A FLAVOUR OF NONCOMMUTATIVE ALGEBRA (PART 2)

VIPUL NAIK

Abstract. This is the second part of a two-part series intended to give the author and readers a flavour of noncommutative algebra. The material is related to topics covered in math 325, a graduate algebra course taught by Professor Ginzburg at the University of Chicago. The author would like to thank Emily Riehl and Michael P. Miller for their comments and suggestions, and other first-year students for their counterexamples.

1. The story for semisimple Artinian rings

1.1. Definition of semisimple Artinian.

Definition (Semisimple Artinian ring)**.** A ring is said to be **semisimple Artinian**(defined) if it is semisimple as a left module over itself.

To explore this a bit more, a quick observation:

Claim. If M is a finitely generated semisimple left R-module, then M is semisimple of finite length over R. In particular if R is semisimple as a left module over itself, then R is semisimple of finite length.

Note that without the assumption of semisimplicity, this result is false: for instance, $\mathbb{Z}$ is finitely generated, but has infinite length as a module over itself.

However, note that we are *not* assuming here that R is Artinian. If R were Artinian, we could drop the hypothesis that M is semisimple – the result would then be true for *any* finitely generated module (this was observed in part 1).

Proof. Express M as a direct sum of simple left modules, and pick a finite generating set for M. Each of the elements of this finite generating set can be expressed as finite linear combinations of elements from the summands. Thus, only finitely many summands suffice to express all the generators. From this, it follows that finitely many summands generate M, hence M is a direct sum of finitely many simple modules. □

Thus a ring which is semisimple as a left module over itself is actually semisimple of finite length, from which it follows that it is Artinian as a left module over itself. This justifies the terminology “semisimple Artinian”.

1.2. What makes life simple for Artinian rings.

We had defined a “left-Artinian ring” as a ring in which any descending chain of left ideals stabilized. After a point, we conveniently forgot to tag along the “left”. That’s for good reason: “left-Artinian” and “right-Artinian” mean the same thing. Here’s a theorem, parts of which we have proved:

Theorem 1 (Characterizations of Artinian ring)**.** Let R be a ring. The following are equivalent:

- R is left-Artinian as a left module over itself
- R is right-Artinian as a right module over itself
- R has finite length as a left module over itself
- R has finite length as a right module over itself

- The quotient of R by its Jacobson radical is semisimple of finite length as a R-module[1] and the Jacobson radical of R is nilpotent.

Thus, there are two ways in which Artinian rings are more tractable than ordinary rings:

- The *bottom is light*: The Jacobson radical is nilpotent.
- The *top is light*: The top of an Artinian ring is semisimple of finite length as a module over itself.

Since the two sources of complexity, namely the top and the bottom, are relatively nice for Artinian rings, we might expect Artinian rings to be a piece of cake. In fact, they are far from that, because terrible complexities could lie at the bottom. However, the *top*, viz., the quotient by the Jacobson radical, is relatively good.

We take a short break and journey into the exotic world of Galois correspondences.

2. The double centralizer property

2.1. **A quick note on Galois correspondences.** Let's forget about rings and do some set theory for a few moments (alas, only a few moments). Suppose A and B are two sets and $R \subset A \times B$ is a "binary relation". Then we can define maps $F : 2^A \to 2^B$ and $G : 2^B \to 2^A$ as follows:

$$\begin{aligned} F(S) &= \{b \in B | (a,b) \in R \ \forall \ a \in S\} \\ G(T) &= \{a \in A | (a,b) \in R \ \forall \ b \in T\} \end{aligned}$$

Such a setup is a **Galois correspondence**(defined).

Theorem 2 (The big theorem of Galois correspondences)**.** (1) F and G are *contravariant*[2], in the sense that if $S \subset S'$ then $F(S') \subset F(S)$ and similarly for G.

(2) $S \subset G(F(S))$ and $T \subset F(G(T))$ for all $S \subset A$, $T \subset B$.

(3) $F \circ G \circ F = F$ and $G \circ F \circ G = G$.

(3) follows from (1) and (2), and both (1) and (2) are easy to check. In isolation (3) would have seemed hard; and though it is easy to check when written as above, it is still pretty miraculous.

Intuitively, when we do $G \circ F$ then we're going to *everything which is related to everything which is related* to what we started out with. And doing $G \circ F$ yet again has no effect; hence $G \circ F$ is a kind of *closure* operator. The million-dollar question is:

> What are the subsets S of A for which $G(F(S)) = S$; what are the subsets T of B for which $F(G(T)) = T$? In other words, what are the *closed* subsets of A and of B?[3]

While we're having fun, let's look at three examples of Galois correspondences, the first in honour of the man behind the very first Galois correspondence, and the second and third because they are directly relevant to what we're doing here:

1. Consider a Galois field extension L/K and let G be its Galois group. Then define the following binary relation between G and L, $g \in G$ is related to $a \in L$ if g fixes a.

   The fundamental theorem of Galois theory states that the closed sets in L are precisely the subfields containing K and the closed sets in G are precisely the subgroups of G (in fact, it says a lot more, but LNGITRN).
2. Consider the polynomial ring $\mathbf{k}[x_1, x_2, \ldots, x_n]$ and the space $\mathbf{k}^n$ of n-tuples over $\mathbf{k}$. Elements of $\mathbf{k}[x_1, x_2, \ldots, x_n]$ define maps from $\mathbf{k}^n$ to $\mathbf{k}$ by *evaluating a polynomial.* The relation between $\mathbf{k}[x_1, x_2, \ldots, x_n]$ and $\mathbf{k}^n$ is defined as follows: $p \in \mathbf{k}[x_1, x_2, \ldots, x_n]$ is related to $v \in \mathbf{k}^n$ iff $p(v) = 0$.

   One of the many versions of Hilbert's nullstellensatz says that when $\mathbf{k}$ is algebraically closed, a set is closed in $\mathbf{k}[x_1, x_2, \ldots, x_n]$ iff it is a radical ideal.

[1] The "finite length" part can be dropped; it's automatic

[2] For the category theorist: F and G are contravariant as functors between the categories of subsets of A and of B; this suggests a natural way to generalize the notion of "Galois correspondence" to arbitrary categories

[3] The "closed" subsets need not correspond to closed subsets for any topology; for that, we need the extra condition that a finite union of closed sets is closed. This condition does not hold for many Galois correspondences; it certainly fails on the "algebraic" side.

(3) Let R be a (noncommutative) ring. Define a binary relation between R and R as follows: x is related to y if $xy = yx$, viz., they *commute*.

The question about which subrings of R are closed in the induced Galois correspondence will haunt us for the next few subsections. It's worth noting that the binary relation is symmetric, so the "closed" subsets on one side are the same as the closed subsets on the other side.

2.2. The centralizer and double centralizer.

Definition (Centralizer of a subset)**.** Given a subset of a ring, the **centralizer**(defined) of the subset in the ring is defined as the set of all elements of the ring which commute with that subset.

In the language of Galois correspondences, it is the Galois correspondent to the given subset for the binary relation of commuting. The centralizer of any subset is a subring.

From the abstract nonsense[4] of Galois correspondences we see immediately that the following are equivalent:

- A subring occurs as the centralizer of some subring
- A subring is the centralizer of its centralizer
- A subring is "closed" in the sense of the Galois correspondence described above

When we have a lot of equivalent things, it's natural to introduce a definition, so let's do that:

Definition (Double-centralizer property)**.** A subring of a ring is said to have the **double-centralizer property**(defined) if it equals the centralizer of its centralizer (also called its double-centralizer).

Subrings with the double-centralizer property can be viewed as "closed" in a suitable topological sense.

2.3. **A topological analogy.** So far, the three examples of Galois correspondences we outlined were algebraic. There's a topological example of a Galois correspondence which comes from inner product spaces: the relation here is that of being *orthogonal.* We know that for any subspace A of an inner product space V, A is contained in $A^{\perp\perp}$, the containment may in general be strict.

This example also lends more credibility to the notion of closed; for instance, it is known that in a Hilbert space, a subspace equals the orthogonal complement of its orthogonal complement iff it is "closed" in a topological sense. Further, we know that for finite-dimensional spaces, every linear subspace is closed.

Even if a subspace is *not* closed, we know that its double-perp subspace equals its closure in a topological sense. In other words, any subspace is dense in its double-perp, and in the finite-dimensional case, that forces it to be closed. We shall see something similar happen in the finite-dimensional case. Subrings which satisfy certain "nice" hypotheses shall be discovered to be "dense" in their double-centralizers, and if we impose finiteness assumptions, then that will force them to have the double-centralizer property.

2.4. **So what subrings have the DCP?.** A good starting point: what subrings of a ring have the double-centralizer property? Here are some quick observations:

(1) The double-centralizer of any subring contained *inside* the center is the whole center. In particular, the only subring inside the center, which has the double-centralizer property, is the whole center.
(2) If the centralizer of a subring is precisely the center, then its double-centralizer is the whole ring. The whole ring is thus another subring which has the double-centralizer property.
(3) Any subring that has the double-centralizer property must contain the center.

The canonical example to keep in mind is the matrix ring over a field: here the center is the scalar matrices, and the whole ring is all matrices.

