Lent 2026
SJW

Noncommutative Noetherian Rings

LECTURE 1

In which we define rings and modules

This course is a first course in noncommutative rings. Familiarity with the theory of commutative rings will be assumed.

Rings arise in a variety of contexts throughout mathematics but one central context is as linear operators on a suitable space. These will rarely commute. As for commutative rings, noetherianity of a ring imposes a degree of control — indeed it is perhaps even more significant in the noncommutative setting in order to avoid pathological examples where very little can be said of a general nature.

1. GENERALITIES

We'll start with some boring but necessary definitions.

In this course ring are associative and unital, but are not necessarily commutative. That is a *ring* $R = (R, +, \cdot)$ is an abelian group under $+$ with unit 0 such that $\cdot$ is a $\mathbb{Z}$-bilinear associative binary operation with identity 1. $\mathbb{Z}$-bilinearity simply says that multiplication distributes over addition on both sides. As usual we will typically suppress the $\cdot$.

Examples 1.1.

(1) Every commutative ring is a ring.
(2) The 0 ring is a ring.
(3) If k is a commutative ring, the ring of $n \times n$-matrices $\mathrm{Mat}_n(k)$ is a ring. It is only commutative if $n < 2$.

Given a ring $(R, +, \cdot)$ we can define a ring $R^{\mathrm{op}} = (R, +, *)$ with $a * b = b \cdot a$ for all $a, b \in R$. Of course if R is commutative then $R = R^{\mathrm{op}}$.

We can define the units of R,

$$R^\times = \{r \in R : sr = rs = 1 \text{ for some } s \in R\}.$$

This is a group under the multiplication in R. For example $\mathrm{Mat}_n(k)^\times = GL_n(k)$.

The *centre* of a ring R is the set

$$Z(R) = \{z \in R : zr = rz \text{ for all } r \in R\}.$$

$Z(R)$ is always a subring of R. For example $Z(\mathrm{Mat}_n(k)) = kI_n$.

A *(two-sided) ideal* I of a ring R is a subgroup of $(R, +)$ such that $axb \in I$ for all $x \in I$ and $a, b \in R$. We write $I \lhd R$. Given such an ideal I, R/I is a ring under operations induced from R.

A *ring homomorphism* $\alpha\colon R \to S$ between two rings is a function $R \to S$ such that

- $\alpha(a+b) = \alpha(a) + \alpha(b)$ and $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in R$ and
- $\alpha(1) = 1$.

Exercise. Show that $\alpha(R^\times) \leqslant S^\times$ but $\alpha(Z(R)) \not\subseteq Z(S)$ in general.

The *kernel* of α,

$$\ker(\alpha) = \{r \in R : \alpha(r) = 0\},$$

and the *image* of α,

$$\mathrm{Im}(\alpha) = \{\alpha(r) \in S : r \in R\}.$$

If k is a commutative ring, a *k-algebra* is a ring R equipped with a ring homomorphism $\iota_R\colon k \to Z(R)$. For example $\mathrm{Mat}_n(k)$ is a k-algebra under $k \to \mathrm{Mat}_n(k)$; $a \mapsto aI$.

A *k-algebra homomorphism* $\alpha\colon R \to S$ is a ring homomorphism $R \to S$ such that $\alpha\iota_R = \iota_S$ as functions $k \to S$. We typically suppress the ι's unless it will cause confusion. Every ring is uniquely a $\mathbb{Z}$-algebra and a $\mathbb{Z}$-algebra homomorphism is the same as a ring homomorphism.

There is an isomorphism theorem.

Proposition 1.2. If $\alpha\colon R \to S$ is a k-algebra homomorphism, $\ker(\alpha) \lhd R$, $\mathrm{Im}(\alpha)$ is a k-subalgebra of S and $\overline{\alpha} : R/\ker(\alpha) \to \mathrm{Im}(\alpha)$; $r + \ker\alpha \mapsto \alpha(r)$ is an isomorphism of k-algebras.

Given a ring R a *(left) R-module* M is an abelian group $(M, +)$ together with a $\mathbb{Z}$-bilinear operation

$$R \times M \to M; (a, m) \mapsto am$$

such that

- $(ab)m = a(bm)$ for all $a, b \in R$ and $m \in M$;
- $1m = m$ for all $m \in M$.

A right R-module can be defined in a similar fashion. If we say R-module without specifying a side we will mean a left R-module.

If M and N are R-modules an *R-module homomorphism* $\varphi\colon M \to N$ is a group homomorphism such that $\varphi(am) = a\varphi(m)$ for all $a \in R$ and $m \in M$. We'll write $\mathrm{Hom}_R(M, N)$ to denote the (additive) group of R-module homomorphisms $M \to N$ under pointwise addition.

Warning: Note that whilst when R is commutative $\mathrm{Hom}_R(M, N)$ is naturally an R-module under $a \cdot \varphi(m) = \varphi(am) = a\varphi(m)$ it is only a $Z(R)$-module under this operation in general since

$$M \to N; m \mapsto \varphi(am)$$

will only typically define an element of $\mathrm{Hom}_R(M,N)$ if

$$ab\varphi(m) = \varphi(abm) = b\varphi(am) = ba\varphi(m)$$

for all $\varphi \in \mathrm{Hom}_R(M,N)$, $b \in R$ and $m \in M$.

For every ring R and set X we may form RX, the free R-module on X, as the set of finitely supported functions $f\colon X \to R$[1] under pointwise operations. When R is a field this is a vector space with basis $\{\delta_x : x \in X\}$. [2]

Lemma 1.3. For every R-module N, restriction along the function

$$\iota\colon X \to RX; x \mapsto \delta_x$$

induces a bijection $\Theta\colon \mathrm{Hom}_R(RX,N) \to N^X := \{f\colon X \to N\}$. [3]

RX together with ι is determined up to unique isomorphism by the property of this lemma. Indeed if M were another R-module equipped with a function $i\colon X \to M$ such that for every R-module N restriction along i induced a bijection $\mathrm{Hom}_R(M,N) \to N^X$ then the R-linear maps $RX \to M$ corresponding to ι and $M \to RX$ corresponding to i are mutual inverses[4] because ι corresponds to id_{RX} and i corresponds to id_M.

When R is a field this is saying that it we have two vector spaces with distinguished bases indexed by the same set X there is a unique isomorphism induced for the canonical bijection of bases coming from the indexing.

2. Some examples of noncommutative rings

If M is an abelian group, let

$$\mathrm{End}(M) = \mathrm{Hom}_{\mathbb{Z}}(M,M)$$

denote the set of homomorphisms $M \to M$. It is a ring under pointwise addition and composition. More generally, if M is an R-module for some k-algebra R, then the set

$$\mathrm{End}_R(M) = \mathrm{Hom}_R(M,M)$$

of R-module homomorphisms $M \to M$ is again a k-algebra with group of units $\mathrm{Aut}_R(M)$.

For example, if $M = \mathbb{Z}^n$ is the free abelian group of rank n then $\mathrm{End}(M)$ is (isomorphic to) the ring $M_n(\mathbb{Z})$ of $n \times n$-matrices with integer entries and usual matrix operations. If k is a field and $V = k^n$ then $\mathrm{End}_k(V)$ is (isomorphic to) the

[1] i.e. $f\colon X \to R$ such that $f(x) = 0$ for all but finitely many $x \in X$

[2] It may be more sophisticated to view RX as a space of distributions on the space of all functions $X \to R$ with δ_x the 'Dirac distribution at x' so $\delta_x(f) = f(x)$ for all $f\colon X \to R$.

[3] Those with some familiarity with category theory will recognise this as saying that $X \mapsto RX$ is a functor from the category of sets to the category of R-modules that is left adjoint to the forgetful functor from R-modules to sets and ι is the unit of the adjunction.

[4] and uniquely determined by the data

k-algebra $M_n(k)$ of $n \times n$-matrices with entries in k and $\mathrm{Aut}_k(V)$ (corresponds to) the group $GL_n(k)$.

Lecture 2

In which we see that every ring is a subring of the ring of endomorphisms of an abelian group and meet group algebras, tensor algebras, symmetric algebras and universal enveloping algebras of Lie algebras

Remarks 2.1.

(a) Suppose that M is an abelian group. There is a 1-1 correspondence between left R-module structures $\cdot$ on M and ring homomorphisms $\theta\colon R \to \mathrm{End}(M)$ given by $\theta(r)(m) = r \cdot m$.

(b) Similarly a right R-module structure on M can be viewed as a ring homomorphism $R \to \mathrm{End}(M)^{\mathrm{op}}$ or (equivalently) $R^{\mathrm{op}} \to \mathrm{End}(M)$.

(c) If R is a k-algebra,

$$\theta\colon R \mapsto \mathrm{End}_k(R);\;\; \theta(a)(r) = ar$$

is an injective k-algebra homomorphism. In fact the image is the subring of $\mathrm{End}_k(R)$ consisting of right R-module endomorphisms of R where R is a right R-module under multiplication in the ring.

Definition 2.2. Let G be a group and let k be a commutative ring. The *group algebra* kG is the k-algebra consisting of finitely supported functions $G \to k$ with pointwise addition and multiplication given by convolution:

$$(f_1 f_2)(g) = \sum_{h_1,h_2 \in G: h_1 h_2 = g} f_1(h_1) f_2(h_2)$$ [5]

Lemma 2.3. Suppose that R is an k-algebra. Restriction along the group homomorphism $G \to (kG)^\times;\ g \mapsto \delta_g$ defines a natural bijection

$$\Theta\colon\ \mathrm{Hom}_{k-alg}(kG, R) \to \mathrm{Hom}_{gp}(G, R^\times).$$ [6]

Proof. If $\alpha\colon kG \to S$ is an k-algebra homomorphism then

$$\Theta(\alpha)\colon G \to R^\times; \Theta(\alpha)(g) = \alpha(\delta_g)$$

is a group homomorphism.

[5] i.e. the only possible multiplication on the free k-module kG such that $G \to kG^\times$ is a group homomorphism and $k \to kG;\ r \mapsto r\delta_e$ makes kG into a k-algebra.

[6] Again for those who know a little category theory this can be expressed as 'the functor from the category of k-algebras to the category of groups sending R to $R^\times$ has a left adjoint given by sending G to kG. Moreover $G \to kG^\times; g \mapsto \delta_g$ is the unit of the adjunction.' Thus kG is characterised by this property as a k-algebra just as it is characterised by a similar universal property as a k-module.

Conversely given a group homomorphism $\beta\colon G \to R^\times$ we can define an k-algebra homomorphism $\Phi(\beta)\colon kG \to R$ via $\Phi(\beta)(f) = \sum_{g\in G} f(g)\beta(g)$. Note $\Phi(\beta)$ is the element of $\mathrm{Hom}_k(kG, R)$ corresponding to $\beta\colon G \to R^\times \to R$ and

$$\begin{aligned}\Phi(\beta)(f_1 f_2) &= \sum_{g\in G}(f_1 f_2)(g)\beta(g) \\ &= \sum_{g\in G}\sum_{h_1,h_2\in G: h_1h_2=g} f_1(h_1)\beta(h_1)f_2(h_2)\beta(h_2) \\ &= \Phi(\beta)(f_1)\Phi(\beta)(f_2)\end{aligned}$$

It is straightforward to verify that Θ and Φ are mutual inverses. □

Definition 2.4. Suppose that k is a field. Recall that a *k-linear representation* of G is a group homomorphism

$$\varphi : G \to \mathrm{Aut}_k(V)$$

where V is some vector space over k.

Corollary 2.5. There is a natural bijection between k-linear representations of G and left kG-modules.

Proof. This follows from Lemma 2.3, Remark 2.1(a) and the observation that $\mathrm{End}_k(V)^\times = \mathrm{Aut}_k(V)$. □

Definition 2.6. A *Lie algebra* over k is a k-module $\mathfrak{g}$, equipped with a k-bilinear map $[.] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ satisfying

(1) $[xx] = 0$ for all $x \in \mathfrak{g}$ and hence $[yz] = -[zy]$ for all $y, z \in \mathfrak{g}$
(2) $[x[yz]] + [y[zx]] + [z[xy]] = 0$ for all $x, y, z \in \mathfrak{g}$.

Note that this bracket is not associative.

Examples 2.7.

(1) Any (associative) k-algebra R becomes a Lie algebra over k under the commutator bracket $[x, y] = xy - yx$.
(2) $\mathfrak{gl}(V) := \mathrm{End}_k(V)$ with the commutator bracket.
(3) $\mathfrak{gl}_n(k) := \mathfrak{gl}(k^n) = M_n(k)$ with the commutator bracket.

Definition 2.8. A k-Lie algebra homomorphism $\theta\colon \mathfrak{g}_1 \to \mathfrak{g}_2$ is a k-linear map such that $\theta[xy] = [\theta(x)\theta(y)]$ for all $x, y \in \mathfrak{g}_1$.

A *representation* of the Lie algebra $\mathfrak{g}$ is a k-Lie algebra homomorphism $\mathfrak{g} \to \mathrm{End}_k(V)$ for some k-module V.

We now wish to find an analogue of the group algebra for representations of Lie algebras.

Definition 2.9. Suppose that V is a k-module. Define $T^0V = k$, $T^1V = V$ and $T^nV = V \otimes_k T^{n-1}V$ for $n \geq 2$. The *tensor algebra* of V

$$TV := \bigoplus_{n \geq 0} T^n V$$

with multiplication given by concatenation; i.e. the bilinear extension of

$$T^nV \times T^mV \to T^{n+m}V;$$

$$(v_1 \otimes \cdots \otimes v_n), (w_1 \otimes \cdots \otimes w_m) \to v_1 \otimes \cdots \otimes v_n \otimes w_1 \otimes \cdots \otimes w_m.$$

There is a natural k-linear map $\iota_V \colon TV;\ v \mapsto v \in T^1V = V$.

If V is the free k-module on $x_1, \ldots x_d$ we write $k\langle x_1, \ldots x_d\rangle := TV$ and call it the *free associative algebra* on $x_1, \ldots x_d$.

Note that in general $k\langle x_1, \ldots, x_d\rangle$ is not finitely generated as a k-module.

For example, if $d = 1$ then $k\langle x\rangle$ has $\{1, x, x^2, \ldots\}$ as a basis. In fact $k\langle x\rangle \cong k[x]$, the polynomial algebra in x.

Similarly, $k\langle x, y\rangle$ has as a k-basis the set $\{1, x, y, x^2, xy, yx, y^2, x^3, x^2y, \ldots\}$. This algebra is not commutative!

Lemma 2.10. Suppose that V is a k-module and R is a k-algebra. There is a natural bijection

$$\Phi \colon \operatorname{Hom}_{k-alg}(TV, R) \to \operatorname{Hom}_k(V, R)$$

given by restricting along ι_V.

Proof. Certainly, given a k-algebra homomorphism $\alpha \colon TV \to R$,

$$\Phi(\alpha) := \alpha \circ \iota \in \operatorname{Hom}_k(V, R).$$

Conversely, given $\beta \colon V \to R \in \operatorname{Hom}_k(V, R)$ we can define k-linear maps

$$T_n(\beta) \colon T^nV \to R$$

via $v_1 \otimes \cdots \otimes v_n \to \beta(v_1) \cdots \beta(v_n)$ and verify that $T(\beta) = \bigoplus_{n \geq 0} T_n(\beta)$ defines a k-algebra homomorphism $T(V) \to R$.

