Noncommutative algebra

Luka Horjak (luka1.horjak@gmail.com)

October 17, 2023

Contents

Introduction

These are my lecture notes on the course Noncommutative algebra in the year 2023/24. The lecturer that year was prof. dr. Igor Klep.

The notes are not perfect. I did not write down most of the examples that help with understanding the course material. I also did not formally prove every theorem and may have labeled some as trivial or only wrote down the main ideas.

I have most likely made some mistakes when writing these notes – feel free to correct them.

1   Finite-dimensional algebras, Wedderburn's structure theory

1.1   Free algebras

Definition 1.1.1. Let $R = K \langle x, y \rangle$ be a free algebra and $F = \{xy - yx - 1\}$. The quotient

$$\mathcal{A}_1(K) = R \Big/ (F)$$

is called the *first Weyl algebra*.

Remark 1.1.1.1. The first Weyl algebra is generated by elements $\overline{x}$ and $\overline{y}$ that satisfy $\overline{x} \cdot \overline{y} - \overline{y} \cdot \overline{x} - 1$.

Remark 1.1.1.2. The first Weyl algebra is the algebra of differential operators – for $D, L \colon K[y] \to K[y]$, defined as $D(p) = \frac{\partial p}{\partial y}$ and $L(p) = yp$, we have $DL - LD = I$.

Definition 1.1.2. Let R be a ring and $\sigma \in \operatorname{End}(R)$. The *skew polynomial ring* is the set

$$R[x, \sigma] = \left\{ \sum_{i=0}^{n} b_i x^i \ \middle| \ n \in \mathbb{N} \wedge b_i \in R \right\}$$

in which for all $b \in R$ the equality in $xb = \sigma(b)x$ holds.

Definition 1.1.3. Let R be a ring and σ a derivation[1] on R. The *skew polynomial ring* is the set

$$R[x, \sigma] = \left\{ \sum_{i=0}^{n} b_i x^i \ \middle| \ n \in \mathbb{N} \wedge b_i \in R \right\}$$

in which for all $b \in R$ the equality in $xb = bx + \sigma(b)$ holds.

---

[1] $\sigma(a + b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = a\sigma(b) + \sigma(a)b$.

1.2   Chain conditions

Definition 1.2.1. Let C be a set and $\{C_i \mid i \in I\}$ a set of subsets of C. The set $\{C_i \mid i \in I\}$ satisfies the *ascending chain condition* if there does not exist an infinite strictly increasing chain

$$C_{i_1} \subset C_{i_2} \subset C_{i_3} \subset \dots$$

The *descending chain condition* is defined analogously.

Definition 1.2.2. Let R be a ring and M an R-module.

i) M is *noetherian* if the set of submodules of M satisfies the ascending chain condition.

ii) M is *artinian* if the set of submodules of M satisfies the descending chain condition.

Proposition 1.2.3. The following statements are true:

i) A module M is noetherian if and only if each submodule of M is finitely generated.

ii) Let $N \leq M$ be a submodule. Then M is noetherian if and only if both N and M/N are noetherian.

iii) Let $N \leq M$ be a submodule. Then M is artinian if and only if both N and M/N are artinian.

Proof.

i) Suppose that each submodule of M is finitely generated and $M_1 \leq M_2 \leq \dots \leq M$. Define the submodule

$$N = \bigcup_{j \in \mathbb{N}} M_j.$$

By assumption, N is finitely generated. But then there exists some $j \in \mathbb{N}$ such that M_j contains all generators of N, so $M_j = N$. Therefore, the chain cannot be strictly increasing.

Now assume that M is noetherian and let $N \leq M$ be a submodule. Define

$$\mathcal{C} = \{S \leq N \mid S \text{ is finitely generated}\}.$$

This set must have some maximal element $N_0 \leq N$. Suppose $N_0 < N$ and consider some element $b \in N \backslash N_0$. The module $N + Rb$ is also finitely generated and contained in N, which is a contradiction as N_0 was maximal. Therefore we must have $N = N_0$ and N is finitely generated.

ii) Suppose that M is noetherian. Consider the following short exact sequence:

$$0 \longrightarrow N \xrightarrow{\ f\ } M \xrightarrow{\ g\ } M/N \longrightarrow 0.$$

It is easy to see that N is also noetherian, as the inclusion of a chain in N is also a chain in M. As preimages of submodules are also submodules, the same conclusion follows for M/N.

Now suppose that both N and M/N are noetherian and consider a chain $M_1 \leq M_2 \leq \dots \leq M$ of submodules. As $f^{-1}(M_i)$ and $g(M_i)$ form increasing chains in

their respective modules, it follows that there exists some $n \in \mathbb{N}$ such that both $f^{-1}(M_i)$ and $g(M_i)$ are constant for all $i \geq n$. Now consider the following diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & f^{-1}(M_n) & \overset{f}{\longrightarrow} & M_n & \overset{g}{\longrightarrow} & g(M_n) & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & f^{-1}(M_i) & \overset{f}{\longrightarrow} & M_i & \overset{g}{\longrightarrow} & g(M_i) & \longrightarrow & 0.
\end{array}
$$

By the short five lemma, i is an isomorphism, so $M_n = M_i$.

iii) Same as ii). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Definition 1.2.4. A ring R is *left-noetherian* if it is noetherian as a left R-module. We analogously define *right-noetherian*, *left-artinian* and *right-artinian* rings.

A ring R is *noetherian*, if it is both left-noetherian and right-noetherian. We similarly define *artinian* rings.