Thus the center and the whole ring are two extreme examples; there are in general other examples. For instance:

[4] A term that category theorists, model theorists and other mathematicians use in self-derisive humour for anything that is considerably more general than the situation at hand demands

(1) Suppose L is a field extension of K of degree n. Then L acts on the vector space K^n (once we choose a basis thereof); this gives an injective ring homomorphism from L to $M_n(K)$. A quick check yields that L is its own centralizer in $M_n(K)$, hence it has the double-centralizer property.
(2) Consider the ring of diagonal matrices over a field K, of order n. This ring is again its own centralizer, and hence its own double-centralizer.
(3) On the other hand, the ring of upper-triangular matrices does *not* have the double-centralizer property; in fact, its centralizer is the scalar matrices (at least over large enough fields).

Each of the examples (1)-(3) is distinct in flavour, as some more exploration shall reveal.

2.5. **Modules and double centralizers.** Suppose R is a ring and M is a left R-module. Then M is, first and foremost, an Abelian group, and left multiplication by any element of R yields an Abelian group endomorphism of M. We have a map:

$$R \to \operatorname{End}_{\mathbb{Z}}(M)$$

This map is a ring homomorphism (in fact the definition of module was designed to make it so). A few points to note here:

- This is analogous to the fact that when a group acts on a set, we get a homomorphism from the group to the symmetric group on that set.
- The kernel of the map is precisely the annihilator of the module M (does that ring a bell? If not, time to go back to part 1!), and the image is isomorphic to the quotient of R by the annihilator of M (which is a *two-sided* ideal).
- M is faithful as a R-module iff the above ring homomorphism is injective, viz., if R embeds into $\operatorname{End}_{\mathbb{Z}}(M)$.
- Even if M is not faithful as a R-module, we can view M as a faithful R_M-module where R_M is the quotient of R by the annihilator of M. For all *practical* purposes, M only "sees" R_M – what R is at large does not affect M.

Remember that for now, every map in the world is a homomorphism of Abelian groups: any map that isn't is anathema to us. Now the ring $\operatorname{End}_R(M)$ is a subring of $\operatorname{End}_{\mathbb{Z}}(M)$, and we can in fact characterize it purely ring-theoretically: it is the centralizer in $\operatorname{End}_{\mathbb{Z}}(M)$ of R_M (the image of R in $\operatorname{End}_{\mathbb{Z}}(M)$).

Definition (Double-centralizer property)**.** A left module M over a ring R is said to have the **double-centralizer property for modules**(defined) if the ring R_M (the image of R in $\operatorname{End}_{\mathbb{Z}}(M)$) has the double-centralizer property. In effect, what this means is that the only Abelian group endomorphisms of M, which commute with all endomorphisms, are precisely those coming from elements of R.

2.6. **Left, right, left.** The typical way we think of the double-centralizer property is by left and right actions. The left-right headache is confusing but it's also illuminating and character-building. I'll begin by defining a bimodule.

Definition (Bimodule)**.** Let R, S be rings. A (R, S)-**bimodule**(defined) is an Abelian group M endowed with the structure of a left R-module and a right S-module, such that for any $r \in R$, $s \in S$ and $m \in M$ we have:

$$(rm)s = r(ms)$$

Phrased in the above way, this looks like an associativity condition, but let's not get misled by that! Some facts:

- A right S-module is equivalent to a left S^{op}-module. Here S^{op} denotes the opposite ring, which I described in Part 1.
- A (R, S)-bimodule can be viewed as an Abelian group M which is a left module over both R and S^{op} such that the images of R and S^{op} inside $\operatorname{End}_{\mathbb{Z}}(M)$ commute element-wise. In other words "associativity" becomes "commutativity" when one switches right to left.

Thinking of things in the bimodule language is sometimes helpful when we want to quickly find operators which centralize a given ring. The classical example is the matrix ring $M_n(R)$ over a (possibly) noncommutative ring R, acting on the module $M = R^n$ by the usual left multiplication of a matrix with a column vector.

We can turn $M = R^n$ into a $(M_n(R), R)$-bimodule where $M_n(R)$ acts by left multiplication (as $n \times n$ matrices) and R acts as right multiplication (as 1×1 matrices). Associativity of matrix multiplication tells us that we indeed have a bimodule, and using the "opposite" stuff mentioned above, we see that R^n is a left R^{op}-module and a left $M_n(R)$-module and the images of both of these in $\text{End}_{\mathbb{Z}}(R^n)$ commute (it is actually a faithful module for both, so the images are the same as the rings themselves).

When R is a *commutative* ring, *right* multiplication by a scalar element corresponds to left multiplication by the *same* scalar matrix, and this is the popular statement that scalars live inside the center of the matrix ring. However, now that the ring is noncommutative, right multiplication is the correct way to think of things.

2.7. **Generalities and specifics.** A list of facts, which, as usual, are not hard to prove them once they're pointed out, but are hard to mechanically come up with:

- If R is a commutative ring, and M is R as a R-module, the centralizer of R in $\text{End}_{\mathbb{Z}}(M)$ contains R. Another way of thinking of it is that the centralizer contains *right* multiplication by elements of R, but right multiplication is the same as left multiplication.
- If R is any ring, and M is R as a R-module, the centralizer of R is *precisely* R^{op}. This may or may not in general be isomorphic to R; rings R which are isomorphic to their opposite ring were called self-opposite in part 1; examples are matrix rings over commutative rings.
- The *intersection* of R with R^{op}, viz., those elements of R which commute with all elements of R, are precisely the *center* of R. Here *intersection* is understood to mean intersection as subrings of $\text{End}_{\mathbb{Z}}(M)$.

2.8. **Back to the old story.** In Part 1, we considered in detail the following problem: given a module over a ring, relate conditions on the module to conditions on the endomorphism ring. We are now trying to complete the triad: relate the original ring, the module on it, and the endomorphism ring. The real question we're after is whether the ring we start with can *itself* be obtained as an endomorphism ring. Clearly, if we were to somehow achieve this, then we would have imposed significant structural constraints on our ring. This is where the double-centralizer property comes in.

For example, if M were an R-module with the double-centralizer property, and if it were further true that M is *semisimple of finite length* as a module over the endomorphism ring, then we've obtained R as the endomorphism ring of a semisimple module of finite length. In Part 1, we proved that the endomorphism ring of any semisimple module of finite length is a direct sum of matrix rings over division rings.

So the million-dollar question: under what condition can we guarantee the existence of such a nice module?

2.9. **Glimpses of the answer.** One answer is to impose conditions such that:

- R is semisimple as a module over itself; and it turns out then that it's also semisimple as a module over R^{op}.
- R has the double-centralizer property as a module over itself.

2.10. **Jacobson density theorem.** The Jacobson density theorem is an extremely important result; its applications and analogues are useful in applications beyond what we'll discuss here. So it's unfortunate that we are giving only a passing mention to it.

Definition (Dense subring)**.** Let M be a left S-module and R be a subring of S. We say that R is a **dense subring**(defined) of S (with respect to the module M) if for any finite collection of elements $m_1, m_2, \dots, m_n$, and any element s, there exists an element r such that $r.m_i = s.m_i$ for $1 \leq i \leq n$.

One way of viewing this is that as far as the effect on finitely many elements goes, there is no way of distinguishing R from S. If M is a *finitely generated* S-module, then this forces $R_M = S_M$.

Theorem 3 (Jacobson density theorem)**.** Given any faithful left module over a ring, the ring is a dense subring of its double-centralizer with respect to that module. More generally, if M is a left R-module, then R_M is a dense subring of its double centralizer in $\mathrm{End}_{\mathbb{Z}}(M)$.

A corollary of this is that if M is a finitely generated R-module, then R has the double-centralizer property.

2.11. **Glimpses of Wedderburn theory.** Suppose R were semisimple of finite length as a module over itself. Note that R as a module over R^{op} is certainly finitely generated (in fact, it's free of rank 1). Then Jacobson density would yield that R equals its double centralizer, and from what we've seen earlier, R is the endomorphism ring of a semisimple module of finite length over R^{op}. Hence R is a direct sum of matrix rings over division rings. Proof!

So the real question is: under what conditions is R semisimple as a module of finite length over itself? It turns out that this is equivalent to the definition of semisimple Artinian ring we gave earlier: R is Artinian and its Jacobson radical is 0 (we won't sketch a proof here). Here are some counterexamples:

- The ring $\mathbb{Z}$ is neither semisimple nor Artinian. In fact given any sequence of integers $a_1, a_2, \dots, a_n$ we have a descending chain of ideals whose n^{th} element is the ideal generated by $a_1 a_2 \dots a_n$.
- A countable direct sum of copies of a simple ring is semisimple (in fact isotypical) but it is not Artinian, and it doesn't have finite length over itself.
- The ring $\mathbb{Z}/p^k\mathbb{Z}$ is Artinian but it is *not* semisimple as a module over itself. The only simple modules over this ring are $\mathbb{Z}/p\mathbb{Z}$s, and $\mathbb{Z}/p^k\mathbb{Z}$ is not a direct sum of these.

2.12. **Simple Artinian rings.** Semisimple Artinian rings are direct sums of matrix rings over division rings, and each of the matrix rings over division rings is a *simple* Artinian ring. Here we mean it's simple as a ring: it has no proper nonzero two-sided ideals. There is a natural left module for such a simple Artinian ring: the left vector space of order n over the division ring, with usual matrix multiplication. If D is the underlying division ring, the centralizer of $M_n(D)$ is D^{op} – right multiplication by elements of D.

