1 \oplus N_1 = M$. If N_1 is not simple, obtain a simple submodule M_2. Now, M_2 has an invariant complement M_2' in M which means that $N_1 = M_2 \oplus M_2' \cap N$. Therefore, M_2 has an invariant complement N_2 in N_1. Continuing this way, obtain a descending chain $N_1 \supset\neq N_2 \supsetneq \dots$. By DCC, this chain must terminate, which means that some N_k is simple. Therefore, $M = M_1 \oplus \cdots \oplus M_k \oplus N_k$ is semisimple. $\square$

Definition. *A finitely generated R-module M is called J-semisimple (or semiprimitive) if $J(M) = 0$.*

We know apply the results above to the left regular module of a ring R. The simple submodules are going to be minimal left ideals. Given a left ideal I in a ring R, the square I^2 is the ideal $\{\sum_{\text{finite}} a_i b_i | a_i, b_i \in I\} \subseteq I$.

Theorem 8. *(Brauer's lemma) Suppose R is a ring and I is a minimal left ideal, then either $I^2 = 0$ or $I = \langle e \rangle$ for some idempotent e. In other words, minimal left ideals are generated by idempotents. In the second case, eRe is a division ring.*

Proof. We know that $I^2 \subseteq I$, so either $I^2 = 0$ or $I^2 = I$. Suppose $I^2 = I$, then there is some $x \in I$ such that $Ix \neq 0$, i.e. the (left) annihilator $\mathrm{Ann}(x) \cap I = 0$. By minimality, $Ix = I$, and there is some $e \in I$, such that $ex = x$. We then have

$$e^2 x = ex \Rightarrow (e^2 - e)x = 0.$$

Because $\mathrm{Ann}(x) \cap I = 0$, we must have $e^2 = e$. Lastly, we know that $e \neq 0$, and $\langle e \rangle \subseteq I$. By minimality, $I = \langle e \rangle$. Observe that $Ie = I$, so $\mathrm{Ann}(e) \cap I = 0$.

Now, suppose $I = \langle e \rangle$ is a minimal left ideal, with $e^2 = e$. We look at the division ring $\mathrm{End}_R(I)$. If $\phi \in \mathrm{End}_R(I)$, then $\phi(e) = ae$ for some $a \in R$. Moreover, $\phi(xe) = x\phi(e) = xae \,\forall\, x \in R$. In particular, we have $eae = ae$. Conversely, suppose $a \in R$ is such that $eae = ae$. Consider the map

$$\begin{aligned} \phi_a \colon I &\to I \\ xe &\mapsto xae \end{aligned}$$

To show that ϕ_a is well defined, observe that if $re = se$, then $(r - s)e = 0$. Now,

$$rae - sae = (r - s)ae = (r - s)eae = 0,$$

therefore, $\phi_a(re) = \phi_a(se)$. It is clear that ϕ_a is an R-module isomorphism when $ae \neq 0$. If a itself is of the form ebe for some $b \in R$, then by the idempotence of e, it is clear that $ae = eae$. In eRe, the element $e = e^2$ functions as 1. This suggests that $\mathrm{End}_R(I) \cong eRe$ as rings. However, the map above is not directly a ring homomorphism, we need to take the opposite ring. Write $\cdot$ for the multiplication in $\mathrm{End}_R(I)^{op}$.

Thus we have maps

$$\begin{aligned} \Phi \colon \mathrm{End}_R(I)^{op} &\to eRe \\ \phi &\mapsto \phi(e) \end{aligned} \qquad\qquad \begin{aligned} \Psi \colon eRe &\to \mathrm{End}_R(I)^{op} \\ eae &\mapsto \{xe \mapsto xeae\} = \phi_{eae} \end{aligned}$$

These maps are clearly additive and send identity to identity. We need to check that they are multiplicative. Given $\phi_1, \phi_2 \in \mathrm{End}_R(I)$, say $\phi_1(e) = ae = eae, \phi_2(e) = be = ebe$, then

$$\Phi(\phi_1 \cdot \phi_2) = \Phi(\phi_2 \circ \phi_1) = \phi_2(\phi_1(e)) = abe = (eae)(ebe).$$

Next, given $eae, ebe \in eRe$, we have $(eae)(ebe) = eabe$, so

$$\Psi(eabe)(e) = abe = \Psi(ebe)(\Psi(eae)(e)) = (\Psi(eae) \cdot \Psi(ebe))(e).$$

In fact, it is easy to see that Φ, Ψ are $Z(R)$-linear as well. It is clear that Φ, Ψ are inverses of each other. Therefore, $\mathrm{End}_R(I)^{op} \cong eRe$ as $Z(R)$-algebras, in particular as rings. The opposite ring $\mathrm{End}_R(I)^{op}$ is still a division ring, therefore eRe is a division ring.

Alternatively, we can prove the same directly as follows. Take $0 \neq a = ebe \in eRe$ (note that every element is of this form). Because $ea = a \in I$ is non zero, $Ra = I$, so $\exists\, x \in R$ such that $xa = e$. Then,

$$e = xa = xebe = (xe)(ebe).$$

Multiplying by e gives $e = (exe)(ebe)$, therefore a has a left inverse in eRe. Now exe has a left inverse in eRe and it is easy to see that its left inverse must be a, therefore exe is the right inverse of a. Therefore, eRe is a division ring. $\square$

Lemma 10. *Suppose I_1, I_2 are (minimal) left ideals generated by idemopotents, say $I_1 = \langle e_1 \rangle, I_2 = \langle e_2 \rangle$, then $Hom_R(I_1, I_2) \cong e_1Re_2$ as $Z(R)$-modules.*

Proof. Take $\phi \in \mathrm{Hom}_R(I_1, I_2)$, then $\phi(e_1) = ae_2$ for some $a \in R$. For any $x \in R$, we have $\phi(xe_1) = x\phi(e_1) = xae_2$. In particular $e_1ae_2 = ae_2$. Conversely, if $a \in R$ is such that $e_1ae_2 = ae_2$, then define

$$\begin{aligned} \phi_a \colon I_1 &\to I_2 \\ xe_1 &\mapsto xae_2 \end{aligned}$$

As before we see that ϕ_a is well-defined for $xe_1 = 0 \Rightarrow xae_2 = xe_1ae_2 = 0$. Clearly, $\phi_a \in \mathrm{Hom}_R(I_1, I_2)$. Now, define

$$\begin{aligned} \Phi \colon \mathrm{Hom}_R(I_1, I_2) &\to e_1Re_2 \\ \phi &\mapsto \phi(e_1) \end{aligned} \qquad \begin{aligned} \Psi \colon e_1Re_2 &\to \mathrm{Hom}_R(I_1, I_2) \\ e_1ae_2 &\mapsto \{xe_1 \mapsto xe_1ae_2\} = \phi_{e_1ae_2} \end{aligned}$$

Again Φ, Ψ are $Z(R)$-linear and inverses of each other. Therefore, $\mathrm{Hom}_R(I_1, I_2) \cong e_1Re_2$ as $Z(R)$-modules. Observe that we did not need I_1, I_2 to be minimal. $\square$

Now assume R is a semisimple ring with unity. Then ${}_RR$ is finitely generated and can be decomposed as $R = V_1 \oplus \cdots \oplus V_k$ where the V_i are simple submodules. Write $1 = \epsilon_1 + \cdots + \epsilon_k$ where $\epsilon_i \in V_i$. Multiplying by ϵ_i on the left, it is easy to see that $\epsilon_i^2 = \epsilon_i$ and $\epsilon_i\epsilon_j = 0$. Therefore, the V_i are minimal left ideals generated by idempotents. Of course, each ϵ_i is non zero because every $x \in R$ can be written as $x = x\epsilon_1 + \cdots + x\epsilon_k$.

Lemma 11. *Upto isomorphism R (as above) has finitely many minimal left ideals that are generated by idempotents.*

Proof. Suppose $I = \langle e \rangle$ is a minimal ideal generated by idempotent e, then $e = e\epsilon_1 + \cdots + e\epsilon_k$. Now, at least one $e\epsilon_i \neq 0$, which means that $eR\epsilon_i \neq 0$. Therefore, by Schur's lemma, $I \cong V_i$. $\square$

7.1 Opposite rings and Wedderburn decomposition

Let R be a ring. The opposite ring R^{op} is a ring with underlying additive group same as R, and multiplication $r \cdot s = sr$ for $r, s \in R^{op}$. It is easy to see that R^{op} defined this way is an associative ring. Observe that when A, B are rings, then $(A \oplus B)^{op} = A^{op} \oplus B^{op}$. In terms of category theory, this is a covariant functor on the category of rings. We make a few observations.

- For any ring R, we have $(R^{op})^{op} \cong R$ (technically, they are not the same objects).
- For two rings $R, S, R \cong S$ if and only if $R^{op} \cong S^{op}$.
- $Z(R^{op}) \cong Z(R)$, so R^{op} is a $Z(R)$-algebra with the usual multiplication.
- A subset I of R is a left ideal of R if and only if it is a right ideal of R^{op}.
- If R is a division ring, then so is R^{op}.

Lemma 12. *Let R be a ring with unity, then $R^{op} \cong End_R({}_RR)$ as $Z(R)$-algebras.*

Proof. First consider for $r \in R$, the right multiplication map

$$\begin{aligned} m_r \colon {}_RR &\to {}_RR \\ x &\mapsto xr \end{aligned}$$

Clearly, $m_r \in \mathrm{End}_R({}_RR)$. Conversely, given any $\phi \in \mathrm{End}_R({}_RR)$, we see that $\phi = m_{\phi(1)}$. Therefore, we have maps

$$\begin{aligned} \Phi \colon R^{op} &\to \mathrm{End}_R({}_RR) \\ r &\mapsto m_r \end{aligned} \qquad\qquad \begin{aligned} \Psi \colon \mathrm{End}_R({}_RR) &\to R^{op} \\ \phi &\mapsto \phi(1) \end{aligned}$$

It is easy to see that both Φ, Ψ are $Z(R)$-algebra homomorphisms and inverses of each other. □

Now, take R to be a semisimple ring with unity. Then we have the decomposition ${}_RR = V_1^{n_1} \oplus \cdots \oplus V_k^{n_k}$ of ${}_RR$ into simple submodules where V_i, V_j are non isomorphic for $i \neq j$. Set $D_i = \mathrm{End}_R(V_i)$. Then as $Z(R)$-algebras,

$$R^{op} \cong \mathrm{End}_R({}_RR) = \prod_{i=1}^{k} M_{n_i}(D_i) = \oplus_{i=1}^{k} M_{n_i}(D_i).$$

Lemma 13. *For a division ring $D, n > 0, M_n(D)^{op} \cong M_n(D^{op})$.*

Proof. Look at the transpose map $A \mapsto A^T, A \in M_n(D)^{op}$. It is easy to see that this is a bijective linear map. We need to check that it is multiplicative. Let $A = (a_{ij}), B = (b_{ij})$. Then on the left side,

$$(A \cdot B)_{ij} = (BA)_{ij} = \sum_{k=1}^{n} b_{ik} a_{kj}$$

and on the right side,

$$(A^T B^T)_{ij} = \sum_{k=1}^{n} a_{ki} \cdot b_{jk} = \sum_{k=1}^{n} b_{jk} a_{ki}.$$

It follows that $(A \cdot B)^T = A^T B^T$. Therefore, $M_n(D)^{op} \cong M_n(D^{op})$ as rings. □

When D is a $Z(R)$-algebra as above, then so is $M_n(D)$, and the isomorphism above is a $Z(R)$-algebra isomorphism. In fact, the elements of $Z(R)$ are the diagonal matrices. Therefore, as $Z(R)$-algebras, in particular as rings $R \cong \oplus_{i=1}^{k} M_{n_i}(D_i^{op})$. Thus, a semisimple ring with unity is isomorphic to a product of matrix algebras over division rings.

