Syllabus: Jacobson density theorem, Artin-Wedderburn structure theorem for Artinian rings, the Jacobson radical, Goldie's theorem and noncommutative localization, PI theory, Gelfand-Kirillov dimension, Brauer groups, other topics.

Throughout this course our focus will be on noncommutative rings, which will mean "not necessarily commutative but definitely associative rings" that have a 1 and $0 \neq 1$. I'll assume that you know the following concepts: ring, left ideal, left module, quotients of modules and submodules, k-algebra, correspondence theorem, first isomorphism thoerem, maximal ideal, centre of a ring, idempotent elements, Zorn's lemma, nilpotent elements, the Chinese remainder theorem for rings, short exact sequences, and I'll assume you know about tensor products (see the appendix, if you don't).

Let's begin by answering the question of how one studies noncommutative rings. For us the main approach will be via seeing "shadows" of the ring and putting together enough of this information to say something meaningful about the ring we are studying. One metaphor I like to employ is that of a bat in a cave; the bat cannot see its surroundings but creates some image of its surroundings by using reflected sound. We can see this as how one can understand a given ring. Under this metaphor a representation of the ring can be seen as the result of emitting a shriek (or whatever it is that bats do) in a specific direction and listening to what is reflected back. A single representation does not tell us so much about the ring, but the sum total of all of them can tell us everything we need to know.

Of course, it's possible that you don't know what a representation is. For us, a representation of a ring R will be a ring homomorphism (not necessarily injective) from a ring R into a ring of linear operators over a division ring D. We recall that a division ring D is a ring R in which every nonzero element has a multiplicative inverse; that is, for every nonzero $x \in D$ there is some $y \in D$ such that $yx = xy = 1$. A division ring can be seen as a noncommutative analogue of a field. Just as we can talk about vector spaces over fields, we can do the same with division rings, although we need to differentiate between left and right.

Given a division ring D, a left vector space V over D is an abelian group endowed with a map $D \times V \to V$ (which we write as $\cdot$) with the property that for $\alpha, \beta \in D$ and $v, w \in V$ we have $\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$; $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$; $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$; $1 \cdot v = v$. Notice this is the same thing as a left module over D.

Just as with fields, the notion of linear independence and spanning go through verbatim and the same Zorn's lemma argument you've seen for ordinary vector spaces over a field shows that a left D-vector space V has a basis and all bases have the same size. We can define right D-vector spaces analogously. We can even have vector spaces V that are both left and right D-vector spaces. Somewhat unexpectedly, there even exist division rings D that have a left-and-right vector space V with the property that as a left vector space V is finite-dimensional and as a right vector space V is infinite dimensional.

Exercise 1. *Give a division ring D and a division subring E such that D is finite-dimensional as a left E-vector space, but infinite-dimensional as a right E-vector space.*

Let's be careful! All left bases have the same size and all right bases have the same size, but left bases and right bases do not necessarily have the same size when both notions make sense.

Now just as with linear algebra, if we have a division ring D and a left D-vector space V, we can consider the ring of D-linear endomorphisms $\mathrm{End}_D(V)$, which consists of all maps $\phi : V \to V$ with the property that for $v, w \in V$ and $\alpha \in D$ we have $\phi(\alpha \cdot v + w) = \alpha \cdot \phi(v) + \phi(w)$. Then we shall call a ring of endomorphisms of this form, a *ring of linear operators over a division ring D*. When D is a field and V is finite-dimensional, this is isomorphic to the ring of $n \times n$ matrices over D, where n is the dimension of D. Then we define a representation of R to be a ring homomorphism from R to a ring of the form $\mathrm{End}_D(V)$. Intuitively, we are mapping R into a ring that looks a lot like a ring of matrices. More generally, if R is a ring and N is a left R-module then we can produce a ring of R-linear endomorphisms $\mathrm{End}_R(N)$, where multiplication is given by composition, addition is addition of maps and the identity is the unit of this ring.

The general philosophy in ring theory is that if one understands enough or ever all representations of R then one understands R. This philosophy is something you've probably encountered before in a few settings. The first is in PM445 (I don't assume you've taken this). Here we have a finite group G. We can then make a ring $R = \mathbb{C}[G]$, which is, as a set, all elements of the form

$$\sum_{g \in G} \alpha_g g$$

with $\alpha_g \in \mathbb{C}$. Multiplication and addition are performed as one would reasonably expect. Representations of R then reduce to group homomorphisms from G into $\mathrm{GL}_n(\mathbb{C})$; equivalently, homomorphisms of R into $M_n(\mathbb{C})$. An important part of representation theory is that if one understands all irreducible representations of G (don't worry if you don't know what an irreducible representation of G is) then you have a pretty good picture of the group.

Another place you might have seen this is if you've taken PM446 and seen the Nullstellensatz. Here, to make things easy let's work with a polynomial ring $R = \mathbb{C}[t_1, \ldots, t_d]$. Since R is commutative, we don't have to worry about representations in which D is not commutative or $\dim(V) > 1$. In fact, all representations reduce to just studying maps from R to $M_1(\mathbb{C}) = \mathbb{C}$. The Nullstellensatz says that the maximal ideals of R correspond exactly to these maps.[1] In general there are various

[1]We recall that in a ring R a maximal left ideal is a left ideal M that is proper but has the property that if $M \subseteq N \subseteq R$ for some other left ideal N then either $N = M$ or $N = R$; such ideals exist by Zorn's lemma.

local-global principles that say understanding what occurs at the maximal ideals of R can be lifted back to say things about R.

If you know about these examples, great; if not, don't worry. But if you do, these examples can really help shape how one produces representations of a ring R. In the case of a polynomial ring, we saw that it suffices to really understand representations that came from reduction maps of the from $R \to R/M$ where M is a maximal ideal of R. In group representations, it is the same thing. In general, if R is a ring and M is a maximal left ideal of R then we can produce a left R-module $N := R/M$. This module N has the advantage of being simple; that is, the only R-submodules of N are (0) and N. In fact, every simple left R-module is isomorphism to a module of the form R/M with M maximal.

As it turns, each simple left R-module N yields a representation of R and to really understand the representations of R it suffices to understand those arising in this manner. (In groups, these correspond to the irreducible representations; in commutative algebra, these correspond to the closed points of the corresponding affine scheme.)

So how do we produce a representation of R from a left R-module N?

First we need to produce a division ring. This is done via Schur's lemma.

Lemma 0.1. *Let R be a ring and let N be a simple left R-module. Then $D := \mathrm{End}_R(N)$ is a division ring.*

Proof. We know that D is a ring. Let $f : N \to N$ be a nonzero R-linear map. Then the kernel of f is a submodule of N and since N is simple it is either (0) or N; if it is N then f is zero, which we assumed not to be the case; thus the kernel is trivial and f is one-to-one. Similarly, the image must of f must be N. Thus f is onto. Hence f is bijective and has a set-theoretic inverse $g : R \to R$. It is straightforward to check that g is also R-linear and $g \circ f = f \circ g = \mathrm{id}$. □

Now as it turns out, if R is a simple left R-module and $D := \mathrm{End}_R(N)$, then N inherits the structure of a left D-vector space. To see this, let $f : N \to N$ be an element of D. Then we define $f \cdot n := f(n) \in N$. It is routine to check the various axioms of a left vector space hold, but a good rule of thumb is that everything is obvious except for the axioms involving multiplication, where it is easy to get the order wrong. So let's just check that if $f, g : N \to N$ then $f \cdot (g \cdot n) = (fg) \cdot n$. Then left side is $f \cdot (g(n)) = f(g(n))$; the right side is $(fg) \cdot n = f \circ g(n)$. OK, that works and was easy, but there really are times where you can screw things up, so be careful.

Now $\mathrm{End}_D(N)$ is a ring of linear operators and we have a map $\phi : R \to \mathrm{End}_D(N)$ given as follows. We define $\phi(r) : N \to N$ via the rule $\phi(r)(n) = r \cdot n$. Then $\phi(r)$ is D-linear: if $f : N \to N$ is an R-linear homomorphism, then $\phi(r)(f \cdot n_1 + n_2) = \phi(r)(f(n_1) + n_2) = r \cdot f(n_1) + r \cdot n_2$. Now f is R-linear, so this is just $f(r \cdot n_1) + (r \cdot n_2) = f \cdot (\phi(r)(n_1)) + \phi(r)(n_2)$. We can also see this is a homomorphism. Again, the important thing to check is multiplication. Notice that for $r, s \in R$, $\phi(rs)(n) = rs \cdot n$, while $\phi(r) \cdot \phi(s) = \phi(r) \circ \phi(s)$, so $\phi(r) \circ \phi(s)(n) = \phi(r)(s \cdot n) = r \cdot s \cdot n$.

So the general philosophy in representation theory is that if one can understand all representations, one can understand the ring; and to understand all representations, it generally suffices to understand those of the form $R \to \mathrm{End}_D(N)$ with N a simple left R-module. Thus we have the meta-theorem that it suffices to understand the simple left R-modules to understand R. This is where things take a turn for the worse. With $R = \mathbb{C}[G]$, G a finite group, or $R = \mathbb{C}[t_1, \ldots, t_s]$, it's fairly easy to get a description of the simple modules. This isn't the case in general. This is where we now move to Dixmier's philosophy. One can obtain a coarser understanding of the simple R-modules by instead understanding their annihilators and one can hope that from there one can still obtain insight into one's ring R. This is actually a very powerful philosophy, but we probably should say more.

Given a ring R and a left R-module N, we define the *annihilator* of N to be the set of $x \in R$ such that $xn = 0$ for all $n \in N$. We'll denote this set by $\mathrm{Ann}(N)$. It's actually a two-sided ideal of R. Notice that $\mathrm{Ann}(N)$ is in fact the kernel of the representation $\phi : R \to \mathrm{End}_D(N)$, $D = \mathrm{End}_R(N)$. Let's check this. If $x \in \mathrm{Ann}(N)$, then $\phi(x)(n) = x \cdot n = 0$ for all $n \in N$ and so x is in the kernel of ϕ; conversely, if x is in the kernel of ϕ, then $\phi(x)$ is the zero map, so $x \cdot n = 0$ for all $n \in N$ and x is in the annihilator. Annihilators of simple left R-modules have a special name: they are called (left) *primitive* ideals. In general, we'll see that it's possible for an ideal to be primitive in the left sense but not the right, but for most nice rings there is no distinction between the two notions, and we'll simply use the term primitive ideal to talk about annihilators of simple left R-modules. A ring R is (left) primitive if (0) is a primitive ideal of R. Notice that being a primitive ring is the same as saying that R has a simple left R-module whose annihilator is trivial. Such a left module is called *faithful*. As mentioned above, left primitive rings need not be right primitive, but we will use primitive to mean left primitive throughout this course.

