# M3P8 LECTURE NOTES 11: SEMISIMPLE ALGEBRAS AND ARTIN-WEDDERBURN

## 1. The ring $R^{\mathrm{op}}$

**Definition 1.1.** Let $R$ be a noncommutative ring. Then $R^{op}$ denotes the (noncommutative) ring with the same underlying abelian group as $R$, but with the multiplication law given by $a \cdot_{R^{op}} b = b \cdot_R a$. It is known as the *opposite algebra* of $R$.

Note that $(R^{\mathrm{op}})^{\mathrm{op}} = R$, and $R^{\mathrm{op}}$ is equal to $R$ when $R$ is commutative.

It is often useful to understand $R^{\mathrm{op}}$ as an endomorphism ring, and there is a natural way to do this. Consider the ring $R$ as a left $R$-module. We can then consider the ring $\mathrm{End}_R(R)$ of left $R$-linear endomorphisms of $R$. There are many natural examples of such morphisms, coming from the *right* $R$-module structure on $R$. In particular, if $s$ is any element of $R$, then there is a map $M_s : R \to R$ of left $R$-modules defined by $M_s(r) = rs$. We can think of $M_s$ as "right multiplication by $s$"; when $R$ is not commutative note that right multiplication gives an endomorphism of left $R$-modules and vice versa! Note that $M_t(M_s(r)) = rst = M_{ts}(R)$, so that $M_t \circ M_s = M_{st}$. Thus the map: $s \mapsto M_s$ defines a homomorphism of noncommutative rings from $R^{\mathrm{op}}$ to $\mathrm{End}_R(R)$ (and *not* from $R$ to $\mathrm{End}_R(R)$ as one might naively expect!) We then have the following, trivial but surprisingly useful observation:

**Proposition 1.2.** *The map $s \mapsto M_s : R^{\mathrm{op}} \to \mathrm{End}_R(R)$ is an isomorphism.*

*Proof.* We first show it is injective. Indeed, if $M_s$ is the zero endomorphism then $M_s(1) = 0$. But $M_s(1) = s$ by definition. As for surjectivity, given $f \in \mathrm{End}_R(R)$, let $s = f(1)$. Then, as $f$ is left $R$-linear, we have $f(r) = rf(1) = rs = M_s(r)$, so $f = M_s$. □

## 2. Simple Algebras

The goal of these notes is to provide a classification of a large subclass of the simple algebras (the so-called *Artinian* simple algebras), with an eye towards applications to representation theory.

We begin by observing that any division algebra $D$ is simple, as such an algebra has no nontrivial left or right ideals, let alone two-sided ideals. In fact, more is true:

**Proposition 2.1.** *Let $D$ be any division algebra, and $n$ a positive integer. Then the ring $M_n(D)$ of $n$ by $n$ matrices with entries in $D$ is simple.*

*Proof.* We must show that any nonzero two-sided ideal of $M_n(D)$ is equal to the unit ideal. Let $I$ be a two-sided ideal of $M_n(D)$ and suppose $I$ contains a nonzero element $A \in M_n(D)$. Then for some $i, j$, an entry $a_{ij}$ of $A$ is nonzero. Let $D_i$ and $D_j$ be the diagonal matrices whose diagonal entries are all zero except for the $i$th entry, which is 1. Then $D_i A D_j$ is a matrix whose only nonzero entry is $a_{ij}$ in position $i, j$. Multiplying by a scalar matrix whose diagonal entries are all equal to $a_{ij}^{-1}$ we find that there is a matrix $B(i, j)$ in $I$ whose $i, j$ entry is 1 and all other entries are zero. If we multiply $B(i, j)$ on the left and right by suitable permutation matrices $W, W'$ we find that $WB(i, j)W'$ is the matrix $B(w(i), w'(j))$, where $w, w'$ are the permutations corresponding to $W$ and $W'$. Thus we find that $B(k, \ell)$ is in $I$ for all $1 \leq k, \ell \leq n$. Since we can express the identity as a sum of such elements $I$ must be the unit ideal. □

The converse of this statement is not true; in particular the Weyl algebra is an example of a simple algebra that is not of the form $M_n(D)$ for a division ring $D$, although we will not prove this. However, the converse becomes true with the addition of a simple extra hypothesis:

**Definition 2.2.** Let $R$ be a simple algebra. We say $R$ is *Artinian* if there exists a minimal nonzero left ideal $I$ in $R$. (That is, a nonzero ideal of $R$ such that the only ideal properly contained in $I$ is the zero ideal.)