7.2 Uniqueness

Theorem 9. *Let D be a division ring, $n > 0$, then $R = M_n(D)$ is a semisimple ring with decomposition ${}_RR = \oplus_{i=1}^n D^n$.*

Proof. **Step 1:**

Each element of R is a transformation $D^n \to D^n$. Therefore, D^n is an R-module. Furthermore, given any $0 \neq x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in D^n$, there is a transformation $M \in M_n(D)$ such that $Mx = y$. For example, suppose $x_1 \neq 0$, then

$$\begin{bmatrix} y_1x_1^{-1} & 0 & \dots & 0 \\ y_2x_1^{-1} & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ y_nx_1^{-1} & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

Therefore, D^n is a simple R-module.

Step 2:

Given a matrix $M \in M_n(D)$, write the columns of M as $C_1, \dots, C_n$, so that $M = \begin{bmatrix} C_1 & \dots & C_n \end{bmatrix}$. Consider the map

$$\begin{aligned} \phi \colon M_n(D) &\to \oplus_{i=1}^n D^n \\ M &\mapsto (C_1, \dots, C_n) \end{aligned}$$

Obviously, ϕ is a bijective additive map. It is also easy to see that ϕ is an R-linear map because the multiplication on the left by a matrix is essentially column-wise. Therefore, as R-modules, $M_n(D) \cong \oplus_{i=1}^n D^n$. Therefore, $R = M_n(D)$ is a semisimple ring with unity. Moreover, this decomposition into simple modules is unique.

Step 3:

The claim is that $\operatorname{End}_R(D^n) = D^{op}$. Suppose $\phi \in \operatorname{End}_R(D^n)$, then given any $(v_1, \dots, v_n) \in D^n$, observe that

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} v_1 & & & \\ & v_2 & & \\ & & \ddots & \\ & & & v_n \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}.$$

So, ϕ depends only on the value at $(1, \dots, 1)$ by R-linearity. Write e_i to be the vector with 1 in the ith coordinate. Now in $M_n(D)$, let E_{ij} be the matrix with 1 in the (i,j)th position and zeros elsewhere. Then, we see that $E_{11}e_1 = e_1$, therefore, $\phi(e_1) = E_{11}\phi(e_1)$ which means that $\phi(e_1) = (r, 0, \dots, 0)$ for some $r \in D$. Using permutation matrices and R-linearity, it follows that $\phi(e_i) = re_i$. Then, $\phi(v_1, \dots, v_n) = (v_1r, \dots, v_nr)$ is multiplication by r from the right.

Conversely, if $r \in D$, then we construct the map $m_r \colon v \mapsto vr, v \in D^n$. This map is $M_n(D)$-linear for the multiplication is from the right. Consider

$$\begin{aligned} \Phi \colon \operatorname{End}_R(D^n) &\to D^{op} \\ \phi &\mapsto r \end{aligned} \qquad\qquad \begin{aligned} \Psi \colon D^{op} &\to \operatorname{End}_R(D^n) \\ r &\mapsto \{v \mapsto vr\} = m_r \end{aligned}$$

It is clear that Φ, Ψ are additive. Now, for $\phi_1, \phi_2 \in \operatorname{End}_R(D^n)$, say $\phi_1(e_1) = (r, 0, \dots, 0), \phi_2(e_1) = (s, 0, \dots, 0)$, then $\phi_1 \circ \phi_2(e_1) = (sr, 0, \dots, 0)$. Therefore, $\Phi(\phi_1 \circ \phi_2) = sr = \Phi(\phi_1) \cdot \Phi(\phi_2)$. Conversely, given $r, s \in D$, it is clear that $\Psi(r \cdot s) = \Psi(r) \circ \Psi(s)$. Therefore, Φ, Ψ are ring homomorphisms and are inverses of each other. We next show that $Z(M_n(D)) = Z(D)$ (as scalar matrices), but assuming that for now, it is clear that Φ, Ψ are in fact $Z(R)$-linear. Therefore, $\operatorname{End}_R(D^n) \cong D^{op}$ as $Z(R) = Z(D)$-algebras, in particular as rings. $\square$

So, $M_n(D)$ is decomposed into $\oplus_{i=1}^n D^n$ where D^n is a simple module. From this decomposition, we obtain a decomposition of $R = M_n(D)$ as a product of matrix algebras over division rings. Because $\operatorname{End}_R(D^n) = D^{op}$ and D^n has multiplicity n, we get back $R = M_n(D)$.

Lemma 14. *For any unital ring $R, Z(M_n(R)) = Z(R)$.*

Proof. Let E_ij be the matrix with 1 in the (i,j)th entry and zeros elsewhere. Let $M = (m_{ij}) \in Z(M_n(R))$, then

$$E_{ii}M = \begin{bmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ m_{i1} & m_{i2} & \dots & m_{in} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} ME_{ii} = \begin{bmatrix} 0 & \dots & m_{1i} & \dots & 0 \\ 0 & \dots & m_{2i} & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & m_{ni} & \dots & 0 \end{bmatrix}$$

Therefore, off-diagonal elements of M are zero. Next, we have for $1 \leq k \leq n$,

$$E_{1k}M = m_{kk}E_{1k}, ME_{1k} = m_{11}E_{1k}.$$

Therefore, M is a scalar matrix. Using other scalar matrices, it is easy to see that the diagonal entries of M must come from $Z(R)$. Therefore, $M = rI$ where I is the identity matrix, $r \in Z(R)$. Conversely, it is obvious that $rI \in Z(M_n(R))$ for $r \in Z(R)$. It is easy to see that $M \mapsto m_{11}$ is a ring isomorphism $Z(M_n(R)) \cong Z(R)$. □

Theorem 10. *The Artin-Wedderburn decomposition is unique, i.e. if R is a ring with untiy decomposed as $R = \prod_{i=1}^n M_{n_i}(D_i)$ (at the level of rings) where D_i are division rings, then the D_i, n_i are uniquely determined by R (upto permutation).*

Proof. First, because $M_n(D)$ is a semisimple ring for any division ring D, R is a semisimple ring. Therefore, there is a unique decomposition of ${}_RR$ into simple left modules.

For each $i, D_i^{n_i}$ is a simple $M_{n_i}(D_i)$-module. Using the projection $\pi_i \colon R \to M_{n_i}(D_i)$, $D_i^{n_i}$ a simple R module. Just as before, we get the decomposition ${}_RR = \oplus_{i=1}^n \oplus_{j=1}^{n_i} D_i^{n_i}$. Furthermore, because the R-module structure on $D_i^{n_i}$ is throught $M_n(D_i)$, we have $\mathrm{End}_R(D_i^{n_i}) = D_i^{op}$. Therefore, the matrix algebra decomposition of R through the decomposition of ${}_RR$ is the same as $\oplus_{i=1}^n M_{n_i}(D_i)$. □

Essentially, we showed that every matrix decomposition of R comes from a decomposition of ${}_RR$ which is unique. Therefore, the decomposition of a semisimple ring R with unity into a product of matrix rings is unique. The division rings are endomorphism rings of simple R modules and the n_is are the multiplicities.

7.3 Burnside's theorem

Let K-be an algebraically closed field, R a semisimple K-algebra and (M, ρ) an R-module that is a finite dimensional K-vector space. Previously we observed that $\rho(R) \subseteq \mathrm{End}_K(M)$.

Theorem 11. *(Burnside's theorem) M is a simple R-module if and only if $\rho(R) = End_K(M)$.*

Proof. If ρ is surjective, given $m \in M$ nonzero, extend $\{m\}$ to a K-basis of M. Given any $n \in M$, look at $T \in \mathrm{End}_K(M)$ that sends $m \mapsto n$, and the other basis elements to 0. Then $\exists\, r \in R$ such that $\rho(r) = T$, which means that $rm = T(m) = n$. Therefore, the R-submodule generated by m is M. Since $m \in M$ was an arbitrary nonzero element, M has no non trivial submodule. This direction does not require the finite dimensionality of M as a K-vector space.

Conversely, suppose M is simple. We know that $\rho(R) \subseteq \mathrm{End}_K(M)$ is an R-module. Since R is semisimple, $\rho(R)$ decomposes into simple R-modules. Suppose N is a simple R-module that appears in the decomposition, then we have the inclusion $N \hookrightarrow \rho(R)$.

Given $m \in M$, let $e_m \colon \mathrm{End}_K(M) \to M$ be the evaluation map. Then we have $N \hookrightarrow \rho(R) \xrightarrow{e_m} M$. This composition is easily seen to be R-linear and by Schur's lemma, we must have $N \cong M$. Therefore, $\rho(R) = M^{(I)}$ for some indexing set I. However $\rho(R)$ is a K-vector subspace of $\mathrm{End}_K(M)$ which is finite dimensional, so I is finite, say $|I| = d$. Take $n = \dim_K M$. Then, $\dim_K \rho(R) = nd$

Next, because K is algebraically closed, $\text{End}_R(M) = K$, therefore, $\text{End}_R(\rho(R)) = K^{d^2}$, so $\dim_K \text{End}_R(\rho(R)) = d^2$. However, $\rho(R)$ is itself a ring, and $\phi\colon \rho(R) \to \rho(R)$ is R-linear if and only if it is $\rho(R)$-linear because the actions are the same. Therefore, as $Z(\rho(R))$-algebras, in particular as K-vector spaces (for K is contained in $\rho(R)$ as scalar matrices), $\rho(R)^{op} \cong \text{End}_{\rho(R)}(\rho(R)) = \text{End}_R(\rho(R))$. Comparing dimensions gives us $d = n$, therefore $\rho(R) = \text{End}_K(M)$. □

8 Idempotents and von Neumann regular rings

Henceforth all rings contain unity.