A direct sum of such simple Artinian rings does not have any faithful simple modules of its own. In fact, if:

$$R = M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \dots \oplus M_{n_k}(D_k)$$

Then the following are true:

- The above is the unique decomposition of R as a sum of minimal two-sided ideals.
- From a minimal two-sided ideal $M_{n_i}(D_i)$ both n_i and D_i can be recovered. D_i is recovered by looking at the centralizer, which is D_i^{op}, and n_i is recovered by the fact that matrix rings of different orders are non-isomorphic.
- Any faithful simple module over R must be annihilated by all but one of the summands, and for that one summand, it looks just like the natural module described above. In other words, a semisimple Artinian ring is left-primitive iff it is simple.

In upshot, the following are equivalent:

Simple Artinian $\iff$ Left-primitive Artinian $\iff$ Right-primitive Artinian $\iff$ matrix ring over division ring

The notions of being simple, left-primitive, and right-primitive could be very different for non-Artinian rings.

2.13. **Jacobson radical for Artinian rings.** What we've seen is that the tops of Artinian rings behave nicely: they're semisimple in more ways than one; they're direct sums of matrix rings over division rings. Using this, we can give many alternative characterizations of the Jacobson radical for Artinian rings:

(1) The Jacobson radical is the intersection of all maximal *two-sided* ideals.
(2) The Jacobson radical is the smallest ideal for which the quotient is "semisimple of finite length" as a module over the ring.

After treating ourselves to some offbeat topics, we shall take a look at how these equivalences and implications fail for the non-Artinian case.

3. Spectral theory and Amitsur theory

3.1. **The spectrum of an element.** At one point in time, we were looking at questions like: how close are elements ab and ba in an arbitrary ring? We had noted that when either a or b is invertible, they are conjugates and hence behave practically in the same way. Otherwise ab and ba could differ in significant ways; however, we had noted that if z is a central invertible element then $z - ab$ is invertible iff $z - ba$ is invertible.

All this, and a lot more, fits nicely into a framework called spectral theory. The idea is to switch to a base field and look at algebras whose center contains that field. Nonzero elements of the field are central invertibles.

Definition (Spectrum of an element)**.** Let R be a $\mathbf{k}$-algebra. The spectrum of an element $a \in R$ is defined as the set of all $z \in \mathbf{k}$ such that $a - z$ (or equivalently, $z - a$) is *not* invertible.[5]

For instance, when R is the matrix ring over $\mathbf{k}$, then the spectrum of R is the set of roots in $\mathbf{k}$ of the characteristic polynomial of a (which is also the same as the set of roots of the minimal polynomial). The letter z is suggestive of complex analysis, and indeed, one can think of the spectrum as the set of points where the function $(z - a)^{-1}$ has a "pole".

The observation we made earlier can be recast in the following manner: if x and y are weakly conjugate elements of R (viz, there exist $a, b \in R$ such that $x = ab$ and $y = ba$) then x and y have the same spectrum. The relation of having the same spectrum is an *equivalence* relation while the relation of being weakly conjugate isn't. So in fact if two elements are equivalent via the equivalence relation generated by being weakly conjugate, then they have the same spectrum.

Another fact of note is that the spectrum of a nilpotent element contains only the element 0: this is due to the explicit formula for inverting $1 - x$ as $1 + x + x^2 + \dots$. One can view nilpotent elements as poles of infinite multiplicity; they're so bad that everything else has to be good.

Putting together our fun observations:

- Any element weakly conjugate to a nilpotent element is nilpotent. In particular, the set of nilpotent elements (remember, it's a set now; no longer closed under addition or multiplication) is closed under the relation of being weakly conjugate; nothing inside is weakly conjugate to anything outside.
- All nilpotent elements have the same spectrum: the one-point set $\{0\}$.
- In general, it may not be true that given any two nilpotent elements a and b, I can find $a = a_1, a_2, \dots, a_n = b$ such that a_i is weakly conjugate to a_{i+1}. However, for a matrix ring over $\mathbf{k}$, this can always be done. The number of steps could be quite huge: for instance, to reach from 0 to an element whose n^{th} power is 0 requires at least n steps, because in each step we can change the nilpotence by only 1.

3.2. **Invertibles and zero divisors.** Again, going back to the fun game we had in Part 1: we had seen that invertible elements can't be zero divisors, and zero divisors can't be invertible. Moreover, if something is a zero divisor, there is no hope that it may become invertible in a suitably enlarged ring. We had looked at three types of elements:

(1) The left-invertible elements
(2) The left-zero divisors
(3) The elements that are neither left-invertible nor left-zero divisors, viz., the left-cancellative elements that are not left-invertible.

Now a question: what can we say about rings for which there are no elements of type (3)? Such rings are definitely very nice. The cool thing about such rings is that elements which are not invertible continue to remain non-invertible in bigger rings.

It would be even nicer if every element either had a two-sided inverse or was *both* a left *and* a right zero divisor. I don't know a name for such rings. Since I'll be referring to these rings a lot, I'll give them a name of my own.

[5] Invertibility means the existence of a "two-sided" inverse.

Definition (IZ-ring)**.** A ring is termed a **IZ- ring**(defined) if for every element of the ring, one of the following holds:

- The element has a two-sided inverse
- The element is both a left and a right zero divisor

IZ stands for "invertible or zero divisor".

The polynomial ring in one variable is an example of a ring which is *not* IZ.

For IZ-rings, the zero divisors need not in general form a two-sided ideal. In the particular case that every element is either invertible or *nilpotent*, it is true that the nilpotents form a two-sided ideal. (Such rings were termed completely primary in part 1). However, a sum of zero divisors need not be a zero divisor in a noncommutative ring.

We thus have the following implications:

- Field $\implies$ Division ring $\implies$ Completely primary ring $\implies$ IZ-ring
- Field $\implies$ Division ring $\implies$ Completely primary ring $\implies$ Local ring

IZ and local are incomparable. The matrix ring over a field is IZ but not local, whereas the ring $\mathbf{k}[[x]]$ is local but not IZ.

Let's prove our first big result:

Theorem 4. Every Artinian ring is IZ.

There are two proofs of this: one proof uses the Artin-Wedderburn theorem; the other proves things directly from the definition of Artinianness. I'll give the latter proof because it illustrates some basic ideas.

Proof. Suppose R is an Artinian ring and $x \in R$. I will first show, from the fact that R is *left-Artinian*, that x is either left-invertible or a *right* zero divisor.

Consider the descending chain of R-submodules:

$$R \supset Rx \supset Rx^2 \supset \dots$$

This chain must stabilize at some point, so we have $Rx^n = Rx^{n+1}$. This yields $a \in R$ such that $ax^{n+1} = x^n$. Rearranging gives:

$$(1 - ax)x^n = 0$$

If $1 - ax = 0$, x has a left inverse. Otherwise, x is a right-zero divisor.

A similar proof shows that since R is *right-Artinian*, x is either right-invertible or a *left* zero divisor.

Now an element which has a left inverse cannot be a left zero divisor, and an element which has a right inverse cannot be a right zero divisor. Thus, the only possibilities are:

- x has a left inverse and a right inverse. Thus, x has a two-sided inverse.
- x is both a left-zero divisor and a right-zero divisor.

This proves that R is an IZ-ring. □

Thus, being an IZ-ring reflects "finiteness" of some sort. Here are some special cases where one could explicitly work out the above proof:

- The case where R is a finite ring. In this case, one simply looks at the powers of x and waits till one finds two equal powers.
- The case where R is a finite-dimensional algebra over a field. In this case one finds a minimal polynomial for any element of R and uses that minimal polynomial to show that the given element is either invertible or a zero divisor.

The above examples also indicate that IZ-rings need not be Artinian. Indeed, all one needs to ensure is that the ring "locally" looks Artinian at every point. Here are some examples:

- Consider the exterior algebra in infinitely many variables. This is an IZ-ring; in fact it is a completely primary ring where every element in the maximal ideal has 0 as its square. However, the maximal ideal is not nilpotent (precisely because there are infinitely many variables).

Nonetheless, for any *specific* element, it lies inside the exterior algebra on finitely many variables, and hence is either invertible or a zero divisor.

- More generally, any ring constructed as a direct limit of IZ-rings is an IZ-ring. Since the property of being Artinian is certainly not preserved on taking direct limits, there are plenty of IZ-rings which are not Artinian.

IZ-rings are the opposite of integral domains:

Definition (Integral domain)**.** A ring is termed an integral domain if no nonzero element is a zero divisor.

Note that the only IZ-rings which are integral domains are division rings. Thus, an integral domain must be non-Artinian unless it is a division ring.

Another interesting fact is that integral domains are indecomposable. This follows from the fact that any nontrivial idempotent e is a zero divisor: $e(1-e) = 0$.

3.3. **The spectral theorem of Amitsur.** The main result of spectral theory that Amitsur proved essentially shows that most of the elements remain of type (3) for non-algebraic elements(actually the precise theorem we state involves two-sided inverses, but there are variants of all sorts). In other words, extensions which are not algebraic over their base field, are as far as possible from being IZ.

Let A be a $\mathbf{k}$-algebra. Suppose $a \in A$. Then evaluation at a gives a homomorphism from $\mathbf{k}[x]$ to A. If the homomorphism is injective, then a does not satisfy any polynomial equation over $\mathbf{k}$, in which case is it termed a **transcendental element**(defined).

Otherwise, the kernel is a two-sided ideal, and a generator of this ideal (unique upto scalar multiple) is termed the **minimal polynomial**(defined) of a. Such an element a is termed an **algebraic element**(defined).

