18.706: Noncommutative Algebra

Nir Elber

Spring 2026

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
Introduction

1.1 February 3

This lecture was given by Pavel Etingof, but the course will be taught by Roman Bezrukavnikov. Today, we will review some ring theory. Almost everything will be the same as in usual (commutative) ring theory, so we will be fast.

1.1.1 Basic Ring and Module Theory

This course is about non-commutative rings.

Definition 1.1. A *ring* R is an abelian group $(R, +)$ equipped with a multiplication $\cdot\colon R \times R \to R$ which is associative, unital, and distributive.

Warning 1.2. A ring in this course is not required to be commutative.

Example 1.3. Given a ring R, there is an opposite ring R^{op}, which is the same underlying additive group but has the opposite multiplicative structure: for any $a^{\mathrm{op}}, b^{\mathrm{op}} \in R^{\mathrm{op}}$, we define

$$a^{\mathrm{op}} \cdot b^{\mathrm{op}} := (ba)^{\mathrm{op}}.$$

Example 1.4. For any ring R, there is a ring $M_n(R)$ of the $n \times n$ matrices with entries in R. The addition and multiplication of matrices is as usual.

Here is are some special kinds of ring.

Definition 1.5 (skew field)**.** A *skew field* is a ring R in which every nonzero element admits a multiplicative inverse.

Remark 1.6. If R is a skew field, then the set $R^\times$ of nonzero elements in R is a group under multiplication.

Rings are understood through the abelian category of modules they produce.

Definition 1.7 (module)**.** Fix a ring R. A *left R-module* is an abelian group M equipped with a bilinear action map $R \times M \to M$ which is

(a) associative: $(ab)m = a(bm)$ for any $a, b \in R$ and $m \in M$, and

(b) unital: $1m = m$ for all $m \in M$.

There is an analogous notion of a *right R-module*.

Remark 1.8. The ring R is both a left and right R-module, where the action is given by the multiplication structure.

Warning 1.9. By convention a "module" is a left module.

Remark 1.10. A left R-module has equivalent data to a right R^{op}-module. The point is that we need to reverse the elements of R appearing in the associativity check.

It will occasionally be useful to have both left and right actions.

Definition 1.11 (bimodule)**.** Fix rings R and S. Then an (R, S)*-bimodule* is an abelian group M with commuting left R-module and right S-module structures. In other words, M is both a left and right R-module, and for any $a \in R$ and $b \in S$ and $m \in M$, we have

$$a(mb) = (am)b.$$

If $R = S$, then we may refer to an (R, S)-bimodule as an R-bimodule.

Example 1.12. The ring R is an R-bimodule.

As usual, one can define relative notions.

Definition 1.13 (submodule)**.** Fix a module M over a ring R. Then a *left R-submodule* N of M is an abelian subgroup which is invariant under the R-action. There are analogous notions of right R-submodules.

Definition 1.14 (quotient)**.** Fix a submodule N of a module M over a ring R. Then we can give the quotient abelian group M/N the structure of a *quotient module* via the R-action

$$r(m + N) \coloneqq rm + N.$$

We will not bother to check that these are in fact well-defined modules.

Definition 1.15 (ideal)**.** Fix a ring R. Then a *left ideal* is a left R-submodule of R. *Right ideals* and *two-sided ideals* are defined analogously.

Example 1.16. If I is a left ideal, then R/I is a left R-module.

Remark 1.17. If I is a two-sided ideal, then R/I is a ring.

Having defined our objects, we may note that there are morphisms.

Definition 1.18 (homomorphism)**.** Fix rings R and S. Then a *homomorphism* $\varphi\colon R \to S$ of rings is a group homomorphism which preserves the multiplication and the unit. An *isomorphism* is an invertible homomorphism.

Definition 1.19 (homomorphism)**.** Fix R-modules M and N. Then a *homomorphism* $\varphi\colon M \to N$ of modules is a group homomorphism which preserves the R-module structures. An *isomorphism* is an invertible homomorphism. An *endomorphism* is a homomorphism from a module to itself. There are analogous notions for right R-modules and bimodules.

Example 1.20. For any module M of a ring R, the set of endomorphisms is denoted $\operatorname{End}_R M$. It is a ring, where the multiplication structure is given by composition. As usual, we will not check this.

