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 $a^{\text{op}}, b^{\text{op}} \in R^{\text{op}}$, we define

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

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

$$r(m + N) := rm + N.$$

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.

Example 1.25. 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 1.26. The ring (0) does not have IBN because $(0) = (0) \oplus (0)$.

Non-Example 1.27. 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 $R := \operatorname{End}_{\mathbb{C}} V$; 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 $V_+ := \mathbb{C}^{2\mathbb{N}}$ and $V_- := \mathbb{C}^{1+2\mathbb{N}}$ 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 1.28. 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 1.29. 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 1.30. Intuitively, we are basically extending scalars functorially from R to S.

Example 1.31. 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 1.25, so we are done by Proposition 1.29.

Here is a different sort of example.

Lemma 1.32. 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 1.33. By Example 1.25, any skew field D has IBN. Thus, Lemma 1.32 implies that $M_n(D)$ also has IBN.

Remark 1.34. Here is an amusing application. By Non-Example 1.27, $\operatorname{End}_{\mathbb{C}} V$ does not have IBN, where $V := \mathbb{C}^{\oplus\mathbb{N}}$. But $M_n(D)$ has IBN for any skew field D by Example 1.33. Thus, by Proposition 1.29, 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 1.35. 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 1.36. Fix a ring R. If every R-module is free, then R is a skew field.

To prove Theorem 1.36, we need Schur's lemma.

Definition 1.37 (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 1.38 (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 1.39. 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

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

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 1.40. 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 1.41. 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 1.36. Fix a simple R-module L, which exists by Lemma 1.39. 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 1.38. Hence, R^{op} is a skew field by Example 1.21, so R is a skew field as well. ■

1.1.4 Semisimple Modules

We close our class by saying something about semisimple modules.

Definition 1.42 (semisimple)**.** Fix a ring R. Then a *semisimple module* M is a module which is isomorphic to a direct sum of simple modules.

Lemma 1.43. 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 $M_J := \bigoplus_{j\in J} M_j$ 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 $M_i \subseteq N + M_J$. ■

BIBLIOGRAPHY

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

List of Definitions