It is easy to verify that T and Φ are mutually inverse. [7] □

Definition 2.11. Suppose that $\mathfrak{g}$ is a k-Lie algebra. The *universal enveloping algebra* $U(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ is

$$U(\mathfrak{g}) := T\mathfrak{g}/I$$

where I is the two-sided ideal of $T\mathfrak{g}$ generated by the set

$$\{xy - yx - [xy] : x, y \in \mathfrak{g} = T^1\mathfrak{g}\}.$$

There is a natural map of Lie algebras $\iota_{\mathfrak{g}} \colon \mathfrak{g} \to U(\mathfrak{g}); x \mapsto x + I \in T^1\mathfrak{g} + I$

[7] Again the categorically minded will note that this says that the functor T from k-modules to k-algebras is left adjoint to the forgetful functor the other direction and ι_V is the unit of the adjunction.

For example, if $\mathfrak{g}$ is the abelian Lie algebra free on $x_1, \dots x_d$, then $U(\mathfrak{g})$ is just the polynomial algebra $k[x_1, \dots, x_d]$. More generally when $V = \mathfrak{g}$ is abelian[8] $U(V)$ is called the *symmetric algebra* on V and written SV.

Lemma 2.12. Suppose that $\mathfrak{g}$ is a k-Lie algebra and R is an (associative) k-algebra. There is a natural bijection

$$\Phi\colon \operatorname{Hom}_{k-alg}(U(\mathfrak{g}), R) \to \operatorname{Hom}_{k-Lie}(\mathfrak{g}, R)^9$$

given by restricting along $\iota_{\mathfrak{g}}$. [10]

Lecture 3

In which we meet derivation rings & Weyl algebras and begin to discuss noetherianity

Proof. If $\alpha\colon U(\mathfrak{g}) \to R$ is a k-algebra homomorphism then α is a k-Lie algebra homomorphism when both $U(\mathfrak{g})$ and R are given their commutator brackets. Since $\iota_{\mathfrak{g}}$ is also a k-Lie algebra homomorphism it follows that $\Phi(\alpha) = \alpha \circ \iota$ is a k-Lie algebra map.

Conversely, if $\beta\colon \mathfrak{g} \to R$ is a k-Lie algebra homomorphism. Then by Lemma 2.10 there is a corresponding k-algebra homomorphism $T(\beta)\colon T\mathfrak{g} \to R$. Moreover, for $x, y \in T^1\mathfrak{g}$,

$$T(\beta)(xy - yx - [xy]) = [\beta(x), \beta(y)] - \beta([x, y]) = 0$$

since $T(\beta) \circ \iota_{\mathfrak{g}} = \beta$ and β is a k-Lie algebra homomorphism. Thus $T(\beta)$ factors through a k-algebra map $U(\beta)\colon U(\mathfrak{g}) \to R$. It is straightforward to verify that Φ and U are mutual inverses. □

Corollary 2.13. There is a natural bijection between representations of $\mathfrak{g}$ and left $U(\mathfrak{g})$-modules.

Proof. This follows from the last lemma applied to $R = \operatorname{End}_k(V)$. □

We will now end this section by introducing a basic example of a ring of derivations.

Definition 2.14. A *derivation* of a k-algebra R is a k-linear map $\delta\colon R \to R$ such that $\delta(1) = 0$ and

$$\delta(ab) = a\delta(b) + \delta(a)b \text{ for all } a, b \in R.$$

Write $\operatorname{Der}_k(R)$ for the set of derivations of R.

Exercise. Suppose that R is a k-algebra.

---

[8] i.e. $\mathfrak{g}$ is just a k-module with $[] = 0$

[9] where R is equipped with the commutator bracket

[10] Once again we may phrase this categorically as $U(-)$ is a left adjoint to the functor from (associative) k-algebras to k-Lie algebras via the commutator bracket. Moreover the unit of this adjunction is $\iota_{\mathfrak{g}}\colon \mathfrak{g} \to U(\mathfrak{g})$.

(a) Show that $\mathrm{Der}_k(R)$ is a k-Lie algebra under the commutator bracket.
(b) Show that for all $a \in R$, $\mathrm{ad}_a \colon R \to R$; $\mathrm{ad}_a(b) = [a, b]$ is a derivation of R.
(c) Show that $\mathrm{ad} \colon R \to \mathrm{Der}_k(R)$; $a \mapsto \mathrm{ad}_a$ is a Lie algebra homomorphism.
(d) When $R = k[x_1, \ldots, x_d]$, show that for every $\delta \in \mathrm{Der}_k(R)$ there are unique $f_1, \ldots f_d \in R$ such that $\delta(y) = \sum_{i=1}^d f_i \partial y/\partial x_i$ for all $y \in R$.

Definition 2.15. Let k be a field and let A be a commutative k-algebra. Let $\Delta(A)$ be the k-subalgebra of $\mathrm{End}_k(A)$ generated by[11] the k-linear operators

$$\widehat{a} \colon A \to A; \quad b \mapsto ab \text{ for } a \in A$$

and $\mathrm{Der}_k(A)$. We call $\Delta(A)$ the *derivation ring* of A.

Definition 2.16. Let k be a field. The *n-th Weyl algebra* $A_n(k)$ over k is

$$A_n(k) := k\langle x_1, \ldots, x_n, y_1, \ldots y_n \rangle / I$$

where I is the ideal of the free algebra $k\langle x_1, \ldots, x_n, y_1, \ldots y_n \rangle$ generated by

$$\begin{array}{ll} x_i x_j - x_j x_i & 1 \leqslant i, j \leqslant n, \\ y_i y_j - y_j y_i & 1 \leqslant i, j \leqslant n, \\ y_i x_i - x_i y_i - 1 & 1 \leqslant i \leqslant n, \\ x_i y_j - y_j x_i & i \neq j. \end{array}$$

For example, if $n = 1$ then $A_1(k) = k\langle x, y \rangle / \langle yx - xy - 1 \rangle$.

Lemma 2.17. There is a surjective k-algebra homomorphism from $A_n(k)$ onto $\Delta(k[x_1, \ldots, x_n])$ which sends x_i to $\widehat{x_i}$ and y_i to $\frac{\partial}{\partial x_i}$.

Proof. $[\widehat{x_i}, \widehat{x_j}] = \left[\frac{\partial}{\partial x_i}, \frac{\partial}{\partial x_j}\right] = 0$ for all $1 \leqslant i, j \leqslant n$. Moreover

$$\left[\frac{\partial}{\partial x_j}, \widehat{x_i}\right](f) = \frac{\partial}{\partial x_i}(x_j f) - x_j \frac{\partial f}{\partial x_i} = \begin{cases} f & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

for all $f \in A$. So the surjective map $k\langle x_1, \ldots, x_n, y_1, \ldots, y_n \rangle \to \Delta(A)$ which sends x_i to $\widehat{x_i}$ and y_i to $\frac{\partial}{\partial x_i}$ factors through $A_n(k)$. □

3. Basics on noetherianity

We will now recall a key finiteness property of modules that is sufficiently restrictive to allow strong structure theorems to be proved, and yet sufficiently general to include large classes of interesting noncommutative rings: the *noetherian condition*.

Definition 3.1. The (left) R-module M is said to be *cyclic* if it can be generated by a single element: $M = Rx = \{rx : r \in R\}$ for some $x \in M$. M is *finitely generated* if it can be written as a finite sum of cyclic submodules $M = Rx_1 + Rx_2 + \ldots + Rx_n$.

Lemma 3.2. Let M be an R-module. The following are equivalent:

[11] i.e. the smallest k-subalgebra containing

(a) Every submodule of M is finitely generated
(b) **Ascending chain condition (acc):** There does not exist an infinite strictly ascending chain of submodules of M
(c) **Maximum condition:** Every non-empty subset of submodules of M contains at least one maximal element. (If $\mathcal{S}$ is a set of submodules, then $N \in \mathcal{S}$ is a *maximal element* if and only if $N' \in \mathcal{S}$, $N \leqslant N'$ implies $N = N'$).

Proof. This is exactly the same as for the case where R is commutative so we will not repeat the details. □

Dually, we have the *descending chain condition (dcc)* and the *minimum condition*; these are also equivalent to each other by considering the same proof as for acc and the maximum condition with reversed ordering.

Definition 3.3. Let R be a ring.

- An R-module satisfying (a), (b), (c) of Lemma 3.2 is *noetherian.*
- A submodule I of R as a left-module is called a *left ideal*; a subgroup I of $(R, +)$ is a left ideal if $ax \in I$ for all $a \in R$ and $x \in I$. We write $I \lhd_l R$.
- The ring R is *left noetherian* if it is noetherian as a left R-module.
- An R-module satisfying the descending chain condition, or equivalently, the minimum condition, is said to be *artinian.*
- The ring R is *left artinian* if it is artinian as a left R-module.

We have similar definitions "on the right hand side". In particular a *right ideal* I of R, $I \lhd_r R$ is a left ideal of R^{op}, R is *right noetherian (resp. artinian)* if and only R^{op} is left noetherian (resp. artinian). If R is *both* left and right noetherian (resp. artinian) then we will simply say that R is *noetherian (resp artinian).*

Here is a key result for proving that certain rings are left noetherian: it is a non-commutative version of *Hilbert's Basis Theorem.*

Theorem 3.4 (McConnell, 1968)**.** Let S be a ring, R a left noetherian subring and suppose that for some $x \in S$ we have

(1) $R + xR = R + Rx$, and
(2) $S = \langle R, x\rangle$.

Then S is also left noetherian.

Lecture 4

In which we prove a non-commutative version of Hilbert's Basis Theorem and use it to prove that group algebras of polycyclic groups are noetherian

Proof of Theorem 3.4. The hypothesis $R + Rx = R + xR$ implies that

$$R + Rx + \cdots + Rx^n = R + xR + \cdots + x^n R \text{ for all } n \geq 0.$$

This can be seen inductively:

$$Rx^n = Rx^{n-1}x \subseteq (R + xR + \cdots x^{n-1}R)x \subset R + xR + \cdots x^n R$$

and, symmetrically,

$$x^n R = xx^{n-1}R \subseteq x(R + Rx + \cdots Rx^{n-1}) \subseteq R + Rx + \cdots Rx^n.$$

It follows that

(a) $S_n := R + xR + \cdots + x^n R$, is both a left and a right R-submodule of S for all $n \geq 0$ — note that it isn't necessarily true that this sum is direct.
(b) $S = \bigcup_{n\geq 0} S_n$ since it is a subring of S containing both R and x. Indeed we can see that $S_n S_m = S_{n+m}$, $R = S_0$ and $x \in S_1$.
(c) For each $r \in R$ and $n \geq 0$ there exists $r' \in R$ such that $r'x^n - x^n r \in S_{n-1}$.

Now, let $I \lhd_l S$. We will show that I is finitely generated.

Let

$$I_n := \{r_n \in R : \exists s \in I \quad \text{with} \quad s - x^n r_n \in S_{n-1}\}$$

Claim: $I_n \lhd_l R$ for all $n \geq 0$.

It is easy to see that I_n is closed under addition in R since I is closed under addition in S. Let $r \in R$ and $s = \sum_{i=0}^n x^i r_i \in I$. By observation (c) above, we can find $r' \in R$ such that $r'x^n - x^n r \in S_{n-1}$ and by observation (a) $r'x^i r_i \in S_{n-1}$ for all $i < n$. Thus,

$$r's - x^n r r_n \in S_{n-1}$$

and as $r's \in I$, since $I \lhd_l S$, we see that $rr_n \in I_n$ and I_n is a left ideal of R as claimed.

Moreover, if $s = \sum_{i=0}^n x^i r_i \in I$, then $xs = \sum_{i=1}^{n+1} x^i r_{i-1} \in I$ so $r_n \in I_{n+1}$. Hence $I_n \leqslant I_{n+1}$ for all $n \geq 0$. By acc. for left ideals in R there exists $m \geq 0$ such that $I_m = I_{m+r}$ for all $r \geq 0$. Since all left ideals of R are f.g. for each $i = 0, \ldots m$ we may choose $\{r_{ij}\}$ a finite generating set for $I_i \lhd_l R$ and choose $s_{ij} \in I$ such that $s - x^i r_{ij} \in S_{i-1}$.

Claim: $X = \{s_{ij} : 0 \leqslant i \leqslant m, \text{ all } j\}$ generates $I \lhd_l S$.

Let $s = \sum_{i=0}^n x^i r_i \in I \cap S_n$. We show by induction on n that $s \in S \cdot X$ and then appeal to observation (b) above.

If $n = 0$ then $I \cap S_0 = I_0$ and $s_{0j} = r_{0j}$ so the result is trivial.

If $0 < n \leqslant m$ then $r_n = \sum a_j r_{nj}$ for some $a_j \in R$, so choosing $a'_j \in R$, such that $a'_j x^n - x^n a_j \in S_{n-1}$ we see that

$$a'_j s_{nj} - x^n a_j r_{nj} \in S_{n-1}$$

and

$$s - \sum a'_j s_{nj} \in I \cap S_{n-1} \subseteq S \cdot X$$

by the induction hypothesis. Thus $s \in S \cdot X$.

If $n > m$ then $r_n \in I_m$ so $r_n = \sum a_j r_{mj}$ for some $a_j \in R$ and again we choose $a'_j \in R$ such that $a'_j x^n - x^n a_j \in S_{n-1}$ and so $a'_j x^{n-m} s_{mj} - x^n a_j r_{mj} \in S_{n-1}$. So

$$s - \sum a'_j x^{n-m} s_{mj} \in I \cap S_{n-1} \subseteq S \cdot X$$

by the induction hypothesis. So $s \in S \cdot X$. □

Of course considering S^{op} yields a similar result for right noetherian rings.

Note that if k is a commutative ring and G is a group then, since $G \cong G^{\mathrm{op}}$ under $g \mapsto g^{-1}$,

$$kG \cong kG^{\mathrm{op}} \cong (kG)^{\mathrm{op}}.$$

It follows that if k is noetherian then kG is left noetherian if and only if it is right noetherian.

Definition 3.5. A group G is said to be *polycyclic* if there is a chain

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_{n-1} \lhd G_n = G$$

of subgroups of G such that each G_i/G_{i-1} is cyclic for each $i = 1, \ldots, n$.

Examples 3.6.

(a) Infinite cyclic $G = \langle x \rangle \cong \mathbb{Z}$.

(b) Free abelian $G = \langle x_1, \ldots, x_n \rangle \cong \mathbb{Z}^n$.

(c) $G = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$. Here we have the chain $1 \lhd G_1 \lhd G_2 \lhd G_3 = G$ where $G_1 = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $G_2 = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(d) $\{I + N \in M_n(\mathbb{Z}) : N \text{ is strictly upper triangular}\}$ is always polycyclic.

Theorem 3.7 (Auslander-Swan)**.** Let G be a polycyclic group. Then

(1) G is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ for some n.

(2) G has a subgroup H of finite index isomorphic to a subgroup of $\mathrm{Tr}_n(\mathcal{O})$, the group of upper-triangular matrices in $GL_n(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of an algebraic number field.

Proposition 3.8. Let k be a commutative noetherian ring and let G be a polycyclic group. Then kG is noetherian.

Proof. Choosing a chain of subnormal subgroups with cyclic quotients

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_{n-1} \lhd G_n = G$$

we see that it's sufficient to show that if kG_{i-1} is left Noetherian then so is kG_i for all $i = 1, \ldots, n$. Choose a generator xG_{i-1} for the cyclic group G_i/G_{i-1}, let

$R = kG_{i-1}$ and let $S = \langle R, \delta_x \rangle$, a subring of kG_i. Suppose that R is left noetherian. Because $x^{-1}G_{i-1}x = G_{i-1}$, we see that $G_{i-1}x = xG_{i-1}$ so $R\delta_x = \delta_x R$. Hence $R + R\delta_x = R + \delta_x R$, and therefore S is left noetherian by Theorem 3.4.