Exercise 2. *(Bergman) Show that the R produced as follows is right primitive but not left primitive. We'll have to give a few steps.*

(i) *Let $K = \mathbb{Q}(x)$ and let $\sigma : K \to K$ be the endomorphism $\sigma(f(x)) = f(x^2)$. Let A denote the ring of polynomials $c_0 + c_1 y + \cdots + c_d y^d$, $d \geq 0$, $c_0, \ldots, c_d \in K$ with sum as usual and multiplication given by $(cy^i)(c'y^j) = c\sigma^i(c')y^{i+j}$. Show that A is a ring and every left ideal of A is principal (that is, it is generated by a single element).*

(ii) *For each prime $p \geq 2$, let ω_p be a primitive p-th root of unity and let $\nu_p : K \to \mathbb{Z} \cup \{infty\}$ be the map (its called a valuation) defined by $\nu_p(0) = \infty$ and if $f(x)$ is nonzero then $\nu_p(f(x)) = 0$ if $f(x)$ does not a zero or pole at ω_p; is a if $f(x)$ has a zero of order a at ω_p and is $-a$ if $f(x)$ has a pole of order a at ω_p. Show that $\nu_p(\sigma(f(x)) = \nu_p(f(x))$ for all $f(x) \in K$ and that for a given nonzero $f(x) \in K(x)$, $\nu_p(f(x)) = 0$ for all but finitely many primes $p \geq 3$.*

(iii) *We extend ν_p to A by declaring that $\nu_p(c_0 + c_1y + \cdots + c_dy^d) = \min_i \nu_p(c_i)$. Show that the set A_p of elements in A such that $\nu_p(a) \geq 0$ is a subring of A and that it contains x and y.*

(iv) *Let $B = \bigcap_{p\geq 3, p \text{ prime}} A_p$. Show that B is not left primitive as follows. Suppose it were! Then there would exist a maximal left ideal I of B such that B/I has zero annihilator. Let $J = AI$ be the principal left ideal of A and let $g(y) = c_0 + c_1y + \cdots + c_dy^d$ be a generator.*

(v) *We'll first show that $g(y)$ must have degree 0 in y. To do this, suppose that g has degree > 0. Show there is a prime $p \geq 3$ such that $\nu_p(c_j) = 0$ for $j = 0, \ldots, d$ and show that $(x - \omega_p) \notin I$. Since I is a maximal left ideal we then have $b(x - \omega_p) + a = 1$ for some $a \in I$ and some $b \in B$. But then show $1 - b(x - omega_p)$ is of the form $a_0 + a_1y + \cdots + a_ry^r$ with $\nu_p(a_0) = 0$ and $\nu_p(a_i) > 0$ for all $i > 0$. Show that an element of this form cannot be in $Ag(y)$ and get a contradiction.*

(vi) *So conclude that $J = AI = A$ and so we can take $g(y) = 1$. Then we have $1 = a_1i_1 + \cdots + a_mi_m$ for some $a_1, \ldots, a_m \in A$ and $i_1, \ldots, i_m \in I$. Show that there is some finite product $u := (x - \omega_{p_1}) \cdots (x - \omega_{p_n})$ such that $b_i := ua_i \in B$ for all i. Then we have $u = b_1i_1 + \cdots + b_mi_m \in I$. Conclude that $I \supseteq Bu$. Show that $uB = Bu$ and conclude that the two-sided ideal $BuB \subseteq I$. Show that this gives that u annihilates B/I and so B is not left primitive.*

(vii) *OK. That was hard. Now let's show that B is right primitive. To do this, we note that $\mathbb{Q}(x)$ is a right A-module via $m \in \mathbb{Q}(x)$, $m \cdot s = (ms)$ for $s \in \mathbb{Q}(x)$ and $m \cdot y = m'(x)$ where $m'(x^2) = (m(x) + m(-x))/2$. Show that this makes $\mathbb{Q}(x)$ a right A-module.*

(viii) *Now let M denote the right B-submodule of $\mathbb{Q}(x)$ given by $M := xB$. Show that M is a faithful simple right B-module.*

Exercise 3. *Show that a commutative primitive ring is a field and hence an ideal in a commutative ring R is primitive if and only if it is maximal.*

We now come to the Jacobson density theorem, which shows that primitive rings embed densely in a ring of linear operators.

Theorem 0.1. *(Jacobson density theorem) Let R be a primitive ring, let M be a faithful simple left R-module, and let $\Delta = \mathrm{End}_R(M)$. Then R embeds in $\mathrm{End}_\Delta(M)$ via the rule $r \mapsto \Phi_r$, where $\Phi_r(m) = rm$. Moreover, if $m_1, \ldots, m_n$ are left Δ-linearly independent elements of M and $w_1, \ldots, w_n$ are in M then there exists some $r \in R$ such that $r \cdot m_i = w_i$ for $i = 1, \ldots, n$.*

Proof. The fact that the map $r \mapsto \Phi_r$ is a homomorphism is routine. The fact that it is injective comes from looking at the kernel: if $\Phi_r = 0$ then $rm = 0$ for all $m \in M$ and so $r = 0$ since M is faithful.

So now we prove the density part by induction on n. When $n = 1$ we have $Rm_1 = M$ since m_1 is nonzero and M is simple, so there is some $r \in R$ such that $rm_1 = w_1$. Now suppose that the claim holds for sets of size less than n. Then we may assume without loss of generality that $rm_1 = \cdots = rm_{n-1} = 0$ implies $rm_n = 0$. This means (using the induction hypothesis) that we have a well-defined R-module homomorphism

$$\Psi : M^{n-1} \to M$$

given by $\Psi((rm_1, \ldots, rm_{n-1})) = rm_n$. Now by the induction hypothesis, there for $j = 1, \ldots, n-1$ there is some r_j such that $r_jm_i = \delta_{i,j}m_j$ for $i = 1, \ldots, n-1$. In particular, $\Psi((0, 0, \ldots, m_j, 0, \ldots, 0)) = \Psi((r_jm_1, \ldots, r_jm_{n-1})) = r_jm_n$. Now the map $f_j : M \to M$ given by $m \mapsto \Psi((0, 0, \ldots, m, 0, \ldots, 0))$, where m is in the j-th slot is an element of $\Delta = \mathrm{End}_R(M)$. So we see that $f_j(m_j) = r_jm_n$. Now consider $(r_1 + \cdots + r_{n-1} - 1)m_i = r_im_i - m_i = 0$. So since $(r_1 + \cdots + r_{n-1} - 1)$ kills $m_1, \ldots, m_{n-1}$, by our assumption, it must also kill m_n. This

$$\sum_{i=1}^{n-1} r_im_n = m_n.$$

In other words,

$$\sum_{i=1}^{n-1} f_i(m_n) = m_n,$$

or

$$m_n - f_1m_1 - \cdots - f_{n-1}m_{n-1} = 0,$$

contradicting independence over Δ. The result follows. □

This is a theorem that a lot of people don't know, but it's actually very powerful and ties in to Jacobson's reduction philosophy for studying rings. We make the remark that if M is finite-dimensional as a left Δ-module then the map from R to $\mathrm{End}_\Delta(M)$ in JDT is in fact an isomorphism. The reason for this is that a Δ-linear endomorphism of M is completely determined by the image of a left Δ basis for N. But such a basis is finite and by JDT we can find an element of R that sends this basis wherever we'd like, and so the map from R to $\mathrm{End}_\Delta(M)$ is onto.

To explain his philosophy, we let R be a ring. We let J denote the intersection of all primitive ideals of R. (This is called the Jacobson radical of R—more on this later.) Notice we have an injective homomorphism $R/J \to \prod_{P \in \mathrm{Prim}(R)} R/P$ given

by $r \mapsto (r+P)_{P\in \mathrm{Prim}(R)}$, where $\mathrm{Prim}(R)$ denotes the set of all primitive ideals of R (often called the primitive spectrum of R).

Thus R/J is a subring of a direct product of primitive rings; by JDT, each primitive ring is a dense subring of a ring of linear operators, so we can understand R/J by studying its image in each of these rings of operators.

Notice that J is the intersection of all primitive ideals; consequently, J is the collection of elements that annihilate *every* simple left R-module.

Jacobson's philosophy, while not a panacea for dealing with all ring theoretic problems, is a very powerful approach. The setting in which one works is that one has a ring with certain properties and one wishes to prove something about this ring. The first step is to show that one can reduce to the case of studying R/J (note: one cannot always implement this step). After that, one uses the fact that R/J is a subring of a direct product of primitive rings and one uses the Jacobson density theorem to try to reduce one's problem to linear algebra.

We'll illustrate this approach by proving Jacobson's famous $x^n = x$ theorem.

Theorem 0.2. *(Jacobson's commutativity theorem) Let R be a ring and suppose that for each $x \in R$ there is some $n = n(x) > 1$ such that $x^n = x$. Then R is commutative.*

Let me be honest about this result: it's beautiful but it's not very useful. Why? Most times I don't need a theorem to tell me that a ring is commutative. During the times that I do need a theorem, probably the Jacobson hypothesis is not going to hold. Nevertheless this is a very striking result and if one understands how this arose then one can appreciate that it is a very difficult result, which shows us the power of Jacobson's philosophy. This theorem arose because during the time that Jacobson was working, Boolean algebras were very much in fashion. If you don't know what a Boolean algebra is, don't worry. The relevant fact is that it is a ring R in which $x^2 = x$ for all $x \in R$. (We think of elements of the ring as being sets and multiplication as being intersection, so if you intersect a set with itself it remains unchanged.) Notice that if R is a ring in which $x^2 = x$ then R is commutative. Let's see why.

Notice that $1 = (-1)^2 = -1$ and so R has characteristic 2. Next, for $x, y \in R$, we have $x+y = (x+y)^2 = x^2+xy+yx+y^2 = x+xy+yx+y$ and so $0 = xy+yx$. Since R has characteristic 2, we see that $xy = yx$ for all $x, y \in R$ and so R is commutative. That wasn't so hard, but let's try the next step: let's show that if R is a ring in which $x^3 = x$ for all $x \in R$ then R is necessarily commutative. This is quite a bit harder and will give us an appreciation for the power of Jacobson's philosophy.

Before we do this, let's introduce some terminology. A ring R is *reduced* if $x^2 = 0$ implies $x = 0$. A useful remark is that in a reduced ring R every idempotent element e (i.e., $e^2 = e$) is in the centre of R. To see this, let R be reduced and let $e \in R$ be idempotent and let $r \in R$. Then $er(1-e)$ has square zero. Since R is reduced, this tells us that $0 = er(1-e) = er - ere$. Similarly, $(1-e)re = 0$ and so $0 = re - ere$. Thus $er = ere = re$ and so $re = er$ for all $r \in R$.

Exercise: Show more generally that if R is a ring and e is idempotent then e is central if and only if it commutes with all nilpotent elements of R.

Now let's get back to studying rings R in which $x^3 = x$ for all $x \in R$. Notice that such a ring is reduced, since if $x^2 = 0$ then $x = x^3 = 0$. Also

$$(x^2)^2 = x^4 = x^3 \cdot x = x^2$$

and so x^2 is idempotent in R for all $x \in R$. Thus by the above remark, we see that all squares in R are central. Next we have $1 + x = (1+x)^3 = 1 + 3x + 3x^2 + x^3 = 1 + 3x + 3x^2 + x$ and so $3x = -3x^2$ and so $3x$ is central for every $x \in R$. Also since $(x+1)^2$ and x^2 are central, $2x + 1 = (x+1)^2 - x^2$ is central, and so $2x$ is central for every $x \in R$. Thus $x = 3x - 2x$ is central for every $x \in R$.

That wasn't too bad, but try doing rings with $x^5 = x$. I hope you can appreciate that it would not be easy to prove Jacobson's result without some machinery. To employ Jacobson's philosophy we need to know a bit about the Jacobson radical. We'll see more about it later, but for now we'll content ourselves with knowing the following.

Proposition 0.2. *Let R be a ring and let J denote its Jacobson radical. Then $x \in J$ if and only if $1 + ax$ is left invertible for every $a \in R$.*

Proof. Suppose that $x \in J$ and $1 + ax$ is not left invertible. Then $I := R(1 + ax)$ is a proper left ideal of R. Then by Zorn's lemma there is a maximal left ideal M of R that contains I (work this out if you haven't seen this fact before). Now $x \in J$ and so it annihilates the simple left R-module R/M. Equivalently, we have $xR \subseteq M$ and since M is a left ideal, we see $RxR \subseteq M$. Thus $ax \in M$. But by construction $1 + ax \in M$ and so $1 \in M$, a contradiction, since M is proper.