Example 1.21. Consider a ring R as a left module over itself. Then the ring $\operatorname{End}_R R$ is isomorphic to R^{op}. Indeed, the isomorphism $R^{\mathrm{op}} \to \operatorname{End}_R R$ is given by sending r to the endomorphism $x \mapsto xr$. The inverse map sends an endomorphism φ to $\varphi(1)$.

One can, as usual, define kernels, images, and cokernels.

Definition 1.22 (direct sum)**.** Fix a ring R. Given a family $\{M_i\}_{i\in I}$ of modules, we define the *direct sum*

$$\bigoplus_{i\in I} M_i$$

to consist of finitely supported sequences from each M_i.

As usual, we will not bother to check that this is an R-module.

1.1.2 Invariant Basis Number

Bases only exist for free modules, which we should now define.

Definition 1.23 (free, rank)**.** Fix a ring R. A *free R-module* is one isomorphic to the R-module $\bigoplus_{i\in I} R$, where I is some set. The *rank* of M, denoted $\operatorname{rank} M$, is the cardinality $|I|$.

Of course, we do not know if the rank is well-defined!

Definition 1.24 (IBN)**.** Fix a ring R. Then R satisfies the *IBN* property (i.e., the *invariant basis property*) if and only if, for any sets I and J, if R^I and R^J are isomorphic, then I and J have the same cardinality.

Remark 1.25. The infinite case turns out to not be very relevant: if I or J is infinite, then one can show directly that $R^I \cong R^J$ implies that $|I| \cong |J|$.

Example 1.26. If R is a commutative field, then linear algebra shows that R satisfies IBN. The same argument works for any skew fields R.

Non-Example 1.27. The ring (0) does not have IBN because $(0) = (0) \oplus (0)$.

Non-Example 1.28. Let V be the direct sum vector space $\mathbb{C}^{\oplus\mathbb{N}}$. For each $i \in \mathbb{N}$, there is a basis vector e_i which is 1 at the ith coordinate and zero elsewhere. Now, consider the ring $R \coloneqq \operatorname{End}_{\mathbb{C}} V$; such an endomorphism φ can be written as a matrix A defined by

$$\varphi(e_i) = \sum_{j\in\mathbb{N}} A_{ji} e_j.$$

Note that A has only finitely many nonzero entries in each column because A_{ji} can only be nonzero for finitely many j! Then R does not have IBN: set $V_+ \coloneqq \mathbb{C}^{2\mathbb{N}}$ and $V_- \coloneqq \mathbb{C}^{1+2\mathbb{N}}$ so that $V = V_+ \oplus V_-$, but there are isomorphisms $V \cong V_+ \cong V_-$ of vector spaces. Thus, there are isomorphisms

$$\operatorname{End}_{\mathbb{C}} V = \operatorname{Hom}_{\mathbb{C}}(V_+ \oplus V_-, V) = \operatorname{Hom}_{\mathbb{C}}(V_+, V) \oplus \operatorname{Hom}_{\mathbb{C}}(V_-, V) \cong \operatorname{End}_{\mathbb{C}} V \oplus \operatorname{End}_{\mathbb{C}} V$$

of left R-modules.

Remark 1.29. There are also examples of rings without IBN which admit no zero divisors, but this is harder.

Let's check that some rings satisfy IBN.

Proposition 1.30. Fix a homomorphism $\varphi\colon R \to S$ of rings. If S has IBN, then R has IBN.

Proof. Suppose that we have an isomorphism $\psi\colon R^{\oplus I} \to R^{\oplus J}$ for two sets I and J; let ψ^{-1} be its inverse. We want to show that $|I| = |J|$.