When R is a semisimple, ${}_RR$ is a sum of minimal left ideals, say ${}_RR = V_1 \oplus \cdots \oplus V_k$. Writing $1 = \epsilon_1 + \cdots + \epsilon_k$, with $\epsilon_i \in V_i$, we have seen that $\epsilon_i^2 = \epsilon_i, \epsilon_i\epsilon_j = 0$ for $i \neq j$. So, the minimal left ideals V_i are generated by idempotents. Of course, to show the idempotence of ϵ_i, we did not need the minimalty.

More generally, suppose ${}_RR$ is a direct sum of left ideals. As before, because ${}_RR$ is finitely generated, we must have a finite number of summands, so ${}_RR = V_1 \oplus \cdots \oplus V_k$ where V_i are just left ideals, not necessarily minimal. Then writing $1 = \epsilon_1 + \cdots + \epsilon_k$ as above, we get the same relations. Any $x \in R$ can be written as $x = x\epsilon_1 + \cdots + x\epsilon_k$, so each V_i is generated by ϵ_i.

Lemma 15. *Any left ideal I of R is a direct summand of ${}_RR$ if and only if I is generated by an idempotent.*

Proof. If ${}_RR = I \oplus J$, then we have seen that I is generated by an idempotent. Conversely, suppose $I = \langle e \rangle$ is generated by an idempotent, then $1 - e$ is also an idempotent. Take $J = \langle 1 - e \rangle$, we have $I \cap J = 0$ for if $xe = y(1 - e)$, then

$$xe = xe^2 = y(1 - e)e = 0.$$

It is clear that ${}_RR = I \oplus J$. □

Corollary. *Suppose R is semisimple, then every left ideal is generated by an idempotent.*

Proof. Suppose I is an ideal of R, then it is a submodule of ${}_RR$, hence a direct summand. By the lemma, I is generated by an idempotent. □

We now look at the Jacobson radical $J(R)$ of R. This was defined to be the intersection of all maximal left ideals. We can similarly define a right-Jacobson radical, however we see below that the two notions are the same.

Definition. *For an R-module M, the annihilator is the set $Ann(M) = \{r \in R | rM = 0\}$.*

Observe that for any module $M, \text{Ann}(M)$ is a two-sided ideal of R.

Theorem 12. *The following are equivalent.*

1. *$x \in J(R)$.*
2. *$1 - yx$ has a left inverse for every $y \in R$.*
3. *$xM = 0$ for any simple R-module M.*

Proof. Suppose $x \in J(R)$, and $y \in R$. If $(1 - yx)$ has no left inverse (i.e. an $a \in R$ such that $a(1 - yx) = 1$), then the left ideal $\langle 1 - yx \rangle$ is a proper ideal contained in some maximal left ideal I. Because $x \in J(R) \subseteq I, yx \in I$. Therefore, $1 = 1 - yx + yx \in I$ which is impossible.

Next, suppose $1 - yx$ has a left inverse for every $y \in R$. Given a simple module M, suppose $xM \neq 0$, then there is an $m \in M$ such that $xm \neq 0$. This means that $R(xm) = M$ by simplicity, so there is a $y \in R$ such that $yxm = m \Rightarrow (1 - yx)m = 0$. However, $1 - yx$ has a left inverse, which means that $m = 0$, a contradiction. Therefore $xM = 0$.

Lastly, suppose $xM = 0$ for every simple module M. Given a maximal left ideal I, the additive group R/I (for I is a subgroup of R) is a left module with the obvious multiplication. Moreover, since submodules of R/I correspond to ideals of R containing I, this is a simple submodule. Therefore, $x(R/I) = 0$, in particular $x(1 + I) = 0$, so $x \in I$. Therefore $x \in J(R)$. □

Corollary. *$J(R) = A$ where A is the intersection of $Ann(M)$ over all simple R-modules M. In particular, $J(R)$ is a two sided ideal.*

Theorem 13. *For a ring R with unity, the following are equivalent.*

1. *For any $a \in R$, there exists $x \in R$ such that $axa = a$.*
2. *Every principal left ideal is generated by an idempotent.*
3. *Every principal left ideal is a direct summand of ${}_RR$.*
4. *Every finitely generated left ideal is generated by an idempotent.*
5. *Every finitely generated left ideal is a direct summand of ${}_RR$.*

Proof. $2 \Leftrightarrow 3, 4 \Leftrightarrow 5$ follow from the lemma above. Now assume 1, and let $I = \langle a \rangle$ be a principal left ideal. Choose $x \in R$ such that $axa = a$, then $I = \langle xa \rangle$ and $(xa)^2 = xaxa = xa$, therefore I is generated by an idempotent. Conversely, if every principal left ideal is generated by an idempotent, then given $a \in R$, there is an x such that $\langle a \rangle = \langle xa \rangle$ and xa is idempotent. This means that there is a $b \in R$ such that

$$bxa = a \Rightarrow (bxa)xa = axa \Rightarrow a = bxa = axa.$$

Therefore $1 \Leftrightarrow 2$. Now, $4 \Rightarrow 2$ is obvious.

Assume 2, and let I be a finitely generated ideal, say $I = \langle a_1, \dots, a_k \rangle$. By induction we need only consider the case $k = 2$. Otherwise, replace $\langle a_1, \dots, a_{k-1} \rangle$ with an appropriate idempotent and use the case $k = 2$. So, take an ideal $I = \langle e, f \rangle$. Now, $f = f(1 - e) + fe$, so $I = \langle e, f(1 - e) \rangle$. Now, replace $f(1 - e)$ by an idempotent e' such that $\langle f(1 - e) \rangle = \langle e' \rangle$. It is clear that $e'e = 0$ and $I = \langle e, e' \rangle$. Now, we have

$$e = e(e + e' - ee'), e' = e'(e + e' - ee')$$

so $I = \langle e + e' - ee' \rangle$ is principal. Moreover, it is easy to see that $e + e' - ee'$ is an idempotent. □

Remark. Of all the conditions, the first one is left-right symmetric, so the same statements hold after replacing left with right. A ring that satisfies any of these conditions is called a *von Neumann regular ring.*

Lemma 16. *For a ring R with unity, we have semisimple $\Rightarrow$ von Neumann regular $\Rightarrow$ J-semisimple.*

Proof. If R is semisimple, then we know that every principal left ideal is generated by an idempotent, so R is von Neumann regular.

Suppose R is a von Neumann regular ring and $a \in J(R)$. Pick $x \in R$ such that $axa = a \Rightarrow a(1 - xa) = 0$. Because $a \in J(R), 1 - xa$ has a right inverse, therefore $a = 0$ and $J(R) = 0$. Thus, R is J-semisimple. □

It is easy to see that $\mathbb{Z}$ is a J-semisimple ring for the maximal ideals are $\langle p \rangle$ for primes p. However, $\mathbb{Z}$ is neither semisimple nor von Neumann regular. Next consider the infinite direct product $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. This is von Neumann regular as each element is idempotent, but is not Artinian (semisimple rings with unity are finitely generated).

For another example, take $k = \mathbb{Z}/2\mathbb{Z}$, and $R = k[x_1, \dots]/I$ where I is the ideal $I = \langle x_i^2 - x_i, x_ix_j | i, j \geq 1, i \neq j \rangle$. It is easy to see that I is a proper ideal, now in R, every element is idempotent, so R is von Neumann regular, but we have the descending chain $(x_1, x_2, \dots) \supsetneq (x_2, \dots) \supsetneq \dots$. This is a strictly descending chain because if , for example $x_1 \in (x_2, \dots)$, then x_1 is a polynomial expression involving variables other than x_1. Multiplying by x_1 gives $x_1 = 0$. Therefore, R is not Artinian, hence not semisimple.

Theorem 14. *(Maschke's theorem) Let G be a finite group. Then $R[G]$ is semisimple if and only if R is semisimple and $|G| \cdot 1$ is a unit in R.*

Proof. We have already proved most of this. All that is left to show is that if $R[G]$ is semisimple, then $|G| \cdot 1$ is a unit. It suffices to show that $p \cdot 1$ is a unit for every prime dividing $|G|$. Given such a prime p, pick an element $\sigma \in G$ of order p. Assuming $R[G]$ to be semisimple, it is von Neumann regular, so there is an $x \in R[G]$ such that

$$(1-\sigma)x(1-\sigma) = (1-\sigma) \Rightarrow (1-(1-\sigma)x)(1-\sigma) = 0.$$

By the following lemma, we can write $(1-(1-\sigma)x) = y(1+\sigma+\cdots+\sigma^{p-1})$, then applying the augmentation map $\epsilon\colon R[G] \to R$ gives $1 = \epsilon(y)(p \cdot 1)$, therefore $p \cdot 1$ has a left inverse. Because $p \cdot 1 \in Z(R)$, it is a unit. □

Lemma 17. *For $x \in R[G], \sigma \in G$ of order $n \geq 1, x(1-\sigma) = 0$ if and only if $x = y(1+\sigma+\cdots+\sigma^{n-1})$ for some $y \in R[G]$.*

Proof. If $x = y(1+\sigma+\cdots+\sigma^{n-1})$, then it is clear that $x(1-\sigma) = 0$. Assume $x = \sum_{g \in G} a_g g$ and $x = x\sigma$. Then, for any $g \in G$, the coefficients of $g, g\sigma, g\sigma^2, \ldots, g\sigma^{n-1}$ are the same, in other words, the coefficients are constant on the left cosets of the cyclic group $\langle\sigma\rangle$. Grouping the terms, it is clear that $x = y(1+\sigma+\cdots+\sigma^{n-1})$. □

9 Introduction to characters

Definition. *Given a ring R, an element $\epsilon \in R$ is called a central idempotent if $\epsilon \in Z(R)$ and is an idempotent. Two central idempotents ϵ_1, ϵ_2 are said to be orthogonal if $\epsilon_1\epsilon_2 = 0$. A central idempotent ϵ is said to be primitive if it is not a sum of two non zero orthogonal central idempotents.*

We know that if R is a semisimple ring with unity, then ${}_RR = V_1 \oplus \cdots \oplus V_k$ where the V_i are minimal left ideals generated by idempotents ϵ_i. Moreover, $\epsilon_i\epsilon_j = 0, i \neq j$. However, it is not guaranteed that these idempotents are central.