Next suppose that $1+ax$ is left invertible for every $a \in R$. We claim that x is in the Jacobson radical. To see this, suppose that this is not the case. Then there is a simple left R-module N such that $xN \neq (0)$. Pick $n \in N$, nonzero, such that $xn \neq 0$. Since N is simple, there is some $a \in R$ such that $a(xn) = -n$. Then $(1 + ax)n = n - n = 0$. But by assumption there is some $r \in R$ such that $r(1 + ax) = 1$ and so $n = r(1 + ax)n = r \cdot 0 = 0$, a contradiction. □

This brings us to the first reduction in Jacobson's theorem.

Lemma 0.3. *If R is a ring in which for each $x \in R$ there is some $n = n(x) > 1$ such that $x^n = x$, then the Jacobson radical of R is (0).*

Proof. Let J denote the Jacobson radical of R and let $x \in J$. Then $x^n = x$ for some $n > 1$ and so $(1 - x^{n-1})x = 0$. Now $1 - x^{n-1} = 1 + ax$ with $a = -x^{n-2}$, and so $1 - x^{n-1}$ is left invertible. Thus multiplying the equation $(1 - x^{n-1})x = 0$ by the left inverse of $1 - x^{n-1}$ gives $x = 0$. □

Now since $J = (0)$ we get that R is a subring of a product of rings of the form R/P where P ranges over the primitive ideals of R. Notice that if R has the property that for each $x \in R$ there is some $n = n(x) > 1$ such that $x^n = x$, then so does each R/P. Thus to show R is commutative it suffices to prove it for primitive rings with this property. So now we have reduced to the primitive case. Next we'll use the density theorem to reduce to the case of a division ring.

Suppose that R is a primitive ring such that for each $x \in R$ there is some $n = n(x) > 1$ such that $x^n = x$. Let N be a faithful simple left R-module and let $D = \mathrm{End}_R(N)$. Then we claim that N must be 1-dimensional as a left D-vector space. To see this, suppose that it is not. Then there exist n_1, n_2 in N that are linearly independent over D. By JDT, there exists some $x \in R$ such that $xn_1 = n_2$ and $xn_2 = 0$. Then we see that for all $n > 1$ we have $x^n n_1 = 0$. But by assumption $x^n = x$ for some $n > 1$ and so we must have $n_2 = xn_1 = 0$, a contradiction. This means that $N \cong D$ as a left R-module and so R is a dense subring of $\mathrm{End}_D(D)$. Since N is finite-dimensional as a left D-vector space, we see that $R = \mathrm{End}_D(D)$ by the above remark. But now you can check that $\mathrm{End}_D(D) \cong D^{\mathrm{op}}$, the opposite ring of D; that is, it is D as a set but with multiplication $a \star b = b \cdot a$. (The map from $\mathrm{End}_D(D) \to D^{\mathrm{op}}$ is just $f : D \to D$ is sent to $f(1)$. Notice that $f \circ g$ is sent to $f \circ g(1) = f(g(1)) = f(g(1) \cdot 1) = g(1)f(1)$, where the last step uses D-linearity.) Since R is dense in $\mathrm{End}_D(D)$, we see that $R = D^{\mathrm{op}}$. So R is a division ring.

So where are we now? We see that to prove Jacobson's commutativity theorem, it suffices to prove it for division rings. Most of this we'll do using the following two exercises (Assignment 1).

Exercise 4. *Let D be a division ring of characteristic $p > 0$ and suppose that $a \in D$ is such that $a^{p^n} = a$ for some $n \geq 1$. If a is not central, then there exists some $x \in D$ and some $i > 1$ such that $a^i \neq a$ and $xax^{-1} = a^i$.*

Exercise 5. *Prove that a finite division ring is a field using the following steps. Let D be a finite division ring.*

1 *Show that the centre Z of D is a field and has size q for some prime power q. Show that D has size q^n for some $n \geq 1$.*
2 *Let $G = D^*$ be the multiplicative group of D. Then $|G| = q^n - 1$. Use the class equation to show that*

$$q^n - 1 = |Z| + \sum_g |C_g| = q - 1 + \sum_g (q^n - 1)/|C(g)|,$$

where the sums runs over a complete set of non-central conjugacy class representatives and C_g denotes the conjugacy class of g and $|C(g)|$ denotes the centralizer of g in G.
3 *Show that if $g \in D^*$ then the centralizer of g in D is a division ring E that properly contains Z. Conclude that $|C(g)| = q^m - 1$ for some m.*
4 *Show that $q^m - 1$ divides $q^n - 1$ if and only if m divides n. Conclude that $|C(g)| = q^d - 1$ for some d dividing n and $d > 1$.*
5 *Rewrite the class equation as*

$$q^n - 1 = (q - 1) + \sum_{j=1}^{r} (q^n - 1)/(q^{d_j} - 1),$$

where r is the number of non-central conjugacy class representatives $d_1, \ldots, d_r > 1$ are divisors of n.
6 *Remember! Our goal is to show that D is a field, so we want to show $D = Z$ and so $n = 1$. Let $P(x) = \prod(x - \zeta)$, where ζ runs over all primitive n-th roots of unity. You can use the following fact: $P(x)$ is a monic polynomial with integer coefficients. (We'll show this later on when we talk about characters, but if you know a bit of Galois theory, you can convince yourself that the coefficients of $P(x)$ are fixed by the Galois group of $\mathbb{Q}(\exp(2\pi i/n))$ over $\mathbb{Q}$ and so the coefficients are rational; also ζ is an algebraic integer since it satisfies $\zeta^n - 1 = 0$—since the algebraic integers form a ring we see the coefficients are rational algebraic integers and hence integers. If you don't understand this, don't worry about it.) Show that $(x^n - 1) = P(x)Q(x)$ where $Q(x)$ is a monic integer polynomial and $x^d - 1$ divides $Q(x)$ in $\mathbb{Z}[x]$ for every divisor d of n with $d < n$.*
7 *Now show from step 5 that $P(q)$ divides $q - 1$.*
8 *Now we're ready to finish. Show that if $n > 1$ then $|P(q)| > q - 1$ and conclude that $n = 1$ and $D = Z$.*

OK. Let's finish off Jacobson's commutativity theorem.

Proposition 0.4. *Suppose that D is a division ring such that for each $x \in D$ there is some $n = n(x) > 1$ such that $x^n = x$. Then D is commutative.*

Proof. Notice that $2^n = 2$ for some $n > 1$ and so D has positive characteristic. In particular, there is some prime number p such that D has characteristic p. Then let P be the copy of $\mathbb{F}_p$ in D coming from the set $\{0, 1, \ldots, p - 1\}$. If D is not commutative then there exists some $a \in D$ that is not central. Let $F = P[a]$. Notice that F is commutative since P is a central subfield of F. By hypothesis, for each $x \in F$ we have $x^n = x$ for some $n > 1$ and so each nonzero x in F is invertible

and thus F is a field. Moreover, since $a^n = a$ for some $a > 1$, we see that F is a finite field. Thus there is some m such that $a^{p^m} = a$. By the above exercise, there is some $x \in D$ such that $xax^{-1} = a^i \neq a$. Now we have that $x^d = x$ for some $d > 1$. Let

$$E = \{ \sum_{s=0}^{p^m-1} \sum_{j=0}^{d-1} p_{s,j} a^s x^j : p_{s,j} \in P \}.$$

Since P is finite, we see that E is finite. Notice that E is a ring, since for $p, p' \in P$ we have

$$pa^s x^j p' a^t x^\ell = pp' a^s (x^j a x^{-j})^t x^{\ell+j} = pp' a^s a^{t \cdot i^j} x^{\ell+j} \in E.$$

Then E is a subring of D and so it inherits the Jacobson property; in particular, every nonzero element of E has an inverse and so E is a finite division ring and hence commutative, a contradiction, since x and a do not commute. The result follows. □

The Artin-Wedderburn theorem

We recall that a ring R is *left artinian* if every descending chain of left ideals of R

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$$

terminates; i.e., there exists some n such that $I_n = I_{n+1} = \cdots$. A ring is left noetherian if every ascending chain of left ideals terminates. Right artinian and noetherian are defined analogously and a ring that is both left and right artinian is called artinian; a ring that is both left and right noetherian is called noetherian.

Exercise 6. *Show that being left artinian is equivalent to every non-empty set of left ideals having a minimal element (not necessarily unique) with respect to inclusion. Conversely show that being left noetherian is equivalent to every non-empty set of left ideals having a maximal element and is equivalent to all left ideals being finitely generated.*

Similarly, if R is a ring we can define left artinian R-modules as those satisfying the descending chain condition on left submodules and we can define left noetherian R-modules.

We won't spend a lot of time on the Artin-Wedderburn theorem, but artinian rings play an important role in the study of rings, which we'll see when we study noncommutative localization and Goldie's theorem. The intuition one should have is that we'll see that if R is a commutative artinian ring whose Jacobson radical is zero then R is a finite product of fields. In general, a reduced commutative ring (i.e., $x^2 = 0 \implies x = 0$) has something like a field of fractions; one can invert the nonzero divisors in the ring and one obtains a finite product of fields.

We'll see that one has a noncommutative analogue of a field of fractions and what one ultimately obtains is an artinian ring with Jacobson radical zero. We pause to highlight the main results that we'll show about artinian rings.

(i) The Jacobson radical of an artinian ring is nilpotent.
(ii) An artinian ring with trivial Jacobson radical is a finite direct product of matrix rings over division rings.
(iii) (Hopkins' theorem) A left artinian ring is left noetherian.

The Jacobson radical

Let's say a bit about the Jacobson radical. The most important result about Jacobson radicals is Nakayama's lemma.

Theorem 0.3. *(Nakayama's lemma) Let R be a ring and let J denote its Jacobson radical. If M is a finitely generated left R-module and $JM = M$ then $M = (0)$.*

Remark 0.5. This is not true if M is not finitely generated. For example, let $R = \{a/b \colon a, b \in \mathbb{Z}, b \text{ odd}\}$. Then R is a ring and one can check using our left invertibility criterion that the Jacobson radical of R is precisely $2R$. Notice that $\mathbb{Q}$ is a left R-module and $J\mathbb{Q} = \mathbb{Q}$ but $\mathbb{Q}$ is nonzero.

Proof. Suppose that M is nonzero. Let $d \geq 1$ be the size of a minimal generating set and let $m_1, \ldots, m_d$ be a set of generators. Then since $JM = M$ we see that $m_d = j_1 m_1 + \cdots + j_d m_d$ for some $j_1, \ldots, j_d \in J$. In particular, $(1 - j_d) m_d = j_1 m_1 + \cdots + j_{d-1} m_{d-1}$. But $1 - j_d$ is left invertible and so $m_d \in Rm_1 + \cdots + Rm_{d-1}$, contradicting the minimality of our generating set. □

We recall that a left ideal I in a ring R is nil if for each $x \in I$ there is some $n = n(x) \geq 1$ such that $x^n = 0$. A left ideal I is *nilpotent* if there is some n such that $I^n = (0)$. A nilpotent ideal is obviously nil. An important fact is that every nil left ideal is contained in the Jacobson radical. To see this, if I is a nil left ideal and $x \in I$ then ax is nilpotent for each $a \in R$ and so $1 + ax$ is left invertible (use the geometric series). This means that x is in the Jacobson radical. The remark above, however, shows that the Jacobson radical need not be nil. For left artinian rings, however, we have a very strong description of the Jacobson radical.