The idea is to pass the isomorphism ψ (and its inverse) to S. Let $\{e_i\}_{i\in I}$ be a basis of $R^{\oplus I}$, and similarly let $\{f_j\}_{j\in J}$ be a basis of $R^{\oplus J}$. Then there are matrix coefficients $\{r_{ij}\}_{ij}$ and $\{s_{ij}\}_{ij}$ for which

$$\psi(e_i) = \sum_{j\in J} r_{ji} f_j \qquad \text{and} \qquad \psi^{-1}(f_j) = \sum_{i\in I} s_{ij} e_i.$$

We can now define $\widetilde{\psi}\colon S^{\oplus I} \to S^{\oplus J}$ and $\widetilde{\psi}^{-1}\colon S^{\oplus J} \to S^{\oplus I}$ by using the same equations. Then $\psi \circ \psi^{-1}$ and $\psi^{-1} \circ \psi$ are the identities, which is just some equalities occurring on the matrix coefficients. Thus, we conclude that $\widetilde{\psi}$ and $\widetilde{\psi}^{-1}$ are inverse isomorphisms, so the IBN property for S implies that $|I| = |J|$. ∎

Remark 1.31. Intuitively, we are basically extending scalars functorially from R to S.

Example 1.32. We show that any commutative ring has IBN. Indeed, any commutative ring R admits a maximal ideal $\mathfrak{m}$ for which $R/\mathfrak{m}$ is a field. Now, $R/\mathfrak{m}$ has IBN by Example 1.26, so we are done by Proposition 1.30.

Here is a different sort of example.

Lemma 1.33. Fix a ring R. If R has IBN, then $M_n(R)$ has IBN.

Proof. Suppose that one has an isomorphism $S^{\oplus I} \cong S^{\oplus J}$ for some sets I and J. As an R-module, $S^{\oplus I}$ is free of rank $n^2 \cdot |I|$, and similar holds for $S^{\oplus J}$. Because R has IBN, we conclude that the cardinalities $n^2 \cdot |I|$ and $n^2 \cdot |J|$ are equal, so $|I| = |J|$ follows.[1] ∎

[1] If I and J are finite, then the last equality follows by counting. If I and J are infinite, then instead we note that $n^2\,|I| = |I|$, which is not hard to show using Cantor–Schröder–Bernstein theorem.

Example 1.34. By Example 1.26, any skew field D has IBN. Thus, Lemma 1.33 implies that $M_n(D)$ also has IBN.

Remark 1.35. Here is an amusing application. By Non-Example 1.28, $\operatorname{End}_{\mathbb{C}} V$ does not have IBN, where $V := \mathbb{C}^{\oplus \mathbb{N}}$. But $M_n(D)$ has IBN for any skew field D by Example 1.34. Thus, by Proposition 1.30, there are no homomorphisms $\operatorname{End}_{\mathbb{C}} V \to M_n(D)$!

1.1.3 Recognizing Skew Fields

For our next big result, we note that it is sometimes possible to classify module categories easily.

Example 1.36. Fix a skew field D. The usual arguments in linear algebra show that every D-module is free.

In fact, this property of modules recognizes skew fields!

Theorem 1.37. Fix a ring R. If every R-module is free, then R is a skew field.

To prove Theorem 1.37, we need Schur's lemma.

Definition 1.38 (irreducible)**.** Fix a ring R. Then an R-module M is *irreducible* or *simple* if and only if it is nonzero and admits no nonzero proper submodules.

Lemma 1.39 (Schur)**.** Fix irreducible modules M and N for a ring R.

(a) Any homomorphism $\varphi\colon M \to N$ is either zero or an isomorphism.

(b) The ring $\operatorname{End}_R M$ is a skew field.

Proof. Note that (b) follows from (a) by taking $M = N$. To show (a), it is enough to check that φ is a bijection if nonzero. Well, it is enough to check that φ is injective and surjective.

- For injectivity, note $\ker \varphi \subseteq M$ is a proper submodule because φ is nonzero, so $\ker \varphi = 0$ because M is irreducible.
- For surjectivity, $\operatorname{im} \varphi \subseteq N$ is a nonzero submodule because φ is nonzero, so $\operatorname{im} \varphi = N$ because N is irreducible. ∎

We will also need some constructions.

Lemma 1.40. Fix a nonzero ring R.

(a) Then R admits a simple module.

(b) Every proper left ideal is contained in a maximal left ideal.

(c) For any module M, a proper submodule $N \subseteq M$ is maximal if and only if the quotient M/N is simple.

Proof. We show each part separately.

(a) This follows from (b) and (c): the R-module R admits a maximal submodule I by (b), so R/I is a simple R-module by (c).