Rewrite ${}_RR = V_1^{n_1} \oplus \cdots \oplus V_k^{n_k}$ where V_i, V_j are not isomorphic for $i \neq j$. Setting $D_i = \mathrm{End}_R(V_i)$, we have the matrix decomposition

$$R = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

and $Z(R) = Z(D_1) \oplus \cdots \oplus Z(D_k)$. For a division ring $D, n > 0$, we have seen that $Z(M_n(D))$ is the ring of diagonal matrices with entries from $Z(D)$. If ϵ is a central idempotent, say $\epsilon = \mathrm{diag}[a, \ldots, a]$, then $a^2 = a$. Since D is a division ring, we must have $a = 0$ or $a = 1$. Therefore, ϵ is either the zero matrix of identity matrix both of which are primitive.

Therefore, if ϵ_i is the identity matrix in $M_{n_i}(D_i)$, then ϵ_i is a primitive central idempotent of D. In fact, these are the only primitive central idempotents, for if $(a_1, \ldots, a_k) \in Z(R)$ is an idempotent, then each $a_i \in M_{n_i}(D_i)$ is an idempotent, hence $a_i = 0$ or $a_i = \epsilon_i$. If $(a_1, \ldots, a_k)$ is to be primitive, then it must be some ϵ_i for $\epsilon_i\epsilon_j = 0$ in R.

Let K be an algebraically closed field, R a semisimple finite dimensional (as a vector space) K-algebra. Then, by Schur's lemma (since R is finite dimensional, all submodules are also finite dimensional), all $D_i = K$ and $R = \oplus_{i=1}^k M_{n_i}(K)$. We have seen that if R decomposes as $\oplus_{i=1}^k M_{n_i}(D_i)$, then $D_i^{n_i}$ is a simple R-module with multiplicity n_i in R. Therefore, in R, each K^{n_i} is a simple module with multiplicity n_i, in otherwords, each simple V appears in the decomposition of $R \dim_K V$ times and

$${}_RR = V_1^{\dim_K V_1} \oplus \cdots \oplus V_k^{\dim_K V_k}.$$

Next, we have $Z(R) = \prod_{i=1}^k K$, which means that $Z(R)$ is a k dimensional K-vector space. When $R = K[G]$ for a finite group $G, \mathrm{char}(K) \nmid |G|$, we know $Z(K[G])$ is the collection of class functions on G, which clearly has dimension (as a K-vector space) equal to the number of conjugacy classes in G (a basis is given by the characteristic class functions). Therefore k is the number of conjugacy classes in G, i.e. the number of irreducible representations of G is the same as the number of conjugacy classes.

9.1 Characters

Let K be an algebraically closed field, R a finite dimensional semisimple K-algebra. Decompose $R = V_1^{r_1} \oplus \cdots \oplus V_k^{r_k}$, where $(V_1, \rho_1), \ldots, (V_k, \rho_k)$ are simple R-modules and $r_i \geq 0$. Suppose $\epsilon_1, \ldots, \epsilon_k$ are the primitive central idempotents forming a basis of $Z(R)$. Then, ϵ_i acts as identity on $V_i^{r_i}$ and zero on the other summands. In particular, ϵ_i acts as identity on each copy of V_i in R.

Let (M, ρ) be any finite dimensional/finitely generated R-module, then $M = V_1^{m_1} \oplus \cdots \oplus V_k^{m_k}$ for some $m_i \geq 0$. To understand M, we need to find the values of m_i. Fix a basis for each of the V_i in M, and join them to form a basis of M. For each $r \in R$, we know that $\rho_i(r) \in M_{n_i}(K)$ where $n_i = \dim_K V_i$. Having fixed the basis, we have

$$\rho(r) = \rho_1(r)^{m_1} \oplus \cdots \oplus \rho_k(r)^{m_k}.$$

Now, take $r = \epsilon_i$ for some i, then $\rho(\epsilon_i) = I_{n_i}^{m_i}$. Taking the trace, we get $m_i \dim_K V_i = Tr(\rho(\epsilon_i))$. We can find m_i when $\dim_K V_i \neq 0$ in K. The important thing is that the trace of $\rho(\epsilon_i)$ does not depend on the basis of M. Therefore, if we can find the simple R-modules and the primitive central idempotents of R, then we can decompose any finitely generated R-module. The problem is to find the primitive central idempotents.

Given an R-module (M, ρ) that is finite dimensional over K, we define the character

$$\begin{aligned} \chi_M \colon R &\to K \\ r &\mapsto Tr(\rho(r)) \end{aligned}$$

Observe that if $(M_1, \rho_1) \cong (M_2, \rho_2)$ are two isomorphic finite dimensional R-modules, then $\chi_{M_1} = \chi_{M_2}$ because the isomorhpism correponds to a change of basis. Suppose we fix a basis for M_1, M_2, and the isomorphism is given by an invertible matrix P, then the R-linearity suggests, $P\rho_1(r) = \rho_2(r)P$, which means that the traces are the same.

We would like to find the primitive central idempotents of $K[G]$. Suppose $\epsilon_1, \ldots, \epsilon_k$ are primitive central idempotents in $K[G]$ such that ϵ_i is identity on $V_i^{n_i}$ and zero on the other factors. We know that ϵ_i are class functions. Number the conjugacy classes $1, \ldots, k$ and say ϵ_i takes value a_{ij} on the jth conjugacy class. Let $\chi_i = \chi_{V_i}$ (having fixed submodules V_i of $K[G]$), then comparing characters we get (because of the way ϵ_i act on the V_i)

$$\sum_j a_{ij} c_j \chi_k(C_j) = \dim_K V_i \delta_{ik}$$

where C_j is the jth conjugacy class, $c_j = |C_j|$ and δ_{ik} is the Kronecker delta symbol. Observe that χ_k is constant on conjugacy classes of G because

$$Tr(\rho_k(ghg^{-1})) = Tr(\rho_k(hg^{-1}g)) = Tr(\rho_k(h)).$$

With $n_i = \dim_K V_i$, we get the matrix relation over K

$$\begin{bmatrix} c_1\chi_1(C_1) & c_2\chi_1(C_2) & \ldots & c_k\chi_1(C_k) \\ c_1\chi_2(C_1) & c_2\chi_2(C_2) & \ldots & c_k\chi_2(C_k) \\ \vdots & \vdots & \ddots & \vdots \\ c_1\chi_k(C_1) & c_2\chi_k(C_2) & \ldots & c_k\chi_k(C_k) \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} & \ldots & a_{k1} \\ a_{12} & a_{22} & \ldots & a_{k2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1k} & a_{2k} & \ldots & a_{kk} \end{bmatrix} = \begin{bmatrix} n_1 & & & \\ & n_2 & & \\ & & \ddots & \\ & & & n_k \end{bmatrix}$$

If the right hand side is invertible (over K), in other words, if the characteristic of K does not divide any of the dimensions, then we conclude that the character matrix $(c_j\chi_i(C_j))_{1 \leq i,j \leq k}$ is invertible and we can find the a_{ij}s. Of course, these a_{ij}s always exist, only it is easier to find it in this case.

We use the orthogonality relations of $\epsilon_1, \ldots, \epsilon_k$. Suppose $a = \sum_{g \in G} a_g g, b = \sum_{b \in G} b_g g$ are two central elements. Then we look at the coefficient of 1_G in the product. This is given by

$$\begin{aligned} (ab)_1 &= \sum_{g \in G} a_g b_{g^{-1}} \\ &= \sum_{i=1}^{k} c_i a(C_i) b(C_i^{-1}) \end{aligned}$$

where the sum is taken over conjugacy classes. Given a conjugacy class C of G, say the conjugacy class of some $g \in$G, then the inverse class C^{-1} is the conjugacy class of g^{-1}. It is clear that there is a bijection between C, C^{-1}, namely $x \mapsto x^{-1}$ for g, h are conjugates in G if and only if g^{-1}, h^{-1} are conjugates. Above, the second equality comes from the fact that a, b are constant on the conjugacy classes.

We know that the numbers $c_1, \ldots, c_k$ are divisors of $|G|$, so they are non zero in K. Since K is algebraically closed, we may talk of their square roots. Fix square roots $\sqrt{c_1}, \ldots, \sqrt{c_k}$ and define matrices L, M, N as

$$L_{ij} = \begin{cases} \dim_K V_i & i = j \\ 0 & i \neq j \end{cases}, M_{ij} = \sqrt{c_j}\chi_i(C_j), N_{ij} = \sqrt{c_i}a_{ji}$$

Previously we assumed $C_1, \ldots, C_k$ to be in any order, but now we make just the simple assumption that C_1 is the conjugacy class of identity 1_G. We next reverse the order of the conjugacy classes, i.e. change the order to $C_1^{-1}, \ldots, C_k^{-1}$. Note that $C_1^{-1} = C_1$. Then we define matrices M_r, N_r as

$$(M_r)_{ij} = \sqrt{c_j}\chi_i(C_j^{-1}), (N_r)_{ij} = \sqrt{c_i}a_{ji-}$$

where a_{ji-} is the value attained by ϵ_j on the inverse class C_i^{-1}. Note that the size of a conjugacy class and its inverse are the same. Now, we know $L = MN = M_r N_r$. The orthogonality relations of $\epsilon_1, \ldots, \epsilon_k$ translate to

$$A = N_r^T N = \begin{bmatrix} a_{11} & & & \\ & a_{21} & & \\ & & \ddots & \\ & & & a_{k1} \end{bmatrix}$$

Now, supposing non of the $\dim_K V_i = 0$ in K, then L, M, N are invertible and we have

$$A = (M_r^{-1}L)^T(M^{-1}L) = L^T(MM_r^T)^{-1}L = L(MM_r^T)^{-1}L.$$

Because the matrices are invertible, so is A, in other words non of the a_{i1} are zero. We obtain

$$MM_r^T = LA^{-1}L.$$

Since L, A are diagonal, so is the product $LA^{-1}L$, i.e. MM_r^T is a diagonal matrix. We obtain

$$\begin{bmatrix} \sqrt{c_1}\chi_1(C_1) & \ldots & \sqrt{c_k}\chi_1(C_k) \\ \vdots & \ddots & \vdots \\ \sqrt{c_1}\chi_k(C_1) & \ldots & \sqrt{c_k}\chi_k(C_k) \end{bmatrix} \begin{bmatrix} \sqrt{c_1}\chi_1(C_1^{-1}) & \ldots & \sqrt{c_1}\chi_k(C_1^{-1}) \\ \vdots & \ddots & \vdots \\ \sqrt{c_k}\chi_1(C_k^{-1}) & \ldots & \sqrt{c_k}\chi_k(C_k^{-1}) \end{bmatrix} = \begin{bmatrix} \frac{n_1^2}{a_{11}} & & \\ & \ddots & \\ & & \frac{n_k^2}{a_{k1}} \end{bmatrix}$$

where $n_i = \dim_K V_i$. In particular,

$$\sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \begin{cases} \frac{\dim_K V_i^2}{a_{i1}} & i = j \\ 0 & i \neq j \end{cases}$$

We can similarly try to find a_x for $x \in Z(G)$ because

$$a_x = \sum_{g \in G} a_{xg}a_{g^{-1}} = \sum_i a(xC_i)a(C_i^{-1})$$

where xC is the conjugacy class of xg when C is the conjugacy class of g. This is because $xhgh^{-1} = hxgh^{-1}$.