WARNING: this is not the usual definition of Artinian. In fact, there is a notion of Artinian ring for arbitrary noncommutative rings (not just simple algebras); the definition we give above is equivalent to the usual definition for simple algebras but not in general. Nonetheless it suffices for our purposes, and giving a proper treatment of Artinian rings would take us a bit too far afield.

We then have:

**Theorem 2.3** (Artin-Wedderburn)**.** *Let $R$ be an Artinian simple algebra. Then there exists a division algebra $D$ and an integer $n$ such that $R$ is isomorphic to $M_n(D)$.*

*Proof.* Let $I$ be a minimal left ideal of $R$. Then $I$ has no left $R$-submodules other than $I$ and $\{0\}$, by definition. Thus $I$ is a simple $R$-module, and by Schur's lemma, the endomorphism ring $\mathrm{End}_R(I)$ is a division algebra $D'$. Let $D = (D')^{\mathrm{op}}$; then $D$ is also a division algebra.

Since $R$ is simple, the two-sided ideal generated by $I$ is all of $R$ (it can't be zero as $I$ is a nonzero ideal). We can thus write 1 as a sum $x_1 s_1 + \ldots x_n s_n = 1$, with $x_i \in I$ and $s_i \in R$. Let us assume we have done so in the simplest possible way (that is, with $n$ as small as possible.) In particular none of the $s_i$ or $x_i$ are zero.

Consider the map $g$ from $I^n$ to $R$ that takes $y_1, \ldots, y_n \in I$ to $y_1 s_1 + \cdots + y_n s_n$. This is a homomorphism of left $R$-modules that takes $x_1, \ldots, x_n$ to 1, and thus takes $rx_1, \ldots, rx_n$ to $r$ for any $r$. It is therefore surjective.

Suppose it were not injective. Suppose that $g(y_1, \ldots, y_n) = 0$, and that some $y_i$ (without loss of generality, say $y_1$) is nonzero. Consider the left ideal generated by $y_1$; it is contained in $I$ and nonzero, hence equals all of $I$. Thus there is some $r$ in $R$ with $ry_1 = x_1$. Then we have:

$$1 = x_1 s_1 + \cdots + x_n s_n = x_1 s_1 + \cdots + x_n s_n - (ry_1 s_1 + \ldots ry_n s_n)$$
$$= (x_2 - ry_2)s_2 + \cdots + (x_n - ry_n)s_n,$$

contradicting the minimality of $n$. It follows that $g$ is bijective; that is, $g$ yields an isomorphism of left $R$-modules: $I^n \cong R$. We then have $R \cong \mathrm{End}_R(R)^{\mathrm{op}} \cong \mathrm{End}_R(I^n)^{\mathrm{op}}$, and it remains to compute $\mathrm{End}_R(I^n)$.

Let $f : I^n \to I^n$ be an $R$-module endomorphism. Then for each $i, j$ between 1 and $n$, we can define $f_{ij} : I \to I$ by letting $f_{ij}(x)$ be the $i$th component of $xe_j$, (here $xe_j$ is the element of $I^n$ that is $x$ in position $j$ and 0 in all other positions). Each $f_{ij}$ is an $R$-linear endomorphism of $I$ and thus an element of $\mathrm{End}_R(I) = D'$. Let $M_f$ be the matrix in $M_n(D')$ whose $ij$ entry is $f_{ij}$. We then have:

$$f(x) = \sum_i (\sum_j f_{ij}(x_j))e_i = M_f x,$$

where to define $M_f x$ we consider $x$ as a column vector with entries $x_j \in I$, and "multiplication by $d \in D'$" means applying the endomorphism of $I$ that corresponds to $d$.

Note that $M_f M_{f'} = M_{f \circ f'}$, so this defines an isomorphism of $\mathrm{End}_R(I^n)$ with $M_n(D')$. Thus $R$ is isomorphic to $M_n(D')^{\mathrm{op}}$, and it is easy to check that the latter is isomorphic to $M_n(D)$. □

## 3. Finite dimensional semisimple algebras

Let $R$ be an Artinian simple algebra. The module theory of such rings has a particularly simple structure:

**Proposition 3.1.** *Let $R$ be an Artinian simple algebra. Then any left $R$-module decomposes as the direct sum of simple left $R$-modules.*

A complete proof of this proposition would require the Axiom of Choice or some equivalent of it, so we will restrict our attention to finitely generated $R$-modules. We begin by showing:

**Lemma 3.2.** *Let $D$ be a division algebra. Then any finitely generated left $D$-module is free.*

*Proof.* The proof is essentially the same as the proof that any vector space has a basis. Let $g_1, \ldots, g_n$ generate a left $D$-module $M$. If the $g_i$ are linearly independent, we are done. If not, we proceed as follows: let $r_1 g_1 + \cdots + r_n g_n = 0$ be a linear dependence, with some $r_i$ (without loss of generality, say $r_n$) nonzero. Then we can write $g_n = -r_n^{-1}(r_1 g_1 + \cdots + r_{n-1} g_{n-1})$, so $g_1, \ldots, g_{n-1}$ is also a generating set for $M$. Repeating as necessary, this

process must terminate, at which point the remaining $g_i$ are a basis for $M$. □

We now compare $D$-modules with $M_n(D)$-modules. If $M$ is a left $D$-module, then we define a left $M_n(D)$-module structure on $M^n$ by regarding an element of $M^n$ as a column vector; a matrix in $M_n(D)$ then acts on $M^n$ via matrix multiplication. Conversely, if $M$ is a left $M_n(D)$-module, let $e_1$ be the diagonal matrix with entry 1 in position $1,1$, and all other entries zero. Then $e_1M$ is a left $D$-module, where $D$ acts via scalar multiplication (note that $e_1$ commutes with scalar matrices!). It is easy to see that $M$ is isomorphic to $e_1(M^n)$. Conversely, if $M$ is a $M_n(D)$-module, then the map:

$$M \to e_1M \oplus e_2M \oplus \cdots \oplus e_nM$$

that takes $m$ to $(e_1m, e_2m, \ldots, e_nm)$ is an isomorphism, where $e_i$ is the diagonal matrix with a 1 in the $i,i$ position and all other entries zero (the inverse map is just summation!) On the other hand, $e_iM$ is isomorphic to $e_1M$ by applying a suitable permutation matrix, since (if $W$ is a permutation matrix corresponding to a permutation $w$), we have $We_iW^{-1} = e_{w(i)}$. Thus $M$ is isomorphic to $(e_1M)^n$ as $M_n(D)$-modules. This gives a bijection between isomorphism classes of $D$-modules and isomorphism classes of $M_n(D)$-modules that preserves many algebraic properties (in fact, this construction is what is known as an "equivalence of categories" between $D$-modules and $M_n(D)$-modules.)

In particular, if $M$ is a finitely generated $M_n(D)$-module, then $e_1M$ is a finitely generated $D$-module and thus has a basis $m_1, \ldots, m_r$ for some $r$; it is then not hard to check that $(m_1, m_1, \ldots, m_1), \ldots, (m_r, m_r, \ldots, m_r)$ is a basis for $(e_1M)^n$ over $M_n(D)$. Thus $(e_1M)^n$ is free over $M_n(D)$, so $M$ is a free $M_n(D)$-module.

We now turn to the proof of the propositon: if $R$ is Artinian simple, then $R$ is isomorphic to $M_n(D)$ for some $n$ and $D$. In particular any finitely generated left $R$-module is isomorphic to $M_n(D)^r$ for some $r$. But as a left $M^n(D)$-module, $M^n(D)$ is the direct sum of $n$ copies of the simple left $M^n(D)$-module $D^n$, so the proposition follows.

**Definition 3.3.** A noncommutative ring $R$ is *semisimple* if every left $R$-module decomposes as a direct sum of simple left $R$-modules.

We have thus shown that $M_n(D)$ is semisimple for $D$ is a division ring. More generally, if $R$ and $S$ are rings and $M$ is a left $R \times S$-module, then $M$ is isomorphic to a product $N \times N'$, where $N$ is a left $R$-module and $N'$ is a left $S$-module. The simple $R \times S$-modules are those of the form $N \times \{0\}$, where $N$ is a simple left $R$-module, and those of the form $\{0\} \times N'$, where $N'$ is a simple left $S$-module. Thus if $R$ and $S$ are semisimple, then $R \times S$ is semsimple. In particular, arbitrary products of semisimple rings are semisimple.