Proposition 0.6. *Let R be a left artinian ring. Then the Jacobson radical, J, of R is nilpotent. That is, there is some $n > 1$ such that $J^n = (0)$.*

Proof. Consider the chain

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots .$$

Then since R is artinian, there is some $n > 1$ such that $J^n = J^{n+1} = \cdots$. In particular, $J^n = J^{2n}$. Suppose that J^n is nonzero. Now let S denote the collection of left ideals L contained in J^n for which $J^n L$ is nonzero. Notice that S is nonempty since J^n is in S. We can pick a minimal element L of S. Then there is some $x \in L$ such that $J^n x \neq 0$ and so $Rx \subseteq L$ is in S. By minimality of L, we see that $Rx = L$. Also, $J^n(J^n L) = J^{2n}L = J^n L \neq (0)$ and so $J^n L = L$ and so we see that $JL = J^{n+1}L = J^n L = L$ and L is finitely generated. By Nakayama's lemma, $L = (0)$, a contradiction. □

A ring with trivial Jacobson radical is called *semiprimitive*. In general, if the intersection of all ideals with a property P is equal to zero, then we call a ring semi-P. So semiprimitive really means that the intersection of the primitive ideals (that is, the Jacobson radical) is zero; semiprime means that the intersection of the prime ideals is zero, etc.

Artin and Wedderburn completely give the structure theory of semiprimitive left artinian rings.

Theorem 0.4. *(Artin-Wedderburn) Let R be a semiprimitive left artinian ring. Then R is isomorphic to a direct product of matrix rings*

$$\prod_{i=1}^{s} M_{n_i}(D_i),$$

where the D_i are division rings.

In the case that R is commutative, notice that the matrix rings must be 1×1 matrix rings and the division rings are fields, so in this case the conclusion is stronger: R is a direct product of fields when R is a commutative artinian ring with no nonzero nil ideals, which is what we asserted above. We make the remark that any ring of the form

$$\prod_{i=1}^{s} M_{n_i}(D_i)$$

is semiprimitive and left artinian. To do this, we remark that $M_n(D)$ is a simple ring (see below for a proof) and thus is primitive[2]. It is left artinian since it is n^2-dimensional as a left D-vector space; since left ideals are D-vector subspaces, looking at dimensions we see that a descending chain must terminate. Now we leave it to the reader to show that a finite product of primitive left artinian rings is semiprimitive and left artinian.

Proposition 0.7. *If R is a left artinian primitive ring then R is isomorphic to $M_n(D)$ for some division ring D and some $n \geq 1$.*

Proof. Let M be a faithful simple R-module and let $\Delta = \mathrm{End}_R(M)$. We claim that M is finite-dimensional as a left Δ-vector space. To see this, suppose that we have an infinite linearly independent set $m_1, m_2, \ldots$. Then by the Jacobson density theorem, for each $i > 0$ there is some $r_i \in R$ such that $r_i m_1 = \cdots r_i m_i = 0$ and $r_i m_{i+1} \neq 0$. Now let $I_i = \{r \in R \colon rm_1 = \cdots = rm_i = 0\}$. Then each I_i is a left ideal and notice that $I_i \supseteq I_{i+1}$ by definition. Finally, $r_i \in I_i$ but is not in I_{i+1} so we get an infinite descending chain of ideals

$$I_1 \supseteq I_2 \supseteq \cdots ,$$

contradicting the left artinian hypothesis. Thus M is finite dimensional—let's say the dimension is n. Now if Δ were a field, we'd feel pretty good: M would be a finite-dimensional vector space and we'd know that the endomorphism ring is matrices over Δ. In the division ring setting there is one subtlety. We have to introduce the *opposite ring*. Given a ring R the opposite ring R^{op} is just R as set with multiplication $r \star s = s \cdot r$; that is, we reverse the order of multiplication. If R is commutative then its opposite ring is itself. If R is a division ring then so is R^{op}. Now let $m_1, \ldots, m_n$ be a basis for M as a left Δ-vector space. We claim that

$$S := \mathrm{End}_\Delta(M) \cong M_n(\Delta)^{\mathrm{op}} \cong M_n(\Delta^{\mathrm{op}}).$$

To define the isomorphism, let $f \in S$. Then $f(m_i) = \sum_j a_{i,j} m_j$ for some $a_{i,j} \in \Delta$. We define a map $\Phi : S \to M_n(\Delta)^{\mathrm{op}}$ by $\Phi(f) = (a_{i,j})$. This is definitely well-defined and it's fine to see that $\Phi(f+g) = \Phi(f) + \Phi(g)$. Suppose that $\Phi(g) = (b_{i,j})$. Notice that

$$f \circ g(e_i) = f(\sum_k b_{i,k} e_k) = \sum b_{i,k} \sum_j a_{k,j} m_j.$$

Thus the (i,j) entry of $\Phi(f \circ g)$ is $\sum_k b_{i,k} a_{k,j}$, and so $\Phi(f \circ g)$ is just the product of $(b_{i,j})$ and $(a_{i,j})$ in $M_n(\Delta)$, which is the product of $(a_{i,j})$ and $(b_{i,j})$ in $M_n(\Delta)^{\mathrm{op}}$. So it is a homomorphism. To see that it is 1-to-1, we remark that if f is in the kernel then it must send each m_i to 0 and so it is the zero map. It remains to see why this map Φ is onto. But this just comes from the fact that M is a free Δ-module so we can send $m_1, \ldots, m_n$ wherever we'd like! Finally, we remark that $M_n(\Delta)^{\mathrm{op}} \cong M_n(\Delta^{\mathrm{op}})$, which is a matrix ring over a division ring. □

Remark 0.8. Observe that $M_n(D)$ is a simple ring.

[2]Why is this, you ask? Well, take a maximal left ideal of a simple ring; the quotient is a simple module. It's faithful because the annihilator is a proper two-sided ideal and hence must be zero. This means that our ring is simple

Suppose we have some nonzero ideal I. Then there is some nonzero $A = (a_{i,j}) \in I$. Pick k, ℓ such that $a_{k,\ell} \neq 0$. Then $E_{i,k}AE_{\ell,j} = a_{k,\ell}E_{i,j}$. Since $a_{k,\ell}$ is in D and nonzero, $E_{i,j} \in I$. But now $1 = \sum E_{i,i} \in I$.

Corollary 0.9. *If R is a primitive left artinian ring then R is simple and so every primitive ideal in a left artinian ring is a maximal ideal.*

Now to finish the proof of Artin-Wedderburn, we introduce the notion of a prime ring. A two-sided ideal P of a ring R is called *prime* if whenever $a, b \in R$ are such that $aRb \subseteq P$ we must have either a or b is in P. A ring is a prime ring if (0) is a prime ideal. We note that primitive ideals are a subset of the prime ideals of a ring. Usually the collection of prime ideals of a ring R is denoted $\mathrm{Spec}(R)$ and the primitive ideals are denoted $\mathrm{Prim}(R)$. We saw from the exercise above that when R is a commutative ring primitive ideals are precisely the maximal ideals.

Proposition 0.10. *A primitive ring is prime; consequently every primitive ideal of a ring is a prime ideal.*

Proof. Let R be a primitive ring and let M be a faithful simple left R-module. Suppose that $aRb = (0)$. Then if $b \neq 0$ there is some $m \in M$ such that $bm \neq 0$ since M is faithful. Thus $Rbm = M$ since M is simple. But $(0) = aRbm = aM$ and so a annihilates M and thus must be zero. Hence R is prime. □

Remark 0.11. If R is a ring and $P_1, \ldots, P_n$ are distinct maximal ideals then $P_1 \not\supseteq P_2P_3 \cdots P_n$.

Proof. We prove this by induction on n. When $n = 2$ it is clear. Suppose that it is true up to $n-1$. Then $P_1 \not\supseteq I := P_2 \cdots P_{n-1}$. In particular, there is some $a \in I \setminus P_1$. Also there is some $b \in P_n \setminus I$. So if $P_1 \supseteq IP_n$ then we have $aRb \subseteq P_1$ with $a, b \notin P_1$, a contradiction since P_1 is prime. □

Proposition 0.12. *Let R be a left Artinian ring. Then R has only finitely many primitive ideals.*

Proof. If $P_1, P_2, \ldots$ is an infinite set of distinct primitive ideals, then since we know primitive ideals are maximal in a left Artinian ring, we have $P_{n+1} \not\supseteq P_1 \cdots P_n$. But

$$P_1 \supseteq P_1P_2 \supseteq \cdots$$

is a descending chain, so we must have $P_1P_2 \cdots P_n = P_1P_2 \cdots P_nP_{n+1} \subseteq P_{n+1}$, contradiction. □

Corollary 0.13. *Let R be a semiprimitive left artinian ring. Then R is a product of matrix rings over division rings.*

Proof. Let $P_1, \ldots, P_n$ be the distinct primitive ideals of R. We note that the P_i are all maximal and hence $P_i + P_j = R$ for $i \neq j$. Then since R is semiprimitive the intersection of the P_i is trivial. We now use the Chinese Remainder theorem: If $P_1, \ldots, P_n$ are distinct maximal ideals whose intersection is (0) then $R \cong \prod R/P_i$. Let's create a homomorphism $\Phi : R \to \prod R/P_i$ via $r \mapsto (r + P_1, \ldots, r + P_n)$. This is 1-to-1 since the intersection of the P_i is zero. To see that it is onto, by the remark we have that $P_i + \prod_{j \neq i} P_j = R$ since P_i is maximal. So there exists $b_i \in \cap_{j \neq i} P_j$ such that $b_i \in 1 + P_i$. Then $\Phi(b_i) = e_i$, where e_i is the i-th coordinate function. So $\Phi(\sum r_ib_i) = (r_1 + P_1, \ldots, r_n + P_n)$ and so Φ is onto. □

In general a left artinian ring need not be right artinian (and vice versa).

Exercise 7. *Let K be a field extension of F and suppose that K is infinite-dimensional over K. Show that the ring*

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a \in F, b, c \in K \right\}$$

is right artinian but not left artinian. Let C be the subring of rational numbers consisting of those numbers that can be written with an odd denominator. Show that the ring

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a \in C, b, c \in \mathbb{Q} \right\}$$

is right noetherian but not left noetherian. (This works more generally when C is a commutative noetherian ring and we replace $\mathbb{Q}$ by the field of fractions of C.)

Exercise 8. *Show that the intersection of the powers of the Jacobson radical of S is nonzero, where S is as in the preceding exercise. (non-Hint: it's probably a good idea to figure out what the Jacobson radical is first.)*

Finally, we note that a left artinian ring is left noetherian. The converse isn't true (e.g., $\mathbb{Z}$). We note that this is trivial for semiprimitive left artinian rings. To see this, observe that such a ring is of the form $\prod_{i=1}^{d} M_{n_i}(D_i)$. It is straightforward to show that a finite product of left noetherian rings is left noetherian, so it suffices to show $M_n(D)$ is noetherian. But $M_n(D)$ is n^2-dimensional as a left D-vector space (regarding D as the subring of scalar matrices) and each left ideal is a D-subspace of $M_n(D)$ and so any ascending chain must terminate.

Exercise 9. *Show more generally that if R is a semiprimitive left artinian ring then an artinian left R-module is left noetherian.*

We'll prove a more general result now.

Theorem 0.5. *Let R be a left artinian ring and let M be an artinian left R-module. Then M is left noetherian.*

Remark 0.14. Taking $M = R$ gives the fact that a left artinian ring is left noetherian.