9.2 Tensor products and duals

Let K be any field, G, H finite groups and $(V_1, \rho_1), (V_2, \rho_2)$ be finite dimensional G-representations and $(W_1, \sigma_1), (W_2, \sigma_2)$ be finite dimensional H-representations. We have seen previously that $V_1 \boxtimes W_1$ is a $G \times H$-representation. Moreover, as $G \times H$-representations, we have $V_1 \boxtimes W_1 \cong \mathrm{Hom}_K(V_1^*, W_1)$ where the action of $(g, h) \in G \times H$ on $T \in \mathrm{Hom}_K(V, W)$ is given by $(g, h) \cdot T = \sigma(h) \circ T \circ \rho(g^{-1})$ for representations $(V, \rho), (W, \sigma)$. In the following theorem, which already has enough symbols, we resort to the notation gv for $\rho(g)(v)$ and it should be clear from the context which representation is under consideration.

Theorem 15. *As $G \times G \times H \times H$-representations, $Hom_K(V_1 \boxtimes W_1, V_2 \boxtimes W_2) \cong Hom_K(V_1, V_2) \boxtimes Hom_K(W_1, W_2)$.*

Given $(g_1, g_2, h_1, h_2) \in G \times G \times H \times H$, for $T \in \mathrm{Hom}_K(V_1 \boxtimes W_1, V_2 \boxtimes W_2)$ and $T_1 \otimes T_2 \in \mathrm{Hom}_K(V_1, V_2) \boxtimes \mathrm{Hom}_K(W_1, W_2)$ the action is given by

$$(g_2, h_2) \circ T \circ (g_1^{-1}, h_1^{-1})$$

$$((g_1, g_2) \cdot T_1) \otimes ((h_1, h_2) \cdot T_2)$$

Proof. Given $T_1 \in \mathrm{Hom}_K(V_1, V_2), T_2 \in \mathrm{Hom}_K(W_1, W_2)$, we denote the tensor product of T_1, T_2 by $T_1 \otimes_m T_2 \in \mathrm{Hom}_K(V_1 \boxtimes W_1, V_2 \boxtimes W_2)$ so as to avoid confusing it with the element $T_1 \otimes T_2 \in \mathrm{Hom}_K(V_1, V_2) \boxtimes \mathrm{Hom}_K(W_1, W_2)$. Thus, we have a map

$$\begin{aligned}\mathrm{Hom}_K(V_1, V_2) \times \mathrm{Hom}_K(W_1, W_2) &\to \mathrm{Hom}_K(V_1 \boxtimes W_1, V_2 \boxtimes W_2)\\ (T_1, T_2) &\mapsto T_1 \otimes_m T_2 : \{x \otimes y \mapsto T_1(x) \otimes T_2(y) \,\forall\, x \in V_1, y \in W_1\}\end{aligned}$$

This map is K-linear, because, for example $(T_1 + T_1') \otimes_m T_2, T_1 \otimes_m T_2 + T_1' \otimes_m T_2$ agree on the basic tensors of $V_1 \boxtimes W_1$. Therefore, we have a K-linear map

$$\begin{aligned}\Phi \colon \mathrm{Hom}_K(V_1, V_2) \boxtimes \mathrm{Hom}_K(W_1, W_2) &\to \mathrm{Hom}_K(V_1 \boxtimes W_1, V_2 \boxtimes W_2)\\ T_1 \otimes T_2 &\mapsto T_1 \otimes_m T_2\end{aligned}$$

Now given $(g_1, g_2, h_1, h_2) \in G \times G \times H \times H$, we have for all $v \in V_1, w \in W_1$

$$\begin{aligned}\Phi((g_1, g_2, h_1, h_2) \cdot T_1 \otimes T_2)(v \otimes w) &= \Phi((g_1, g_2) \cdot T_1 \otimes (h_1, h_2) \cdot T_2)(v \otimes w)\\ &= (((g_1, g_2) \cdot T_1) \otimes_m ((h_1, h_2) \cdot T_2))(v \otimes w)\\ &= g_2 T_1(g_1^{-1} v) \otimes h_2 T_2(h_1^{-1} w)\\ &= (g_2, h_2) T_1 \otimes_m T_2((g_1^{-1}, h_1^{-1})(v \otimes w))\\ &= ((g_1, g_2, h_1, h_2) \cdot (T_1 \otimes_m T_2))(v \otimes w)\end{aligned}$$

Since they agree on basic tensors, we have

$$\Phi((g_1, g_2, h_1, h_2) \cdot (T_1 \otimes T_2)) = (g_1, g_2, h_1, h_2) \cdot \Phi(T_1 \otimes T_2).$$

By K-linearity of Φ and the linearity of the action of $G \times G \times H \times H$, this equality holds on $\mathrm{Hom}_K(V_1, V_2) \boxtimes \mathrm{Hom}_K(W_1, W_2)$, i.e.,

$$\Phi(\alpha \cdot T) = \alpha \cdot \Phi(T) \,\forall\, \alpha \in G \times G \times H \times H, T \in \mathrm{Hom}_K(V_1, V_2) \boxtimes \mathrm{Hom}_K(W_1, W_2).$$

Now we find the inverse map. So far, we haven't used the finite dimensionality of V_i, W_i. So, let $\{e_1^i, \ldots, e_{n_i}^i\}$ be a basis of $V_i, i = 1, 2$, similarly let $\{f_1^i, \ldots, f_{m_i}^i\}$ be a basis of $W_i, i = 1, 2$. For $1 \le i \le n_1, 1 \le j \le n_2$, define $E_{ij} \in \mathrm{Hom}_K(V_1, V_2)$ by

$$E_{ij}(e_k^1) = \begin{cases} 0 & k \neq i \\ e_j^2 & k = i \end{cases}$$

Given $T \in \mathrm{Hom}_K(V_1 \boxtimes W_1, V_2 \boxtimes W_2)$, and $1 \le i \le n_1, 1 \le r \le m_1$, we have unique coefficients $a^{ir}_{js} \in K, 1 \le j \le n_2, 1 \le s \le m_2$ such that

$$T(e^1_i \otimes f^1_r) = \sum_{j,s} a^{ir}_{js} e^2_j \otimes f^2_s$$

because the bases of V_i, W_i provide a basis for $V_i \boxtimes W_i$. Set $T_{ij} \in \mathrm{Hom}_K(W_1, W_2)$ to be the map

$$T_{ij}(f^1_r) = \sum_{1 \le s \le m_2} a^{ir}_{js} f^2_s.$$

Basically, it is the coefficients of $e^2_j \otimes f^2_1, \dots, e^2_j \otimes f^2_{m_2}$ in $T(e^1_i \otimes f^1_r)$. Consider the map

$$\begin{aligned} \Psi \colon \mathrm{Hom}_K(V_1 \boxtimes W_1, V_2 \boxtimes W_2) &\to \mathrm{Hom}_K(V_1, V_2) \boxtimes \mathrm{Hom}_K(W_1, W_2) \\ T &\mapsto \sum_{\substack{1 \le i \le n_1 \\ 1 \le j \le n_2}} E_{ij} \otimes T_{ij} \end{aligned}$$

It is clear that Φ is a K-linear map. We show that it is the inverse of Φ and the rest follows.

$$\begin{aligned} \Phi(\Psi(T))(e^1_i \otimes f^1_r) &= \sum_{\substack{1 \le k \le n_1 \\ 1 \le j \le n_2}} E_{kj} \otimes_m T_{kj}(e^1_i \otimes f^1_r) \\ &= \sum_{1 \le j \le n_2} E_{ij} \otimes_m T_{ij}(e^1_i \otimes f^1_r) \\ &= \sum_{1 \le j \le n_2} e^2_j \otimes (\sum_{1 \le s \le m_2} a^{ir}_{js} f^2_s) \\ &= \sum_{\substack{1 \le j \le n_2 \\ 1 \le s \le m_2}} a^{ir}_{js} e^2_j \otimes f^2_s \end{aligned}$$

Therefore, Ψ is injective. Comparing the K-vector space dimensions (for Ψ, Φ are K-linear), we conclude that Φ, Ψ are isomorphisms. By the bijective nature, Φ, Ψ are in fact isomorphic as $G \times G \times H \times H$ representations. □

Corollary. *Suppose $V_1 = V_2 = V, W_1 = W_2 = W$, then the isomorphism above is also a ring isomorphism.*

Proof. It suffices to show that Φ is multiplicative, then by the bijective nature, Ψ is also multiplicative (but it is harder to show). Take $T_1, T'_1 \in \mathrm{End}_K(V), T_2, T'_2 \in \mathrm{End}_K(W)$. We need to show that

$$\begin{aligned} \Phi((T_1 \otimes T_2) \circ T'_1 \otimes T'_2)) &= \Phi((T_1 \circ T'_1) \circ (T_2 \otimes T'_2)) \\ &= (T_1 \circ T'_1) \otimes_m (T_2 \circ T'_2) \\ &= (T_1 \otimes_m T_2) \circ (T'_1 \otimes_m T'_2) \\ &= \Phi(T_1 \otimes T_2) \circ \Phi(T'_1 \otimes T_2) \end{aligned}$$

which is now obvious. □

By Burnside's theorem, when $(V, \rho), (W, \sigma)$ are simple G, H representations respectively, then $\rho(K[G]) = \mathrm{End}_K(V), \sigma(K[H]) = \mathrm{End}_K(W)$. Therefore, all the basic tensors in $\mathrm{End}_K(V) \boxtimes \mathrm{End}_K(W)$ are covered by $\rho \otimes \sigma$ which means that

$$\rho \otimes \sigma(K[G \times H]) = \mathrm{End}_K(V) \boxtimes \mathrm{End}_K(W).$$

Lastly, the action of $G \times H$ on $V \boxtimes H$ is precisely $\Phi \circ (\rho \otimes \sigma)$, therefore $(\Phi \circ \rho \otimes \sigma)(K[G \times H]) = \mathrm{End}_K(V \boxtimes W)$ and by Burnside's theorem, $V \boxtimes W$ is a simple $G \times H$-representation.