There is a partial converse to this:

**Proposition 3.4.** *Let $R$ be a noncommutative ring whose center contains a field $K$, and suppose that $R$ is semisimple and finite dimensional over $K$. Then $R$ is isomorphic to a product $\prod_i M_{n_i}(D_i)$ for some integers $n_i$ and division algebras $D_i$.*

*Proof.* Consider $R$ as a left $R$-module, and write $R$ as a finite direct sum $\oplus_{i=1}^r M_i^{n_i}$, where each $M_i$ is simple and the $M_i$ are pairwise non-isomorphic. We have

$$R \cong \mathrm{End}_R(R)^{\mathrm{op}} \cong \mathrm{End}_R(\oplus_{i=1}^r (M_i)^{n_i}).$$

But there are no nonzero maps from $M_i$ to $M_j$ for $i \neq j$, hence no nonzero maps from $(M_i)^{n_i}$ to $(M_j)^{n_j}$ for $i \neq j$. Thus any endomorphism of $\oplus_{i=1}^r (M_i)^{n_i}$ preserves each summand; that is, it is given by an $r$-tuple of endomorphisms $f_1, \ldots, f_r$, with $f_i \in \mathrm{End}_R((M_i)^{n_i})$. Let $D_i'$ be the endomorphism ring of $M_i$; since $M_i$ is simple this is a division algebra by Schur's lemma. Then $\mathrm{End}_R((M_i)^{n_i})$ is isomorphic to $M_{n_i}(D_i')$. Thus

$$R \cong \mathrm{End}_R(R)^{\mathrm{op}} \cong \prod_i M_{n_i}(D_i),$$

where $D_i = (D_i')^{\mathrm{op}}$ and the claim follows. □

## 4. Group rings and Maschke's theorem

A very important class of semisimple rings comes from representation theory. Let $G$ be a finite group, of $N$ elements, and let $K$ be a field in which $N$ is invertible (that is, the characteristic of $K$ does not divide $N$). We can then consider the group ring $K[G]$ (see the previous set of notes.)

Before we show that $K[G]$ is semisimple, we first point out the connection between $K[G]$ and representation theory.

**Definition 4.1.** A *representation* of $G$ over $K$ is a homomorphism $f$ from $G$ to the matrix group $\mathrm{GL}_n(K)$ of $n$ by $n$ matrices with entries in $K$. Two representations $f, f'$ are *equivalent* if there is a matrix $A \in \mathrm{GL}_n(K)$ such that $f(g) = Af'(g)A^{-1}$ for all $g \in G$.

There is a natural correspondence between representations of $G$ over $K$ and left $K[G]$-modules that are finite dimensional when considered as $K$-vector spaces.

First, given a representation $f : G \to \mathrm{GL}_n(K)$, we can form a $K[G]$-module $M_f$, whose underlying $K$-vector space is $K^n$, and for which

$$(\sum r_g g) \cdot m = \sum r_g f(g) m,$$

for $r_g \in K$ and $m \in K^n$. Note that if $f$ is equivalent to $f'$, then the matrix $A$ such that $f(g) = Af'(g)A^{-1}$ gives an isomorphism from $M_f$ to $M_{f'}$. Conversely, if one has an isomorphism of $M_f'$ with $M_f$, then (since the underlying vector spaces of both modules are $K^n$), this isomorphism is given by a matrix $A$ such that $f(g) = Af'(g)A^{-1}$ for all $g$.

In the other direction, if we start with a $K[G]$-module $M$, then for all $g \in G$, "multiplication by $g$" gives a $K$-linear map from $M$ to $M$. Fix a choice of basis for $M$; then "multiplication by $g$" is given by a matrix $A_g \in \mathrm{GL}_n(K)$. Define $f : G \to \mathrm{GL}_n(K)$ by $f(g) = A_g$; then $f$ is a homomorphism, so this gives rise to a representation of $G$ over $K$. Note that if we had chosen a different basis, and obtained a different map $f'$, then the change of basis matrix $A$ satisfies $f(g) = Af'(g)A^{-1}$, so up to equivalence the representation associated to $M$ is independent of choices.

We say a representation $f : G \to \mathrm{GL}_n(K)$ is *irreducible* if the attached $K[G]$-module $M_f$ is simple.

We now show:

**Theorem 4.2** (Maschke's Theorem)**.** *Let $G$ be a finite group and $K$ a field in which the order of $G$ is invertible. Then every finitely generated left $K[G]$-module is a direct sum of simple left $K[G]$-modules.*