(b) This is an application of Zorn's lemma. For example, to show (b), we can show more generally that, for any finitely generated R-module M, any proper R-submodule $N \subseteq M$ is contained in a maximal ideal. Indeed, let $\mathcal{F}$ be the family of proper submodules of M containing N. Then $\mathcal{F}$ is partially ordered by inclusion, and it is nonempty because it contains N. To show that $\mathcal{F}$ admits a maximal element, we need to show that any ascending chain $\{N_\alpha\}_{\alpha\in\Lambda}$ admits an upper bound. Well, consider

$$N' \coloneqq \bigcup_{\alpha\in\Lambda} N_\alpha.$$

Certainly N' contains N and upper-bounds the chain, so it merely remains to check that N' is proper. For this, recall that M is finitely generated, so we may select a finite set of generators $S \subseteq M$. It is enough to check that $S \not\subseteq N'$, which we show by contradiction: if $S \subseteq N'$, then each element of S lives in some N_α, so by taking maximums, there is β large enough so that $S \subseteq N_\beta$, from which $M = N_\beta$ follows, which is a contradiction.

Thus, Zorn's lemma provides us with some maximal element N' of $\mathcal{F}$. We can see that N' is maximal among submodules in $\mathcal{F}$, but it is then not hard to see that in fact N' is a maximal submodule.

(c) On one hand, if M/N is simple, then any submodule E sitting between N and M descends to a submodule $E/N \subseteq M/N$. Thus, $E/N = 0$ (and so $E = N$) or $E/N = M/N$ (and so $E = M$). Conversely, if $N \subseteq M$ is maximal, then any submodule $E \subseteq M/N$ lifts to an R-submodule of M containing N. Thus, $E = N/N$ and so is zero, or $E = M/N$ and so is everything. ■

Remark 1.41. It is worthwhile to remember that we have shown that any finitely generated R-module admits a maximal submodule and hence a simple quotient.

Non-Example 1.42. It is not in general true that infinitely generated modules have simple quotients. Indeed, the $\mathbb{Z}$-module $\mathbb{Q}$ has no simple quotient. Indeed, the simple $\mathbb{Z}$-modules arise from the maximal ideals of $\mathbb{Z}$ and are thus the fields $\mathbb{F}_p$ where p is prime. But there is no homomorphism $\mathbb{Q} \to \mathbb{F}_p$ of groups for any prime p because $\mathbb{Q}$ is divisible!

We are finally ready for our proof.

Proof of Theorem 1.37. Fix a simple R-module L, which exists by Lemma 1.40. Note that L cannot have an R-submodule isomorphic to R^2 because then L would contain a smaller submodule isomorphic to R. However, L is known to be free, so its rank must be 1, so we conclude that $L \cong R$.

Thus, R is simple as an R-module, so it follows that $\operatorname{End}_R R$ is a skew field by Lemma 1.39. Hence, R^{op} is a skew field by Example 1.21, so R is a skew field as well. ■

1.2 February 5

We continue.

1.2.1 Semisimple Modules

Last class, we were talking about semisimple modules.

Definition 1.43 (semisimple)**.** Fix a ring R. Then a *semisimple module* M is a module which is isomorphic to a direct sum of simple modules.

This is a fairly rigid definition. For example, does the collection of semisimple modules form an abelian category? To add some flexibility, we want the following tool.

Proposition 1.44. Fix a ring R and a semisimple module $M = \bigoplus_{i\in I} M_i$. For any R-submodule $N \subseteq M$, there is a subset $J \subseteq I$ so that

$$M = N \oplus \bigoplus_{j\in J} M_j.$$

Proof. For brevity, we define $M_J \coloneqq \bigoplus_{j\in J} M_j$ for each subset $J \subseteq I$. The idea is to use Zorn's lemma to construct J. We have two steps.