Nilpotent elements are algebraic over $\mathbf{k}$; but being invertible or being a zero divisor says nothing either way about being algebraic or transcendental. The inverses or annihilating elements may live anywhere inside the ring A and may not be polynomials over the element we start with.

Let's now state Amitsur's spectral theorem:

Theorem 5 (Spectral theorem of Amitsur)**.** Suppose $\mathbf{k}$ is an uncountable field, and A is an algebra of at most countable dimension over $\mathbf{k}$. Then for any $a \in A$, the spectrum of a is nonempty. Moreover:

(1) a is algebraic iff its spectrum is finite
(2) a is transcendental iff the set of elements in its spectrum which are neither left nor right zero-divisors, is cocountable. In other words, for all but countably many z, $a - z$ is not invertible, is not a left zero-divisor, and is not a right zero-divisor.

The proof of this essentially rests on showing that if a is transcendental, then each of the three sets we are trying to avoid, is at most countable. The trick is to demonstrate that each of these sets gives rise to vector subspaces of A of at least that much cardinality.

3.4. **Amitsur's theorem.** We now state the main theorem of Amitsur, that he proved using the spectral theorem, and which leads to a number of useful consequences, including the nullstellensat for uncountable fields:

Theorem 6 (Amitsur theorem)**.** Let A be a $\mathbf{k}$-algebra such that either of the following holds:

- A is finite-dimensional over $\mathbf{k}$
- The dimension of A over $\mathbf{k}$ is countable, but $\mathbf{k}$ is uncountable and every element of A is either a zero divisor or is invertible (In our language, A is an IZ-ring).

Then every element of A is algebraic over $\mathbf{k}$.

The first case is easy (because A is anyway forced to be an IZ-ring); in the second case, we invoke the spectral theorem of Amitsur to see that the existence of transcendental elements leads to a contradiction.

3.5. **The nullstellensatz: that multi-headed fountain.** Spectral theory provides an easy proof of Hilbert's nullstellensatz for *uncountable* algerbaically closed fields. The nullstellensatz is actually true for all algebraically closed fields; however, it's pretty believable that you might get away without working with any algebraically closed field other than $\mathbb{C}$, and $\mathbb{C}$ is uncountable.

Theorem 7 (Hilbert's nullstellensatz: Amitsur form)**.** Let $\mathbf{k}$ be an algebraically closed uncountable field. Then any finitely generated division ring over $\mathbf{k}$ is $\mathbf{k}$ itself (by finitely generated, I mean finitely generated as a $\mathbf{k}$-algebra.

Proof. For a division ring, every element is either invertible or zero; hence every element is either invertible or a zero divisor. Hence, Amitsur's theorem applies, and we conclude that every element of the division ring is algebraic over $\mathbf{k}$. We now use the fact that $\mathbf{k}$ is algebraically closed, and *again* use the fact that the ring at hand is a division ring, to conclude that the algebraic element must lie in $\mathbf{k}$ itself. □

The hard part in the above proof is going from *finitely generated* to *algebraic*, and this is where Amitsur theory helps us: it shows us that transcendental elements are just too bad.

Of course, this is not the usual format in which the nullstellensatz is stated. First a little definition:

Definition (Radical ideal)**.** An ideal I in a commutative ring R is termed a **radical ideal**(defined) if whenever $f^N \in I$ for some positive integer N, $f \in I$.

In commutative rings, radical ideals contain all the nilpotent elements (viz., any radical ideal contains the nilradical) but in general a radical ideal could be a lot bigger.

I list some typical formulations of the nullstellensatz:

Theorem 8 (Hilbert's nullstellensatz: various forms)**.** Let $\mathbf{k}$ be an algebraically closed field.

(1) Any maximal ideal in $\mathbf{k}[x_1, x_2, \ldots, x_n]$ has quotient isomorphic to $\mathbf{k}$ (in fact, $\mathbf{k}$ sits as a vector space complement to the ideal).
(2) There is a bijective correspondence between the points of $\mathbf{k}^n$ and maximal ideals of $\mathbf{k}[x_1, x_2, \ldots, x_n]$ where a point $(a_1, a_2, \ldots, a_n)$ is mapped to the ideal of all polynomials which vanish at the point $a_1, a_2, \ldots, a_n$.
(3) Consider the Galois correspondence induced by the following binary relation between $\mathbf{k}[x_1, x_2, \ldots, x_n]$ and $\mathbf{k}^n$: p is related to a if $p(a) = 0$. Then the closed sets in $\mathbf{k}[x_1, x_2, \ldots, x_n]$ are precisely the radical ideal; in other words, it is an ideal such that if p^N vanishes on the set, so does p.

There are also versions of Hilbert's nullstellensatz that can be stated for arbitrary non-algebraically closed fields; there are model-theoretic formulations. Alternative proofs and formulations of Hilbert's nullstellensatz use techniques from commutative algebra, model theory and many other parts of mathematics.

4. Some finite and infinite-dimensional fun

4.1. **Double-checks.** Given a module M over a ring R, we can define $M^\vee$ (called M-check) to be the right R-module given by the set of all R-homomorphisms from M to R. For a right R-module, we can define its *left* check as all right module maps from the module to the base ring. In general, we have a map from a module to its double-check; a question might be: when is this map an isomorphism?

There are in general two kinds of obstructions. One obstruction is finiteness. Infinite-dimensional vector spaces are not equal to their double duals, so it is hard to expect that an infinite-dimensional module over an arbitrary ring will satisfy the conditions. Thus in this case the double-check is actually *bigger*

The second obstruction is torsion. Without going into the details of this, consider the particular case that $M = R/I$ where I is a nonzero left ideal. Then there are in general no nonzero homomorphisms from M to R.

However, interesting and surprising things happen when we combine these obstructions. Here's a fun theorem:

Theorem 9 (Countable direct sum equals double-check)**.** Let R be a PID with at least two distinct primes. Let N be a countable direct product of copies of R and M be the countable direct sum of copies of R, embedded as a submodule of N. Then any element of $N^\vee$ is determined by its action on M.

Proof. With some thought, it suffices to show that if a map from N to R is zero on all elements which have only finitely many nonzero coordinates, then it is zero everywhere.

We first show that for any prime p, a tuple of the form $(a_0, a_1p, a_2p^2, \ldots)$ gets mapped to 0. We then use the fact that R contains at least two distinct primes p and q, to show that for any sequence $(c_0, c_1, \ldots)$, there exist sequences $(a_0, a_1p, \ldots)$ and $(b_0, b_1p, \ldots)$ which sum up to the give sequence. Since each of these goes to 0, so does the sum. □

Here's a corollary of that.

Theorem 10. If R is a PID with at least two distinct primes, then the countable direct product of R with itself is not semisimple as a R-module.

Proof. As before, let N denote the countable direct product of R with itself, and M the submodule which is the countable direct sum. If N is semisimple as a R-module, then M is a direct summand of N, so there exists a semisimple complement M'. But there should then be a nonzero homomorphism from M' to R (this follows from the fact that M' is torsion-free, and contains a rank one submodule). We can thus define a homomorphism from N to R which is zero on N but nonzero on M, contradicting the previous result. □

In particular, this shows that the countable direct product of $\mathbb{Z}$s with itself is not semisimple as a $\mathbb{Z}$-module.

4.2. **In the infinite world.** In the infinite world funny things happen. For one, direct sums become different from direct products: a direct product is just a Cartesian product of the underlying sets with the operations coordinate-wise.[6]

We consider analogoues of the matrix ring in the infinite world and prove interesting things. Let's consider everything over a field, for convenience. Let V be a countable direct sum of copies of $\mathbf{k}$. Let A be the ring of all $\mathbf{k}$-linear maps from V to V.

Claim. A is left-primitive, with V a faithful simple left A-module.

Proof. It is clear that one can go from any element of V to any other element of V by an element of A, hence V is clearly simple as a left A-module. Faithfulness is also clear from the definition. □

If we enumerate a basis for V, we can actually write out a matrix for every element of A in that basis. Such a matrix must be *column-finite*: every column can have only finitely many nonzero entries. In fact, the ring of column-finite matrices under multiplication is precisely the ring of $\mathbf{k}$-linear endomorphisms of V.

The transpose operation, which stood us in good stead in finite dimensions, now fails us. Applying transpose to a column-finite matrix yields a row-finite matrix, which in general is not column-finite. So it is not clear whether this ring is self-opposite, and hence it is not clear whether it is also right-primitive.

[6] Category-theorists may prefer to say that "products" and "coproducts" get distinguished in infinite dimensions. Of course, the fact that they coincide in finite dimensions is because the objects we are dealing with are "Abelian".

A is *not* simple. It contains a two-sided ideal, namely the ideal of all linear transformations with finite image.

Let us now describe a subring B of A. In matrix form, once we have chosen a basis, B consists of those matrices which are both row-finite and column-finite. It turns out that with respect to the module V, B is a dense subring of A. If we have a dense subring with respect to a simple module, the module remains simple with respect to the subring, hence B is also a left-primitive ring with faithful simple module V.

Note that B is a self-opposite ring: in fact, the transpose works. On the other hand, the description of B depends on a choice of basis, unlike that of A.

Here's an easy-to-check fact:

> The double-centralizer of B with respect to the module V is the whole ring A.

Before introducing yet another subring of A, let's step back a bit and define the unitization of an ideal.

4.3. **Unitization of an ideal.** A left ideal of a ring is closed under addition and multiplication; the only problem is that it doesn't have a 1. This problem can be remedied by "throwing" in a 1.