*Proof.* Let $M$ be a finitely generated $K[G]$-module. Then $M$ is finite-dimensional as a $K$-vector space (if $m_1, \ldots, m_r$ generate $M$ over $K[G]$, then the set $\{gm_i : g \in G, 1 \leq i \leq r\}$ spans $M$ over $K$). Let $V$ be a nonzero $K[G]$-submodule of $M$ of lowest possible dimension. Then $V$ is simple (any proper left $K[G]$-submodule of $V$ would be a submodule of $M$ of smaller dimension). Let $W$ be any $K$-subspace of $M$ complementary to $V$, and let $\pi : M \to V$ be the projection onto $V$ with kernel $W$; that is, the unique $K$-linear map $M \to V$ such that $\pi(v) = v$ for all $v \in V$ and $\pi(w) = 0$ for all $w \in W$. The map $\pi$ will (usually) not be $K[G]$-linear. Define

$$\pi'(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gv).$$

Note that $\pi'(v) = v$ for all $v \in V$, and, for any $m \in M$, and $h \in G$ we have:

$$\pi'(hm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(ghm) = \frac{1}{|G|} \sum_{g' \in G} (g'h^{-1})^{-1}\pi(g'm) = h\pi'(m).$$

Thus $\pi'$ is a homomorphism of $K[G]$-modules. Let $W'$ be its kernel. We have a map:

$$M \to V \oplus W'$$

of $K[G]$-modules that takes $m$ to $(\pi'(m), m - \pi'(m))$; the inverse map takes $(v, w)$ to $v + w$. Thus $M$ is isomorphic to $V \oplus W'$ with $V$ simple. Applying the same argument to $W'$ and proceeding inductively gives a decomposition of $M$ into simple left $K[G]$-modules. □

**Corollary 4.3.** *Let $G$ be a finite group and $K$ a field in which the order of $G$ is invertible. Then there are integers $n_i$, and division algebras $D_i$ that contain $K$ in their centers, such that $K[G]$ is isomorphic to the product $\prod_i M_{n_i}(D_i)$.*

In terms of representations $f : G \to \mathrm{GL}_n(K)$, rather than modules $M_f$, Maschke's theorem states that "every representation of $G$ is a direct sum

of irreducible representations", which is the starting point of representation theory. If the characteristic of $K$ divides the order of $G$, Maschke's theorem fails completely (think about $\mathbb{F}_p[G]$ where $G$ is cyclic of order $p$ for an example) and representation theory becomes much harder; the study of representations of $G$ in situations where Maschke's theorem fails is called "modular representation theory" and is very much an area of active research.

We conclude with an example: recall that the *quaternion group* $Q_8$ is the subgroup of $\mathbb{H}^\times$ consisting of the eight elements $\{\pm 1, \pm i, \pm j, \pm k\}$, and consider the ring $\mathbb{R}[Q_8]$. In this case, we have a product decomposition:

$$\mathbb{R}[Q_8] \mapsto \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}.$$

Indeed, we can write the isomorphism as follows: for $r \in \mathbb{R}[Q_8]$ given by:

$$r = r_1 + r_{-1}(-1) + r_i i + r_{-i}(-i) + r_j j + r_{-j}(-j) + r_k k + r_{-k}(-k)$$

we can define $\chi_1, \chi_i, \chi_j, \chi_k : \mathbb{R}[Q_8] \to \mathbb{R}$ by:

$$\begin{aligned}
\chi_1(r) &= r_1 + r_{-1} + r_i + r_{-i} + r_j + r_{-j} + r_k + r_{-k} \\
\chi_i(r) &= r_1 + r_{-1} + r_i + r_{-i} - r_j - r_{-j} - r_k - r_{-k} \\
\chi_j(r) &= r_1 + r_{-1} - r_i - r_{-i} + r_j + r_{-j} - r_k - r_{-k} \\
\chi_k(r) &= r_1 + r_{-1} - r_i - r_{-i} - r_j - r_{-j} + r_k + r_{-k}
\end{aligned}$$

(These homomorphisms correspond to the one-dimensional real representations of $Q_8$. We can also define $\tau : \mathbb{R}[Q_8] \to \mathbb{H}$ by:

$$\tau(r) = (r_1 - r_{-1}) + (r_i - r_{-i})i + (r_j - r_{-j})j + (r_k - r_{-k})k.$$

Then the isomorphism

$$\mathbb{R}[Q_8] \mapsto \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}.$$

takes $r$ to $(\chi_1(r), \chi_i(r), \chi_j(r), \chi_k(r), \tau(r))$.

The homomorphism $\tau : \mathbb{R}[Q_8] \to \mathbb{H}$ makes $\mathbb{H}$ into a simple left $\mathbb{R}[Q_8]$-module; it corresponds to the four-dimensional real representation of $Q_8$ that takes $g \in Q_8$ to the matrix of "left multiplication by $g$" on the four-dimensional real vector space $\mathbb{H}$.