1. We use Zorn's lemma. Let $\mathcal{F}$ to be the collection of J for which $M_J \cap N = \varnothing$, which we order by inclusion. We now use Zorn's lemma to find a maximal element of $\mathcal{F}$, which we note is nonempty (it has $\varnothing$) and partially ordered by inclusion. It remains to show that $\mathcal{F}$ has upper bounds for all it chains. Well, choose a chain $\{J_\alpha\}_{\alpha\in\Lambda}$, and we consider the set

$$J' \coloneqq \bigcup_{\alpha\in\Lambda} J_\alpha.$$

   Certainly J' is an upper bound for the chain, provided that we check that in fact $M_J \cap N = \varnothing$. We want to show that any $n \in M_J \cap N$ has $n = 0$. Then note that $n \in M$ is only nonzero in finitely many coordinates, so we merely have to find $\alpha \in \Lambda$ large enough so that J_α includes all these coordinates; then $n \in M_{J_\alpha} \cap N$, so $n = 0$.

   Thus, Zorn's lemma provides us with a maximal element J of $\mathcal{F}$.

2. We complete the proof. Note $M_J \cap N = 0$ by construction, so it remains to check that $M_J + N = M$. It is enough to check that each copy of M_i lives in $M_J + N$. If $i \in J$, there is nothing to do. Otherwise, $i \notin J$, so the maximality of J implies that $M_{J\cup\{i\}} \cap N$ is nonempty. Thus, we can find some $n \in M_{J\cup\{i\}} \cap N$, and we see that it must have nonzero component in M_i. By adding in an element from M_J, we see that $n + M_J$ includes an element m_i whose only nonzero component is in M_i. But M_i is simple, so $Rm_i = M_i$, so $M_i \subseteq N + M_J$. ∎

Corollary 1.45. Submodules, quotients, and sums of semisimple modules are semisimple.

Proof. Quickly, sums of semisimple modules are just quotients of direct sums, so we only have left to handle submodules and quotients. Note that Let $M = \bigoplus_{i\in I} M_i$ be a semisimple module, and let $N \subseteq M$ be a submodule. Then there is a subset $J \subseteq I$ with

$$M = N \oplus \bigoplus_{j\in J} M_j.$$

Thus, the quotient $M/N \cong \bigoplus_{j\in J} M_j$ is semisimple. Further, the canonical map $\bigoplus_{i\notin J} M_i \to N$ is an isomorphism because this is a direct sum decomposition, so the submodule N is semisimple. ∎

Example 1.46. Fix a skew field D, and consider the ring $R \coloneqq M_n(R)$. Then we note that the left module D^n (with the natural action by R) because any nonzero vector in D^n generates D^n. Now, R is isomorphic to n copies of D^n as a left module, so it follows that R is semisimple over itself.

1.2.2 The Socle

Not all of our modules will be semisimple, but it will be useful to be able to measure how far a module is from being semisimple.

Definition 1.47 (socle)**.** Fix a module M over a ring R. Then the *socle*, denoted $\operatorname{soc} M$, is the sum of all semisimple submodules of M.

Example 1.48. Fix the ring $R \coloneqq \mathbb{C}[t]$, and consider the R-module $M \coloneqq R$. Then R is a principal ideal domain, so all nonzero R-submodules of M are isomorphic to R, which is not simple because R is not a field. It follows that $\operatorname{soc} M = 0$.

Example 1.49. Fix the ring $R \coloneqq \mathbb{C}[t]/(t^n)$ for some $n \geq 1$, and consider the R-module $M \coloneqq R$. By the classification of finitely generated modules over the principal ideal domain $\mathbb{C}[t]$, we see that the R-modules all take the form $R/(t^\bullet)$. Thus, we see that M admits a unique simple submodule $\mathbb{C}t^{n-1}/t^n$.

Example 1.50. Fix a finite p-group G, and let k be a field of characteristic p. Then

$$\operatorname{soc} k[G] = k \cdot \sum_{g \in G} g.$$

Proof. Then main claim is that every simple $k[G]$-module (i.e., every irreducible representation of G over k) is one-dimensional. This means that a simple submodule of $k[G]$ amounts to the image of a $k[G]$-linear map $k \to k[G]$. But a k-linear map $k \to k[G]$ simply picks out a vector $\sum_g a_g g$, and to be G-equivariant, all the coefficients must be the same, so we conclude that the only such map $k \to k[G]$ has image contained in $k \cdot \sum_{g \in G} g$.