Remark. In fact, we can replace $K[G], K[H]$ by any K-algebras R, S with V, W finite dimensional modules. Of course, the isomorphism in the theorem is only as K-vector spaces, but Burnside's theorem still applies to make $V \boxtimes W$ a simple $R \otimes_K S$-module.

Theorem 16. *Suppose $(V_1, \rho_1), (V_2, \rho_2)$ are simple G-representations, $(W_1, \sigma_1), (W_2, \sigma_2)$ are simple H-representations and $V_1 \boxtimes W_1 \cong V_2 \boxtimes W_2$ as $G \times H$-representations, then $V_1 \cong V_2, W_1 \cong W_2$ as representations.*

Proof. Suppose $\psi\colon V_1 \boxtimes W_1 \to V_2 \boxtimes W_2$ is an isomorphism of $G \times H$ representations. Then $\tilde{\psi}\colon \mathrm{End}_K(V_1 \boxtimes W_1) \to \mathrm{End}_K(V_2 \boxtimes W_2)$ with $\tilde{\psi}(T) = \psi \circ T \circ \psi^{-1}$ is an isomorphism of $G \times G \times H \times H$-representations and a K-algebra isomorphism. It is easy to see that it is a K-algebra homomorphism, to see $G \times G \times H \times H$-linearity, observe that

$$\begin{aligned} \tilde{\psi}((g_1, g_2, h_1, h_2) \cdot T) &= \psi \circ (g_1, g_2, h_1, h_2) \cdot T \circ \psi^{-1} \\ &= \psi \circ (g_2, h_2) \circ T \circ (g_1^{-1}, h_1^{-1}) \circ \psi^{-1} \\ &= (g_2, h_2) \circ \psi \circ T \circ \psi^{-1} \circ (g_1^{-1}, h_1^{-1}) \\ &= (g_1, g_2, h_1, h_2) \cdot (\psi \circ T \circ \psi^{-1}) \end{aligned}$$

Now $\rho_1 \otimes \sigma_1\colon K[G \times H] \to \mathrm{End}_K(V_1 \boxtimes W_1)$ is a ring homomorphism, which we restrict to $K[G \times 1_H]$. We then have the following diagrams

$$\begin{tikzcd} \mathrm{End}_K(V_1) \arrow[d, "\cdot \otimes I_{W_1}"'] & K[G] \arrow[l, "\rho_1"'] \arrow[r, "\rho_2"] \arrow[d] & \mathrm{End}_K(V_2) \arrow[d, "\cdot \otimes I_{W_2}"] \\ \mathrm{End}_K(V_1) \boxtimes \mathrm{End}_K(W_1) \arrow[d, leftrightarrow] & K[G \times H] \arrow[l, "\rho_1 \otimes \sigma_1"] \arrow[r, "\rho_2 \otimes \sigma_2"'] & \mathrm{End}_K(V_2) \boxtimes \mathrm{End}_K(W_2) \arrow[d, leftrightarrow] \\ \mathrm{End}_K(V_1 \boxtimes W_1) \arrow[rr, "\tilde{\psi}"'] & & \mathrm{End}_K(V_2 \boxtimes W_2) \end{tikzcd}$$

Observe that all these are commutative:

- $\rho_1(g) \otimes I_{W_1} = (\rho_1 \otimes \sigma_1)(g, 1_H)$ and $\rho_2(g) \otimes I_{W_2} = (\rho_2 \otimes \sigma_2)(g, 1_H) \, \forall \, g \in G$
- $\tilde{\psi}(\rho_1(g) \otimes_m \sigma_1(h)) = \tilde{\psi}((1, g, 1, h) \cdot (1_{V_1} \otimes_m 1_{W_1})) = (1, g, 1, h) \cdot (1_{V_2} \otimes_m 1_{W_2}) = \rho_2(g) \otimes_m \sigma_2(h)$

Lastly, note that $T \mapsto T \otimes I_{W_1}, T \in \mathrm{End}_K(V_1)$ is injective. Consider the map

$$\begin{aligned} \theta\colon \mathrm{End}_K(V_1) &\to \mathrm{End}_K(V_2) \\ \rho_1(x) &\mapsto \rho_2(x) \end{aligned}$$

Because V_1, V_2 are simple ρ_1, ρ_2 are surjective. We need to verify that θ so defined is well defined, suppose $\rho_1(x) = \rho_1(y)$, i.e. $\rho_1(x - y) = 0$, then

$$\tilde{\psi}(\rho_1(x - y) \otimes_m I_{W_1}) = 0 \Rightarrow \rho_2(x - y) \otimes \sigma_2(1_H) = 0 \in \mathrm{End}_K(V_2) \boxtimes \mathrm{End}_K(W_2)$$

this means that $\rho_2(x - y) = 0 \Rightarrow \rho_2(x) = \rho_2(y)$. Therefore, θ is a well defined map. It is easy to see that θ is in fact a K-algebra isomorphism. As a consequence, $\dim_K V_1 = \dim_K V_2 = n$, say.

Fixing bases for V_1, V_2 obtain algebra isomorphisms $\tilde{\theta}\colon M_n(K) \to \mathrm{End}_K(V_1) \xrightarrow{\theta} \mathrm{End}_K(V_2) \to M_n(K)$. By the following lemma, this K-algebra automorphism of $M_n(K)$ is inner, i.e. $\exists P \in \mathrm{GL}_n(K)$ such that $\tilde{\theta}(A) = PAP^{-1}$. What this means is that the matrix of $\rho_2(r), r \in K[G]$ is the matrix $P\rho_1(r)P^{-1}$ in the previously fixed bases.

This in turn, gives us a "change of basis" matrix P giving us an isomorphism $V_1 \to V_2$. Identify V_1, V_2 with K^n. Consider the map $\phi\colon v \mapsto Pv$ from K^n corresponding to V_1 to V_2. Given $r \in K[G]$, the action of r on the first K^n is through ρ_1, and on the send through ρ_2. Then,

$$\phi(r \cdot v) = P\rho_1(r)v = P\rho_1(r)P^{-1}Pv = \rho_2(r)\phi(v).$$

Therefore, ϕ is $K[G]$-linear. It follows that $V_1 \cong V_2$ as G-representations. Similarly, $W_1 \cong W_2$ as H-representations. $\square$

Lemma 18. *If $\theta\colon M_n(K) \to M_n(K)$ is a K-algebra automorphism, where K is any field, then θ is an inner automorphism, i.e. $\exists P \in M_n(K)$ invertible such that $\theta(A) = PAP^{-1}$.*

Proof. Recall that when $R = M_n(K)$, the left regular module decomposes as ${}_RR = \oplus_{i=1}^n K^n$. This means that upto isomorphism, there is only one simple R-module. Now, via θ, we have two actions of R on $M_n(K)$:

$$\begin{aligned} \rho_1\colon R &\to \mathrm{End}_K(K^n) \\ r &\mapsto \{x \mapsto rx, x \in K^n\} \end{aligned} \qquad \begin{aligned} \rho_2\colon R &\to \mathrm{End}_K(K^n) \\ r &\mapsto \{x \mapsto \theta(r)x, x \in K^n\} \end{aligned}$$

In both cases, it is easy to see that the resulting R-module structure on K^n is simple. Therefore, the two K^n, i.e., $V_1 = (K^n, \rho_1), V_2 = (K^n, \rho_2)$ must be isomorphic as K-modules. Suppose $\phi\colon V_1 \to V_2$ is an isomorphism. Since ϕ is a K-vector space isomorphism as well (because $R = M_n(K)$ is a K-algebra), it must be given by an invertible matrix P, i.e. $\phi(v) = Pv\,\forall\, v \in V_1$ (keep in mind that V_1, V_2 are both K^n as K-vector spaces). The R-linearity gives

$$PAv = \phi(\rho_1(A)(v)) = \rho_2(A)(\phi(v)) = \theta(A)Pv\,\forall\, A \in M_n(K), v \in K^n.$$

This directly gives $\theta(A) = PAP^{-1}$ as required. □

Remark. The lemma above is a specific case of the more general Noether-Skolem Theorem.

Corollary. *If R, S are finite dimensional K-vector spaces, $M = \oplus_i V_i^{m_i}$ is a semisimple R-module decomposed into simple R-modules and similarly $N = \oplus_j W_j^{n_j}$ is a semisimple S-module, then $M \otimes_K N = \oplus_{i,j}(V_i \otimes W_j)^{m_i n_j}$ is the decomposition of the $R \otimes_K S$-module $M \otimes_K N$ into simple modules.*

Next, given a finite group G, a simple finite dimensional representation (V, ρ), we know that V^* is also a G-representation. Moreover, as K-vector spaces, $V \cong V^*$, therefore, $\mathrm{End}_K(V^*) = M_n(K)$ where $n = \dim_K V$. By simplicity, $\rho(G) = \mathrm{End}_K(V)$. Since the action of $g \in G$ on $f \in V^*$ is $f \circ \rho(g^{-1})$, we can, by swapping coefficients in $K[G]$, obtain any matrix in $M_n(K)$. Therefore, V^* is a simple G-representation.

Theorem 17. *Let G be any group, V is any G-representation. If V^* is a simple G-representation, then so is V.*

Proof. Suppose $W \subseteq V$ is an invariant submodule. Consider $W^\perp = \{f \in V^* | f(w) = 0\,\forall\, w \in W\}$. Given $g \in G, f \in W^\perp$, we have $g \cdot f(w) = f(g^{-1}w) = 0\,\forall\, w \in W$. Therefore, $g \cdot f \in W^\perp$, hence $W^\perp$ is a $K[G]$-submodule of V^*. By simplicity, we must have $W^\perp = 0$ or $W^\perp = V^*$.

If $W^\perp = V^*$, then we must have $W = 0$ by considering duals of basis elements of W. If $W^\perp = 0$, then $W = V$ by considering the dual basis of a basis of V. Therefore, V is simple. □

Theorem 18. *When V is a finite dimensional G-representation, $V^{**} \cong V$ as G-representations.*

Proof. For each $v \in V$, the evaluation map $e_v\colon V^* \to K$ is a K-linear map, hence $e_v \in V^{**}$. Let $\{v_1, \ldots, v_n\}$ be a basis for V, $\{v_1^*, \ldots, v_n^*\}$ the corresponding dual basis for V^*. Set $e_i = e_{v_i}$, then if $a_1e_1 + \cdots + a_ne_n = 0 \in V^{**}$, then evaluating at each v_i^* gives $a_i = 0$. Since $\dim_K V = \dim_K V^* = \dim_K V^{**}$, $\{e_1, \ldots, e_n\}$ is a basis for V^{**}.