Let I be a left ideal of kG_i. Now, $I \cap S \lhd_l S$ so has a finite generating set:

$$I \cap S = \sum_{i=1}^{r} S s_i,$$

say. If $t \in I$, then $\delta_x^m t \in I \cap S$ for some $m \geq 0$, so $t = \sum_{i=1}^r \delta_x^{-m} a_i s_i$ for some $a_i \in S$. Hence the $s_1, \ldots, s_r$ generate I as a left ideal of RG_i and RG_i is left noetherian.[12] □

It remains an open problem whether the only noetherian group algebras $\mathbb{Z}G$ are those where G has a finite index polycylic subgroup (so called virtually polycyclic groups). It is not too hard (see examples sheet 1) to show that if $\mathbb{Z}G$ is noetherian then G must have the property that its collection of subgroups satisfies the ascending chain condition but there are groups that are not virtually polycyclic that satisfy this condition such as the 'Tarski monsters'. In 2019 Kropholler and Lorenson published a paper showing that in fact G must be 'amenable' and have the property that every subgroup of G is finitely generated. The only groups known to have these properties are virtually polycyclic. The definition of amenable is beyond the scope of this course.

We note now and will prove later that $U(\mathfrak{g})$ is noetherian whenever $\mathfrak{g}$ is a finitely generated k-module and k is notherian. The converse is open.

That Weyl algebras are noetherian is Example Sheet 1 Q5(a).

Lecture 5

In which we meet simple modules and primitive ideals

4. Simple modules and Artinian rings

Throughout this chapter, R denotes an arbitrary ring, unless stated otherwise. As we have noted previously one way to try to understand a ring it to try to understand its modules. As for commutative rings we have an isomorphism theorem for R-modules.

Proposition 4.1. Suppose M and N are R-modules and $\varphi \in \mathrm{Hom}_R(M, N)$ then $\ker\varphi$ is a submodule of M, $\mathrm{im}\varphi$ is a submodule of N and

$$M/\ker\varphi \cong \mathrm{im}\varphi$$

is an isomorphism of R-modules.

[12] A member of the audience noted after the lecture that we could instead complete the proof by applying Theorem 3.4 to S and $RG_i = \langle S, \delta_x^{-1} \rangle$.

Definition 4.2. An R-module M is *simple* or *irreducible* if $M \neq 0$ and the only submodules of M are 0 and M.

Suppose M is simple. Choose $0 \neq x \in M$; then $M = Rx$ so $M \cong R/\operatorname{ann}_R(x)$ where

$$\operatorname{ann}_R(x) := \{r \in R : rx = 0\} = \ker(R \to M; r \to rx) \lhd_l R$$

is the *point annihilator of* x. Note that $\operatorname{ann}_R(x)$ need *not* be equal to $\operatorname{ann}(y)$ if x, y are distinct nonzero elements of M, unless R is commutative.

It is easy to see that $M = Rx$ is simple if and only if $\operatorname{ann}(x)$ is a maximal left ideal of R since if $J \lhd_l R$ is a proper left ideal that properly contains I then J/I is a proper submodule of R/I and every proper submodule arises in this way.

Recall Zorn's Lemma.

Theorem 4.3 (Zorn's Lemma)**.** Let $(\mathcal{S}, \leqslant)$ be a poset. If every totally ordered subset of $\mathcal{S}$ has an upper bound then, for every $s \in S$, $\mathcal{S}$ has a maximal element x with $s \leqslant x$.

This is equivalent to the Axiom of Choice, which we will always assume holds.

As in the commutative case we can use Zorn's Lemma to show that every left ideal I of a ring R is contained in a maximial left ideal.

Lemma 4.4. Suppose L is a proper left ideal of R. Then L is contained in a maximal left ideal I of R.

Proof. Recall that the proper left ideals are precisely those that don't contain 1. Let $\mathcal{S} = \{K \lhd_l R : K \text{ proper}\}$. $\mathcal{S}$ is partially ordered by inclusion. Since $L \in \mathcal{S}$, by Zorn, it suffices to show that every chain in S has an upper bound. Let $\mathcal{C}$ be a chain in $\mathcal{S}$. Then $\bigcup \mathcal{C}$ is a left ideal that doesn't contain 1, i.e. $\bigcup \mathcal{C} \in \mathcal{S}$ and $\mathcal{C}$ has an upper bound in $\mathcal{S}$. □

It is clear that the same proof works for right ideals and for two-sided ideals.

Corollary 4.5. Every nonzero finitely generated R module M has a simple quotient.

Proof. Suppose that M generated by $x_1, \ldots, x_n$ but not by $x_1, \ldots, x_{n-1}$. Then, letting $N = \sum_{i=1}^{n-1} Rx_i$, we get

$$M/N \cong R/\operatorname{ann}_R(x_n + N)$$

is nonzero and cyclic.

Taking I to be a maximal left ideal of R containing $\operatorname{ann}_R(x_n + N)$ we see that M has a quotient isomorphic to R/I which is simple. □

We note the finitely generated condition is necessary since, for example, $\mathbb{Q}$ has no simple quotient as a $\mathbb{Z}$-module.

Note that the *annihilator*

$$\mathrm{Ann}_R(M) := \{a \in R : aM = 0\} = \bigcap_{m \in M} \mathrm{ann}_R(m)$$

of any R-module M is a (two-sided) ideal of R. Moreover if I is an ideal then $\mathrm{Ann}_R(R/I) = I$ so every ideal in R arises as the annihilator of an R-module.

An R-module M is *faithful* if $\mathrm{Ann}_R(M) = 0$, equivalently if the natural map $R \to \mathrm{End}(M)$ is injective.

Definition 4.6. Let I be a two-sided ideal of R. Then I is *left primitive* if I is the annihilator of a simple left R-module M.

The ring R itself is called *left primitive* if its zero ideal is left primitive, or equivalently, if R has at least one faithful simple left module.

There are examples due to George Bergman of rings which are left primitive, but not right primitive.

Lemma 4.7. Let $M = Rx$ be a cyclic left R-module. Then $\mathrm{Ann}_R(M)$ is the largest two-sided ideal contained in $L = \mathrm{ann}_R(x)$.

Proof. Note that this largest two-sided ideal I exists, since the sum of all two-sided ideals contained in L is itself a two-sided ideal contained in L.

Certainly $\mathrm{Ann}_R(M) \subseteq L$, so $\mathrm{Ann}_R(M) \subseteq I$.

Now $IM = IRx \subseteq Ix \subseteq Lx = 0$ since I is two-sided, so $I \subseteq \mathrm{Ann}_R(M)$. □

Corollary 4.8. Every maximal ideal of R is left and right primitive. Moreover, if R is commutative, every primitive ideal is maximal.

Definition 4.9. The *Jacobson radical* $J(R)$ of R is defined to be the intersection of all left primitive ideals of R.

Note that $J(R)$ is the set of elements of R which annihilate every simple left R-module.

Lemma 4.10. $J(R)$ is equal to the intersection K of all maximal left ideals of R.

Proof. If $x \in J(R)$ and $L \lhd_l R$ is a maximal left ideal then $x \cdot R/L = 0$ so $x \in L$. Thus $J(R) \subseteq K$.

Now suppose P is a left primitive ideal, so $P = \mathrm{Ann}_R(M)$ for some simple R-module M. Then $P = \bigcap_{0 \neq x \in M} \mathrm{ann}_R(x)$ is an intersection of maximal left ideals, so $K \subseteq P$. It follows that $K \subseteq J(R) = \bigcap_{P \text{ primitive}} P$ as required. □

Lemma 4.11 (Nakayama)**.** Let M be a finitely generated nonzero left R-module. Then $J(R)M$ is strictly contained in M.

Proof. Since M is finitely generated it has a simple quotient M/K. Then

$$J(R)(M/K) = 0$$

so $J(R)M \subseteq K$ which is strictly contained in M. □

Note the condition that M is finitely generated is necessary even when R is commutative. For example if $p \in \mathbb{Z}$ is prime then $J(Z_{(p)}) = p\mathbb{Z}_{(p)}$ but $p\mathbb{Q} = \mathbb{Q}$.

Corollary 4.12. Let M be a finitely generated left $R-$module. If N is a submodule of M such that $M = N + J(R)M$ then $M = N$.

Proof. Apply the Lemma to M/N. ☐

Proposition 4.13.

$$J(R) = \{x \in R : 1 - axb \in R^\times \quad \text{for all} \quad a, b \in R\} =: K.$$

Proof. Since $J(R)$ is a two-sided ideal, to show that $J(R) \subseteq K$ it's sufficient to show $x \in J(R)$ implies $1 - x$ is a unit. Now $R = R(1-x) + Rx$, so, as $Rx \subseteq J(R)$, Corollary 4.12 implies that $R(1-x) = R$. Hence there exists $y \in R$ such that

$$y(1-x) = 1.$$

Now, $1 - y = -yx \in J(R)$, so by the same argument applied to $1 - y$, we can find $z \in R$ such that

$$z(1-(1-y)) = zy = 1.$$

Hence $z = zy(1-x) = 1-x$. Thus we have $yz = 1$ and $zy = 1$ and $z = 1-x \in R^\times$.

Now let $x \in K$, let I be a maximal left ideal of R with $x \notin I$. Since I is maximal, $I + Rx = R$, so $1 - ax \in I$ for some $a \in R$. Since $x \in K$, $1 - ax$ is a unit, a contradicting the fact that I is a proper ideal. Hence x in the intersection of all maximal left ideals. So by Lemma 4.10, $K \subseteq J(R)$. ☐

This result shows that $J(R)$ is the largest ideal two-sided A of R such that $1 - A$ consists entirely of units of R.

Corollary 4.14. As sets $J(R) = J(R^{\text{op}})$. It follows that the intersection of all maximal left ideals of R is equal to the intersection of all maximal right ideals.

Lecture 6

In which we prove the Jacobson Density Theorem and Artin-Wedderburn for left primitve left artinian rings

We will now work towards understanding the structure of left artinian rings. Let V be a left R-module and let $D = \text{End}(V)^{\text{op}}$. We can view V as a right D-module via $V \times D \to D$; $(v, \phi) \mapsto v\phi = \phi(v)$ since this corresponds to the natural inclusion $D \to \text{End}_{\mathbb{Z}}(V)^{\text{op}}$.

Then V becomes an *R-D-bimodule*: this means that V is simultaneously a left R-module and a right D-module via the rule $v \cdot \varphi = v\varphi$, and the two structures are compatible in the following sense:

$$r(v\varphi) = (rv)\varphi \quad \text{for all} \quad r \in R, \varphi \in D, v \in V.$$

Of course, this just says that every element of D is an endomorphism of the left R-module V.

Theorem 4.15 (Schur's Lemma)**.** Let V be a simple left R-module. Then $D := \operatorname{End}(V)$ is a division ring.

Proof. Let $\varphi : V \to V$ be a nonzero R-module homomorphism. Then $\ker(\varphi) < V$ and $\operatorname{im}(\varphi) > 0$. The simplicity of V forces $\ker(\varphi) = 0$ and $\operatorname{im}(\varphi) = V$, so φ is an isomorphism. Thus every nonzero element of D is a unit. □

So whenever V is a simple left R-module, V becomes a right vector space over the division ring $D = \operatorname{End}_R(V)$.

Lemma 4.16. Let V be a simple left R-module, let $D = \operatorname{End}_R(V)$, let X be a finite subset[13] of V, and let

$$I := \operatorname{ann}_R(X) = \bigcap_{x \in X} \operatorname{ann}_R(x).$$

Suppose that $I \cdot y = \{0\}$ for some $y \in V$. Then $y \in X \cdot D$, the D-linear span of X.

Proof. We proceed by induction on $n = |X|$. When $n = 0$, we have $\operatorname{ann}(\emptyset) = R$ and $\emptyset \cdot D = \{0\}$. So since $R \cdot y = \{0\}$ by assumption, we have $y = 0 \in \emptyset \cdot D$.

Assume now that $n \geq 1$ and let $J = \operatorname{ann}(X \backslash \{x\})$ for some $x \in X$ so that $I = J \cap \operatorname{ann}(x)$. If $J \subseteq \operatorname{ann}(x)$ then $J = I$, so $J \cdot y = 0$ and we can apply the induction hypothesis. So we can assume that J is not contained in $\operatorname{ann}(x)$. But then the R-submodule $J \cdot x$ of V is non-zero, so $J \cdot x = V$ by the simplicity of V.

Define $d : V \to V$ by the rule $(r \cdot x)d = r \cdot y$, whenever $r \in J$. This is well-defined, because if $r \cdot x = 0$ for some $r \in J$ then $r \in \operatorname{ann}(x) \cap J = I$, so $r \cdot y = 0$ since $I \cdot y = 0$ by assumption. This function is left R-linear because $(s \cdot (r \cdot x))d = (sr \cdot x)d = sr \cdot y = s \cdot (r \cdot y) = s \cdot ((r \cdot x)d)$ for all $s \in R$. Thus we have found an element $d \in D$ such that $J \cdot (y - x \cdot d) = 0$. Hence $y - x \cdot d \in (X \backslash \{x\}) \cdot D$ by induction and therefore $y \in X \cdot D$. □

Theorem 4.17 (Jacobson's Density)**.** Let V be a simple left R-module, and let $X \subset V$ be a finite D-linearly independent subset of V where $D := \operatorname{End}_R(V)$. Then for every $\alpha \in \operatorname{End}_D(V)$ there exists $r \in R$ such that $\alpha(x) = rx$ for all $x \in X$.

Proof. Write $X = \{x_1, \ldots, x_n\}$, fix $i \in \{1, \ldots, n\}$ and write $X_i := X \backslash \{x_i\}$. Since $x_i \notin X_i \cdot D$, Lemma 4.16 below gives $\operatorname{ann}(X_i) \cdot x_i \neq 0$. So there is some $r_i \in \operatorname{ann}(X_i)$ such that $r_i \cdot x_i \neq 0$. Since V is simple, $R \cdot (r_i \cdot x_i) = V$, so we can find some $s_i \in R$ such that $s_i \cdot (r_i \cdot x_i) = \alpha(x_i)$. Now

$$\sum_{j=1}^{n} s_j r_j \cdot x_i = s_i \cdot r_i \cdot x_i = \alpha(x_i) \quad \text{for all} \quad i = 1, \ldots, n.$$

[13]In the lecture I imposed the additional assumption that X is D-linearly independent but on reflection this is obviously redundant because if the result is true for a D-linearly independent set X then it is also true for every (finite) subset Y of V with $YD = XD$ since $\operatorname{ann}_R(X) = \operatorname{ann}_R(XD) = \operatorname{ann}_R(Y)$. That is the result as really about finite dimensional D-linear subspaces of V. Moreover, as noted by a member of the audience, the proof does not use linear independence

So we can take $r = \sum_{j=1}^{n} s_j r_j$. ☐

Lemma 4.16 also has the following interesting consequence.

Lemma 4.18. Let R be a left artinian ring, let V be a simple left R-module and let $D = \mathrm{End}_R(V)^{\mathrm{op}}$. Then V is finite dimensional as a right D-vector space.