It remains to prove the claim. For this, it is enough to show that any nontrivial representation V of G over k admits a nonzero fixed vector. Quickly, we note that we can reduce to $k = \mathbb{F}_p$ by choosing a nonzero vector v_0 and passing from V to the finite subspace $V_0 \coloneqq \mathbb{F}_p[G]v_0$. But the class equation implies that

$$\#V_0^G \equiv \#V_0 \pmod{p},$$

so V_0^G is some $\mathbb{F}_p$-subspace with positive dimension. Thus, $\mathbb{F}_p[G]v_0$ admits a nonzero vector fixed by G, and we are done. ∎

Note that the decomposition of a semisimple module into simple components need not be canonical. It is possible to salvage this slightly.

Definition 1.51. Fix a simple module L over a ring R. For a module M, the L-isotypic component M_L is the sum of the images of all maps $L \to M$.

Remark 1.52. By Lemma 1.39, any map $L \to M$ either vanishes or has image isomorphic to L. Thus, we see that we are basically collecting all copies of L in M.

Example 1.53. Suppose that $M = \bigoplus_{i \in I} M_i$ is semisimple, where M_i is simple for each i. Then L can only map to some M_i if $M_i \cong L$ by Lemma 1.39, so it follows that

$$M_L \cong \bigoplus_{\substack{i \in I \\ M_i \cong L}} L.$$

Thus, when M is semisimple, we see that M is the sum of its isotypic components M_L, where L varies isomorphism classes of simple modules.

As an application of the socle, we provide another characterization of semisimple modules.

Proposition 1.54. Fix a module M over a ring R. Then M is semisimple if and only if any short exact sequence of the form

$$0 \to M' \to M \to M'' \to 0$$

splits.

Remark 1.55. Recall that a splitting is the data of a map $M'' \to M$ such that the composite $M \to M'' \to M$ is the identity. This is equivalent to the data of a map $M \to M'$ such that the composite $M' \to M \to M'$ is the identity.

Proof. If M is semisimple, we use Proposition 1.44: we may identify M' with its image in M, and then Proposition 1.44 has realized the quotient $M'' = M/M'$ as a direct summand of M. The splitting follows.

The other direction is harder. Suppose that every short exact sequence with M in the middle splits. Well, $\operatorname{soc} M$ embeds into M, so the quotient $N \coloneqq M/\operatorname{soc} M$ must also embed into M. Thus, N admits no simple submodules, or else we would violate the maximality of $\operatorname{soc} M$. We would like to show that $N = 0$.

Quickly, we claim that any submodule $Q \subseteq N$ is a direct summand. It is enough to show that the short exact sequence

$$0 \to Q \to N \to N/Q \to N \to 0$$

splits. Well, consider the short exact sequence

$$0 \to \operatorname{soc} M \oplus Q \to M \to N/Q \to 0.$$

This short exact sequence splits, so we receive a splitting map $N/Q \to M$, which then projects back down to a splitting map $N/Q \to N$ of the projection $N \to N/Q$.

Now, suppose for the sake of contradiction that we have found a nonzero element $a \in N$. By Remark 1.41, Ra admits a simple quotient L. The previous paragraph tells us that Ra is in fact a direct summand of N, so there is a projection $N \twoheadrightarrow L$. Letting Q be the kernel, the previous paragraph tells us that the short exact sequence

$$0 \to Q \to N \to L \to 0$$

splits, so L is a direct summand of N as well. This is our contradiction! ∎

1.2.3 Semisimple Rings

We are now ready to define semisimple rings.

Definition 1.56. Fix a ring R. Then R is *semisimple* if and only if R is semisimple as a module over itself.

Example 1.57. Given skew fields $\{D_i\}_{i=1}^m$ and integers $\{n_i\}_{i=1}^m$, we see that $M_{n_i}(D_i)$ is semisimple by Example 1.46. We can see that a finite product of semisimple rings will be semisimple (because then each of the summand rings is a semisimple module, and the sum of semisimple modules is semisimple by Corollary 1.45), so the ring

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

is semisimple.

Here are some nicer conditions.

Theorem 1.58. Fix a ring R. Then the following are equivalent.

(a) Every R-module M is semisimple.

(b) The ring R is semisimple.

(c) The ring R is isomorphic to a finite product of matrix algebras over skew fields.