Consider the map $v_i \mapsto e_i$. This map is K-linear isomorphism between V, V^{**}. Now, given $g \in G$, suppose $gv_1 = a_1v_1 + \cdots + a_nv_n$, then $gv_1 \mapsto a_1e_1 + \cdots + a_nv_n$. Next,

$$\begin{aligned} g \cdot e_1(v_i^*) &= e_1(g^{-1} \cdot v_i^*) \\ &= (g^{-1} \cdot v_i^*)(v_1) \\ &= v_i^*(gv_1) \\ &= a_i \end{aligned}$$

Therefore, $g \cdot e_1 = a_1e_1 + \cdots + a_ne_n$. Similarly, $gv_i \mapsto g \cdot e_i\,\forall\, i$, therefore, the isomorphism is G-linear and $V \cong V^{**}$ as G-representations. □

Remark. We showed that if the dual V^* is simple, then so is V. In the finite dimensional case, $V^{**} \cong V$, so if V is simple, then so is V^{**}, hence V^*. However, the same is not true when V is not finite dimensional. See [4].

9.3 A different decomposition of $K[G]$

Let K be an algebraically closed field, G a finite group with $\text{char}(K) \nmid |G|$. Given a simple finite dimensional G-representation (V, ρ), we know that $V^* \boxtimes V$ is a simple $G \times G$ representation and is isomorphic to $\text{End}_K(V)$ (as $G \times G$-representation). Next, we have the obvious map

$$\begin{aligned} E_V \colon\ V^* \boxtimes V &\to K \\ f \otimes v &\mapsto f(v) \end{aligned}$$

Now fix a basis $\{e_1, \dots, e_n\}$ of $V, \{e_1^*, \dots, e_n^*\}$ corresponding dual basis of V^*, then the map $\text{End}_K(V) \to V^* \boxtimes V$ sends $T \mapsto \sum e_i^* \otimes T(e_i)$. Combining these, we get

$$\begin{tikzcd} V^* \boxtimes V \arrow[r, "E_V"] & K \\ \text{End}_K(V) \arrow[u] \arrow[ur, "\text{trace}"'] & \end{tikzcd}$$

because $E_V(e_i^* \otimes T(e_i))$ is going to be the coefficient of e_i in $T(e_i)$, i.e. the ith diagonal entry in the matrix of T with respect to the basis $\{e_1, \dots, e_n\}$. The map to $V^* \boxtimes V$ is $G \times G$ linear, but E_V is not. In fact, upon the action of $(g, h) \in G \times G$

$$E_V \circ (g, h)(f \otimes v) = f(g^{-1}hv)$$

and

$$T \mapsto Tr((g, h) \cdot T) = Tr(hTg^{-1}) \,\forall T \in \text{End}_K(V).$$

Suppose ${}_{K[G]}K[G] = V_1^{n_1} \oplus \cdots \oplus V_k^{n_k}$. We know that $n_i = \dim_K V_i$. Then, as rings $K[G] \cong \oplus_{i=1}^k M_{n_i}(K)$. However, we also know that $M_{n_i}(K) = \text{End}_K(V_i)$ as sets and that $\text{End}_K(V_i) \cong V^* \boxtimes V$ as $G \times G$-representations.

For (V, ρ) as above, we try to make sense of $M_n(K)$ as a $G \times G$-representation isomorphic to $\text{End}_K(V)$. Having fixed the basis $\{e_1, \dots, e_n\}$ of V, there is the obvious K-vector space isomorphism that sends $T \in \text{End}_K(V)$ to its matrix with respect to this basis.

Given $(g_1, g_2) \in G \times G$, we have $(g_1, g_2) \cdot T = \rho(g_2)T\rho(g_1^{-1})$. If we were to carry this action to $M_n(K)$, and ultimately to $K[G]$, then we make $K[G]$ a $G \times G$ representation with action

$$(g_1, g_2) \cdot x = g_2 x g_1^{-1} \,\forall x \in K[G].$$

In this way $K[G]$ becomes a $G \times G$-representation. Since $K[G \times G]$ is semisimple, we can decompose $K[G]$ into simple representations.

We look for $G \times G$-linear maps $V^* \boxtimes V \to K[G]$. Suppose ϕ is such a map, then we want

$$\phi((g, h) \cdot f \otimes v) = (g, h) \cdot \phi(f \otimes v) = h\phi(f \otimes v)g^{-1}.$$

Given $\sum_{\alpha \in G} a_\alpha \alpha \in K[G]$, we have

$$h(\sum_\alpha a_\alpha \alpha)g^{-1} = \sum_\alpha a_\alpha h\alpha g^{-1} = \sum_\alpha a_{h^{-1}\alpha g}\alpha.$$

Moreover, the coefficients are maps $V^* \boxtimes V \to K$. We already have one such map E_V. Observe that $E_V \circ (g, h)(f \otimes v) = f(g^{-1}hv)$. Putting these together, we can take

$$\begin{aligned} \phi_V \colon V^* \boxtimes V &\to K[G] \\ f \otimes v &\mapsto \sum_{\alpha \in G} f(\alpha^{-1}v)\alpha \end{aligned}$$

Observe that ϕ_V is well defined because the map $(f, v) \mapsto \sum_\alpha f(\alpha^{-1}v)\alpha$ is K-bilinear on $V^* \times V$. Next we see that this is $G \times G$-linear because

$$\begin{aligned}\phi_V((g,h) \cdot f \otimes v) &= \sum_\alpha f(g^{-1}\alpha^{-1}hv)\alpha \\ &= \sum_\alpha f(\alpha^{-1}v)h\alpha g^{-1} \\ &= (g,h) \cdot \phi_V(f \otimes v)\end{aligned}$$

Lastly, ϕ_V is non zero because we can make the coefficient of 1_G non zero for some specific choices of f, v in $f \otimes v$. Because $V^* \boxtimes V$ is a simple $G \times G$-representation, ϕ_V is injective.

Now, we run through the simple representations of G to get a $G \times G$-linear map

$$\begin{aligned}\Phi\colon\ &\oplus_{(V_i,\rho_i)} V_i^* \boxtimes V_i \to K[G] \\ &\sum_i f_i \otimes v_i \mapsto \sum_i \sum_\alpha f_i(\alpha^{-1}v_i)\alpha\end{aligned}$$

Because each $V_i^* \boxtimes V_i$ appears with multiplicity 1 (for the products are not isomorphic when $i \neq j$), the kernel of Φ is a direct sum of some of the $V_i^* \boxtimes V_i$. However, because ϕ_{V_i} is injective, none of the $V_i^* \boxtimes V_i$ is in the kernel, hence Φ is injective. Comparing dimensions (for Φ is also K-linear), we conclude that Φ is an isomorphism of $G \times G$-representations.

We then have the isomorphism

$$\begin{aligned}\Psi\colon\ &\oplus_{i=1}^k \operatorname{End}_K(V_i) \to K[G] \\ &T_i \mapsto \sum_{\alpha \in G} Tr(\rho_i(\alpha^{-1}) \circ T_i)\alpha\end{aligned}$$

We have an obvious map we haven't looked at so far,

$$\begin{aligned}\rho\colon\ &K[G \times G] \to \oplus_i \operatorname{End}_K(V_i) \\ &x \mapsto \sum_i \rho_i(x)\end{aligned}$$

This is obviously a K-linear map, but it is also $G \times G$-linear because for any $(g,h) \in G \times G$, we have

$$\begin{aligned}\rho((g,h) \cdot x) &= \rho(hxg^{-1}) \\ &= \sum_i \rho_i(hxg^{-1}) \\ &= \sum_i \rho_i(h)\rho_i(x)\rho_i(g^{-1}) \\ &= (g,h)\rho(x)\end{aligned}$$

Now as $G \times G$-representations, we know that $\operatorname{End}_K(V_i) \ncong \operatorname{End}_K(V_j), i \neq j$. Furthermore, the projection of ρ to the ith coordinate is ρ_i which is surjective by simplicity of V_i. Combining these two facts, we see that ρ is surjective, then by comparing dimensions, it must be an isomorphism.

Look at $\rho \circ \Psi$. This is a $G \times G$-linear automorphism of $\oplus_i \operatorname{End}_K(V_i)$. By Schur's lemma (recall K is algebraically closed), it is going to be a scaling of each coordinates, i.e. there are non zero constants $b_1, \ldots, b_k$ such that

$$\rho \circ \Psi(T_1, \ldots, T_k) = (b_1 T_1, \ldots, b_k T_k).$$

Consider $\epsilon_1 \in K[G]$, we know that it acts as identity on V_1 and zero on $V_j, j \neq 1$. Therefore, $\rho(\epsilon_1) = (I_{V_1}, 0, \ldots, 0)$ (this also shows that ρ is surjective), which means that $\Psi(I_{V_1}, 0, \ldots, 0) = b_1\epsilon_1$. In other words,

$$\epsilon_1 = \frac{1}{b_1} \sum_{\alpha \in G} Tr(\rho_1(\alpha^{-1}))\alpha.$$

Similarly, for other ϵ_i. Now, we know that as G-representations,

$$ {}_{K[G]}K[G] = \oplus_i V_i^{\dim_K V_i}. $$

Fix a basis for each of the summands, and fix the basis $\{g | g \in G\}$ for $K[G]$. We look at the action of $g \in G$ on the whole vector space $K[G]$ and on the individual summands.