Proof. Let J be the Jacobson radical of R. Then $J^n = (0)$ for some n. Then we have a chain

$$M \supseteq JM \supseteq J^2M \supseteq \cdots \supseteq J^{n-1}M \supseteq (0).$$

Notice that each $J^iM/J^{i+1}M$ is an R/J-module and by correspondence we see it is left artinian. Hence by the exercise it is left noetherian. Now we claim that M is left noetherian. To do this, suppose that M is not left noetherian. Then there is a biggest $j \geq 0$ with $j < n$ such that J^jM is not left noetherian. Then we have a short exact sequence

$$0 \to J^{j+1}M \to J^jM \to J^jM/J^{j+1}M.$$

We now leave it to the reader to verify the following straightforward claim: in a short exact sequence, if the modules on the ends are left noetherian then so is the modules in the middle. Then $J^{j+1}M$ is left noetherian by maximality of j; $J^jM/J^{j+1}M$ is annihilated by J and hence can naturally be viewed as an R/J-module, where we saw it was left noetherian. The result follows. □

Noncommutative localization and Goldie's theorem

Ore's theorem

One of the important facts in commutative algebra is that an integral domain has a field of fractions. One obtains this field by inverting the nonzero elements of the integral domain, a process that falls under the umbrella of what is called *localization*. In the noncommutative setting, inverting elements is not so straightforward. For example, imagine we have a noncommutative ring R with no nontrivial zero divisiors. Then we'd like to form a division ring of fractions as a generalization of the field of fractions construction in commutative ring theory. The problem one first encounters is that writing r/s for $r, s \in R$ with s nonzero is now ambiguous since if r and s do not commute then $sr \neq rs$ and so if we try to multiply both sides on the left and right by s^{-1}, we see that we should expect $rs^{-1} \neq s^{-1}r$. This first problem is easy enough to resolve: we can just declare that we are only going to work with left fractions; i.e., elements of the form $s^{-1}r$. But now one encounters a much more serious problem: multiplication. If we take $s_1^{-1}r_1$ and multiply it on the right by $s_2^{-1}r_2$, we'd like to be able to write this as some $s_3^{-1}r_3$. But all we actually get is $s_1^{-1}r_1s_2^{-1}r_2$. Ore (although he is not the first person to notice this) discovered a fix! Suppose in our ring R we could somehow ensure that any element of the form rs^{-1} could be written as $(s')^{-1}r'$ for some nonzero s' and some r in R? Then we could take the expression $s_1^{-1}r_1s_2^{-1}r_2$ and write it as $s_1^{-1}(r_1s_2^{-1})r_2$. We could then rewrite $r_1s_2^{-1}$ as $(s')^{-1}r'$ for some nonzero s' and some r' in R and then we would have

$$s_1^{-1}r_1s_2^{-1}r_2 = s_1^{-1}(r_1s_2^{-1})r_2 = s_1^{-1}(s')^{-1}r'r_2 = (s's_1)^{-1}(r'r_2),$$

and so we would have a way, at least in principle, of multiplying fractions. This is obviously very imprecise and needs to be made rigorous, but this is the main idea behind how one performs localization in the noncommutative setting. We now make these notions precise.

Definition 0.15. *Let R be a ring and let S be a subset of R that is closed under multiplication and has no left or right zero divisors (we call such a set with no left or right zero divisors* regular *and an element that is not a left or right zero divisor is called a regular element). We say that S is a* left Ore *set in R if whenever $r \in R$ and $s \in S$ there exist $r' \in R$ and $s' \in S$ such that $s'r = r's$. Equivalently $Sr \cap Rs$ is non-empty.*

Intuitively, this is saying that we can rewrite $rs^{-1} = (s')^{-1}r'$ as described above.

Theorem 0.6. *(Ore's theorem) Let R be a ring and let S be a regular multiplicatively closed left Ore subset of R. Then there exists a ring, which we denote $S^{-1}R$ with the following properties:*

(i) *there is an injective ring homomorphism from $R \to S^{-1}R$, so that we can regard R as a subring of $S^{-1}R$;*
(ii) *every element of S is left and right invertible in $S^{-1}R$;*
(iii) *every element of $S^{-1}R$ can be written in the form $s^{-1}r$ for some $s \in S$ and some $r \in R$.*

We note that the converse holds: that is, if there exists an overring of R with the above properties then by the third condition we can write rs^{-1} in the form $(s')^{-1}r'$ and so $sr' = s'r$.

Proof. We let $T = \{(s, r) \colon s \in S, r \in R\}$. (We think of a pair (s, r) as corresponding to the element $s^{-1}r$.) Then just as when we form the field of fractions, we have to put an equivalence on elements of T. By hypothesis, there is some $r_1 \in R$ and $s_1 \in S$ such that $s_1s = r_1s'$. We then declare that $(s, r) \sim (s', r')$ if $s_1r = r_1r'$ for some $s_1 \in S$ and $r_1 \in R$ such that $s_1s = r_1s'$. Notice that s_1s plays the role of a "common denominator" for (s, r) and (s', r') in the sense that $s_1ss^{-1} \in R$ and $s_1s(s')^{-1} = r_1 \in R$.

Exercise 10. *Show that this is an equivalence relation on T and that if $s_1r = r_1r'$ for some $s_1 \in S$ and $r_1 \in R$ such that $s_1s = r_1s'$ then it holds for* every *tuple $(s_1, r_1) \in S \times R$ such that $s_1s = r_1s'$.*

We let $s^{-1}r$ denote the equivalence class of (s,r) in T. (We'll also denote it as $[(s,r)]$ if we want to be careful.) We now show that T is a ring with identity $[(1,1)]$ and zero $[(1,0)]$. Notice that if we think of $s_1 s$ as being a common left denominator then addition in T is performed as follows $s^{-1}r + (s')^{-1}r' = (s_1 s)^{-1}s_1 r + (s_1 s)^{-1}r_1 r'$, so we define the sum to be $(s_1 s)^{-1}(r_1 r' + s_1 r)$. Similarly, multiplication is defined using the left Ore condition. It is tedious to check, but it can be seen that T becomes a ring under these operations. (I leave it to you to check!) Now we have a homomorphism from $R \to T$ given by $r \mapsto [(1,r)] = 1^{-1}r$. It is easy to see that under our addition and multiplication that this gives a homomorphism from R to T. Moreover $[(s,1)] \cdot [(1,s)] = [(1,s)] \cdot [(s,1)] = [(1,1)]$ and so all elements of S are left and right invertible in T. Finally, we have $[(s,r)] = [(s,1)] \cdot [(1,r)] = s^{-1}r$. □

When S is the set of regular elements of R, we'll often denote $S^{-1}R$ by $Q(R)$ and think of it as the quotient ring of R (like a field of fractions).

Anyway, this is great, but unfortunately the Ore condition is not always satisfied. For example, if we take a free algebra $R = k\{x,y\}$, that is a noncommutative polynomial ring on x and y with no relations, and we let S denote the set of nonzero elements of R then $xS = yR$ has no solutions.

Goldie to the rescue!

Alfred Goldie determined exactly when one can invert the nonzero regular elements of a ring R to obtain a noncommutative analogue of the field of fractions. Rings satisfying Goldie's conditions are today called *Goldie* rings in his honour. The most important fact here is that a semiprime noetherian ring is a Goldie ring and so we have the analogue of the field of fractions construction in this setting.

Definition 0.16. *Let R be a ring. We say that a left ideal L is a left annihilator if there is some subset S of R such that $\{x \in R\colon xs = 0 \forall s \in S\}$. We say that R is* (left) Goldie *if R satisfies the ascending chain condition on left annihilators and R contains no infinite direct sum of left ideals.*

It is clear that a left noetherian ring is left Goldie. The converse is not true!

Exercise 11. *Give an example of a left Goldie ring that is not left noetherian.*

We'll try to give an overview of the strategy behind Goldie's theorem. We recall that a ring R is semiprime if R has no nonzero nilpotent ideals. Equivalently, if I is a nonzero ideal and $I^2 = (0)$ then $I = (0)$.

Theorem 0.17. *(Goldie) Let R be a semiprime left Goldie ring. Then is S is the set of regular elements of R then S is a left Ore set and $Q(R) := S^{-1}R$ is a semiprimitive Artinian ring. In particular when R is a domain, we have a division ring of quotients.*

To prove this, we need the notion of an essential ideal. One can intuitively think of essential as meaning "large". A left ideal I is an essential left ideal of R if $I \cap L \neq (0)$ for every nonzero left ideal L of R. For example in $R \times R$ the ideal $R \times \{0\}$ is not essential, but if R is a commutative integral domain then every nonzero ideal is essential. So the strategy behind proving Goldie's theorem can be summed up as follows.

(i) Show that if $a \in R$ is a regular element then Ra is an essential left ideal of R.
(ii) So now we'd like to show that S, the set of regular elements of R, is a left Ore set, so we need to show that if $a \in S$ and $r \in R$ then $r'a = a'r$ for some $a' \in S$ and some $r' \in R$. To do this, we let $J = \{x \in R\colon xr \in Ra\}$. Since Ra is essential, we know J is non-empty. So the next step is to show that J is essential.
(iii) (Tricky step) Then show that if J is essential then it contains a regular element. From there we'll get the Ore condition: there is some $a' \in J \cap S$ such that $a'r \in Ra$ and we are done with the Ore condition.
(iv) So now we at least know we can form the quotient $Q(R) := S^{-1}R$. We'd like to show that this is a semiprimitive Artinian ring. (That is, it's isomorphic to a finite product of matrix rings over division rings.)
(v) First we show that $Q(R)$ has no nonzero nilpotent ideals. The reason for this is that if I is a two-sided nilpotent ideal then if I is nonzero, then there is some nonzero $s^{-1}r \in I$ and so $r \in I \cap Q(R)$. Then $I \cap Q(R)$ is a nilpotent ideal of R. Since the Jacobson radical contains all nil ideals of R we see that $Q(R)$ has zero Jacobson radical.
(vi) (Other tricky step) Next we want to show that $Q(R)$ is left artinian. This takes a bit of arguing, but it is not so bad.

So let's look at Step 1.

Lemma 0.18. *Let R be a left Goldie ring and let a be an element whose left annihilator is zero (in particular if a is regular then this holds). Then Ra is an essential left ideal.*

Proof. If Ra is not essential then there is some nonzero left ideal I such that $I \cap Ra = (0)$. Now consider the left ideals $I, Ia, Ia^2, \ldots$. We claim these must form an infinite direct sum. To see this, suppose that this is not direct. Then there is some $n \geq 1$ and $x_0, \ldots, x_n \in I$, not all zero, such that $x_0 + x_1 a + x_2 a^2 + \cdots + x_n a^n = 0$. Notice that $x_0 \in I \cap Ra$ so $x_0 = 0$. Since the left annihilator of a is zero, we then see $x_1 + \cdots + x_n a^{n-1} = 0$ and we can repeat this and get that all the $x_i = 0$. Since R is left Goldie, we can't have an infinite direct sum of left ideals and so Ra is essential. □

On to Step 2. Let's see that the left ideal J is an essential left ideal. Suppose that there is some left ideal I such that $I \cap J = (0)$. Now if Ir is nonzero then $Ir \cap Ra$ is nonzero and so there is some nonzero $x \in I$ such that $xr \in Ra$ and so $x \in J \cap I$; if $Ir = 0$ then I is contained in J. Either way, we have J is essential.Jr is contained in Ra, which is essential, so if Ir is nonzero then there is some $x \in I$ such that xr is nonzero and $xr = ua$ for some $r \in R$. That means that $Ir \oplus Jr$ is direct. And we're done with step 2.

Let's move on to Step 3. Like I said, this is a bit tricky. The good news is that once we are done with this, the only step that remains unproven is Step 6 (which is also tricky). To do this, we need a few lemmas and we'll start with a basic remark, which is easy but very important: the acc on left annihilators in a ring is equivalent to dcc on right annihilators (and vice versa). First basic lemma.