Proof. Since R is left artinian, the set $\{\mathrm{ann}(X) : X \subset V, |X| < \infty\}$ of left ideals has a minimal element $I = \mathrm{ann}(X)$, say. We will show that $V = X \cdot D$. Let $y \in V$ and consider $\mathrm{ann}(X \cup \{y\}) \subseteq \mathrm{ann}(X)$. The minimality of $\mathrm{ann}(X)$ forces these to be equal. Hence $I \cdot y = 0$, so $y \in X \cdot D$ for any $y \in V$ by Lemma 4.16. Hence $V = X \cdot D$. ☐

Theorem 4.19 (Artin-Wedderburn)**.** Let R be a left primitive, left artinian ring. Then $R \cong M_n(D)$ for some division ring D and integer $n \geq 1$.

The proof requires the following Lemma.

Lemma 4.20. Let S be a ring, let N be a right S-module and let $n \geq 1$ be an integer. Then the ring of endomorphisms of N^n as a right S-module is isomorphic to $\mathrm{Mat}_n(\mathrm{End}_S(N))$.

Proof. This is best seen by writing elements of N^n as column vectors $x = (x_j)_{j=1}^n$ and thinking of S-module endomorphisms acting by matrix multiplication on the *left* of these column vectors.

Formally, let $\sigma_j : N \hookrightarrow N^n$ and $\pi_j : N^n \twoheadrightarrow N$ for $j = 1, \ldots, n$ be given by

$$\sigma_j(x)_i = x\delta_{ij} \quad \text{and} \quad \pi_j(x) = x_j.$$

These are right S-module homomorphisms. We define $\alpha : \mathrm{End}((N_S)^n) \to M_n(T)$ by setting the (i, j) element of $\alpha(f)$ to be the composition

$$N \overset{\sigma_j}{\to} N^n \overset{f}{\to} N^n \overset{\pi_i}{\to} N;$$

thus $\alpha(f)_{ij} = \pi_i f \sigma_j$. We can also define $\beta : M_n(T) \to \mathrm{End}((N_S)^n)$ by

$$\beta(A) = \sum_{i,j=1}^{n} \sigma_j A_{ji} \pi_i.$$

It is a pleasant exercise to show that α and β are mutually inverse ring homomorphisms. ☐

Proof of Theorem 4.19. Let V be a faithful simple left R-module, and let $D = \mathrm{End}({}_R V)$. Then D is a division ring by Theorem 4.15. Now there is an isomorphism $V \cong D^n$ of right D-modules for some positive integer n by Lemma 4.18 and $\theta\colon D \cong \mathrm{End}(D)$[14] via $\theta(d)(d') = dd'$. So

$$\mathrm{End}((D)^n) \cong \mathrm{Mat}_n(\mathrm{End}(D)) \cong \mathrm{Mat}_n(D)$$

[14] where D is viewed as a right D-module

by Lemma 4.20. Now we have a natural ring homomorphism

$$\psi : R \to \mathrm{End}(V_D)$$

given by $\psi(r)(v) = r \cdot v$. It is injective because V is faithful, and it is surjective by Theorem 4.17. We conclude that $R \cong \mathrm{Mat}_n(D)$. □

Theorem 4.21 (Chinese Remainder Theorem)**.** Let R be a ring, and let $P_1, \dots, P_n$ be two-sided ideals in R such that $P_i + P_j = R$ whenever $i \neq j$. Then

$$R/(P_1 \cap P_2 \cap \cdots \cap P_n) \cong (R/P_1) \times (R/P_2) \times \cdots \times (R/P_n).$$

Proof. There is a natural ring homomorphism $\varphi : R \to \bigoplus_{i=1}^n R/P_i$ given by $\varphi(r) = (r + P_i)_{i=1}^n$. Its kernel is $P_1 \cap \cdots \cap P_n$, so by the First Isomorphism Theorem for rings it will be sufficient to show that φ is surjective. We prove this by induction on n, the case $n = 1$ being clear.

Since $P_i + P_n = R$ for all $i < n$, we can find $a_i \in P_i$ and $b_i \in P_n$ such that $a_i + b_i = 1$ for all $i = 1, \dots, n-1$. Let $a := a_1 \cdots a_{n-1} \in P_1 \cap \cdots \cap P_{n-1}$ and let $b := 1 - a$. Then

$$b = 1 - a = (a_1 + b_1) \cdots (a_{n-1} + b_{n-1}) - a_1 \cdots a_{n-1} \in P_n.$$

Now, given $(r_i + P_i) \in \oplus_{i=1}^n R/P_i$, we can find some $s \in R$ such that $s - r_i \in P_i$ for all $i < n$ by induction. Let $r := sb + r_n a$; then

$$r + P_n = r_n(1 - b) + P_n = r_n + P_n$$

and

$$r + P_i = sb + P_i = r_i + P_i \text{ for each } i < n.$$

So $\varphi(r) = (r_i + P_i)_{i=1}^n$ and φ is surjective. □

Lecture 7

In which we classify semiprimitive left artinian rings, introduce semisimple modules and prove that every left artinian ring is left noetherian

Definition 4.22. We call a ring R such that $J(R) = 0$ *semiprimitive.*[15] We call a non-zero ring with no non-zero proper two-sided ideals *simple.*

Exercise 4.1. Show that if D is a division ring and $n \geq 1$ then $\mathrm{Mat}_n(D)$ is simple.

Corollary 4.23. Let R be a semiprimitive left artinian ring. Then there exist division rings $D_1, \dots, D_n$ and integers $d_1, \dots, d_n \geq 1$ such that

$$R \cong \mathrm{Mat}_{d_1}(D_1) \times \cdots \times \mathrm{Mat}_{d_n}(D_n).$$

[15] Recall that we proved that $J(R) = J(R^{\mathrm{op}})$ so there is no need to distinguish between left semiprimitive and right semi-primitive.

Proof. Let $\mathcal{S}$ be the set of finite intersections of left primitive ideals of R; it is non-empty by Lemma 4.4. Since R is left artinian, this set has a minimal element $I := P_1 \cap \cdots \cap P_n$ say. If Q is another left primitive ideal of R then $I \cap Q = I$ by the minimality of I, so that $I \subseteq Q$. Hence $I \subseteq J(R) = \{0\}$ by assumption. Now. R/P_i is left primitive and left artinian so by Artin-Wedderburn $R/P_i \cong M_{d_i}(D_i)$ for some division ring D_i and positive integer d_i, and such a ring has no non-trivial two-sided ideals (Exercise). So each P_i is a maximal two-sided ideal, and therefore $P_i + P_j = R$ whenever $i \neq j$. Now apply Theorem 4.21. □

Exercise 4.2. By directly computing the set of left ideals of R, show that

$$R := \mathrm{Mat}_{d_1}(D_1) \times \cdots \times \mathrm{Mat}_{d_n}(D_n)$$

is a semi-primitive left artinian ring for any family of division rings $D_1, \ldots, D_n$ and positive integers $d_1, \ldots, d_n$. Deduce that a semiprimitive left artinian ring is right artinian.

Definition 4.24. A (left) R-module M is *semisimple* if M is a direct sum of simple R-modules: $M = \bigoplus_{i \in I} M_i$.

Note that a ring is R semiprimitive if and if R has a faithful semisimple module.

Lemma 4.25. Any subquotient N of a semisimple module M is semisimple.

Warning: If $M = \bigoplus_{i \in I} M_i$ for simple R-modules M_i it is not true in general that every submodule is of the form $\bigoplus_{j \in J} M_j$ for some $J \subset I$. For example it fails when R is a field and $M = Re_1 \oplus Re_2$ since $R(e_1 + e_2)$ is not of this form.

Proof. It suffices to show that every submodule of M and every quotient module of M is semisimple.

Suppose that $M = \bigoplus_{i \in I} M_i$ with M_i simple and N is a submodule of M. Despite the warning we'll show it is true that N has a complement of the form $\bigoplus_{j \in J} M_j$ for some $J \subset I$.

To this end, consider the collection

$$\mathcal{S} := \left\{ J \subset I : N \cap \bigoplus_{j \in J} M_j = 0 \right\}.$$

If $\mathcal{C}$ is a chain in $\mathcal{S}$ we claim that $K = \bigcup_{J \in \mathcal{C}} J \in \mathcal{S}$.

Indeed, if $n \in N \cap \bigoplus_{k \in K} M_k$ there is a finite subset $\{k_1 \ldots, k_n\} \subset K$ such that $n \in \bigoplus_{i=1}^n M_{k_i}$. But then there is some $J \in \mathcal{C}$ such that $\{k_1, \ldots, k_n\} \subset J$ and then $n \in N \cap \bigoplus_{j \in J} M_j$ is zero. It thus follows from Zorn that there is a maximal element J of $\mathcal{S}$.

Now if $N + \bigoplus_{j \in J} M_i$ is a proper submodule of M then there is some M_i not contained in $N + \bigoplus_{j \in J} M_j$. As M_i is simple $\left(N + \bigoplus_{j \in J} M_j\right) \cap M_i = 0$ and so

$J \cup \{i\} \in \mathcal{S}$ contradicting the maximality of J. Thus $M = N \oplus \bigoplus_{j \in J} M_j$ and so

$$M/N \cong \bigoplus_{j \in J} M_j$$

and

$$N \cong M/\bigoplus_{j \in J} M_j \cong \bigoplus_{i \in I \setminus J} M_i. \qquad \square$$

Lemma 4.26. Let M be a semisimple R-module. Then the following are equivalent:

(a) M is noetherian;
(b) M is artinian;
(c) M is a *finite* direct sum of simple modules.

We'll call a module satifying these conditions *semisimple artinian.*

Proof. Since a simple module is necessarily noetherian and artinian, by Example Sheet 1 Q6(a) and its dual version for artinian modules[16] (c) implies both (a) and (b).

If (c) does not hold then M has a submodule $N = \bigoplus_{n \geq 1} N_n$ with each N_n simple. Then

$$N_1 < N_1 \oplus N_2 < N_1 \oplus N_2 \oplus N_3 < \cdots$$

is a strictly ascending chain of submodules of M and

$$\bigoplus_{n \geq 1} N_n > \bigoplus_{n \geq 2} N_n > \bigoplus_{n \geq 3} N_n > \cdots$$

is a strictly descending chain of submodules of M. Thus neither (a) not (b) holds. $\square$

We note that any subquotient of a semisimple artinian module is semisimple artinian.

Exercise 4.3. Show that the following are equivalent for a ring R

(a) All left R-modules are semisimple;
(b) All right R-modules are semisimple;
(c) R is a semisimple left R-module;
(d) R is a semisimple right R-module;
(e) R is semiprimitive and left artinian.

We conclude this section by proving some general results about left artinian rings.

Proposition 4.27. The Jacobson radical of a left artinian ring R is nilpotent.

[16] with the same proof

Proof. Let $J = J(R)$. The descending chain $J \supseteq J^2 \supseteq J^3 \supseteq \dots$ must terminate since R is left artinian. Hence $J^n = J^{n+1} = \dots$ for some $n \geq 0$.

Conisder $I := \{x \in R : J^n x = 0\}$, this is a two-sided ideal of R. It suffices to prove that $I = R$, so suppose for a contradiction that this is not the case. Then R/I has a minimal non-zero left R-submodule K/I, since R is left-artinian and so R/I is artinian. Then K/I is a simple R-module, so $J \cdot (K/I) = 0$ and $JK \subseteq I$. It follows that

$$J^n K = J^{n+1} K \subseteq J^n I = 0,$$

so $K \subseteq I$ leading to the desired contradiction since $K/I \neq 0$. □

Theorem 4.28 (Hopkins–Levitski, 1939)**.** Let R be a left artinian ring. Then R is also left noetherian.

Proof. Let $J = J(R)$. For any $i \geq 0$, Since R is left artinian, J^i is an artinian left R-module and so J^i/J^{i+1} is a left artinian R/J-module. Since R/J is semiprimitve and left artinian it follows by the last exercise that J^i/J^{i+1} is also semisimple as a left R/J-module and hence as a left R-module. Thus it has finite length and is also left noetherian. Since J is nilpotent by Proposition 4.27, R is a finite extension of left noetherian R-modules, and is therefore itself left noetherian by Example Sheet 1 Q6(a). □

Lecture 8

In which we introduce prime ideals and semiprime ideals and consider some of their basic properties.

5. Prime Ideals

Definition 5.1. Suppose that R is a ring. A *prime ideal* P of R is a proper ideal $P \lhd R$ such that if $I, J \lhd R$ with $IJ \subseteq P$ then $I \subseteq P$ or $J \subseteq P$. The ring R is *prime* if 0 is a prime ideal.

When R is commutative our definition agrees with the usual definition: P is prime if $x, y \in R$ with $xy \in P$ then $x \in P$ or $y \in P$ since $(x)(y) = (xy)$. However these two definitions don't agree in general when R is noncommutative.

Definition 5.2. We say a proper ideal $P \lhd R$ is *completely prime* if R/P has no non-trivial zero-divisors. We say that R is a *domain* if (0) is a completely prime ideal

We will construct a family of prime ideals that are not completely prime using the following proposition.

Proposition 5.3. Every primitive ideal $P = \mathrm{Ann}_R(M)$ of a ring R is prime and so, in particular, every maximal ideal is prime.

Proof. WLOG M is a simple R-module Let $I, J \lhd R$ such that $IJ \subseteq P$. If $JM = 0$ then $J \subseteq P$. If $JM \neq M$ then $JM = M$ since M is simple and so $IM = IJM = 0$ and $I \subseteq P$. □

Example 5.1. Suppose D is a division ring and consider $R = \mathrm{Mat}_n(D)$. Then D^n is simple D-module under matrix multiplication and $\mathrm{Ann}_R(D^n) = 0$. Thus 0 is a primitive and hence prime ideal of R. However R is not a domain when $n > 1$. In fact by an exercise from last time $M_n(D)$ is simple so 0 is a maximal ideal.

We have the following containments for a general ring.

$$\mathrm{MaxSpec}\, R \subseteq \mathrm{Prim}\, R \subseteq \mathrm{Spec}\, R \supseteq \{\text{completely prime ideals of} R\}$$

where

$$\mathrm{MaxSpec}\, R = \{\text{maximal ideals of} R\},$$

$$\mathrm{Prim}\, R = \{\text{primitive ideals of } R\},$$

$$\mathrm{Spec}\, R = \{\text{prime ideals of } R\}.$$

We've seen that MaxSpec R is always non-empty but {completely prime ideals of R} can be empty. Moreover in general all of these inclusions can be proper.

However if R is commutative then

$$\mathrm{MaxSpec}\, R = \mathrm{Prim}\, R \text{ and } \mathrm{Spec}\, R = \{\text{completely prime ideals of } R\}$$

so these four concepts become two.

If instead R is left artinian then, since $J(R)$ is nilpotent, and so is contained in every prime ideal of R,and $R/J(R)$ is a finite direct product of matrix rings over division rings all of which are simple,

$$\mathrm{Spec}\, R = \mathrm{MaxSpec}\, R.$$

Proposition 5.4. Every prime ideal P in a ring R contains a minimal prime ideal.

Proof. This follows from Zorn's Lemma applied to the poset of prime ideals under reverse inclusion provided that we can show that the intersection of any chain of prime ideals of R contains a prime ideal of R.

In fact we will show that if $\mathcal{C}$ is a chain of prime ideals of R then $Q = \bigcap_{P \in \mathcal{C}} P$ is a prime ideal of R.

To this end, suppose for contradiction that $I_1, I_2 \lhd R$ are ideals not contained in Q but $I_1 I_2 \subseteq Q$. Then we can find $P_1, P_2 \in \mathcal{C}$ such that $I_j \not\subseteq P_j$ for $j = 1, 2$. Indeed since $\mathcal{C}$ is a chain we see that $P = P_1 \cap P_2 \in \{P_1, P_2\}$ and $I_1, I_2 \not\subseteq P$. Since P is prime it follows that $I_1 I_2 \not\subseteq P$. Since $I_1 I_2 \subseteq Q \subseteq P$ we reach our desired contradiction. □

By considering the ring R/I for an ideal I it follows that every such I has a minimal prime P containing it. We call such a P a *minimal prime over* I.