Claim. If I is a left ideal of a ring R, the smallest subring of R containing I is, as an Abelian group $I \oplus J$ where J is the subring generated by 1 (in characteristic 0, it is $I \oplus \mathbb{Z}$). The direct sum decomposition given above is not a direct sum decomposition as *rings*. Rather, the multiplication is defined as:

$$(a_1, n_1)(a_2, n_2) = (a_1a_2 + n_2a_1 + n_1a_2, n_1n_2)$$

where the multiplication na means a added to itself n times.

This is an analogue of a "semidirect product"; it describes how to multiply between a subring and an ideal.

If we are working with $\mathbf{k}$-algebras, then the $\mathbf{k}$-subalgebra generated by an ideal I is defined as $I \oplus \mathbf{k}$, with a similar multiplication rule.

The above procedure of passing from an ideal to the subring (or $\mathbf{k}$-subalgebra) generated by it is termed **unitization**(defined). Note the following:

- The unitization of a left ideal in a $\mathbf{k}$-algebra is a local ring, and the left ideal is the unique maximal two-sided ideal in that local ring.[7]
- In fact, it is a special kind of local ring in the sense that it is "split": there is an embedding of the residue field inside the ring. Such local rings are termed equicharacteristic local rings.

There are concrete ways of viewing the localization. Here's one. Recall the Galois correspondence we had set up between the polynomial ring and points of $\mathbf{k}^n$. Under that Galois correspondence, we may ask: given a subset of $\mathbf{k}^n$ (like a line, or circle), what are the polynomials that are *constant* on that subset? There is a relation between the polynomials that are constant on the subset, and polynomials which vanish on the subset:

> The subring of $\mathbf{k}[x_1, x_2, \dots, x_n]$ of polynomials which are constant on a subset of $\mathbf{k}^n$ is the unitization of the ideal of polynomials which vanish on the subset.

Like a lot of mathematical statements, this is easy to prove once stated, but it is profound. This means that the problem of computing what polynomials vanish on a subset is equivalent to the problem of computing the subring which is constant on the subset. This leads us into the realm of invariant theory, but we shall desist from entering that and get back to where we were.

4.4. **Another subring of the endomorphism ring.** Let's recall the situation two subsections back:

- V is a countable direct sum of copies of $\mathbf{k}$
- A is the ring of all endomorphisms of V (as a $\mathbf{k}$-vector space). A is a left-primitive ring; in fact, V is a faithful simple A-module.
- After choosing a basis, we can write elements of A as column-finite matrices. B is the subring of A comprising matrices that are both row-finite and column-finite. B is also left-primitive. B is a dense subring of A.

[7] There is a related concept of "idealizer": the largest subring in which a given left ideal is a two-sided ideal. This is analogous to "normalizer" in group theory. The unitization of an ideal is contained in its idealizer.

- A contains a two-sided ideal I : the ideal of linear transformations having finite image.

Define C as the $\mathbf{k}$-subalgebra of A generated by I. Note that C is again defined in a basis-independent manner. Again, C is a dense subring of A, and C is again left-primitive. Neither C nor B is contained inside the other:

- An infinitary permutation matrix lives inside B but not inside C.
- On the other hand, the linear transformation sending everything to the first basis vector lives inside C but not inside B.

Similarly to B, it turns out that the double-centralizer of C with respect to the module V is the whole ring A.

5. Back to the Artinian world

5.1. **Semisimple finite-dimensional algebras over fields.** Note: When we are considering algebras over a field, the "world" of maps is the world of all $\mathbf{k}$-linear maps, instead of all Abelian group homomorphisms.

A finite-dimensional algebra over a field is an Artinian ring. More generally, if A is a $\mathbf{k}$-algebra and M is an A-module which is finite-dimensional as a $\mathbf{k}$-vector space, M is Artinian as an A-module.

Thus, the entire classification that we did for semisimple Artinian rings, works for semisimple rings that are finite-dimensional over their ground field. More can be said in this case: the mysterious "division rings" we have are now all division rings which contain the base field in their center.

Now if the ring that we start out with is finite-dimensional over the ground field, then each of the corresponding division rings we get is also finite-dimensional over the ground field, so the problem of classifying all simple Artinian $\mathbf{k}$-algebras reduces to the problem of classifying all division rings whose center contains $\mathbf{k}$, and which are finite-dimensional over $\mathbf{k}$. In general, this could be a hard problem; however, when $\mathbf{k}$ is algebraically closed, it's a superbly easy problem: the only finite-dimensional division algebra over $\mathbf{k}$ is $\mathbf{k}$ itself.

Thus, Artin-Wedderburn theory over an algebraically closed field $\mathbf{k}$ states that if A is a finite-dimensional semisimple $\mathbf{k}$-algebra, then A is a direct sum of matrix rings over $\mathbf{k}$. This looks nice!

5.2. **When the field is not algebraically closed.** To take an illustration, consider the field $\mathbb{R}$. $\mathbb{R}$ is not algebraically closed: it has a quadratic extension $\mathbb{C}$ which is algebraically closed. The division rings over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$ and the Hamiltonian quaternions, so any finite-dimensional semisimple $\mathbb{R}$-algebra can be expressed as a direct sum of matrix rings over $\mathbb{R}$, $\mathbb{C}$ and the Hamiltonians.[8]

I'll illustrate this (later on) with an example of the group algebra over $\mathbb{R}$ of the quaternions.

There is a more general construction paralleling the construction of the Hamiltonian quaternions, called generalized quaternion algebras, which we again might come to later.

5.3. **When the algebra is not assumed to be finite-dimensional.** Just because A is a $\mathbf{k}$-algebra and A is an Artinian ring, does *not* imply that A is finite-dimensional as a $\mathbf{k}$-algebra. For an easy counterexample, consider $\mathbb{C}$ as a $\mathbb{Q}$-algebra, or $\mathbb{C}(t)$ as a $\mathbb{C}$-algebra. Thus, we have not really classified all semisimple Artinian algebras over fields; we have classified only the *finite-dimensional* ones.

However, for algebraically closed fields, we can say something better: we have classified all the *finitely generated* semisimple algebras over $\mathbf{k}$. This is because the nullstellensatz actually tells us that any finitely generated division ring over a field is the field itself.

6. Ring and module properties seen so far

Let's take some time off to review the ring properties seen so far, and the implications among them.

First a list of the properties, along with some notes on how much left/right symmetry they possess. When I say a property possesses *left-right symmetry*, I mean that a ring has the property iff its opposite ring also does. This does *not* mean that the ring is isomorphic to its opposite ring:

[8] The Hamiltonians contains $\mathbb{C}$ as a subring, but is *not* a $\mathbb{C}$-algebra because $\mathbb{C}$ is not in the center of the Hamiltonians.

Property	Left-right symmetry
Field	Yes (commmutative)
Division ring	Yes
Integral domain	Yes
Simple ring	Yes
Left-primitive ring	No
Right-primitive ring	No
Involutory ring	Yes
Self-opposite ring	Yes
Semisimple Artinian ring	Yes
Artinian ring	Yes
Local ring	Yes
Completely primary ring	Yes
IZ-ring	Yes
Additively generated by invertibles	Yes
Indecomposable ring	Yes
Commutative ring	Yes
Simple Artinian ring	Yes
Matrix ring of order n	Yes
Matrix ring over commutative ring	Yes

It seems that apart from primitivity, all the notions we have defined have eventually been shown to be left-right symmetric. This is more an indicator of the fact that we have remained in shallow waters, than of any inherent left-right symmetry in most rings.

Let's now look at the major implication chains (try coming up with counterexamples to the converse of each implication):

(1) Field $\implies$ Division ring: We only remove the hypothesis of commutativity
(2) Division ring $\implies$ Integral domain $\implies$ Indecomposable ring: This follows from the definitions.
(3) Division ring $\implies$ Simple ring: We weaken from demanding the absence of left and right ideals, to demanding the absence of two-sided ideals
(4) Division ring $\implies$ Completely primary ring $\implies$ IZ-ring: We successively weaken our demands here. For division rings, every non-invertible element must be 0, for completely primary rings, every non-invertible element must be nilpotent, and for IZ-rings, every non-invertible element must be both a left and a right zero divisor.
(5) Division ring $\implies$ Completely primary Artinian ring $\implies$ Local Artinian ring $\implies$ Artinian ring: I've just thrown in an "Artinian" everywhere, since division rings are clearly Artinian.
(6) Completely primary ring $\implies$ Local ring $\implies$ Indecomposable ring
(7) Division ring $\implies$ Simple Artinian ring $\implies$ Semisimple Artinian ring
(8) Simple ring $\implies$ Left-primitive ring: The forward implication uses the existence of maximal left ideals. The converse implication is true under the additional assumption of Artinianness.
(9) Matrix ring over commutative ring $\implies$ Involutory ring $\implies$ Self-opposite ring

6.1. **Module properties.** Given a ring, we want to study properties of left modules over the ring. We have so far seen the following properties for left modules: simple, semisimple, indecomposable, finite length, indecomposable of finite length, semisimple of finite length, finitely generated. Let's view the relation between these properties:

(1) Simple $\implies$ Isotypical $\implies$ Semisimple: A semisimple module could be a direct summand of more than one simple module. Isotypical modules are those semisimple modules which have only one isomorphism type of simple module.
(2) Simple $\implies$ Indecomposable: Simple modules are indecomposable. In fact a simple module is the same thing as an indecomposable semsimple module.
(3) Simple $\implies$ Indecomposable of finite length $\implies$ Strongly indecomposable $\implies$ Indecomposable
(4) Simple $\implies$ Semisimple of finite length $\implies$ Semisimple
(5) Finite length $\implies$ Finitely generated: The converse implication holds if the module is semisimple; it also holds if the ring is Artinian (the two conditions are fairly different in nature).