Proof. Note that (a) implies (b) with no content. To show that (b) implies (a), it is enough by Corollary 1.45 to show that any module is a quotient of a free one, which is not difficult: for any module M, we see that there is a quotient map

$$\bigoplus_{m \in M} R \to M$$

given by sending the mth copy of R to the map $R \to M$ given by $1 \mapsto m$.

We already know that (c) implies (b) by Example 1.57, so it remains to show that (b) implies (c). Well, by definition, we may write R as a direct sum of simple modules $\bigoplus_{i \in I} M_i$. We begin by claiming that I is finite: there is some finite subset $J \subseteq I$ for which

$$1 = \sum_{i \in J} m_i,$$

where $m_i \in M_i$. But then the R-submodule generated by 1 is exactly R, so it follows that R is the submodule $\bigoplus_{i \in J} M_i$, so $I = J$.

We now pass to isomorphism classes. Enumerate the simple modules appearing in the decomposition of R by $\{L_1, \dots, L_m\}$, so we have a decomposition

$$R = \prod_{j=1}^{m} L_j^{\oplus n_j}$$

for some multiplicities n_j. It follows by Lemma 1.39 that R^{op} is the ring

$$\operatorname{End}_R R = \prod_{j=1}^{m} M_{n_j}(D_j),$$

where $D_j = \operatorname{End}_R(L_j)$. (Namely, each L_j in R can only map to other copies of L_j in R.) Each D_j is a skew field by Lemma 1.39, so we are done upon noting that $M_{n_j}(D_j)^{\text{op}}$ is isomorphic to $M_{n_j}(D_j^{\text{op}})$ by taking the transpose. ∎

Example 1.59. Let's use these ideas to classify the simple modules of $R \coloneqq \prod_{j=1}^{m} M_{n_j}(D_j)$. Any simple module L is generated by a single nonzero element, so it is a quotient of R. Because R admits a sum decomposition, it follows that L is a quotient of one of the $M_{n_j}(D_j)$s, so L is a simple module of $M_{n_j}(D_j)$. It thus remains to classify the simple modules of a ring of the form $M_n(D)$. Well, $M_n(D)$ is semisimple over itself by Example 1.46, so L is in fact a direct summand of $M_n(D)$. But Example 1.46 has shown that $M_n(D)$ is isomorphic to the R-module $(D^n)^n$, so $L \cong D^n$ follows.

Here is an application.

Theorem 1.60 (Maschke)**.** Fix a finite group G, and let k be a field of characteristic p where $\#G \not\equiv 0 \pmod{p}$. Then the ring $k[G]$ is semisimple.

Proof. By Theorem 1.58, it is enough to show that every module is semisimple, so it is enough by Proposition 1.54 to show that every short exact sequence

$$0 \to N \to M \to L \to 0$$

splits. It is enough to show that the map $\mathrm{Hom}_G(L,L) \to \mathrm{Hom}_G(M,L)$ is surjective, for then we could induce a splitting by looking for the image of id_L. But $\mathrm{Hom}_k(L,L) \to \mathrm{Hom}_k(M,L)$ is surjective, so it is enough to check that it induces a surjection on G-invariants.

In general, given any surjection $V \to W$ of $k[G]$-modules, we will show that there is an induced surjection $V^G \to W^G$ on invariants; this will complete the proof. Well, for any $w \in w^G$, find some $v \in V$ in its pre-image. Then we define

$$v_G \coloneqq \frac{1}{\#G} \sum_{g \in G} gv.$$

Then $v_G \in V^G$ by construction, and its image in W is simply w, so we are done. ■

Remark 1.61. The condition on the characteristic is necessary: see Example 1.50.

1.2.4 Simple Rings

With a notion of "semisimple," we should have a notion of "simple."

Definition 1.62 (simple)**.** Fix a ring R. Then R is *simple* if and only if it is nonzero, and the only two-sided ideals are 0 and R.

Remark 1.63. Equivalently, we can say that R is simple as an R-bimodule.

Example 1.64. If D is a skew field, then D is simple because the only D-submodules of D are zero and D.