Theorem 5.5. If R is a left or right noetherian ring then R has only finitely many minimal prime ideals. Moreover there is a finite product of minimal prime ideals (possibly with repeats) that is zero.

Proof. If we can find prime ideals $P_1, \dots, P_n$ with $P_1 \cdots P_n = 0$. By replacing each P_j by a minimal prime contained in it, we may assume that all the P_j are minimal. Then, if P is any minimal prime, $P_1 \cdots P_n \subseteq P$ so by primality of P, and an easy induction on n, there is some $P_j \subset P$ and by minimality of P, $P = P_j$. Thus every minimal prime is one of the P_j.

So suppose for contradiction that no product of prime ideals is 0 and consider the set $\mathcal{S}$ of ideals $I \lhd R$ that contain no product of prime ideals. $0 \in \mathcal{S}$ by assumption. Thus by the noetherian hypothesis $\mathcal{S}$ contains a maximal element K. K cannot be a prime ideal because it is contained in itself. Thus there are ideals I, J such that $IJ \subseteq K$ but $I, J \not\subseteq K$. Since $(I+K)(J+K) \subseteq IJ + K \subseteq K$ we may assume that $K \subsetneq I, J$. Thus by the maximality hypothesis there are prime ideals $P_1 \dots, P_n, Q_1, \dots, Q_m$ such that $P_1 \cdots P_n \subseteq I$ and $Q_1 \cdots Q_m \subseteq J$. Then

$$P_1 \cdots P_n Q_1 \cdots Q_m \subset IJ \subseteq K$$

which is our desired contradiction. □

Remark 5.2. We only used the noetherian hypothesis in the form that any collection of two-sided ideals of R has a maximial element which is weaker than either the left or right noetherian hypotheses. However we do need some finiteness hypothesis. For example if X is an infinite set and $R = k^X$ is the ring of all functions $X \to k$ for some field k under pointwise operations then for each $x \in X$,

$$P_x := \ker(R \to k; \quad f \mapsto f(x))$$

is a minimal prime ideal of R so we have infinitely many minimal primes. We can see this by noting that if $x, y \in X$ are distinct then $\delta_x \delta_y = 0$ so $\delta_x \in P$ or $\delta_y \in P$ and $P_x = (\delta_y : y \neq x)$ is the minimal prime ideal not containing δ_x.

Definition 5.6. A *semiprime ideal* in a ring R is an intersection of prime ideals.[17] A ring is *semiprime* if 0 is a semiprime ideal.

Since in a commutative ring every nilpotent element lives in every prime ideal, a semiprime ideal must contain all nilpotent elements. However the example of a matrix ring $M_n(D)$ over a division ring D for $n \geq 2$ shows that this is not true in the noncommutative setting. However we have the following criterion.

Theorem 5.7. An ideal I is semiprime if and only if

$$\text{for every } x \in R \text{ with } xRx \subseteq I, x \in I. \qquad (*)$$

[17]In particular R is semiprime as the empty intersection of prime ideals as is any prime ideal as the intersection of one prime ideal.

Proof. Suppose that $I = \bigcap_{P\in\mathcal{S}} P$ is an intersection of prime ideals and $xRx \subseteq I$. Then $RxRxR \subset P$ for all $P \in \mathcal{S}$ so $RxR \subset P$ for all $P \in \mathcal{S}$ by definition of primality. Thus $x \in I$.

Conversely suppose that (*) holds.

Claim: $I = \bigcap_{I\subseteq P : P \text{ prime}} P$.

That the LHS is contained in the RHS is obvious so we consider $x \in R\backslash I$ and try to prove that there is a prime ideal P containing I but not x. To this end we define $x_0 = x$. By (*) $x_0Rx_0 \not\subseteq I$ so we may choose $x_1 \in x_0Rx_0\backslash I$. We then use (*) again to choose $x_2 \in x_1Rx_1\backslash I$. Continuing in this fashion we obtain a sequence $x = x_0, x_1, x_2, \ldots$ such that $x_i \in x_{i-1}Rx_{i-1}\backslash I$ for all $i \geq 1$. We observe that if J is an ideal then $x_n \in J \implies x_m \in J$ for all $m \geq n$. Moreover $x_n \notin I$ for all n.

By Zorn's Lemma, we may choose $P \supseteq I$ an ideal maximal subject to $x_n \notin P$ for all n. Since $x_0 \notin P$, P is a proper ideal. If we can prove P is prime then we complete the proof.

Suppose $J, K \lhd R$ with $J, K \supsetneq P$. By maximality of P there is some $x_n \in J$ and some $x_m \in K$. Then taking $N = \max(n, m)$ we see that $x_N \in J \cap K$ and so $x_{N+1} \in x_NRx_N \in JK$. Thus $JK \not\subseteq P$ as required. □

Lecture 9

In which we continue our discussion of semiprime ideals and introduce injective modules.

Corollary 5.8. For $I \lhd R$ the following are equivalent:

(a) I is semiprime.

(b) If $J \lhd R$ then $J^2 \subseteq I$ implies $J \subseteq I$.

(c) If J is a one-sided ideal of R then $J^2 \subseteq I$ implies $J \subseteq I$.

Proof. If (a) holds and J is a one-sided ideal with $J^2 \subseteq I$ then for $x \in J$, $xRx \subseteq J^2 \subseteq I$. Thus $x \in I$. Thus (c) holds. (c) implies (b) is trivial. Suppose that (b) holds and pick $x \in I$ with $xRx \subseteq I$. Then $(RxR)^2 \subseteq I$ so by (b) $x \in (RxR) \subseteq I$. Thus (a) holds. □

Corollary 5.9. A semiprime ring has no nilpotent one-sided ideals except 0.

Proof. Suppose that J is a non-zero nilpotent one sided ideal and choose n least such that $J^n = 0$. Since $J \neq 0$, $n > 1$ and then $(J^{n-1})^2 = J^{2n-2} \subseteq J^n = 0$. Thus $J^{n-1} = 0$ by the last corollary. □

Definition 5.10. The *prime radical* $N(R)$ of a ring R is the intersection of all the prime ideals of R, equivalently the intersection of all the minimal prime ideals of R.

Note that $N(R)$ is a proper ideal of R unless R is the zero ring since every non-zero ring has a maximal, and hence prime, ideal. A ring is semiprime precisely if the prime radical is zero.

Theorem 5.11. Suppose that R is a left noetherian ring. Then $N(R)$ is a nilpotent two-sided ideal containing all one-sided nilpotent ideals.

Proof. We've noted that R/N is semiprime and so contains no non-zero one-sided nilpotent ideals. Thus N contains all nilpotent one-sided ideals of R. Since R is a left noetherian ring there are $P_1, \dots, P_n$ prime ideals of R (possibly with repeats) such that $P_1 \cdots P_n = 0$. Since $N \subseteq P_i$ for all i, $N^n = 0$. □

Corollary 5.12. If R is left artinian then $J(R) = N(R)$.

6. Injective modules

Definition 6.1. We say an R-module E is *injective* for every short exact sequence

$$0 \to L \stackrel{g}{\to} M \stackrel{f}{\to} N \to 0$$

of R-modules the induced sequence

$$0 \to \mathrm{Hom}_R(N, E) \stackrel{-\circ f}{\to} \mathrm{Hom}_R(M, E) \stackrel{-\circ g}{\to} \mathrm{Hom}_R(L, E) \to 0$$

is exact. [18]

Exercise 6.1. Show that an R-module E is injective if and only if for every inclusion $L \hookrightarrow M$ of R-modules, and every map $\alpha \in \mathrm{Hom}_R(L, E)$ there exists $\beta \in \mathrm{Hom}_R(M, E)$ such that $\beta|_L = \alpha$.

Hint: First prove $0 \to L \to M \to N \to 0$ exact implies

$$0 \to \mathrm{Hom}_R(N, E) \to \mathrm{Hom}_R(M, E) \to \mathrm{Hom}_R(L, E)$$

is exact for every R-module E.

In fact we have the following stronger result.

Theorem 6.2 (Baer's Criterion for injectivity)**.** A (left) R-module E is injective if and only if for every left ideal I in R every R-module map $I \to E$ can be extended to an R-module map $R \to E$.

Proof. The only if direction is clear by taking $L = I$ and $M = R$ and g the inclusion map in the definition.

Conversely, suppose that the criterion holds and L is a submodule of M and $\alpha\colon L \to X$. Consider the set of all R-linear extensions (L', α') with $L \leqslant L' \leqslant M$ and $\alpha' \in \mathrm{Hom}_R(L', E)$ such that $\alpha'|_L = \alpha$ and make it into a poset by $(L', \alpha') \leqslant (L'', \alpha'')$ precisely if $L' \leqslant L''$ and $\alpha' = \alpha''|_{L'}$. It is easy to check that the conditions of Zorn's lemma hold, and so this set has a maximal element, (N, β), say. We need to show $N = M$.

[18] In categorical language $\mathrm{Hom}_R(-, E)$ is an exact (contravariant) functor from R-modules to abelian groups.

Suppose there is $m \in M \backslash N$, then consider $I = \{r \in R \mid rm \in N\}$, a left ideal in R. By assumption the composite $I \xrightarrow{-\cdot m} N \xrightarrow{\beta} E$ extends to an R-linear map $f\colon R \to E$.

Define $\beta'\colon Rm + N \to E$ by $\beta'(rm + n) = f(r) + \beta(n)$. This is a well-defined R-module map since if $rm = n \in N \cap Rm$ then $f(r) = \beta(n)$ by construction. Thus we have extended β contradicting its maximality, and we are done. □

Definition 6.3. An R-module is M *divisible* if for every $r \in R \backslash 0$ and $n \in M$ there is $m \in M$ such that $rm = n$; equivalently if $r\colon M \to M; m \mapsto rm$ is surjective.

Injective modules can be hard to pin down in general but we do have the following result for (commutative) principal ideal domains using Baer's criterion.

Corollary 6.4. If A is a principal ideal domain, then an A-module M is injective if and only if M is divisible. In particular $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are injective as $\mathbb{Z}$-modules.

Proof. By Baer, M is injective precisely if for every $a \in A$ every A-linear map $f\colon (a) \to M$ extends to an A-linear map $g\colon A \to M$. This extension problem is trivial for $a = 0$. For $a \neq 0$ there is a natural bijection $\mathrm{Hom}_A((a), M) \to M$; $f \mapsto f(a)$. As a special case there is a natural bijection $\mathrm{Hom}_A(A, M) \to M$; $g \mapsto g(1)$. Moreover g extends f if and only if $ag(1) = f(a)$.

It is easy to verify that $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ satisfy this criterion as modules over the PID $\mathbb{Z}$. □

Remarks 6.5. It is easy to see, by the same argument, that injective R-modules are always divisible but the converse is not true in general.

It turns out to be very important in homological algebra that every R-module is a submodule of an injective R-module. Our next goal is to prove this. We will do it first for $\mathbb{Z}$-modules. Given a $\mathbb{Z}$-module A, consider the $\mathbb{Z}$-module

$$E(A) := \{f\colon \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}\}$$

under pointwise $+$. Then $E(A)$ is an injective $\mathbb{Z}$-module because it is divisible (as we can solve the divisibility problem pointwise).

Lemma 6.2. *The canonical map $e_A : A \to E(A)$ defined by $e_A(a)(f) = f(a)$ is an injective homomorphism of $\mathbb{Z}$-modules.*

Proof. That $e_A \in \mathrm{Hom}_{\mathbb{Z}}(A, E(A))$ is clear.

Suppose $e_A(a) = 0$ then every element of $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ acts as zero on a.

But letting B be the submodule of A generated by a, if $a \neq 0$, we can define a group homomorphism $g\colon B \to \mathbb{Q}/\mathbb{Z}$ with $g(a) \neq 0$: if B is isomorphic to $\mathbb{Z}$ this is easy, otherwise it is cyclic of order n and we may define $g(ma) = m/n + \mathbb{Z}$.

Now by the injectivity of $\mathbb{Q}/\mathbb{Z}$ we can extend g to an element of $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ not acting as zero on a. Thus $e_A(a) \neq 0$ and we may deduce that e_A is an injection. □

Lecture 10

In which we show every module is contained in an injective R-module, discuss essential extensions and their relationship to injective modules and conclude by defining the injective hull of a module.

Definition 6.6. If M and N are R-modules, a *monomorphism* $M \to N$ is an injective R-linear homomorphism.

Corollary 6.7. If R is a ring and E is an injective $\mathbb{Z}$-module then $\mathrm{Hom}_{\mathbb{Z}}(R,E)$ is an injective R-module under

$$R \times \mathrm{Hom}_{\mathbb{Z}}(R,E) \to \mathrm{Hom}_{\mathbb{Z}}(R,E); \quad (a \cdot f)(r) = f(ra).$$

Moreover, given any R-module M we can find an injective R-module $E(M)$ and a monomorphism $M \to E(M)$.

Proof. Suppose that $I \lhd_l R$ and $f \in \mathrm{Hom}_R(I, \mathrm{Hom}_{\mathbb{Z}}(R,E))$. We can consider $g \in \mathrm{Hom}_{\mathbb{Z}}(I,E)$ given by $g(x) = f(x)(1)$ for $x \in I$. As E is an injective $\mathbb{Z}$-module, g extends to a $\hat{g}$ in $\mathrm{Hom}_{\mathbb{Z}}(R,E)$. Then $\hat{f}\colon R \to \mathrm{Hom}_{\mathbb{Z}}(R,E)$;

$$\hat{f}(a)(r) = (a \cdot \hat{g})(r) = \hat{g}(ra)$$

is an R-linear map and $\hat{f}|_I = f$. Thus $\mathrm{Hom}_{\mathbb{Z}}(R,E)$ is an injective R-module.

Now given an R-module M there is an injective $\mathbb{Z}$-module E containing M viewed as a $\mathbb{Z}$-module, by the last lemma. Then $e\colon M \to \mathrm{Hom}_{\mathbb{Z}}(R,E)$ given by $e(m)(r) = rm$ is a monomorphism since

$$e(am)(r) = ram = e(m)(ra) = (a \cdot e(m))(r)$$

and if $e(m) = 0$ then $0 = e(m)(1) = m$. □

Corollary 6.8. An R-module M is injective if and only if M is a direct summand of every R-module that contains it.

Proof. If M is injective and $M \leqslant N$ then id_M extends to some $\pi \in \mathrm{Hom}_R(N,M)$ and $N = M \oplus \ker\pi$ since $M \cap \ker\pi = 0$ and for $n \in N$, $\pi(n - \pi(n)) = 0$.

Conversely, if M is a direct summand of every module that contains it then it is a direct summand of an injective module E: $E = M \oplus N$, say. Then given $I \lhd_l R$ and $f \in \mathrm{Hom}_R(I,M)$ we can extend it to an element of $\mathrm{Hom}_R(R,E)$ and then compose this with the projection $E \to M$ to get an extension of f in $\mathrm{Hom}_R(R,M)$. □

There is a strong relationship between the notion of injective modules and the notion of essential submodules/extensions.

Definition 6.9. An *essential submodule* of an R-module M is any submodule N such that $N \cap L \neq 0$ for every nonzero R-submodule L of M. We write $N \leqslant_e M$ and also say M is an *essential extension* of N. An essential extension $N \leqslant_e M$ is *proper* if $N < M$.

If $M = R$ as a left module we call N an *essential left ideal*.