Semisimple modules are those built horizontally from the simple building blocks: the building blocks are laid one to the side of the other. Indecomposable modules are stacked vertically: each simple piece is stacked on top of a previous one. Arbitrary modules could be stacked in a vertical-horizontal mix.

6.2. **Correspondence between module properties and endomorphism rings.** We have the following correspondence between properties of modules and properties of their endomorphism rings, first seen in part 1:

Module property	Implied endomorphism ring property	Proof
Simple	Division ring	Schur's lemma
Indecomposable of finite length	Completely primary ring	Fitting's lemma
Strongly indecomposable	Local ring	(By definition)
Indecomposable	Indecomposable ring	(part 1)
Isotypical of finite length	Matrix ring over division ring	(part 1)
Semisimple of finite length	Direct sum of matrix rings over division rings	(part 1)

7. Morita theory

Given a ring, one way to study it is to look at the "category" of its left modules, viz., the category whose objects are left modules over the ring and whose morphisms are module homomorphisms. The category of left modules of a ring captures some properties of the ring, but not all. In fact, it is the ability of this category to "forget" some aspects of ring structure that is useful to us.

Definition (Morita-equivalent rings)**.** Two rings R and S are termed Morita-equivalent if there is an equivalence of categories between the category of left R-modules and the category of left S-modules.

By "equivalence of categories" we mean that there exist functors both ways such that the composite both ways is equivalent to the identity functor via a natural transformation. Let's explore this a little more carefully, by the following theorem:

Theorem 11. Let R be any ring and $n \geq 1$. R is Morita-equivalent to the matrix ring $M_n(R)$.

The proof may seem unilluminating at this stage, so we'll prove it as a special case of something more general.

Theorem 12. Suppose A is a ring and e is an idempotent in A. Then eAe is a ring in its own right (it is *not* a subring of A). Let M be a left A-module. Then if M is simple as an A-module, eM is simple as an eAe-module.

Proof. The idea is that of "going up": given an eAe-submodule N of eM, we prove that:

$$AN \cap eM = N$$

Hence any proper nonzero eAe-submodule of eM gives rise to a proper nonzero A-submodule of M. □

Now let's get back to business, with what's called a decomposition of 1. In the matrix ring $M_n(R)$, we can decompose 1 as a sum of matrix elements e_{ii} where e_{ii} is 1 in the ii^{th} place and 0 elsewhere. Each of these is an idempotent, and it cannot be expressed as a sum of idempotents.

Now if M is a $M_n(R)$-module, then we have:

$$M = \sum_{i=1}^{n} e_{ii}M$$

From the theorem above, each $e_{ii}M$ is simple as a $e_{ii}M_n(R)e_{ii}$-module, which is the same as a R-module, with R acting only in the place e_{ii}. But this also implies that it's simple as a R-module where R acts as scalar matrices. The upshot is that if we view R as embedded inside $M_n(R)$ as scalar matrices, then M is a sum of simple modules over R; hence, M is a semisimple R-module. What we've proved is thus:

> Any simple $M_n(R)$-module is semisimple as a R-module, where R embeds inside $M_n(R)$ as scalars.

7.1. **The hidden ideas.**

The reasoning in the previous part may seem abstruse, but there is something very concrete going on. What we're secretly doing is thinking of R as a field $\mathbf{k}$, and M as the vector space $\mathbf{k}^n$. In this case, we know that M decomposes as a direct sum of n copies of $\mathbf{k}$ (the choice of decomposition is tantamount to a choice of basis upto scalar factors).

The problem is that we want to "abstractly" find a decomposition of M without knowing that it actually "looks like" a vector space. So, we construct abstract analogues of the projection operators by considering formally the subgroups $e_{ii}M$ where e_{ii} are the matrices with 1 in the ii^{th} place and 0s elsewhere.

Of course, when R is not a field, R^n is certainly *not* a simple $M_n(R)$-module; rather, examples of simple $M_n(R)$-modules would be N^n where N is a simple R-module. Nonetheless, the idea of projection works.

7.2. **Idempotent decompositions.**

We had earlier noted that a ring is indecomposable as a left module over itself iff it contains no nontrivial idempotents. This leads to the natural question: what is the relation between idempotents and decomposition of a ring into left submodules? Here's the answer:

1. A **primitive idempotent**(defined) is an idempotent in a ring which cannot be expressed as a sum of two nonzero idempotents. The left ideal generated by a primitive idempotent is a minimal left ideal; similarly, the right ideal generated by a primitive idempotent is a minimal right ideal. Primitive idempotents may or may not exist.
2. A **central idempotent**(defined) is an idempotent in a ring which commutes with every element of the ring.
3. Two idempotents are said to be **orthogonal**(defined) if their product is 0. Note that orthogonal idempotents must commute. A sum of two orthogonal idempotents is again an idempotent.

Let's return to Artin-Wedderburn theory. Artin-Wedderburn theory tells us that any semisimple Artinian ring can be expressed as:

$$R = M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \dots M_{n_r}(D_r)$$

where each D_i is a division ring. Then:

1. Each $M_{n_i}(D_i)$ is a minimal two-sided ideal in R, and is generated by a central idempotent, namely the element which is identity in that component and 0 elsewhere.
2. The central idempotents are precisely the $(0,1)$-linear combinations of the r central idempotents given above. Thus, there are 2^r of them.
3. The central idempotent for the matrix ring $M_{n_i}(D_i)$ can be decomposed as a sum of n_i primitive, pairwise orthogonal idempotents. This decomposition is not unique, and is tantamount to choosing a basis for the corresponding vector space.[9] The n_i idempotents are projections onto each of the basis directions.
4. Every minimal left ideal is generated by a primitive idempotent. Every left ideal is generated by an idempotent (first write the left ideal as a sum of minimal left ideals, and then add up the idempotents for each of them).

In general, primitive idempotents need not exist; it may be possible to keep decomposing an idempotent further and further. As an amusing example, let (X, μ) be a measure space. Consider the ring $L^\infty(X)$ of essentially bounded real-valued measurable functions on X (upto a.e. equivalence). This is indeed a $\mathbb{R}$-algebra. The idempotents in this $\mathbb{R}$-algebra are the indicator functions of measurable subsets of X. Then:

- Idempotents correspond to measurable subsets (upto a.e. equivalence): Any idempotent is the indicator function of a measurable subset.

[9] One has to be a bit careful while dealing with division rings

- Primitive idempotents correspond to measurable subsets of positive measure which do not contain any measurable subset of strictly smaller positive measure.

Thus, for measure spaces where every set of positive measure contains a subset of strictly smaller positive measure, there are no primitive idempotents. $\mathbb{R}$ is an example of such a measure space. Thus, $L^\infty(\mathbb{R})$ is far from Artinian.

7.3. **Back to Morita-equivalence.** We shall here show that under reasonably "nice" hypotheses, A is Morita-equivalent to the ring eAe. Here A is a ring and e is an idempotent.

In particular it shows that any ring is Morita-equivalent to a matrix ring of finite order over it.

Theorem 13 (Morita theorem)**.** Suppose e is an idempotent in a ring A such that $AeA = A$ (viz the two-sided ideal generated by e is the whole ring A). Then the rings A and eAe are Morita-equivalent.

This condition is readily satisfied for the matrix ring over any ring.

Here's the intuition behind this (this intuition will turn useful when we look at quivers). The idea is that eAe may in general be much smaller than A. However, if $AeA = A$, then e "generates" A as a two-sided ideal, which means that A looks like a whole lot of copies of eAe, joined to each other such that all the copies look more or less the same. Thus collapsing A to eAe is a bit like collapsing an entire equivalence class into a single representative of that class.

8. A little more of non-Artinian ring theory

We shall now revisit lovely examples like the Weyl algebra that we constructed earlier, in a little more general light, and also see just how good or bad they can get.

8.1. **Failure of the double-centralizer property.** The Jacobson density theorem tells us that if the module at hand is a simple module over the ring, then the ring is dense in its double-centralizer. Thus there are two ways in which the double-centralizer property can fail:

- The module is not simple over the ring: For instance, the vector space $\mathbf{k}^n$ over the ring of upper triangular matrices.
- The module is simple over the ring but is infinite-dimensional: A few sections ago, we saw many examples of *dense* subrings of the ring of all linear transformations from a countable-dimensional vector space to itself. These dense subrings are examples of subrings that do not have the double-centralizer property.