Lemma 0.19. *(proper containment of right annihilators give a direct sum) Let R be a semiprime left Goldie ring. If $A \supseteq B$ are left ideals of R with distinct right annihilators then there is some $a \in A$ such that $Aa \neq (0)$ and $Aa \cap B = (0)$.*

Proof. Notice that $rann(A) \subseteq rann(B)$; by hypothesis, this containment is proper. Now since R is left Goldie we have acc on left annihilators. Thus we have dcc on right annihilators. It follows that there is some right annihilator U that is minimal with respect to being contained in $rann(B)$ and strictly containing $rann(A)$. Since U properly contains $rann(A)$ we see that AU is nonzero. It's a two-sided ideal! Since R is semiprime $(AU)^2$ is nonzero, so there is $u \in U$, $a \in A$ such that $AuaU \neq (0)$. Now we have $ua \in A$, Aua is nonzero, and we claim that $Aua \cap B = (0)$—this will finish the proof. Steps.

(i) So if not, there is $x \in A$ such that $xua \in B$ is nonzero. That means that $xua \cdot rann(B) = 0$.
(ii) Since U is contained in $rann(B)$, we see that $xuaU = (0)$.
(iii) That means that uaU is contained in $rann(x)$.
(iv) Notice that uaU is also contained in U since $u \in U$ and U is a right ideal.
(v) Thus $rann(x) \cap U \subseteq U$; since $x \in A$, $rann(x) \supseteq A$.
(vi) Thus $rann(x) \cap U$ is either A or U by minimality of U.
(vii) It can't be A, since $A(uaU)$ is nonzero and uaU is in the intersection.
(viii) So $rann(x) \cap U = U$. That means $rann(x) \supseteq U$. But xua is nonzero and $u \in U$. Done!

□

This gives us the interesting fact: in a Goldie ring we also have dcc on left annihilators.

Let's see why. If

$$L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots$$

is an infinite strictly descending chain of left annihilators then we know that

$$rann(L_1) \subseteq rann(L_2) \subseteq rann(L_3) \subseteq \cdots$$

is an infinite strictly ascending chain of right annihilators. By the lemma, since the containments are proper, there is some $a_i \in L_i$ such that $L_i a_i$ is nonzero and $L_i a_i \cap L_{i+1}$ is zero. Then

$$L_1 a_1 + L_2 a_2 + \cdots$$

is direct. To see this, suppose that $x_1 a_1 + \cdots + x_n a_n = 0$ with $x_i \in L_i$. Then since $a_2, \ldots, a_n$ are all in L_2 we have $x_1 a_1 \in L_1 a_1 \cap L_2 = (0)$ so $x_1 a_1 = 0$. Continuing in this manner, we see that all of the $x_i a_i = 0$ and we get directness.

Now we can prove that an essential left ideal in a semiprime left Goldie ring R contains a regular element. We first do the case when R is a prime ring. Let I be an essential left ideal of R. So we proved this fact and that we have acc and dcc on left and right annihilators. Notice that as a consequence we can prove that a semiprime Goldie ring has no nonzero nil left or right ideals.

Proof. Suppose that I is a nonzero nil left ideal. Choose $a \in I$ with $a \neq 0$ and maximal right annihilator wrt this property. If $r \in R$ then ra is nilpotent so there is some $d \geq 0$ such that $(ra)^{d+1} = 0$; we take d minimal. If $d > 1$ then we get $(ra)^d(ra) = 0$, so ra is in the right annihilator of $(ra)^d$. But clearly $rann((ra)^d)$ contains $rann(a)$ so by maximality they are the same unless $ra = 0$, which gives $d = 0$, a contradiction. Thus $Ra \subseteq rann(a)$ and so $aRa = (0)$. But this contradicts the fact that R has no nilpotent ideals $(RaR)^2 = (0)$. So $a = 0$. □

Lemma 0.20. *Let R be a semiprime left Goldie ring. If I is an essential left ideal of R then I contains a regular element c.*

Proof. Let $a_1, \ldots, a_n \in I$ be a maximal length sequence satisfying $a_i \in lann(a_j)$ whenever $j < i$ and $lann(a_i) \cap Ra_i = (0)$ for all i. We note we cannot have an infinite sequence because $Ra_1 + Ra_2 + \cdots$ is direct. (Why?) Then $J = lann(a_1) \cap lann(a_2) \cap \cdots \cap lann(a_n) \cap I = (0)$. Why? Otherwise, there would be some a_{n+1} in the intersection. Notice that a_{n+1} is in the left annihilator of a_j for $j < n+1$. We claim we can pick a_{n+1} so that $lann(a_{n+1}) \cap Ra_{n+1} = (0)$. To see this notice that we can pick some $x \in J$ that is not nilpotent. Then there is some d such that $lann(x^d)$ is maximal. Now we'll let $a_{n+1} = x^d$. If $y = ra_{n+1}$ satisfies $ya_{n+1} = 0$ then we have $r \in lann(a_{n+1}) = lann(x^{2d}) = lann(x^d)$ and so $y = ra_{n+1} = 0$.

Now we're almost done. We just showed that $J = (0)$ and since I is essential this means that the intersection of the left annihilators of the a_i is trivial. Now let $s = a_1 + \cdots + a_n$. Then since the sum of the left ideals is direct, $lann(s) = \bigcap lann(a_i)$ and so s is left regular. Now if s is not right regular then $rann(s)$ is a nonzero right ideal. As before there is some $x \in rann(s)$ that is not nilpotent. We pick x^d such that the left annihilators stabilize from x^d onward. Now since s is left regular we know

from above that Rs is essential. So $Rs \cap Rx^d \neq (0)$. Pick $0 \neq a = rs = r'x^d$. Then $ax = rsx = r'x^{d+1}$. But now $sx = 0$ so $0 = r'x^{d+1}$ but the left annihilator of x^d is the same as that of x^{d+1} so $r'x^d = 0$, a contradiction.

□

OK, so now it just remains to show that Step 5 holds. As we said, we'd do this via the following lemma.

Lemma 0.21. *Let I be a left ideal in $Q(R)$. Then there is some left ideal J such that $I \oplus J = Q(R)$.*

Proof. Let $I_0 = I \cap Q(R)$. Now by no infinite direct sums there is some left ideal J_0 such that $I_0 + J_0$ is essential in R and the sum is direct. Let $J = Q(R)J_0$. We claim that $I \cap J = (0)$ and they sum to $Q(R)$. If $x \in I \cap J$ then there is some $s \in S$ such that $sx \in I_0 \cap J_0 = (0)$ so $x = 0$ since s is regular. Since $I_0 + J_0$ is essential there is some s in $I_0 + J_0$ that is essential. Then $1 = s^{-1}s \in I + J$. □

So now to finish the proof it suffices to show that if A is a ring in which every left ideal is a direct summand then A is semiprimitive left artinian. Let's first show semiprimitivity. If J is the Jacobson radical of A and J is nonzero then we know $A = J \oplus I$ for some proper ideal I of A. So we can write $1 = j + i$ with $j \in J$, $i \in I$. Then $i = 1 - j$. But $1 - j$ is left invertible so i is a unit so $I \supseteq Ai = A$, so $J = (0)$. Now let's show that A is left artinian. To do this let I denote the sum of all minimal nonzero left ideals of A (a priori we don't know these exist, so we take the sum to be (0) if it is an empty sum. Notice that $I = A$ since if not, $I \subseteq M$ for some maximal left ideal M (Zorn) and then $M \oplus I' = A$ for some I'. Notice I' is simple since M is maximal, so we get that $I' + I$ is direct, a contradiction. So $I = A$. This means $A = \sum L_\alpha$, the L_α simple. But 1 is in the sum, so the sum is finite. This means $A = L_1 \oplus \cdots \oplus L_d$. Now each L_i is a simple module and this shows that A has finite composition length and so it is Artinian by the Jordan-Holder theorem. (See exercise on Assignment 2)

We note that a converse to Goldie's theorem holds. First, it is possible to sometimes localize at the regular elements even when a semiprime ring is not left Goldie. But if one wishes to get a semiprimitive left Artinian ring then one needs the Goldie condition. This is not bad to see. If you start with a semiprime ring that has an infinite direct sum of left ideals, $Q(R)$ will have this property and that's impossible in a semiprimitive Artinian ring. (Why?) Also if our ring does not have acc on left annihilators, $Q(R)$ will not either. But a semiprimitive artinian ring is noetherian (well, show $M_n(D)$ is and then use the fact that a finite product of noetherian rings is noetherian to do the rest).

Polynomial Identity rings

Now we'll study PI rings. This is a mature area of study in the sense that the fundamental questions in the area have all been resolved. Having said that, it's an interesting theory and much of it is used in the study of central simple algebras and Brauer groups. We recall that if k is a field then a ring R is a k-algebra if there is a subring of R that is isomorphic to k that lies in the centre of R; I should point out that when we use the term subring we really mean that the identity of k should be the identity of R, so really one can say there is an injective homomorphism from k into $Z(R)$, the centre of R. This makes R into a k-module, which, as we know, is just a k-vector space. With this in mind, we can define a polynomial identity ring.

Definition 0.22. *Let k be a field and let R be a k-algebra. We say that a ring R satisfies a* polynomial identity *if there exists a nonzero noncommutative polynomial $f(x_1, \ldots, x_d) \in k\{x_1, \ldots, x_d\}$ such that $f(a_1, \ldots, a_d) = 0$ for every $(a_1, \ldots, a_d) \in R^d$.*

The first example one should consider is a commutative ring. Here we have $x_1x_2 - x_2x_1 = 0$. A more exotic example is $M_2(k)$ with k a field. Wagner showed that it satisfies the identity $x_1(x_2x_3 - x_3x_2)^2 - (x_2x_3 - x_3x_2)^2x_1 = 0$. In fact, if k is a field and A is a finite-dimensional k-algebra then A satisfies a polynomial identity. To see this, use Cayley-Hamilton. Let

$$S_n(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) x_{\sigma(1)} \cdots x_{\sigma(n)},$$

where $\mathfrak{S}_n$ is the symmetric group on n letters.

Notice also that if A satisfies a PI then so does any subring and any homomorphic image, in fact they will satisfy the same PI as A.

We claim if A is n-dimensional then A satisfies the identity S_{n+1}. To see this, we fix a basis for $e_1, \ldots, e_n$ for A over k. We note that S_n is a special type of identity. It is called a multilinear homogeneous identity. It is homogeneous because every monomial occurring in S_n has the same degree, namely n. It is multilinear, because for every i, if we fix every variable except for the i-th one, then the function becomes linear.

Remark 0.23. If $f(x_1, \ldots, x_n)$ is a multilinear homogenous polynomial then f is a polynomial identity for A if and only if $f(v_1, \ldots, v_n) = 0$ whenever $(v_1, \ldots, v_n) \in B^n$, where B is a basis for A.