Examples 6.10.

(a) An injective module has no proper essential extensions.
(b) Since any two non-zero $\mathbb{Z}$-submodules of $\mathbb{Q}$ meet non-trivially, $\mathbb{Q}$ is an essential extension of every non-zero $\mathbb{Z}$-submodule.
(c) If M is a semisimple R-module then M has no essential proper submodules.
(d) Suppose R is a prime ring and $0 \neq I \lhd R$ then I is an essential left ideal since if $J \lhd_l R$ then $0 \neq IJ \leqslant I \cap J$.

Exercise 6.3. Suppose M is a left R-module. Prove the following statements.

(a) If $N \leqslant_e M$ and $L \leqslant_e N$ then $L \leqslant_e M$.
(b) If $L_1, L_2, N_1, N_2 \leqslant_e M$ with $L_1 \leqslant_e N_1$ and $L_2 \leqslant_e N_2$ then $L_1 \cap L_2 \leqslant_e N_1 \cap N_2$.
(c) If $N \leqslant_e M$ and $m \in M$ then $Nm^{-1} := \{r \in R : rm \in N\} \leqslant_e R$.
(d) If $N_i \leqslant_e M_i$ for $i \in I$ then $\bigoplus_{i \in I} N_i \leqslant_e \bigoplus_{i \in I} M_i$.
(e) If M has no proper essential submodules then M is semisimple.

Proposition 6.11. Suppose that M is an R-module and $N_i \leqslant_e M_i \leqslant M$ for $i \in I$ and $\sum_{i \in I} N_i$ is a direct sum. Then $\sum_{i \in I} M_i$ is a direct sum.

Proof. If $\sum_{i \in I} M_i$ is not direct then there is some finite set $J \subseteq I$ such that $\sum_{j \in J} M_j$ is not direct.[19]

Thus we have reduced to the case $I = \{1, \dots, n\}$ say and we may continue by induction on n, the case $n = 1$ being trivial. The induction hypothesis gives that $\sum_{i=1}^{n-1} M_i$ is direct and we must show that $\left(\bigoplus_{i=1}^{n-1} M_i\right) \cap M_n = 0$. Part (d) of the exercise gives that $\bigoplus_{i=1}^{n-1} N_i \leqslant_e \bigoplus_{i=1}^{n-1} M_i$ and we're given that $N_n \leqslant_e M_n$ so by part (b) of the exercise

$$0 = \left(\bigoplus_{i=1}^{n-1} N_i\right) \cap N_n \leqslant_e \left(\bigoplus_{i=1}^{n-1} M_i\right) \cap M_n.$$

Thus $\left(\bigoplus_{i=1}^{n-1} M_i\right) \cap M_n = 0$ as required. □

Proposition 6.12. Suppose that $N \leqslant M$ are R-modules and $L \leqslant M$ is maximal subject to $L \cap N = 0$. Then $L \oplus N \leqslant_e M$ and $(L \oplus N)/L \leqslant_e M/L$.

Proof. If $K \leqslant M$ such that $(L \oplus N) \cap K = 0$ then $N \cap (L \oplus K) = 0$[20] thus $K = 0$ by the maximality of L. So $L \oplus N \leqslant_e M$.

If K/L is a non-zero submodule of M/L then $L \leqslant K$ and $N \cap K \neq 0$ by the maximality of L. Thus $(L \oplus N) \cap K > L$ and so $(L \oplus N)/L \cap K/L \neq 0$. □

Corollary 6.13. An R-module E is injective if and only if it has no proper essential extensions.

[19]If the sum is not direct the natural map $\oplus_{i \in I} M_i \to \sum M_i$ has nonzero kernel but any element of this kernel must live in a finite sub-direct sum.

[20]If $n = l + k$ with $n \in N$, $l \in L$ and $k \in K$ then $k = l - n \in (L \oplus N) \cap K$ so $k = l = n = 0$

Proof. We've already proven the forward implication. So suppose that M is non injective. Then we can find an R-module N containing M such that M is not a direct summand of N. By Zorn we can find $L \leqslant N$ maximal subject to $L \cap M = 0$. Then $L \oplus M < N$. By the last result $(L \oplus M)/L < N/L$ is a proper essential extension. But the composite $M \to (L \oplus M)/L \to N/L$ is a monomorphism with the same image as $L \oplus M/L$. So M has a proper essential extension. □

Definition 6.14. Suppose $N \leqslant M$ are R-modules. We say that N is *essentially closed* in M if $N \leqslant_e L \leqslant M$ implies $L = N$ i.e. if N has no proper essential extensions that are submodules of M.

Proposition 6.15. Suppose that E is an injective R-module and $M \leqslant E$. Then M is injective if and only if M is essentially closed in E.

Proof. The forward implication follows immediately from the last result. So suppose that M is essentially closed in E. We will show that M has no proper essential extensions and then the last corollary will complete the argument. So suppose that $M \leqslant_e N$. Since E is injective the inclusion $M \to E$ extends to $f\colon N \to E$. Since $\ker f \cap M = 0$ and $M \leqslant_e N$, $\ker f = 0$. Thus $f\colon N \to f(N)$ is an isomorphism and $M \leqslant_e f(N) \leqslant E$. Thus $M = f(N)$ since M is essentially closed and $M = N$ since f is injective. □

Definition 6.16. An *injective hull* of an R-module M is an injective module that is an essential extension of M.

Example 6.17. $\mathbb{Q}$ is an injective hull of $\mathbb{Z}$ as a $\mathbb{Z}$-module.

Exercise 6.4. Show that if A is a commutative domain then its field of fractions $Q(A)$ is an injective hull of A as an A-module.

Lecture 11

In which we prove that injective hulls exist and are unique up to isomorphism and then discuss the rank of a module

Theorem 6.18. Let M be an R-module.

(a) Any injective module containing M contains an injective hull E of M.

If E is any injective hull for M then

(b) If $M \leqslant_e N$ then id_M extends to a monomorphism $N \to E$.

(c) If $M \leqslant F$ with F injective then id_M extends to a monomorphism $E \to F$.

Thus an injective hull can be viewed as a maximal essential extension of M and a minimal injective extension of M.

Proof. (a) Consider any injective module F containing M and let

$$\mathcal{S} := \{N : M \leqslant_e N \leqslant F\}.$$

If $\mathcal{C}$ is a chain in $\mathcal{S}$, then taking $L = \bigcup_{N \in \mathcal{C}} N$, L is an R-module contained in F and containing M. Moreover if $0 \neq X \leqslant L$ then $X \cap N \neq 0$ for some $N \in \mathcal{C}$ and so $X \cap M = (X \cap N) \cap M \neq 0$ since $M \leqslant_e N$. Thus $M \leqslant_e L$ and so $\mathcal{S}$ is chain complete and has a maximal element E, say. Now if E' is a proper essential extension of E contained in F then by transitivity E' is an essential extension of M contradicting maximality. Thus E is essentially closed in F and so is injective. Therefore E is an injective hull of M.

(b) Since E is injective, id_M extends to an R-linear map $g\colon N \to E$. Then $M \cap \ker g = 0$ so, as $M \leqslant_e N$, g is a monomorphism.

(c) Since F is injective the inclusion map $M \to F$ extends to an R-linear map $g\colon E \to F$. As in (b) it is easy to see that g is a monomorphism. □

Proposition 6.19. If M and N are R-modules with injective hulls E and F respectively then any isomorphism $f\colon M \to N$ extends to an isomorphism $E \to F$. In particular if $M = N$ then id_M extends to an isomorphism $E \to F$.

Proof. Since f can be viewed as a monomorphism $M \to F$ and F is injective it extends to an R-linear map $\hat{f}\colon E \to F$. Since $M \leqslant_e E$ and $\ker f = 0$, $\ker \hat{f} = 0$ and $\hat{f}$ is a monomorphism. It remains to show that it is also surjective. But $N = f(M) = \hat{f}(M) \leqslant \hat{f}(E)$. Thus $\hat{f}(E) \leqslant_e F$. However as $\hat{f}(E)$ is injective it has no proper essential extension so we're done. □

Definition 6.20. Given an R-module M we will write $E(M)$ to denote an injective hull of M. Since $E(M)$ is only unique up to (possibly non-unique) isomorphism a true assertion about $E(M)$ must be true about every choice of $E(M)$.

Examples 6.21. If M_1 and M_2 are R-modules then $E(M_1) \oplus E(M_2) \cong E(M_1 \oplus M_2)$ since $E(M_1) \oplus E(M_2)$ may be viewed as an injective hull of $M_1 \oplus M_2$. Similarly, if $M \leqslant N$ there is a monomorphism $E(M) \to E(N)$ since for any choice of $E(M)$ and $E(N)$ the inclusion $M \to E(N)$ extends to a monomorphism $E(M) \to E(N)$. If moreover $M \leqslant_e N$ then the monomorphism $E(M) \to E(N)$ is in fact an isomorphism.

Lemma 6.22. If A is a torsionfree $\mathbb{Z}$-module then $E(A) \cong \mathbb{Q} \otimes_{\mathbb{Z}} A$.

Proof. We can view $\mathbb{Q} \otimes_{\mathbb{Z}} A$ as the localisation of A at the multiplicatively closed set $S = \mathbb{Z} \backslash \{0\}$. Since A is torsionfree, the natural map $A \to A_S$ is injective. Moreover if $M \leqslant A_S$ is a nonzero $\mathbb{Z}$-submodule, then there is some nonzero element of the form a/s for $0 \neq a \in A$ and $s \in S$. Then $a = a/1 \in A \cap M \leqslant A_S$ so A_S is an essential extension of A. Finally A_S is a divisible A-module and so injective. □

There is a classical notion of the rank of a torsion-free abelian group A that corresponds to the dimension of $\mathbb{Q} \otimes_{\mathbb{Z}} A$. We'd like to extend this to more general R-modules using injective hulls.

Definition 6.23. An R-module M is *indecomposable* if it cannot be written as a direct sum $M = L \oplus N$ with L and N both nonzero.

We'd like to define the rank of an R-module in terms as the number of summands when you decompose its injective hull as a direct sum of indecomposable injective modules. This would generalise the notion of the rank of a torsion-free abelian group, the dimension of a vector space and the function on semisimple artinian modules $\bigoplus_{i \in I} M_i$ that counts the number of simple modules M_i. There are two difficulties: first an injective module may not decompose as a direct sum of indecomposable modules and second the number of factors in the sum might depend on the choice of decomposition. Of course these are already issues for defining the dimension of a vector space.

Definition 6.24. An R-module M has *finite (Goldie) rank* if $E(M)$ is a finite direct sum of indecomposable injective modules.

This leads us naturally to the following notion.

Definition 6.25. An R-module is M *uniform* if it is nonzero and the intersection of any two nonzero submodules of M is nonzero; equivalently if every nonzero submodule of M is an essential submodule of M.

It is easy to see that every nonzero submodule of a uniform module is uniform.

Lemma 6.26. A nonzero R-module M is uniform if and only if $E(M)$ is indecomposable.

Proof. Suppose M is uniform and $E(M) = L \oplus N$. Then $(L \cap M) \cap (N \cap M) \leqslant L \cap N = 0$. Since M is uniform it follows that $L \cap M = 0$ or $N \cap M = 0$. Since $M \leqslant_e E(M)$, $L = 0$ or $N = 0$.

Conversely, if M is not uniform then we can find $L, N \leqslant M$ nonzero such that $L \cap N = 0$. Now there is a monomorphism $f \colon E(N) \to E(M)$ extending the inclusion $N \to E(M)$ and $f(E(N)) \cap L = 0$ since $N \leqslant_e E(N)$. Thus $E(N)$ is (isomorphic to) a proper submodule of $E(M)$. Thus $E(N)$ is a non-trivial direct summand of $E(M)$ and $E(M)$ is not indecomposable. □

It follows that a nonzero injective module is uniform if and only if it is indecomposable.

Proposition 6.27. An R-module M has finite rank if and only if it has an essential submodule that is a finite direct sum of uniform modules.

Proof. Suppose that $\bigoplus_{i=1}^n M_i \leqslant_e M$ with each M_i uniform then $\bigoplus_{i=1}^n M_i \leqslant_e E(M)$ by transitivity. It follows that

$$E(M) \cong E\left(\bigoplus_{i=1}^n M_i\right) \cong \bigoplus_{i=1}^n E(M_i).$$

Since each $E(M_i)$ is indecomposable it follows that M has finite rank.

Conversely, if M has finite rank then $E(M) \cong \bigoplus_{i=1}^n E_i$ for some uniform injective R-modules E_i. Now $M_i := M \cap E_i \neq 0$ since $M \leqslant_e E(M)$. Moreover each M_i is uniform since each E_i is so. Now $M_i \leqslant_e E_i$ so

$$\bigoplus_{i=1}^n M_i \leqslant_e \bigoplus_{i=1}^n E_i \cong E(M).$$

So $\bigoplus_{i=1}^n M_i \leqslant_e M$. □

Exercise 6.5. Let $A = k[x,y]/(x,y)^2$ for a field k. Show that A viewed as a left A-module has finite rank but is not a direct sum of uniform submodules.

Lecture 12

In which we define the Goldie rank of a module and consider some basic properties

Lemma 6.28. If an R-module M is a direct sum of n uniform submodules then it contains no direct sum of $n+1$ nonzero submodules.[21]

Proof. If $n = 0$ or 1 the result is clear. So suppose $n > 1$ and work by induction.

We suppose for contradiction that $M = \bigoplus_{i=1}^n M_i$ with each M_i uniform and M contains a direct sum $\bigoplus_{j=1}^{n+1} N_j$ with each N_j nonzero. Let $N = \bigoplus_{j=1}^n N_j$. If $N \cap M_k = 0$ for some k then N is isomorphic to a submodule of $\bigoplus_{i=1, i\neq k}^n M_i$ via the projection M/M_k. This contradicts the induction hypothesis. Thus $N \cap M_k \neq 0$ for all k. Since the M_i are all uniform $N \cap M_i \leqslant_e M_i$ for all i and so

$$\bigoplus_{i=1}^n N \cap M_i \leqslant_e \bigoplus_{i=1}^n M_i = M.$$

It follows that $N \leqslant_e M$. But $N \cap N_{n+1} = 0$ so we have a final contradiction. □

Definition 6.29. If M is an R-module of finite rank and $E(M) \cong \bigoplus_{i=1}^n E_i$ with each E_i a uniform injective module then we call n the *(Goldie) rank* of M and write $\operatorname{rank} M$.

We have established that the rank of M does not depend on the choice of decomposition of $E(M)$.

It is easy to see that if $M_1, \ldots, M_n$ are R-modules of finite rank then

$$\operatorname{rank} \bigoplus_{i=1}^n M_i = \sum_{i=1}^n \operatorname{rank} M_i < \infty.$$

Proposition 6.30. Let M be an R-module and $n \geq 0$. The following are equivalent:

(a) $\operatorname{rank} M = n$;

---

[21] This can be compared with the statement in linear algebra that a vector space with a basis of size n contains no linearly independent subset of size $n+1$. Indeed it is a generalisation of it since if R is a field a uniform module is a 1-dimensional vector space.

(b) M has an essential submodule which is a direct sum of n uniform submodules.[22]

(c) M contains a direct sum of n nonzero submodules but no direct sum of $n+1$ nonzero submodules. [23]

Proof. Suppose (a) holds. Then $E(M) = \bigoplus_{i=1}^{n} E_i$ with E_i uniform injective modules. It follows by the last lemma that $E(M)$ contains no direct sum of $n+1$ nonzero submodules so nor does M. However each $E_i \cap M \neq 0$ since $M \leqslant_e E(M)$ and M contains $\bigoplus_{i=1}^{n} E_i \cap M$. Thus (c) holds.