On $K[G]$ each $g \in G$ acts as a permutation matrix. This means that the trace is given by

$$ Tr(g) = \begin{cases} |G| & g = 1_G \\ 0 & g \neq 1_G \end{cases} $$

However, at the same time (in K) $Tr(g) = \sum_i \dim_K V_i Tr(\rho_i(g))$. Therefore in K,

$$ \begin{aligned} \sum_i b_i \dim_K V_i \epsilon_i &= \sum_i \sum_{\alpha \in G} \dim_K V_i Tr(\rho_i(\alpha^{-1}))\alpha \\ &= \sum_i \dim_K V_i Tr(\rho_i(1_G))1_G \\ &= \sum_i \dim_K V_i^2 1_G \\ &= |G| 1_G \end{aligned} $$

where we have used $|G| = \dim_K K[G] = \sum_i \dim_K V_i^2$ in $\mathbb{Z}$, but it holds true even in K (it gets reduced modulo $\mathrm{char}(K)$). Now, 1_G is the identity of $K[G]$, which we know is also given by $\epsilon_1 + \cdots + \epsilon_k$. Therefore,

$$ \sum_i b_i \dim_K V_i \epsilon_i = |G| \sum_i \epsilon_i. $$

Using orthogonal properties of $\epsilon_1, \ldots, \epsilon_k$, we see must have $\dim_K V_i \neq 0$ in K and

$$ b_i = \frac{|G|}{\dim_K V_i}. $$

This also gives

$$ \epsilon_i = \frac{\dim_K V_i}{|G|} \sum_{\alpha \in G} \chi_i(\alpha^{-1})\alpha. $$

In particular, $a_{i1} = \dim_K V_i^2 / |G|$. Which means we have the following orthogonality relations, called the *Schur's orthogonality relations*

$$ \sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \begin{cases} |G| & i = j \\ 0 & i \neq j \end{cases} $$

In fact, if we look at the coefficient of any $x \in G$ in $\epsilon_i \epsilon_j$, we have

$$ (\epsilon_i \epsilon_j)_x = \frac{\dim_K V_i \dim_K V_j}{|G|^2} \sum_{\alpha \in G} \chi_i(\alpha^{-1}x^{-1})\chi_j(\alpha) = \begin{cases} \frac{\dim_K V_i}{|G|}\chi_i(x^{-1}) & i = j \\ 0 & i \neq j \end{cases} $$

In other words, for any $x \in G$, we have

$$ \frac{1}{|G|} \sum_{\alpha \in G} \chi_i(\alpha)\chi_j(\alpha^{-1}x) = \delta_{ij} \frac{\chi_i(x)}{\chi_i(1_G)}. $$

This suggests that the elements $\frac{\dim V_i}{|G|} \sum_{\alpha \in G} \chi_i(\alpha)\alpha$ should also be a central idempotent and that is in fact true.

Let (V, ρ) be a finite dimensional representation of G, then look at the action of $g \in G$ on V^*. It sends each $\rho^* \colon f \mapsto f \circ \rho(g)$. By taking a dual basis of V, it is easy to see that the matrix of $\rho^*(g)$ on V^* is precisely $\rho(g^{-1})^T$, which means that (since trace is preserved under transpose)

$$ \chi_{V^*}(g) = \chi_V(g^{-1}) \,\forall\, g \in G. $$

Therefore, the new elements are just the same $\epsilon_1, \ldots, \epsilon_k$ permutated. Keep in mind that as representations $V^{**} \cong V$, so the characters are the same.

9.4 Applications and more relations

As a first application of characters, we decompose any finite dimensional G-representation. Continuing with the notation above, suppose $M = V_1^{m_1} \oplus \cdots \oplus V_k^{m_k}$ is a finite dimensional G-representation. Then, we have

$$\chi_M = m_1\chi_1 + \cdots + m_k\chi_k$$

where χ_i can be thought of as both a function on G and a central idempotent of $K[G]$. To find the m_i, we take the product with χ_i, so that

$$m_i = \frac{1}{|G|}\sum_{g\in G}\chi_M(g)\chi_i(g^{-1}).$$

This way, we can decompose any finite dimensional representation into simple modules. Essentially we are using the fact that $\epsilon_1, \ldots, \epsilon_k$ are linearly independent and form a basis for the vector space of class functions in $K[G]$. Since χ_M is a class function, it is in the linear span of $\epsilon_1, \ldots, \epsilon_k$, and the coefficients are found using the orthogonality.

Next, we look closely at a previous matrix equation to obtain more relations between the characters. We had

$$\begin{bmatrix} c_1\chi_1(C_1) & c_2\chi_1(C_2) & \ldots & c_k\chi_1(C_k) \\ c_1\chi_2(C_1) & c_2\chi_2(C_2) & \ldots & c_k\chi_2(C_k) \\ \vdots & \vdots & \ddots & \vdots \\ c_1\chi_k(C_1) & c_2\chi_k(C_2) & \ldots & c_k\chi_k(C_k) \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} & \ldots & a_{k1} \\ a_{12} & a_{22} & \ldots & a_{k2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1k} & a_{2k} & \ldots & a_{kk} \end{bmatrix} = \begin{bmatrix} n_1 & & & \\ & n_2 & & \\ & & \ddots & \\ & & & n_k \end{bmatrix}$$

Define the following matrices, all of which are invertible over K

$$\begin{aligned} M_{ij} &= \chi_j(C_i) \\ L &= \operatorname{diag}[n_1, \ldots, n_k] \\ N &= \operatorname{diag}[c_1, \ldots, c_k] \end{aligned}$$

Keep in mind that these are different from the previous M, L, N. Then the above equation translates to

$$\frac{1}{|G|}M^T N M_r L = L.$$

where M_r is as previously mentioned, the matrix M with C_i replaced by C_i^{-1}. Rearranging this gives

$$\begin{bmatrix} \chi_1(C_1^{-1}) & \chi_2(C_1^{-1}) & \ldots & \chi_k(C_1^{-1}) \\ \chi_1(C_2^{-1}) & \chi_2(C_2^{-1}) & \ldots & \chi_k(C_2^{-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_1(C_k^{-1}) & \chi_2(C_k^{-1}) & \ldots & \chi_k(C_k^{-1}) \end{bmatrix} \begin{bmatrix} \chi_1(C_1) & \chi_1(C_2) & \ldots & \chi_1(C_k) \\ \chi_2(C_1) & \chi_2(C_2) & \ldots & \chi_2(C_k) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_2(C_1) & \chi_k(C_2) & \ldots & \chi_k(C_k) \end{bmatrix} = \begin{bmatrix} \frac{|G|}{c_1} & & & \\ & \frac{|G|}{c_2} & & \\ & & \ddots & \\ & & & \frac{|G|}{c_k} \end{bmatrix}$$

which in particular means

$$\sum_{i=1}^{k}\chi_i(C_\alpha^{-1})\chi_i(C_\beta) = \begin{cases} \frac{|G|}{|C_\alpha|} = |Z(C_\alpha)| & \alpha = \beta \\ 0 & \alpha \neq \beta \end{cases}$$

where $Z(g)$ is the centralizer of $g \in G$. Here $Z(C_\alpha)$ denotes the centralizer of any element in C_α. Since conjugate elements have conjugate centralizers, the cardinality of the centralizer is unambiguous. In particular, the function

$$\frac{|C_\alpha|}{|G|}\sum_{i=1}^{k}\chi_i(C_\alpha^{-1})\chi_i \colon G \to \{0, 1\} \subset K$$

serves as an indicator function 1_{C_α} of the conjugacy class C_α.

Of course, the indicator function is itself a class function in $K[G]$. If we were to decompose it as $1_{C_\alpha} = a_1\chi_1 + \cdots + a_k\chi_k$, then

$$a_i = \frac{1}{|G|}\sum_{g\in G} 1_{C_\alpha}(g)\chi_i(g^{-1}) = \frac{|C_\alpha|}{|G|}\chi_i(C_\alpha^{-1})$$

which is exactly what we got above.

One last thing and this is directly from Amritanshu Prasad's book, specifically Exercise 1.7.17. Suppose we were to calculate the cardinality of $\{x \in C_j, y \in C_k | xy = z\}$ where C_i, C_j are fixed conjugacy classes and z is some fixed element of G. Perhaps we were to look at the coeffcient of z in some product. This then is the convolution of the indicator functions $1_{C_j}, 1_{C_k}$ at z, i.e.

$$|\{x \in C_j, y \in C_k | xy = z\}| = \sum_{xy=z} 1_{C_j}(x)1_{C_k}(y).$$

If we now substitute the expansion of $1_{C_j}, 1_{C_k}$, then, we get

$$\begin{aligned}
\sum_{x\in G} 1_{C_j}(x)1_{C_k}(x^{-1}z) &= \frac{|C_j||C_k|}{|G|^2}\sum_{x\in G}\Big(\sum_{\alpha=1}^{k}\chi_\alpha(C_j^{-1})\chi_\alpha(x)\Big)\Big(\sum_{\beta=1}^{k}\chi_\beta(C_k^{-1})\chi_\beta(x^{-1}z)\Big)\\
&= \frac{|C_j||C_k|}{|G|^2}\sum_{\alpha,\beta}\chi_\alpha(C_j^{-1})\chi_\beta(C_k^{-1})\sum_{x\in G}\chi_\alpha(x)\chi_\beta(x^{-1}z)\\
&= \frac{|C_j||C_k|}{|G|}\sum_{\alpha=1}^{k}\frac{\chi_\alpha(C_j^{-1})\chi_\alpha(C_k^{-1})\chi_\alpha(z)}{\chi_\alpha(1_G)}
\end{aligned}$$

where in the last step we used an identity from the previous subsection.

10 Conclusion

In this document I have detailed a certain development of Module Theory, Representation Theory, and Character Theory, mostly on my own but there is no such thing as originality in a subject this old. Of course, the material here is far from complete and there are lots and lots of things left to explore. Since the beginning my goal was to develop character theory and Artin-Wedderburn Theory from a place that was intuitive to me, from a perspective where every step has a motivation. It is natural to ask how to decompose a module because it helps us understand a big object as being made up of smaller objects, it is natural to ask about group representations because that's how groups first came to be, i.e. as groups of transformations of different objects (vector spaces and Lie groups, roots of polynomials and Galois groups etc).

As usual, the project had a mind of its own and went to places I hadn't anticipated, and is longer and far richer than I expected and that's a good thing. I learnt a few things on the way and I am now confident in at least the foundational aspects of the subject. This "research" of mine has opened a few doors, noncommutative ring theory, Brauer's theory, modular representations (I have completely ignored the case when $K[G]$ is not semisimple) to name a few and I hope to pursue these subjects.

Representation theory doesn't stop here, one can study the representations of S_n or study representations over $\mathbb{C}$ which is a very nice field or study modular representations, for example. Then there is also the subject of representations of Lie groups, which I have, at the time of writing (22 July 2020) no knowledge about. We can also study the ideals of $K[G]$ or more generally $R[G]$ from a ring theoretic point of view and ask purely ring theoretic questions about the rings themselves.

But I won't pursue these subjects here; this is long enough as it is. I have accomplished my goal of at least developing the subject and motivating it.

References

[1] Prasad, Amritanshu, *Representation Theory: A Combinatorial Viewpoint*, Cambridge Studies in Advanced Mathematics, vol. 147, Cambridge Univesity Press, Delhi, 2015

[2] T.Y. Lam, *A First Course in Noncommutative Ring Theory*, Springer-Verlag New York, (GTM-131), 1991

[3] W.K. Nicholson (1993), A short proof of the Wedderburn-Artin Theorem (PDF), New Zealand Journal of Mathematics, Volume 22, p. 83-86

[4] https://math.stackexchange.com/questions/49907/is-the-dual-representation-of-an-irreducible -representation-always-irreducible