Proof. One direction is trivial. Let B be a basis for A. Then if $r_1, \ldots, r_n \in R$, we can write $r_i = \sum_{b \in B} c_{i,b} b$, where $c_{i,b}$ is zero for all but finitely many $b \in B$. Then

$$f(r_1, \ldots, r_n) = f(\sum_b c_{1,b} b, r_2, \ldots, r_n) \sum_b c_{1,b} f(b, r_2, \ldots, r_n),$$

notice that we can then use multilinearity in the other indices to express $f(r_1, \ldots, r_n)$ as a linear combination of $f(b_1, \ldots, b_n)$ with the $b_i \in B$. □

For us, this shows that if $|B| = n$ and f is multilinear and homogenous of degree $n+1$ then $f(b_1, \ldots, b_{n+1})$ will always have $b_i = b_j$ for some $i < j$. Now we claim that $S_{n+1}(b_1, \ldots, b_{n+1}) = 0$ if $b_i = b_j$. This isn't hard. Notice that if $\sigma \in \mathfrak{S}_n$ and $\tau = (i, j)$ then we can pair elements in S_{n+1} off as $\{\sigma, \tau\sigma\}$; this is just cosets of $\{id, \tau\}$. Now what? Notice that σ and $\tau\sigma$ have different signs and if $\sigma(a) = i$ and $\sigma(b) = j$ then $\tau\sigma(a) = j$ and $\tau\sigma(b) = i$ and you can check the two terms from each pair cancel with one another.

Then we can see from this that $M_n(k)$ satisfies the identity S_{n^2+1}. In fact, a theorem of Amitsur and Levitzki shows that it satisfies S_{2n} and does not satisfy an identity of degree $< 2n$. We'll prove that it satisfies S_{2n} on the assignment, but let's see why it can't satisfy any identity of degree less than $2n$.

Let's first prove that any ring satisfying a polynomial identity, satisfies a non-trivial homogeneous multilinear polynomial identity whose total degree is at most as large as that of the original identity.

Proof. Let $m(f)$ be the maximum degree of a variable appearing in f. Among all nonzero polynomial identities we pick one with the property that $m(f)$ is minimal; let's say that m is the minimum. Among all such identities with $m(f) = m$ we pick one with the property that the number of variables of degree m is minimal. Let $f(x_1, \ldots, x_d)$ be such a minimal polynomial identity for a ring R. By permuting the variables, we may assume that m is the maximum degree of x_1. Consider the identity $g(x_1, y_1, \ldots, x_d) := f(x_1 + y_1, \ldots, x_d) - f(x_1, \ldots, x_d) - f(y_1, \ldots, x_d) \in k\{x_1, y_1, x_2, \ldots, x_d\}$. Then you can check by induction that this transforms a monomial of degree m in x_1 to a monomial of total degree m in x_1 and y_1 and no terms of degree m in just x_1 or just y_1. That means that either $m(g) < m$ or $m(g) = m$ but the number of variables of degree m in g is strictly less than that of f. By minimality of f we have that $g = 0$. But you can show that this occurs only if $m = m(f) = 1$. So having $m = 1$ says that every monomial appears with degree at most 1. Now pick a monomial occurring in f with nonzero coefficient of smallest degree, say $r \leq d$, By relabelling indices, we may assume that the monomial is $x_1 \cdots x_r$. Then consider $f(x_1, \ldots, x_r, 0, \ldots, 0)$. This is nonzero and must be homogeneous. Why? That means it's multilinear too. □

Notice this gives us an algorithm to convert an identity to a multilinear identity. The idea is that if it is not of degree 1 in some variable, say x_1, then we add a new variable y_1 and we look at $f(x_1 + y_1, - - -) - f(x_1, - - -) - f(y_1, - - -)$. This makes more variables but the degree in x_1 and y_1 is lower than the original degree in x_1, so it is smaller in some sense. If we keep repeating this process, we can use the argument above to see that it must terminate. Then we pick a monomial of minimal length and set all variables not occurring in it equal to zero to get a homogeneous multilinear identity. Notice also that the total degree never increases at any step, so we see the total degree of the identity is at most that of the original identity.

Exercise 12. *Run this algorithm on the Wagner identity to get a multilinear, homogeneous identity for $M_2(k)$ of degree 5.*

Notice that multilinearity immediately shows that PI rings behave well under base change.

Theorem 0.7. *Let A be a PI ring over a field k and let F be a field extension of k. Then $A \otimes_k F$ is a PI F-algebra.*

Proof. We know that A satisfies a non-trivial homogeneous multilinear identity $f(x_1, \ldots, x_d)$. Since $A \otimes_k F$ has an F-basis of the form $a \otimes 1$ with a running over a k-basis for A and since $f(a_1 \otimes 1, \ldots, a_d \otimes 1) = 0$ for all $a_1, \ldots, a_d \in A$, we see the result follows from the above remark. □

But now let's get back to showing that S_{2n} is a minimal identity in some sense.

Theorem 0.8. *Let k be a field. Then $M_n(k)$ does not satisfy a non-trivial polynomial identity of total degree $< 2n$.*

Proof. Suppose that it did. Then it would satisfy a homogeneous multilinear identity of degree $r < 2n$. Then by relabelling our variables if necessary and multiplying by a nonzero scalar, the identity can be assumed to be of the form

$$x_1 x_2 \cdots x_r + \sum_{\sigma \in \mathfrak{S}_r \setminus \{id\}} c_\sigma x_{\sigma(1)} \cdots x_{\sigma(r)} = 0$$

with $c_\sigma \in k$. Now plug in $x_1 = e_{1,1}$, $x_2 = e1, 2$, $x_3 = e_{2,2}$, $x_4 = e2, 3$, and so on. Notice that if $r = 2n - 1$ we'd end at exactly $e_{n,n}$, so we're not going to run out of room. Then $x_1 \cdots x_r = e_{1,j}$ where $j = \lfloor (r+2)/2 \rfloor$. On the other hand if σ is not the identity then $x_{\sigma(1)} \cdots x_{\sigma(r)} = 0$. Why? We must have some x_j appearing immediately to the left of x_i with $j < i$ in that case. Notice that $x_j x_i = 0$ for $j < i$. □

Using this fact, we can quickly prove a nice theorem of Kaplansky.

Theorem 0.9. *(Kaplansky) Let k be a field and let A be a primitive PI k-algebra. Then $A \cong M_d(D)$ where D is a division ring that is finite-dimensional over its centre, Z. Moreover, if A satisfies a polynomial identity of degree n then we must have $4d^2[D : Z] \leq n^2$.*

Proof. Let M be a faithful simple left A-module and let $D = \mathrm{End}_A(M)$. Then by Jacobson's density theorem, we have that A is a dense subring of $\mathrm{End}_D(M)$. We claim that M must be finite-dimensional as a left D-vector space. Let n be the PI degree of A. We claim that M must have dimension at most $\lfloor n/2 \rfloor$ as a left D-vector space. To see this, suppose that $r > \lfloor n/2 \rfloor$. Then $2r > n$. Pick linearly independent elements $e_1, \ldots, e_r$. By JDT for every matrix $C := (c_{i,j}) \in M_r(D)$ there exists some $a = a(C) \in A$ such that the action of a on $e_1, \ldots, e_r$ is the same as the action induced by C. This means that

there is a subring B of A that surjects onto $M_r(D^{\mathrm{op}})$. Here we're just taking B to be the set of elements of A that send the space $De_1 + \cdots + De_r$ into itself. Then since A satisfies a PI of degree n, so does B; and since $M_r(D^{\mathrm{op}})$ is a homomorphic image of B, so does $M_r(D^{\mathrm{op}})$ as it is a homomorphic image. Finally, since $M_r(Z)$ is a subring, where Z is the center of D^{op}, we see $M_r(Z)$ satisfies an identity of degree n. But by the above result, we know $M_r(Z)$ satisfies no identity of degree $< 2r$ and $2r > n$, this is a contradiction. So now we know that we have M is finite-dimensional as a left D-vector space. Then JDT now gives that $A \cong M_d(D^{\mathrm{op}})$ for some d. OK, so now let's replace D by its opposite ring. Next we claim that D is finite-dimensional over its centre. To see this, we remark that D is isomorphic to a subring of A so it satisfies a PI. Let K be a maximal subfield of D. Why does it exist? Let $B = D \otimes_Z K$. Then B is PI from the extension of scalars result. Notice that D is a faithful simple B-module with action given by $d \otimes \lambda \cdot b = db\lambda$. (This needs K to be commutative to work—that is, K is equal to its opposite ring so the right action works—think about it!) Now let $\Delta = \mathrm{End}_B(D)$. What is this? It turns out, it is exactly K. Think about it! If $f : D \to D$ is B-linear then f is determined by $f(1)$ since B contains $D \otimes 1$. Then we need

$$df(1)\lambda = f((d \otimes \lambda) \cdot 1) = f(d\lambda)$$

for all $d \in D$ and all $\lambda \in K$. Now if we take $d = d\lambda$ and $\lambda = 1$ we get $d\lambda f(1) = f(d\lambda) = df(1)\lambda$. So if d is nonzero, we see that $f(1)$ and λ commute for all $\lambda \in K$. Since K is a maximal subfield we see $f(1) \in K$. On the other hand, if we take $f(1) \in K$, we see this gives an endomorphism. So we see that B embeds densely in $\mathrm{End}_K(D)$ by JDT. But now we just saw that since B is PI we must have D is finite-dimensional as a left K-vector space, let the dimension be e. Then $B \cong M_e(K)$. Notice that the centre of B is K and $e^2 = \dim_K(B) = \dim_Z(D)$. So finally, put it all together. We have $A \cong M_d(D)$. So

$$A \otimes_Z K \cong M_d(D) \otimes_Z K \cong M_d(D \otimes_Z K) \cong M_d(M_e(K)) \cong M_{de}(K).$$

Now $A \otimes_Z K$ satisfies a PI of degree n by the above remark on change of basis. So by the bounds on PIs of matrix rings we have $n \geq 2de$ and we saw $e^2 = [D : Z]$, so $n^2 \geq 4d^2[D : Z]$. □

Prime PI rings are Goldie

Let's prove that a prime PI ring is a left Goldie ring. This will show us that there is a ring of quotients $Q(R)$ of a prime PI ring R and this ring is simple Artinian, so it is isomorphic to $M_n(D)$. We'll show that it is PI and so Kaplansky's theorem shows that D is finite-dimensional over its centre.

So first, suppose that R is a prime PI k-algebra. Then we know R satisfies a homogeneous multilinear identity

$$f(x_1, \ldots, x_d) = x_1 \cdots x_d + \sum_{\sigma \neq \mathrm{id}} c_{sigma} x_{\sigma(1)} \cdots x_{\sigma(d)}.$$

We claim that R cannot contain a direct sum of d nonzero left ideals. To see this, suppose that $I_1 + \cdots + I_d$ is direct with each I_i a nonzero left ideal. We now fix $a_i \in I_i$, nonzero. We now pick the nonzero homogeneous multilinear polynomial $g(x_1, \ldots, x_e)$ with $e \leq d$ minimal such that after a suitable permutation of the I_i we have $g(r_1a_1, \ldots, r_ea_e) = 0$ for all $r_1, \ldots, r_e \in R$. (Notice that f above works, so $e \leq d$.)

We write $g = g_1x_1 + \cdots + g_ex_e$, where each g_i is homogeneous multilinear of degree $e-1$ on the variables $\{x_1, \ldots, x_e\} \setminus \{x_i\}$ and by minimality of e any nonzero f_i is not an identity for R. Pick nonzero $a_i \in I_i$. Notice that if we take $x_i = r_ia_i \in I_i$ then directness of the sum of the I_i gives that $g_i(r_1a_1, \ldots, r_ea_e)r_ia_e = 0$ for all $r_1, \ldots, r_d \in R$. Now by assumption some g_i is nonzero and $g_i(r_1a_1, \ldots, r_ea_e)$ is not identically zero by minimality of e. Then since R is prime and r_i can be anything and a_i is nonzero, we see that $g_i(r_1a_1, \ldots, r_ea_e) = 0$ for all $r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_e \in R$ (recall that g_i does not involve the variable x_i). But we can then relabel our indices to get a smaller identity, a contradiction. Thus we are half-way there. Now we need to show that we have acc on left annihilators. Suppose that $L_1 \subseteq L_2 \subseteq \cdots$ is an infinite strictly ascending chain of left annihilators. Then there exist $x_1, x_2, \ldots$ in R such that $x_iL_i \neq 0$ but $x_iL_j = 0$ for $j < i$. Now as before we claim that the chain must terminate after d steps. We again consider a minimal identity such that $g(r_1x_1, \ldots, r_ex_e) = 0$ for all $r_1, \ldots, r_e \in R$. (As before $e \leq d$.) Then we can write this as $\sum g_i(r_1x_1, \ldots, r_ex_e)r_ix_i$ and there is some smallest i such that g_i is nonzero. Then by assumption there is some $a \in L_i$ such that $x_ia \neq 0$. But $x_ja = 0$ for all $j > i$. Then multiplying on the left by a gives that $g_i(r_1x_1, \ldots, r_ex_e)r_i(x_ia) = 0$. As before, we get a contradiction.