8.2. **Subrings with the double-centralizer property.** Let me make a few more comments. When $\mathbf{k}$ is not algebraically closed, there are examples of subrings of $M_n(\mathbf{k})$ which have the double-centralizer property with respect to $\mathbf{k}^n$, namely, *field* extension of $\mathbf{k}$. For instance, when $\mathbf{k} = \mathbb{R}$ and $n = 4$, the subring $M_2(\mathbb{C})$ of $M_4(\mathbb{R})$ has the double centralizer property, and so does the subring corresponding to the Hamiltonians.[10]

In essence, any subring of $M_n(\mathbf{k})$ which has the double-centralizer property must, by the Artin-Wedderburn theorem, "look like" a matrix ring over a division ring. In particular when $\mathbf{k}$ is algebraically closed, any subring of $M_n(\mathbf{k})$ which has the double centralizer property must "look like" a smaller matrix ring over the same field. Here are some examples. In $M_4(\mathbb{C})$, we can embed $\mathbb{C}$ as scalar matrices. We can also embed $M_2(\mathbb{C})$ as block scalar matrices, where each 2-by-2 matrix is a scalar. In general:

> Suppose $M_{nd}(\mathbb{C})$ is a matrix ring, where $n, d \in \mathbb{N}$. Then, we can embed $M_n(\mathbb{C})$ in $M_{nd}(\mathbb{C})$ as block scalar matrices. $\mathbb{C}^{nd}$ is a semisimple module for the embedded $M_n(\mathbb{C})$: it is a direct sum of d simple modules. Moreover, the embedded $M_n(\mathbb{C})$ has the double-centralizer property.

The particular case $n = 1$ yields the scalar matrices embedded inside the matrix ring. The case $d = 1$ yields the whole matrix ring.

[10] The "the" is misleading. There are many possible choices.

8.3. **The Weyl algebra.** We already constructed examples in the infinite-dimensional case of dense subrings which do not satisfy the double-centralizer property. The idea here is that as far as finitely many elements can tell, there are enough linear transformations; however, there are not enough linear transformations to move infinitely many elements the way we please. We will now try to revisit some algebras we touched upon in part 1, and verify whether these algebras have the double-centralizer property.

Recall that for any ring R, we can define its algebra of differential operators as the algebra generated by all R-module maps from R to itself, generated by left multiplications and derivations. When R is the polynomial ring in one variable over $\mathbf{k}$, we recover precisely the Weyl algebra $\mathbf{k}\langle x, y\rangle / \langle\langle xy - yx - 1\rangle\rangle$. When R is the polynomial ring in many variables, we require a corresponding multi-variable analogue of the Weyl algebra.

Although we did not view it that way, the Weyl algebra can be viewed as a subring of the ring of all *linear* maps from $\mathbf{k}[t]$ to itself. This is a countable-dimensional vector space, hence we can represent linear maps by column-finite matrices. In this language, the multiplication operator corresponds to a matrix with a 1 in the *subdiagonal* and the differentiation operator corresponds to a matrix with entries $1, 2, 3, \dots$ in the superdiagonal. The Weyl algebra is thus a *subalgebra* of the algebra of all $\mathbf{k}$-linear transformations, generated by the subdiagonal matrix and the superdiagonal matrix.

It can once again be checked that the centralizer of the Weyl algebra is precisely the algebra of all scalar multiplications, and hence its double centralizer is the whole of A. We can also see, more directly, that the Weyl algebra is dense in the ring of all linear transformations: given finitely many source and target polynomials, it is possible to explicitly write down a differential operator which sends each source polynomial to its corresponding target polynomial.

I list some more facts (when $\mathbf{k}$ has characteristic 0). Most of these facts can either be proved directly or can be easily proved using the idea of Lie ideals mentioned in part 1:

- The Weyl algebra is simple. We proved this earlier.
- The Weyl algebra is involutory. The exchange mapping of x and y is an involution.
- The Weyl algebra does not have finite length as a module over itself (because it's non-Artinian). Hence it is *not* semisimple over itself, because any semisimple finitely generated module must have finite length (we proved this right at the start).
- The Weyl algebra is an integral domain in the noncommutative sense: it has no zero divisors other than 0. Hence it is very far from being an IZ-ring.
- The Weyl algebra is non-Artinian, because it's not an IZ-ring. Recall that we had proved that any Artinian ring is IZ.
- The center of the Weyl algebra is precisely $\mathbf{k}$. Moreover, any invertible element is in the center. In fact every invariant element is in the center. Thus the Weyl example is an example of an algebra which is *not* additively generated by its invariant elements. (these statements are proved easily using the notion of Lie ideals developed in part 1).
- The Weyl algebra is a typical illustration of the spectral theorem of Amitsur: every element which is not scalar is transcendental, and hence for most elements, the spectrum is the whole field.

8.4. **The translation ring.** The translation ring was defined as $\mathbf{k}\langle x, y\rangle / \langle\langle xy - yx - x\rangle\rangle$. In Part 1, we did not give a rationale as to the importance of this ring. Here are some contexts in which the translation ring comes up (none of them is relevant for our purpose, but I list them for completeness):

- The translation ring is the universal enveloping algebra of the Lie algebra with two generators x and y over a field $\mathbf{k}$, governed by the relation $[x, y] = x$.
- The translation ring is the skew polynomial ring over $\mathbf{k}[y]$ corresponding to the "shift" automorphism $y \mapsto y + 1$. More concretely, the translation ring can be viewed as acting on $\mathbf{k}[t]$ with y acting as multiplication by t, and x acting as the automorphism induced by $t \mapsto t + 1$.[11]
- The translation ring occurs as deformations of the Weyl algebra. For instance, the algebra $\mathbf{k}\langle x, y\rangle / \langle\langle xy - yx - cx - 1\rangle\rangle$ can, by change of variables, be viewed as a translation ring.

We proved that any nonzero ideal in the translation ring must contain a power of x.

Here are some interesting facts about the translation ring:

- The element x is an *invariant* element: The left ideal and right ideal generated by x are equal.
- The translation ring is involutory. The involution is $y \mapsto -y$.

[11] For a general theory of skew polynomial rings, refer "Abstract Algebra and Applications" by P. M. Cohn, Section 7.3

- $\mathbf{k}[t]$ is a faithful simple left module over the translation ring. Here y acts as multiplication by t and x acts as the ring automorphism of $\mathbf{k}[t]$ induced by the map $t \mapsto t + 1$.
- Thus the translation ring is a left-primitive ring. Since it is involutory, this also shows that it is right-primitive. However, it is not simple.
- If M is a non-faithful simple module over the translation ring, then $xM = 0$. To see this, note that xM is a submodule of M, and thus either $xM = 0$ or $xM = M$. Further since M is not faithful, its annihilator is a nonzero two-sided ideal, and hence must contain some power of x, forcing $x^n M = 0$ for some M.
- Thus if M is a non-faithful simple module over the translation ring, it descends to a module over the polynomial ring $\mathbf{k}[y]$.

8.5. **The intuition so far.** What we have seen so far should convince us that in the infinite-dimensional case:

- There are a whole lot of primitive rings which aren't simple. Primitivity simply requires that we should have a faithful simple left module.
- Most of the rings we see do *not* have the double-centralizer property. They are in fact dense in the ring of all linear transformations. Their centralizers are only the scalar transformations, and their double centralizer is usually the ring of all linear operators.
- Even those rings that happen to be simple, are usually very far from being Artinian. The prime example is the Weyl algebra, which, though simple, is not Artinian, and is hence not semisimple as a module over itself.

9. Quivers and representation theory

9.1. **A quick look at quivers.** The matrix ring over a field is the ring of all linear maps from a vector space over the field to itself. We can alternatively think of each map from the vector space $\mathbf{k}^n$ to itself, as follows:

- Make n labelled copies of $\mathbf{k}$. This corresponds to a direct sum decomposition of $\mathbf{k}^n$ in terms of n one-dimensional spaces.
- View any linear map from $\mathbf{k}^n$ to $\mathbf{k}^n$ as specifying a homomorphism from each labelled copy of $\mathbf{k}$ to each labelled copy of $\mathbf{k}$. Thus, there are n^2 linear maps between one-dimensional vector spaces that give rise to the single linear map from $\mathbf{k}^n$ to $\mathbf{k}^n$.

Thus we may try to draw the matrix ring by making n vertices and a directed edge from every vertex to every vertex (this includes n loops and $n(n-1)$ edges between distinct vertices). Specifying an element of the matrix ring is equivalent to specifying, for every edge, a homomorphism from its source to its target. Adding two elements of the matrix ring involves adding the homomorphisms on each edge. Composing two elements of the matrix ring corresponds to composing the homomorphisms graphically along the edges.

In other words, we are viewing the matrix ring as the direct sum of the homomorphism groups between one-dimensional vector spaces, with the multiplication given by composition.

We already did something like this (in reverse) long ago, when we showed that the endomorphism ring of an isotypical component is a matrix ring over the endomorphism ring of the associated simple module.

The problem with this model is that the picture is too messy: we have an edge betwee any two vertices, and we have a lot of relations of the form: a product of two edges gives a third edge. What we'd ideally like is a situation where there are as few explicit edges as possible, and the elements of the ring are really obtained as composites of edges. Such a theory is incapable of representing rings of the complexity of matrix rings, because in such a ring there are many ways of going back and forth. However, we can represent rings upto "Morita-equivalence", and the matrix ring over a field is Morita-equivalent to the field itself.

A little note about the "upto Morita-equivalence" business. When we will draw a quiver which represents a ring upto Morita equivalence, what we're really doing is this: we're hiding the deeper complexity inside each vertex.

9.2. **A quiver and its path algebra.**

Definition (Quiver, path algebra)**.** A **quiver**(defined) is a finite directed graph. The **path algebra**(defined) Path (Q) of a quiver Q over a field $\mathbf{k}$ is defined as follows:

- As a vector space, Path (Q) has basis all the paths in Q. A path of length 0 is a single vertex; in general a path of length r is a sequence of r directed edges such that the head of each is the tail of the next.
- The product of two paths is 0 if the head of the first does not match up with the tail of the second, and is the path obtained by concatenating them if the head and tail do match up.