Suppose (c) holds and let $N = \bigoplus_{i=1}^{n} M_i \leqslant M$. We claim $N \leqslant_e M$ and each M_i is uniform. If some M_j were not uniform we could find $L_1, L_2 \leqslant M_j$ such that $L_1 \cap L_2 = 0$. Then $\bigoplus_{\substack{i=1 \\ i \neq j}}^{n} M_i \oplus L_1 \oplus L_2 \leqslant M$ is a direct sum of $n+1$ nonzero submodules, a contradiction. Similarly if N were not an essential submodule of M we could find $L \leqslant M$ such that $N \cap L = 0$ and $N \oplus L \leqslant M$ would be a direct sum of $n+1$ nonzero submodules. Thus (b) holds.

Finally suppose (b) holds so $N = \bigoplus_{i=1}^{n} N_i \leqslant_e M$ with each N_i uniform. Then $E(M) \cong E(N) \cong \bigoplus_{i=1}^{n} E(N_i)$ and each $E(N_i)$ is uniform so M has rank n. □

Corollary 6.31. Suppose $N \leqslant M$ are R-modules.

(a) If M has finite rank then $\operatorname{rank} N \leqslant \operatorname{rank} M$.

(b) If N has finite rank $\operatorname{rank} N = \operatorname{rank} M$ if and only if $N \leqslant_e M$.

(c) If N and M/N both have finite rank then $\operatorname{rank} M \leqslant \operatorname{rank} N + \operatorname{rank} M/N$.

Proof. (a) By (a) implies (c) in the last proposition if M has finite rank, m say, it contains no direct sum of $m+1$ nonzero submodules. Therefore N also contains no such direct sum and so by (c) implies (a) in the last proposition $\operatorname{rank} N \leqslant n = \operatorname{rank} M$.

(b) By (a) implies (b) in the last proposition , if N has finite rank, n say, N contains an essential submodule that is a direct sum $\bigoplus_{i=1}^{n} N_i$ of n uniform submodules N_i.

Now if $N \leqslant_e M$ then $\bigoplus_{i=1}^{n} N_i \leqslant_e M$. Hence, by (b) implies (a) in the proposition, $\operatorname{rank} M = n = \operatorname{rank} N$.

Conversely if $\operatorname{rank} M = n$ then by (a) implies (c) in the proposition M does not contain a direct sum of $n+1$ nonzero submodules. Thus we can deduce that $N \leqslant_e M$.

(c) Let $L \leqslant M$ be maximal subject to $L \cap N = 0$. Then L is isomorphic to a submodule of M/N. Thus, by (a), $\operatorname{rank} L \leqslant \operatorname{rank} M/N$. Moreover $L \oplus N \leqslant_e M$. Thus by, (a) again,

$$\operatorname{rank} M = \operatorname{rank} N + \operatorname{rank} L \leqslant \operatorname{rank} N + \operatorname{rank} M/N.$$ □

[22]You can think of this as a generalisation of a vector space having a basis of size n.

[23]You can think of this as a generalisation of having a linearly independent subset of size n but no linearly independent subset of size $n+1$.

Corollary 6.32. If M is an R-module of finite rank then for every monomorphism $f\colon M \to M$, $f(M) \leqslant_e M$.

Proof. Since $f(M) \cong M$, $\operatorname{rank} M = \operatorname{rank} f(M)$. Thus $f(M) \leqslant_e M$ by part (b) of the last result. □

Corollary 6.33. If R has finite rank as a left R-module and $x \in R$ is not a right zerodivisor, i.e. $rx = 0$ for $r \in R$ implies $r = 0$, then $Rx \leqslant_e R$ and for all $a \in R$, $(Rx)a^{-1} = \{r \in R : ra \in Rx\} \leqslant_e R$.

Proof. The map $R \to R$; $r \mapsto rx$ is a monomorphism. The second part follows by Examples Sheet 2 Q14(c) which was also an exercise in Lecture 10. □

Theorem 6.34 (Goldie)**.** An R-module M has finite rank if and only if M does not contain an infinite direct sum of nonzero submodules.

Proof. The forward implication is an immediate consequence of previous results.

Conversely, if M is not of finite rank then $X_0 := E(M)$ is not a finite direct sum of indecomposable injective modules. Thus $X_0 = X_1 \oplus Y_1$ for some nonzero injective modules X_1 and Y_1. Moreover X_1 and Y_1 can't both be finite direct sums of indecomposable injective modules so, WLOG, X_1 is not. We can repeat this argument to construct sequences X_n and Y_n of nonzero injective R-modules such that $X_n \oplus Y_n = X_{n-1}$ and X_n is not a finite sum of indecomposable injective modules for all n.

Now $Y_n \cap (\sum_{m \geq n+1} Y_m) \leqslant Y_n \cap X_n = 0$ for all $n \geq 0$. Since $M \leqslant_e E(M)$, $M \cap Y_n \neq 0$ for each $n \geq 1$ and the sum $\sum_{n\geq 1} M \cap Y_n$ is direct. Thus M contains an infinite direct sum of nonzero submodules. □

Corollary 6.35. If M is a noetherian R-module then M has finite rank.

Proof. It now suffices to show that such an M cannot contain an infinite direct sum $\bigoplus_{n\geq 1} M_n$ of nonzero submodules. But it is did then it would contain a strictly ascending chain

$$M_1 < M_1 \oplus M_2 < M_1 \oplus M_2 \oplus M_3 < \cdots$$

contradicting the noetherian hypothesis. □

Exercise 6.6. Show that if R is a left noetherian domain then R is uniform as a left R-module.

Lecture 13

In which we classify indecomposable injective modules in a commutative noetherian ring and begin to discuss torsion

Theorem 6.36. A ring R is left noetherian if and only if every direct sum of injective (left) R-modules is injective.

Proof. First suppose that R is left noetherian and $E = \bigoplus_{j\in J} E_j$ is a direct sum of injective R-modules. Suppose $I \lhd_l R$ and $f \in \mathrm{Hom}_R(I, E)$. We must show that f extends to an element of $\mathrm{Hom}_R(R, E)$. Since R is left noetherian, I is finitely generated by $x_1, \ldots, x_n$, say. Now each $f(x_i) \in \bigoplus_{j\in J_i} \leqslant E$ for some finite $J_i \subset J$. Let $K = \bigcup_{i=1}^n J_i$ and $F = \bigoplus_{k\in K} E_k$. Then F is a finite direct sum of injective modules and so is injective and $f(I) \leqslant F$. Thus we may extend f to an element of $\mathrm{Hom}_R(R, F)$ and postcompose with the inclusion $F \to E$.

Conversely suppose that every direct sum of injective R-modules is injective and consider an ascending chain of left ideals $I_1 \leqslant I_2 \leqslant \cdots \leqslant I_n \leqslant \cdots$ and define $I = \bigcup_{j\geq 1} I_j \lhd_l R$ and

$$E = \bigoplus_{j\geq 1} E(R/I_j)$$

an injective left R-module by assumption. Consider $f\colon I \to E$ such that $f(x)_j = x + I_j \in R/I_j \leqslant E(R/I_j)$. Note that for all $x \in I$, there is some $n(x) \geq 1$ such that $x \in I_j$ for all $j \geq n(x)$ and so f does land in E. It is clear that f is R-linear so f extends to $g \in \mathrm{Hom}_R(R, E)$. Since $g(1) \in E$ there is some n such that $g(1)_n = 0$. Now for all $x \in I$, $f(x) = g(x) = xg(1)$. Thus $f(x)_n = 0$ for all $x \in I$ that is $I \subset I_n$ and the chain terminates. □

Corollary 6.37. If R is left noetherian then every injective (left) R-module is a direct sum of uniform injective R-modules.

Proof. Let E be an injective left R-module and let $\mathcal{S} = \{M_i : i \in I\}$ be a maximal family of finitely generated submodules of E such that the sum $\sum_{i\in I} M_i$ is direct.[24] We claim that $\bigoplus_{i\in I} M_i \leqslant_e E$. If not, then we could find $0 \neq N \leqslant E$ such that $\bigoplus_{i\in I} M_i \cap N = 0$. By replacing N by a nonzero finitely generated submodule we may suppose that N is finitely generated and make $\mathcal{S}$ bigger by adding N to it.

Now each M_i has an injective hull $E(M_i)$. Since $M_i \leqslant_e E(M_i)$ and the sum $\sum_{i\in I} M_i \leqslant E$ is direct it follows that the sum $\sum_{i\in I} E(M_i) \leqslant E$ is direct. Moreover $\bigoplus_{i\in I} E(M_i) \leqslant_e E$. Since $\bigoplus_{i\in I} E(M_i)$ is injective by the last result it follows that $E = \bigoplus_{i\in I} E(M_i)$. Now each M_i is noetherian and so has finite rank. Thus each $E(M_i)$ is a finite direct sum of uniform injective modules. Thus E is a direct sum of uniform injective modules. □

Lemma 6.38. Suppose that U is a uniform R-module over a left noetherian ring R. There is a unique prime ideal P of R such that P is the annihilator of a nonzero submodule of U and P contains the annihilators of all non-zero submodules of U.

Definition 6.39. We call the prime ideal described by the lemma the *assassinator of* U and write $\mathrm{ass}_R(U)$.

[24]Such a family exists by Zorn.

Proof of Lemma. Since R is left noetherian we may find $M \leqslant U$ such that $P := \mathrm{Ann}_R(M)$ is maximal amongst the annihilators of nonzero submodules of U. If $N \leqslant U$ is nonzero then $N \cap M \neq 0$ since U is uniform. Thus since $P(N \cap M) = 0$, $P = \mathrm{Ann}_R(N \cap M) \geq \mathrm{Ann}_R(N)$ by maximality of P. The result follows if we can establish that P is prime.

If $I, J \lhd R$ with $IJ \subseteq P$ then $IJM = 0$. Thus $JM = 0$ and $J \leqslant P$ or $JM \neq 0$ and $I \leqslant P$. □

Lemma 6.40. Let P be a prime ideal in a left noetherian ring R, and let $U = I/P$ be a uniform left R-submodule of R/P. Then $E(U)$ is a uniform injective R-module with assassinator P.

Proof. Since U is uniform as an R-module, $E_R(U)$ is a uniform injective module and $\mathrm{ass}_R(E(U)) = \mathrm{ass}_R(U)$. Certainly $PU = 0$ so $\mathrm{ass}_R(U)$ contains P. But if $J \lhd_l R$ with $P < J \leqslant I$ and $K \lhd R$ with $KJ/P = 0$ then $KJ \leqslant P$ so $K \leqslant P$ since P is prime. □

Proposition 6.41. Let A be a commutative noetherian ring then $P \mapsto E(A/P)$ defines a bijection between $\mathrm{Spec}\, A$ and the set of isomorphism classes of uniform injective A-modules.

Proof. Since A/P is a uniform A-module whenever $P \in \mathrm{Spec}(A)$[25] , $E(A/P)$ is uniform for all $P \in \mathrm{Spec}(A)$ and by the last lemma has assassinator P. Thus the map in the statement is a well-defined injection.

Now suppose E is any uniform injective module and let P be the assassinator of E, $P = \mathrm{Ann}_R(M)$ for $0 \neq M \leqslant E$, say. Now if $x \in M$ then $Ax \cong A/P$ and so $E(A/P) \cong E(Ax)$ is isomorphic to a submodule of E. Since E is uniform and $E(Ax)$ is injective, $E = E(Ax) = E(A/P)$ so the map in the statement is surjective. □

A strong case can be made that the correct analogue of $\mathrm{Spec}\, A$ for a noncommutative (left) noetherian ring is the collection of isomorphism classes of uniform injective modules.

7. Torsion and noncommutative localisation

Definition 7.1. A *multiplicatively closed (m.c.)* subset of a ring R is a subset S of R containing 1 and closed under multiplication in the ring.

Given a m.c. subset S of R and M a (left) R-module let

$$t_S(M) := \{m \in M : sm = 0 \text{ for some } s \in S\}$$

Definition 7.2. If S is a m.c. subset of R we say that an M-module is *S-torsion* if $t_S(M) = M$ and we say that M is *S-torsionfree* if $t_S(M) = 0$.

[25]if $a, b \notin P$ then $ab \notin P$ and $(ab) \subset (a) \cap (b)$

We recall that if R is a commutative ring and S is a m.c. subset of A then $t_S(M)$ is always the unique largest S-torsion submodule and $M/t_S(M)$ is the largest S-torsionfree quotient of M.

Example 7.1. Consider

$$R = \begin{pmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{pmatrix} \quad \text{and } S = \left\{ \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \in R : a \neq 0 \right\} \text{ a m.c. subset of } R.$$

Let M be the left R-module

$$M = \left\{ \begin{pmatrix} \lambda \\ \mu \end{pmatrix} : \lambda, \mu \in \mathbb{Z}/p\mathbb{Z} \right\}$$

for some prime p with R-action by matrix multiplication. Then

$$t_S(M) = M \backslash \left\{ \begin{pmatrix} 0 \\ \mu \end{pmatrix} : \mu \neq 0 \right\}$$

since

$$\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 0 \\ \mu \end{pmatrix} = \begin{pmatrix} 0 \\ \mu \end{pmatrix} \text{ for all } a, b \in \mathbb{Z}$$

and

$$\begin{pmatrix} p & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} 0 \\ \lambda b + \mu \end{pmatrix}$$

and for any choice of $\lambda \neq 0 \in \mathbb{Z}/p\mathbb{Z}$ and $\mu \in \mathbb{Z}/p\mathbb{Z}$ we may choose $b \in \mathbb{Z}$ such that $\lambda b + \mu = 0$. Thus $t_S(M)$ is not closed under addition in this case so is not a submodule of M.

Lecture 14

In which we introduce the Ore conditions, record basic properties of S-torsion submodules for S a left Ore set, introduce left rings of fractions for Ore sets consisting of regular elements and begin to prove that they are uniquely determined up to unique isomorphism via a univeral property.

A necessary condition for a m.c. subset S of R to have the property that for every left R-module M the set $t_S(M)$ is an R-submodule of M can easily be obtained as follows: for each $s \in S$, since $1 + Rs \in t_S(R/Rs)$, if $t_S(R/Rs)$ is a submodule of R/Rs then $t_S(R/Rs) = R/Rs$. This can be rephrased as for all $a \in R$ there is $t \in S$ such that $ta \in Rs$. This condition turns out to also be sufficient for $t_S(M)$ to always be an S-torsion submodule of M.

Definition 7.3. We say that a m.c. subset S of R satisfies the *left Ore condition* if for every $s \in S$ and $a \in R$ there exist $t \in S$ and $b \in R$ such that $ta = bs$. We call such a set a *left Ore set*. The *right Ore condition* and *right Ore sets* are defined analogously. An *Ore set* in R is a m.c. subset that is both a left Ore set and a right Ore set.

Of course in a commutative ring R every m.c. subset of R is an Ore set. More generally, any m.c. subset of $Z(R)$ is an Ore set. In our last example, S was not a left Ore set in R.

Exercise 7.2. Show that if R is a left noetherian domain then $R\backslash 0$ is a left Ore set.

Exercise 7.3. Show that $\{1, x, x^2, \ldots\}$, $\{1, y, y^2, \ldots\}$, $k[x]\backslash 0$ and $k[y]\backslash 0$ are all Ore sets in $A_1(k) = k\langle x, y\rangle/(yx - xy - 1)$.