Example 1.65. If R is simple, then we claim that $M_n(R)$ is also simple. Indeed, choose some nonzero sub-bimodule $M \subseteq M_n(R)$, and we want to show that $M = M_n(R)$. Well, let E_{ij} denote the usual elementary matrix which is zero everywhere except for a 1 in row i and column j. We know that M contains a nonzero matrix, say A, so there is a nonzero entry A_{ij}. By hitting A with $E_{i1}E_{j1}$, we see that we can move the nonzero entry to A_{11}. Now, the collection of $r \in R$ generated by A_{11} over R is a nonzero submodule of R, so it follows that M contains all matrices of the form rE_{11} and in particular E_{11}. Multiplying by other elementary matrices, we see that $E_{ij} \in M$ for each i and j, so $M = M_n(R)$ follows by taking linear combinations.

Non-Example 1.66. Set $V \coloneqq \mathbb{C}^{\oplus \mathbb{N}}$. Then the ring $R \coloneqq \mathrm{End}\, V$ is not simple: it admits a two-sided ideal I given by those operators with finite-dimensional image. Indeed, composing any operator with one in I stays in I.

Example 1.67. Consider the Weyl algebra A generated over $\mathbb{C}$ by the symbols x and ∂ with the relation $\partial x = 1 + x\partial$. Using this commutativity, we see that we can write any element of A uniquely in the form

$$\sum_{i=1}^{n} p_i(x)\partial^i,$$

where $p_i(x)$ is some polynomial in x. One can check that this ring A is simple.

Remark 1.68. A simple ring does not have to be semisimple. For example, the Weyl algebra A is not semisimple. Indeed, it turns out that the short exact sequence

$$0 \to \mathbb{C}[x] \to \mathbb{C}\left[x, x^{-1}\right] \to \frac{\mathbb{C}\left[x, x^{-1}\right]}{\mathbb{C}[x]} \to 0$$

of A-modules is not split.

With a size condition, we can fix the previous remark.

Definition 1.69 (Noetherian)**.** A ring R is *left Noetherian* if and only if every ascending chain of left ideals stabilizes. One can similarly define a notion of *right Noetherian*.

Remark 1.70. By Zorn's lemma, it is equivalent to say that any collection of left ideals admits a maximal element.

Remark 1.71. The corresponding notion of "two-sided Noetherian" is not very useful: for example, it immediately includes all simple rings.

Remark 1.72. There are rings which are left Noetherian but not right Noetherian. Most examples are pathological.

Definition 1.73 (Artinian)**.** A ring R is *left Artinian* if and only if every descending chain of left ideals stabilizes. Again, there is an analogous notion of *right Artinian*.

Remarks 1.70 and 1.71 apply.

Remark 1.74. We will show later that Artinian implies Noetherian.

We can classify Artinian simple rings.

Theorem 1.75 (Wedderburn)**.** Fix a ring R. Then the following are equivalent.

(a) The ring R is simple and left Artinian or right Artinian.

(b) Every R-module is semisimple, and R admits a unique simple module (up to isomorphism).

(c) The ring R is isomorphic to $M_n(D)$ for some skew field D and $n \geq 1$.

Proof. We show our implications in sequence.

- We show (c) implies (b): Example 1.46 shows that $M_n(D)$ is semisimple, and its only simple module is D^n by Example 1.59.
- We show (b) implies (c): by Theorem 1.58, we see that R takes the form $\prod_{j=1}^{m} M_{n_j}(D_j)$. But Example 1.59 shows that each factor produces a new simple module, so $m = 1$ follows.
- We show (c) implies (a): we know $M_n(D)$ is simple by example 1.65. Further, R is finite-dimensional over D, so any descending chain of ideals is a descending chain of finite-dimensional subspaces, so it must stabilize.

- We show (a) implies (c); we work in the left Artinian case. Let $L \subseteq R$ be a minimal left ideal. Then every element of L generates L, so L is simple. Now, LR is a two-sided ideal, and it is nonzero because L is nonzero, so $LR = R$ because R is simple. Thus, $R = \sum_{r \in R} Lr$, so R is a sum of some copies of L. It follows that R is semisimple by Corollary 1.45. Thus, R is a direct sum of Ls, and this sum must be finite because R is Artinian. The argument of Theorem 1.58 thus shows that R^{op} is isomorphic to $M_n(\operatorname{End} L)$, from which (c) follows by Lemma 1.39. ■

BIBLIOGRAPHY

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

List of Definitions