Let's try drawing some quivers, and seeing what their path algebras look like:

(1) The quiver with one vertex and no paths is $\mathbf{k}$ itself.
(2) The quiver with one vertex and r loops at that vertex is the free associative algebra in r variables.
(3) The quiver with r vertices and no edges is $\mathbf{k}^r$ as a r-algebra.
(4) The disjoint union of two quivers has as its path algebra the direct sum of the path algebras for each of them.
(5) The quiver which is a straight-line graph has as its path algebra the ring of upper triangular matrices over a field. The vertices correspond to the projection operators on each of the basis elements, and the edge from vertex i to vertex $i-1$ is the basis element $e_{i-1}i$.

9.3. **Obtaining an algebra as a path algebra.** A natural first question: which $\mathbf{k}$-algebras can be obtained as path algebras for quivers? The first thing to note is that a path algebra cannot encode any algebraic extensions. Hence, if we want to have any hope of representing a reasonable fraction of all $\mathbf{k}$-algebras as path algebras, we should choose $\mathbf{k}$ to be algebraically closed. This will avoid having to think about impossible problems like trying to represent $\mathbb{C}$ as a path algebra over $\mathbb{R}$.

The second thing to note is that algebras like the matrix algebra, which have a lot of "circular" relations, again have no hope. However, we know that whenever an algebra has a lot of transitivity and a lot of circularity, it is likely to be Morita-equivalent to a more tractable algebra. Indeed, the matrix ring is Morita-equivalent to the underlying field, and hence a direct sum of matrix rings is Morita-equivalent to a direct sum of fields, which we know how to represent.

The third thing to note is that however nice the algebra, it is unlikely that all its relations can be coded into something as naive as a path algebra. The best we can hope for is to say that the algebra is a path algebra, modulo a sufficiently "small" ideal.

We can now state the grand theorem of quivers.

Theorem 14 (Grand theorem of quivers)**.** Suppose $\mathbf{k}$ is algebraically closed and A is an Artinian $\mathbf{k}$-algebra. Then there exists a quiver Q and a homomorphism from Path (Q) to A whose kernel lives inside the ideal generated by paths of length 2. Moreover, the quiver Q is unique (upto isomorphism).

For semisimple Artinian rings, the quiver is just a discrete set of points, where the number of points is the number of minimal two-sided ideals (or number of simple summands, with multiplicity). In this case, since there are no paths at all, the ideal we are quotienting out by is the zero ideal; on the other hand, the ideal we are quotienting out can also be described as the entire ideal of paths of length at least 2.

For non-Artinian rings, the construction of the quiver is using the "top"; however, actually realizing the given algebra as a quotient of a path algebra by an ideal involves some hardwork. I won't do all the hardwork, but will develop the main idea behind it, and then take yet another foray into interesting stuff.

9.4. **The idempotent-lifting property.** This question might seem a bit artificial if asked in isolation, but it has concrete motivation from quivers, and in fact from many other contexts:

Definition (Idempotent-lifting property)**.** Suppose R is a ring and A is an additive subgroup of R. Then A is said to have the **idempotent-lifting property**(defined) in R if whenever $e \in R$ is such that $e^2 - e \in A$, there exists $e' \in R$ such that $e'^2 = e'$ and $e' - e \in A$. In other words, idempotents can be lifted modulo A.

We shall largely be interested in the problem of lifting elements modulo ideals.

Some obvious candidates for ideals with the idempotent-lifting property are direct summands. Here's a claim:

Claim. Suppose $R = A \oplus B$ where A and B are two-sided ideals in R. Then both A and B have the idempotent-lifting property in R.

The proof is direct, and shows in particular that the whole ring and the 0 ideal both have the idempotent-lifting property.

It is also true that if we take a *prime* ideal in a commutative ring, then any idempotent modulo that ideal must lift to an idempotent in the whole ring. Specifically, this is because if the equation $e(e-1) = 0$ mod I where I is a prime ideal, then either $e = 0$ mod I or $e - 1$ is 0 mod I. In the former case we can choose $e' = 0$; in the latter case we choose $e' = 1$.

On the other hand, ideals in $\mathbb{Z}$ or $\mathbf{k}[x]$ usually do not have the idempotent-lifting property. In other words, there may be solutions to the polynomial equation $x^2 - x = 0$ in the quotient by an ideal that do not lift to the whole ring. For instance, $4^2 - 4$ is 0 mod 6, but 4 does not lift to an idempotent in $\mathbb{Z}$.

Theorem 15 (Nilpotent ideals have idempotent-lifting property)**.** Any nilpotent left ideal in R (and more generally, any nil left ideal in R) has the idempotent-lifting property.

This is funny, because the collection of ideals which satisfy the idempotent-lifting property certainly seems a funny collection: it contains all two-sided ideals which have complements (as two-sided ideals), it contains all prime ideals (which in the noncommutative case would translate to ideals for which the quotient ring is an integral domain), and it contains all nilpotent ideals.

9.5. **Relevance of idempotent-lifting.** Starting with an Artinian algebra A over a field $\mathbf{k}$, we can look at its top, and construct the quiver associated with that. This is just a discrete set of points, with no edges. We now need to "fill" in the edges based on relations that live a little below. The hope is that we can completely model behaviour that goes in in the ring $A/(J(A))^2$ by throwing in appropriate edges.

Let's go over this more carefully. Start with any Artinian $\mathbf{k}$-algebra A, where $\mathbf{k}$ is algebraically closed. Consider the ring $B = A/J(A)$. Then B is a direct sum of matrix rings over $\mathbf{k}$, as follows:

$$B = M_{n_1}(\mathbf{k}) \oplus M_{n_2}(\mathbf{k}) \oplus \ldots \oplus M_{n_r}(\mathbf{k})$$

Now pick a *primitive idempotent* p_i in each $M_{n_i}(\mathbf{k})$. Let p be the sum of the p_is. Then B is Morita-equivalent to pBp, and $pBp = \mathbf{k}^n$. And for $\mathbf{k}^n$ our quiver would just be one point for each p_i, with no edges. So we've got a quiver whose path algebra is Morita-equivalent to B.

Unfortunately, we are far from done, because we wanted something whose path algebra is Morita-equivalent to A. The hope is that a Morita equivalence on "top" gives rise to a Morita-equivalence on the whole thing. Indeed, this hope is justified, and the first step towards justifying it is the following amazing fact:

> We can find a collection of idempotents q_i in A such that q_i mod $J(A)$ gives p_i for every i, and such that the q_i are primitive pairwise orthogonal idempotents in A.

The result we obtained in the previous subsection can prove this partially. Since A is Artinian, $J(A)$ is nilpotent, so we can lift each p_i individually to an idempotent in A. However, it is not clear that we can simultaneously ensure that the p_is can be lifted in a way that the lifts are pairwise orthogonal; this requires some proof.

Assume that it can be done. Then let q be the sum of the q_is. Clearly q is an idempotent, and it turns out that $AqA = A$. Thus, we obtain that A is Morita-equivalent to qAq. Moreover, the Jacobson radical of qAq is precisely pBp, a direct sum of fields.

The argument above "shows" that a Morita-equivalence on top does give a Morita-equivalence throughout.

9.6. **Constructing the paths.** We may assume from now on that the top of A is a direct sum of copies of $\mathbf{k}$ (because if not, we can repeat the painful construction above to get a Morita-equivalence with an algebra for which the top is a direct sum of copies of $\mathbf{k}$). The next step is to draw the paths of the quiver. The paths are determined by what goes on in $J(A)/J^2(A)$.

To gain some intuition, let's revert to the "familiar" case where A is the ring of upper triangular matrices over $\mathbf{k}$. In this case, the paths were determined by matrices of the form $e_{(i+1)i}$.

Now, $J(A)$ is the strictly upper triangular matrices, and $J^r(A)$ is the ideal of matrices which are pushed r places up-right of the diagonal. So the paths that we constructed lived in $J(A)$ but outside $J^2(A)$, and this is the general idea: we look at $J(A)/J^2(A)$ to tell us what paths to draw.

Here is a rough sketch of the plan:

- View $A/J(A)$ as an A-module. In fact, $A/J(A)$ is a vector space over $\mathbf{k}$, and A acts as $\mathbf{k}$-linear transformations over it.
- For every element in $J(A)$, consider the induced linear transformation on $A/J(A)$. This can be viewed as a combination of n^2 linear maps, one for every pair. However, it turns out that $J(A)/J^2(A)$ can be given a suitable basis as an $A/J(A)$-module for which the induced operations "look like" paths. *I'm not sure of the precise details; this is meant to be only a rough sketch.*

If I have time, I will add stuff on group representation theory, and how it ties up with various facets. I will also develop the examples a bit better, and indicate more correlations.

Index

algebraic element, 9

bimodule, 4

central idempotent, 16
centralizer, 3

dense subring, 5
double-centralizer property, 3
double-centralizer property for modules, 4

element
  algebraic, 9
  transcendental, 9

Galois correspondence, 2

ideal
  radical, 10
idempotent
  central, 16
  primitive, 16
idempotent-lifting property, 20
idempotents
  orthogonal, 16
IZ- ring, 8

minimal polynomial, 9

orthogonal idempotents, 16

path algebra, 20
primitive idempotent, 16

quiver, 20

radical ideal, 10
ring
  IZ-, 8
  semisimple Artinian, 1

semisimple Artinian ring, 1

transcendental element, 9

unitization, 12