Remark 7.4. If S is a left Ore set and $s_1, \ldots, s_n \in S$ then we can show inductively that there exist $a_1, \ldots, a_n \in R$ such that

$$a_1 s_1 = a_2 s_2 = \cdots = a_n s_n \in S.$$

Lemma 7.4. Suppose that S is a left Ore set in R. Then for any (left) R-module M, $t_S(M)$ is an R-submodule of M.

Proof. Suppose $m_1, m_2 \in t_S(M)$. Then there are $s_1, s_2 \in S$ such that $s_1 m_1 = s_2 m = 0$. By the remark we can find $a_1, a_2 \in R$ such that $s = a_1 s_1 = a_2 s_2 \in S$. Then

$$s(m_1 + m_2) = a_1 s_1 m_1 + a_2 s_2 m_2 = 0.$$

Thus $t_S(M)$ is closed under $+$. Moreover given any $a \in R$ we can find $t \in S$ and $b \in R$ such that $ta = bs_1$. Then $tam_1 = bs_1 m_1 = 0$. □

Definition 7.5. If S is a left Ore set in R and M is a left R-module. The submodule $t_S(M)$ is called the *S-torsion submodule* of M.

Exercise 7.5. Suppose S is a left Ore set in a ring R and M is a left R-module.

(a) $t_S(M)$ is an S-torsion module and $M/t_S(M)$ is S-torsionfree.
(b) If N is a left R-module and $f \in \mathrm{Hom}_R(M, N)$ then $f(t_S(M)) \leqslant t_S(N)$.
(c) If $N \leqslant M$, then M is S-torsion if and only if both N and M/N are S-torsion.
(d) If $N_i \leqslant M$ for $i \in I$ and each N_i is S-torsion then $\sum_{i\in I} N_i$ is S-torsion.
(e) All submodules and products of S-torsionfree modules are S-torsionfree.
(f) If $N \leqslant_e M$ and N is S-torsionfree then M is S-torsionfree.
(g) If $N \leqslant M$ with N and M/N both S-torsionfree then M is S-torsionfee.

Definition 7.6. We call $a \in R$ a *regular element* if a is not a zero-divisor i.e. if $b \in R$ with $ab = 0$ or $ba = 0$ then $b = 0$.

Let R be a ring and S a m.c. subset of R consisting of regular elements. Recall that if R is commutative then there is a localisation R_S of R at S such that every element of R_S can be written as r/s with $r \in R$ and $s \in S$.

Definition 7.7. A ring T equipped with an injective ring homomorphism

$$\phi\colon R \to T$$

is a *left ring of fractions of R with respect to S* if

(a) $\phi(S) \leqslant T^\times$ and
(b) every element of T can be written as $\phi(s)^{-1}\phi(a)$ for some $a \in R$ and $s \in S$.

There is an obvious parallel notion of right ring of fractions of R with respect to S.

Lemma 7.8. Suppose that $\phi\colon R \to T$ makes T a left ring of fractions with respect to S, a m.c. subset consisting of regular elements.

(a) S is a left Ore set.
(b) For $s, t \in S$ and $a, b \in R$, $\phi(s)^{-1}\phi(a) = \phi(t)^{-1}\phi(b) \in T$ if and only if there are $c, d \in R$ such that $ca = db$ and $cs = dt \in S$.
(c) Given any $t_1, \dots, t_n \in T$ there are $a_1, \dots, a_n \in R$ and $s \in S$ such that $t_i = \phi(s)^{-1}\phi(a_i)$ for each $i = 1, \dots, n$.

Proof. (a) Suppose that $s \in S$ and $a \in R$ then, by condition (a) for a left ring of fractions, $\phi(s) \in T^\times$ so $\phi(a)\phi(s)^{-1} \in T$. Thus by condition (b) there is $b \in R$ and $t \in S$ such that $\phi(a)\phi(s)^{-1} = \phi(t)^{-1}\phi(b)$. This in turn implies $\phi(ta) = \phi(bs)$. Thus, since ϕ is injective, we have proven the left Ore condition.

(b) Now if $c, d \in R$ satisfy the given conditions then, as $\phi(cs) = \phi(dt) \in T^\times$,

$$\phi(s)^{-1}\phi(a) = \phi(cs)^{-1}\phi(ca) = \phi(dt)^{-1}\phi(db) = \phi(t)^{-1}\phi(b)$$

Conversely if $\phi(s)^{-1}\phi(a) = \phi(t)^{-1}\phi(b)$ then by the left Ore condition there are $c, d \in R$ such that $cs = dt \in S$. Then

$$\phi(ca) = \phi(cs)\phi(s)^{-1}\phi(a) = \phi(dt)\phi(t)^{-1}\phi(b) = \phi(db).$$

(c) We can find $b_1, \dots, b_n \in R$ and $s_1, \dots, s_n \in S$ such that $t_i = \phi(s_i)^{-1}\phi(b_i)$ for each $i = 1, \dots n$. The left Ore condition guarantees that there are $c_1, \dots, c_n \in R$ such that $s = c_1 s_1 = c_2 s_2 = \cdots = c_n s_n \in S$. It follows that $\phi(s)t_i = \phi(c_i b_i)$ and so $t_i = \phi(s)^{-1}\phi(c_i b_i)$ for each $i = 1, \dots, n$. □

Proposition 7.9 (Universal Property for left localisation)**.** Let R be a ring and $S \subset R$ a left Ore set consisting of regular elements and let $\phi\colon R \to T$ make T a left ring of fractions of R with respect to S. Then for every ring homomorphism $\theta\colon R \to U$ such that $\theta(S) \leqslant U^\times$ there is a unique ring homomorphism $\psi\colon T \to U$ such that $\psi\phi = \theta$.

Proof. It $\psi\colon T \to U$ exists it must be unique: necessarily

$$\psi(\phi(s)^{-1}\phi(a)) = \theta(s)^{-1}\theta(a) \text{ for all } a \in R, s \in S$$

so we must show this formula gives a well-defined ring homomorphism.

First suppose that $\phi(s)^{-1}\phi(a) = \phi(t)^{-1}\phi(b)$. We saw earlier that there are $c, d \in R$ such that $ca = db$ and $cs = dt \in S$. Thus as $\theta(dt) = \theta(cs) \in T^\times$,

$$\theta(s)^{-1}\theta(a) = \theta(cs)^{-1}\theta(ca) = \theta(dt)^{-1}\theta(db) = \theta(t)^{-1}\theta(b)$$

Thus ψ is well-defined. Moreover since $\phi(1) = 1$, $\psi\phi(a) = \theta(a)$. In particular $\psi(1) = 1$.

Next suppose that $t_1, t_2 \in T$. We've seen that there are $a_1, a_2 \in R$ and $s \in S$ such that $t_i = \phi(s)^{-1}\phi(a_i)$ for $i = 1, 2$.

Then $t_1 + t_2 = \phi(s)^{-1}\phi(a_1 + a_2)$ and

$$\psi(t_1 + t_2) = \theta(s)^{-1}\theta(a_1 + a_2) = \theta(s)^{-1}\theta(a_1) + \theta(s)^{-1}\theta(a_2) = \psi(t_1) + \psi(t_2)$$ [26]

Finally there are $s' \in S$ and $b \in R$ such that $\phi(a_1)\phi(s)^{-1} = \phi(s')^{-1}\phi(b)$ then $t_1t_2 = \phi(s)^{-1}\phi(s')^{-1}\phi(b)\phi(a_2)$ and

$$\psi(t_1t_2) = \theta(s)^{-1}\theta(s')^{-1}\theta(b)\theta(a_2) = \theta(s)^{-1}\theta(a_1)\theta(s)^{-1}\theta(a_2) = \psi(t_1)\psi(t_2)$$

so ψ is a ring homomorphism. □

Lecture 15

In which we construct left localisations with respect to left Ore sets consisting of regular elements and begin to consider localising at the set of all regular elements

Corollary 7.10. Suppose that $S \subset R$ is a left Ore set consisting of regular elements and $\phi_1 \colon R \to T_1$ and $\phi_2 \colon R \to T_2$ make T_1 and T_2 into left rings of fractions for R with respect to S then there a unique isomorphism $\psi \colon T_1 \to T_2$ such that $\psi\phi_1 = \phi_2$.

Proof. This is a standard universal property argument. □

We've now seen that if a left ring of fractions of R with respect to S exists then it is unique up to unique isomorphism and S must be a left Ore set. In fact the left Ore condition on a m.c. subset of regular elements suffices for a left ring of fractions to exist. We will now discuss how to construct one.

One strategy to do this is to mimic the argument from the commutative case:

(1) Consider the relation $\sim$ on $S \times R$ given by $(s, a) \sim (t, b)$ if and only if there are $c, d \in R$ such that $ca = db$ and $cs = dt \in S$ and check that this in an equivalence relation. Then T as a set is $S \times R/\sim$.

(2) Given $[(s, a)], [(t, b)] \in T$ the left Ore condition provides $c, d \in R$ such that $cs = dt \in S$ so check addition given by

$$[(s, a)] + [(t, b)] = [(cs, ca + db)]$$

is well-defined and makes $(T, +)$ into an abelian group.

(3) Given $[(s, a)], [(t, b)] \in T$ the left Ore condition gives $c \in R$ and $u \in S$ such that $ua = ct$ so check multiplication defined by

$$[(s, a)] \cdot [(t, b)] = [(su, cb)]$$

is well-defined and makes $(T, +, \cdot)$ into a ring with unit $[(1, 1)]$.

---

[26] In reality Lecture 14 ended at this point for which apologies!

(4) Check $R \to T$; $r \mapsto [(1,r)]$ is an injective ring homomorphism making T a left ring of fractions of R with respect to S.

This works without serious difficulty but there are a lot of tedious checks to make here so we will take a different approach.

The idea is to note that if T exists then it can be viewed as a left R-module via ϕ and there is a ring isomorphism $T \to \mathrm{End}_R(T)^{\mathrm{op}}$ by right multiplication[27]. Moreover one can see that $\phi(R) \leqslant_e T$ as left R-modules so there is a monomorphism of left R-modules $T \to E(R)$. Additionally it is relatively easy to see that this induces an isomorphism $T/\phi(R) \to t_S(E(R)/R)$. Thus we try to identify T as a ring with $\mathrm{End}_R(X)$ where $X/R = t_S(E(R)/R)$.

Proposition 7.11 (Asano)**.** Let R be a ring and $S \subset R$ a m.c. subset consisting of regular elements then R has a left ring of fractions with respect to S if and only if S is a left Ore set.

Proof. We've already proven the forwards implication.

Suppose that S is a left Ore set and let $E = E(R)$, the injective hull of R as a left R-module, and let $X = \{x \in E : sx \in R \text{ for some } s \in S\}$. Note that $R \leqslant X$ and $X/R = t_S(E/R)$. Thus X/R is an S-torsion left R-module by the left Ore condition. Moreover $E/X \cong (E/R)/(X/R)$ is S-torsionfree. Since S consists of regular elements, $t_S(R) = 0$ so, as $R \leqslant_e E$, $t_S(E) = 0$. So E and X are also S-torsionfree.

Let $T = \mathrm{End}_R(X)^{\mathrm{op}}$. We aim to show that T is a left ring of fractions of R with respect to S. First we try to identify $\phi\colon R \to T$.

For each $r \in R$, $a \mapsto ar$ defines an element of $\mathrm{End}_R(R)$. Since E is injective this extends to an element of $f \in \mathrm{End}_R(E)$. Moreover given $x \in X$, there is $s \in S$ such that $sx \in R$ and so $sf(x) = f(sx) \in f(R) \leqslant R$. Thus $f(x) \in X$ and f restricts to an element ϕ_r of $T = \mathrm{End}_R(X)$ such that $\phi_r(a) = ar$ for all $a \in R$. Moreover if ϕ is any other element of T such that $\phi(a) = ar$ for all $a \in R$ then $\phi_r - \phi \in T$ and $R \leqslant \ker(\phi_r - \phi)$. It follows that $\phi - \phi_r$ induces an element of $\mathrm{Hom}_R(X/R, X)$. Since X/R is S-torsion and X is S-torsionfree we can deduce $\phi - \phi_r = 0$.

Thus $r \mapsto \phi_r$ defines a function $\phi\colon R \to T$ completely characterised by the formula $\phi_r(a) = ar$ for all $a \in R$. Since for $r, r, a' \in R$

$$(\phi_r + \phi_{r'})(a) = ar + ar' \text{ and } \phi_r(\phi_{r'}(a)) = ar'r = \phi_{r'r}(a), \quad \phi_1(a) = \mathrm{id}_X(a)$$

this function is a ring homomorphism. If $\phi_r = 0$ then $0 = \phi_r(1) = r$. Thus ϕ is injective.

It remains to show that $\phi_s \in T^\times$ for all $s \in S$ and every element of T is of the form $\phi_s^{-1}\phi_r$ for some $r \in R$ and $s \in S$.

[27]If $\alpha \in \mathrm{End}_R(T)$ then for $s \in S$ and $r \in R$, $s \cdot \alpha(\phi(s)^{-1}\phi(r)) = \alpha(\phi(r)) = r \cdot \alpha(1)$ so as $T \to T; t \mapsto s \cdot t$ is a bijection α is determined by $\alpha(1)$

To prove the former we fix $s \in S$. Since s is regular $\ker \phi_s \cap R = 0$ thus $\ker \phi_s = 0$ since $R \leqslant_e X$.

Now we claim that for all $t \in S$, $t\colon X \to X; x \mapsto tx$ is surjective. To see this we note that $Rt \cong R$ as left R-modules since t is regular and so given $x \in X$ there is $f \in \mathrm{Hom}_R(Rt, X)$ such that $f(t) = x$. By injectivity of E this extends to $g \in \mathrm{Hom}_R(R, E)$. Then $tg(1) = g(t) = f(t) = x$. Since E/X is S-torsionfree and $x \in X$ it follows that $g(1) \in X$ and the claim is proved.

Now since X/R and R/Rs are both S-torsion, X/Rs is S-torsion, that is, for any $x \in X$ there is $t \in S$ and $b \in R$ such that $tx = bs = \phi_s(b)$. By the claim, there is $y \in X$ such that $ty = b$, and then $t\phi_s(y) = \phi_s(b) = tx$. Since X is S-torsionfree it follows that $\phi_s(y) = x$ i.e. $\phi_s \in T$ is surjective. We have thus proved that ϕ_s is an isomorphism and so invertible in T.

Now suppose that ϕ is an arbitrary element of T. Since $\phi(1) \in X$, and X/R is S-torsion there is $s \in S$ and $r \in R$ such that $s\phi(1) = r$. Thus for $a \in R$, $\phi(\phi_s(a)) = \phi(as) = as\phi(1) = ar$. That is $\phi(\phi_s(a)) = \phi_r(a)$ for all $a \in R$. Since $T = \mathrm{End}_R(X)^{\mathrm{op}}$ it follows that $\phi = \phi_s^{-1}\phi_r \in T$. □

Definition 7.12. If R is a ring and $S \subset R$ is a left Ore set consisting of regular elements we'll write $S^{-1}R$ to denote a left ring of fractions of R with respect to S. Similarly if S is a right Ore set consisting of regular elements we'll write RS^{-1} to denote a right ring of fractions of R with respect to S. We will routinely identify R with its image in $S^{-1}R$ (resp RS^{-1}).

Proposition 7.13. If $S \subset R$ is an Ore set consisting of regular elements then $S^{-1}R = RS^{-1}$.

Proof. This also follows immediately from the universal property and its right version. □

Exercise 7.6. Show that if R is a left noetherian ring and S is a left Ore set then $S^{-1}R$ is a left noetherian ring.