So this means that if R is a prime PI k-algebra then it has a ring of quotients $Q(R)$.

Appendix: Tensor products for noncommutative rings

Now a general fact about rings is that given a subring R of a ring S, if one has a left R-module M then one can "extend scalars" and create a left S-module, which we denote by $M \otimes_R S$. We'll spend the next little while doing this construction rigorously, but then we'll give a concrete interpretation for group algebras.

First, if you have seen tensor products in the commutative setting or in the setting of vector spaces, you are in good shape—still there are some subtleties that arise in the noncommutative setting. We start by letting R be a ring that is not necessarily commutative. Given a right R-module M and a left R-module N we can form an abelian group $M \otimes_R N$, which is called the tensor product of M and N, as follows.

First, we recall that in this setting, if A is an abelian group then a map $f : M \times N \to A$ is said to be *bilinear* if $f(m + m', n) = f(m, n) + f(m', n)$ for all $m, m' \in M$ and $n \in N$; $f(m, n + n') = f(m, n) + f(m, n')$ for all $m \in M$, $n, n' \in N$ and for $m \in M, n \in N$ and $r \in R$ we have $f(mr, n) = f(m, rn)$.

Important Remark! Notice that we really need the right/left pairing here to make this work in general. If M and N were both left R-modules then if we tried to impose $f(rm,n) = f(m,rn)$ then we'd have for $r,s \in R$

$$f(m,(rs)n) = f((rs)m,n) = f(sm,rn) = f(m,srn) = f(m,(sr)n),$$

so we'd have $f(m,(rs-sr)n) = 0$ for all $(m,n) \in M \times N$ and every $r,s \in R$. Now in certain rings, one can have $1 = rs - sr$ for some $r,s \in R$. For example, if one takes the ring of all linear operators on $\mathbb{C}[x]$ then the differentiation operator and multiplication by x operator have this relation. So in this situation one would have $f(m,n) = 0$ for all m,n. But the way we have defined it, we now have $f(m,(rs)n) = f(m(rs),n) = f(mr,sn) = f(m,rsn)$ and there is no problem now.

Second, we let T denote the free $\mathbb{Z}$-module on all symbols $e_{m,n}$ where $(m,n) \in M \times N$. That is, T is all finite integer linear combinations of elements of the form $e_{m,n}$. Then we let U denote the subgroup of T generated by the relations

$$e_{m+m',n} - e_{m,n} - e_{m',n} = 0$$

$$e_{m,n+n'} - e_{m,n} - e_{m,n'} = 0$$

$$e_{mr,n} = e_{m,rn}$$

for all $m,m' \in M$, $n,n' \in N$, and $r \in R$. What we are in fact doing is choosing our relations so that the function $M \times N \to T/U$ given by $(m,n) \mapsto e_{m,n} + U$ is now *R-bilinear*. We define $M \otimes_R N$ to be the abelian group T/U. We then use the symbol $m \otimes n$ (read "m tensor n") to denote the image of $e_{m,n}$ in T/U. Now in general, there is no additional structure, but in the case where M is both a left S-module and right R-module (we call this a S-R-bimodule), we can actually give $M \otimes_R N$ the structure of a left S-module as follows: we define $s \cdot (m \otimes n) = (sm) \otimes n$. Notice that if we did not have the bimodule structure on M we'd be in trouble. One might hope that we could still at least put a left R-module structure on the tensor product using the fact that N is a left R-module and define $r \cdot (m \otimes n) = m \otimes (rn)$, but this is problematic: by definition of our relations $m \otimes (rn) = (mr) \otimes n$ and so we'd have to have $(rs)m \otimes n = m \otimes (rs)n = m(rs) \otimes n$ and $(rs)m \otimes n = r \cdot (s \cdot m \otimes n) = r \cdot m \otimes sn = r \cdot (ms \otimes n) = ms \otimes rn = m(sr) \otimes n$. Notice this really only works if $m(rs - sr) = 0$ for all $r,s \in R$. But if we have that M is a bimodule then there is a whole other untapped side which we can use to endow the tensor product with a left module structure.

We remark that in general not every element of $M \otimes_R N$ is of the form $m \otimes n$—we must take sums of elements of this form. An element of the form $m \otimes n$ is called a *pure tensor*. People who have worked with tensor products before know that it is actually hard to prove even basic properties about them. The way one does this is by using what is known as the *Universal property* of tensor products.

Universal property

For any abelian group A and any bilinear map $f : M \times N \to A$, there exists a unique homomorphism of abelian groups $\widehat{f} : M \otimes_R N \to A$ such that $\widehat{f} \circ i = f$, where $i : M \times N \to M \otimes_R N$ is the $\mathbb{Z}$-module homomorphism induced by $(m,n) \mapsto m \otimes n$.

Let's see that $M \otimes N$ has this universal property. We define $\widehat{f}(m \otimes n) = f(m,n)$ and extend via linearity. We must check that this is well-defined. Notice that f induces a group homomorphism $f' : T \to A$ via $f'(\sum c_i e_{m_i,n_i})$. Saying that f is bilinear is exactly the same as saying that f is zero on U. Thus we can define $\widehat{f} : T/U \to A$ via $\widehat{f}(t+U) = f'(t)$ and this is well-defined. Moreover, this is the only way to define this map!

The universal property actually means that the tensor product is the unique $\mathbb{Z}$-module (up to isomorphism) with this property given a right R-module M and a left R-module N. To see this, suppose that we have two abelian groups A and B that have the universal property for (M,N). Then we have maps $i_1 : M \times N \to A$ and $i_2 : M \times N \to B$ such that if $f : M \times N \to C$ is a $\mathbb{Z}$-module homomorphism then there exist f_1 and f_2 from A and B to C respectively such that $f_1 \circ i_1 = f = f_2 \circ i_2$. Now take $C = A$ and let $f = i_1$. Then there is a map $f_2 : B \to A$ such that $f_2 \circ i_2 = i_1$. Similarly, there exists a unique f_1 such that $f_1 \circ i_1 = i_2$. Then

$$(f_1 \circ f_2) \circ i_2 = f_1 \circ (f_2 \circ i_2) = f_1 \circ i_1 = i_2.$$

Notice also that $i_2 : M \times N \to B$ is onto since we can use the universal property to get that there is some $g : M \times N \to B$ such that $g \circ i_2 = i_2$. Since $g = \mathrm{id}$ works, by *uniqueness* of the universal property we see that g is the identity. But we see that $g = f_1 \circ f_2$ works too, so we see that $f_1 \circ f_2$ is the identity. By symmetry we get that $f_2 \circ f_1$ is the identity and so A and B are isomorphic.

The universal property is how one proves *anything* about tensor products in practice. Let's do a few examples.

Let $R = M_2(\mathbb{C})$ and let M be the right R-module $\mathbb{C}^{1\times 2}$, the 1×2 row vectors; let $N = \mathbb{C}^{2\times 1}$ be the column vectors. Then what is $M \otimes_R N$? Notice that $M \otimes_{\mathbb{C}} N \cong \mathbb{C}^4$, but when we tensor over R we get a different result. First, this will be an abelian group, so we just need to find out what it is as an abelian group. As before we let T be the free $\mathbb{Z}$-module on the generators $e_{v,w}$ where v is a row vector and w is a column vector. Now let $v_1 = [1,0]$ and let $w_1 = [0,1]$ be a nonzero column vector. Then for $v \in M$ and $w \in N$ there is some $r \in R$ such that $v = v_1 r$. So $e_{v,w} = e_{v_1 r,w} = e_{v_1,rw}$. Now if $w' = rw$ then we have that the tensor product is generated by the images in T/U of things of the form $e_{v_1,w'}$ with w' a column vector. If

s is an element of R whose first row is $(1,0)$ then $v_1 s = v_1$ and so in T/U we have $e_{v_1,w'} = e_{v_1 s,w'} = e_{v_1,sw'}$. Notice that by picking s appropriately, we may arrange things so that $sw' = \lambda w_1$ for some scalar λ. So now we see we are spanned by things of the form $e_{v_1,\lambda w_1}$. Now by the other bilinear relations, we see that $e_{v_1,\lambda_1 w_1} + e_{v_2,\lambda_2 w_1} = e_{v_1,(\lambda_1+\lambda_2)w_1}$ and so we see that we have a map from the abelian group $\mathbb{C}$ to $T/U = M \otimes_R N$ via the rule $\lambda \mapsto e_{v_1,\lambda w_1} + U$ and we have shown that this map is onto. Now it would be pretty difficult to show that this is 1-to-1 in general, but we can use the universal property to do this. Notice that we have a bilinear map $f : M \times N \to \mathbb{C}$ via the rule $(v,w) \mapsto v \cdot w$. Then under this map $(v_1, \lambda w_1)$ maps to λ. So if λ is in the kernel it must be zero. Thus the tensor product is just the complex numbers in this case.

Exercise 13. *Let R be a ring, let M be a right R-module, and let N be a left R-module. Suppose we regard R as a left R-module. Show that $M \otimes_R R \cong M$. Show that if we regard R as a right R-module then $R \otimes_R N \cong N$. (Hint: use the bilinear map $M \times R \to R$ given by $(m,r) \mapsto mr$.)*

Exercise 14. *Let R be the ring of upper-triangular 2×2 complex matrices and let $M = \mathbb{C}^{1\times 2}$ be the 1×2 row vectors; let $N = \mathbb{C}^{2\times 1}$ be the column vectors. What is $M \otimes_R N$?*

Exercise 15. *Use the universal property to show that if M_1 and M_2 are two right R-modules and N is a left R-module then $(M_1 \oplus M_2) \otimes_R N \cong (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$. Show that if M_1 and M_2 are also left S-modules then this is an isomorphism of left S-modules, too.*

Extension of scalars

One of the nicest features of tensor products is that they can be used to extend scalars. For this set-up, let R be a subring of a ring S and let M be a left R-module. Then we can create a left S-module from M via tensor products as follows. Notice that S is both a left S-module and a right R-module and thus we can form $S \otimes_R M$. If we only used the right R-module structure of S, this would just be an abelian group, but since S is a left S-module, we can give it a left S-module structure. We can give $S \otimes_R M$ a left S-module structure via the rule $s \cdot (s' \otimes m) = (ss') \otimes m$. Since the left S-module structure does not interfere with the right R-module structure this does not create any problems.

Exercise 16. *Let R be a subring of a ring S and suppose that S is a free right R-module with basis $s_1, \ldots, s_d$. Show that if N is a left R-module then as an abelian group $S \otimes_R N \cong N^d$ with isomorphism induced from*

$$(s_1 r_1 + \cdots + s_d r_d) \otimes n = \sum_i s_i \otimes (r_i n) \mapsto (r_1 n, r_2 n, \ldots r_d n).$$