Remark 1.2.4.1. A ling R is left-noetherian if and only if each left ideal of R is finitely generated.

Proposition 1.2.5. If R is a notherian ring and M is a finitely generated R-module, M is noetherian.

Proof. As M is finitely generated, there exists an endomorphism $\varphi\colon R^n \to M$ for some $n \in \mathbb{N}$. Consider the short exact sequence

$$
0 \longrightarrow R \longrightarrow R^n \longrightarrow R^{n-1} \longrightarrow 0.
$$

By induction on n, R^n is noetherian. As M is a quotient of R^n, M is also noetherian. $\quad\square$

1.3   Simple modules

Definition 1.3.1. A nontrivial R-module M is *simple* if it has no proper nontrivial submodules. An R-module M is *cyclic* with generator $m \in M$ if $M = R \cdot m$.

Proposition 1.3.2. For R-modules M, the following are equivalent:

i) The module M is simple.

ii) The module M is cyclic and its every non-zero element is a generator.

iii) We have $M \cong R/_I$ for some maximal left ideal $I \triangleleft R$.

Proof. Suppose that M is simple. Then for every $m \in M \setminus \{0\}$, $Rm \leq M$ is a nontrivial submodule. It follows that m is a generator.

Suppose now that every non-zero element is a generator. Define the homomorphism $\phi \colon R \to M$ with $\phi(r) = rm$. Set $I = \ker \phi = \operatorname{ann}(m)$. By the isomorphism theorem, we have $Rm = M \cong R/_I$. There is bijective correspondence between ideals $I \triangleleft J \triangleleft R$ and submodules of M. As any element of a proper submodule cannot generate M, I must be maximal.

Suppose now that $M \cong R/_I$ for some maximal $I \triangleleft R$ and suppose that $M' \leq M$ is a submodule. It follows that M' corresponds to a left ideal J such that $I \triangleleft J \triangleleft R$. Thus, $J = I$ or $J = R$, or equivalently, $M' = M$ or $M' = (0)$.   □

Corollary 1.3.2.1. Let D be a division ring and V be an n-dimensional vector space over D. Let $R = \operatorname{End}_D(V)$. Then, V is a simple R-module.

Proof. For every $v \in V \setminus \{0\}$ we have $Rv = V$.   □

Theorem 1.3.3 (Schur's lemma)**.** Let M and N be simple R-modules and $f \colon M \to N$ a homomorphism. Then f is either and isomorphism or the zero map. In particular, $\operatorname{End}_R(M)$ is a division ring.

Proof. Note that $\ker f \leq M$ and $\operatorname{im} f \leq N$. The conclusion follows.   □

Proposition 1.3.4. Let D be a division ring and V a D-module. Then, $D \cong \operatorname{End}_R(V)$, where $R = \operatorname{End}_D(V)$.

Proof. Define a homomorphism $\Psi \colon D \to \operatorname{End}_R(V)$ as $\Psi(d) = (f \mapsto df)$. It is clear that Ψ is injective. Now let $T \in \operatorname{End}_R(V)$ be an arbitrary endomorphism. Choose a $v \in V \setminus \{0\}$. For any $w \in V$ there exists an endomorphism of V that sends w to v, therefore, $V = R \cdot v$. Every R-endomorphism is therefore determined by its image on v. To prove that Ψ is surjective, it is hence enough to show that $Tv = d \cdot v$ for some $d \in D$.

Let $p \in R$ be a projection onto Dv. It is easy to check that

$$Tv = T(p(v)) = p(T(v)) \in Dv. \qquad\qquad □$$

Lemma 1.3.5. A finite dimensional division algebra D over an algebraically closed field k is k itself.

Proof. Note that, for $\alpha \in D$, $k(\alpha)\big/k$ is a finite field extension, but as k is algebraically closed, $k(\alpha) = k$. $\qquad\square$

1.4   Semisimple modules

Definition 1.4.1. A module is *semisimple* if it is a direct sum of simple modules.

Proposition 1.4.2. If an R-module M is a sum of simple submodules M_i for $i \in I$, then M is semisimple. Moreover, there exists a subset $I' \subseteq I$ such that

$$M = \bigoplus_{i \in I'} M_i.$$

Proof. Set

$$\mathcal{I} = \left\{ J \subseteq I \;\middle|\; (M_j)_{j \in J} \text{ is independent} \right\}.$$

As $\mathcal{I}$ is a non-empty set and every chain in M has an upper bound, we can apply Zorn's lemma. Let I' be a maximal element of $\mathcal{I}$. Note that

$$M' = \bigoplus_{i \in I'} M_i \le M.$$

If $M' \cap M_i = \{0\}$ for some $i \in I$, the set I' is not maximal as we can take $I' \cup \{i\}$. Therefore, $M' \cap M_i = M_i$ for all i as M_i are simple modules. It follows that $M' = M$. $\square$

Corollary 1.4.2.1. If M is semisimple, then so is every submodule and quotient of M. Furthermore, every submodule of M is a direct summand.

Proof. Let

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

be a direct sum of simple modules and $M' \le M$. The module M/M' is then generated by the images $\overline{M}_i$ of M_i under the quotient map. If $\overline{M}_i \ne \{0\}$, we have $\overline{M}_i \cong M_i$ since M_i is simple. Therefore, M/M' is a sum of modules M_i, and as such semisimple. As we can write

$$M = \left(\bigoplus_{i \in I'} M_i \right) \oplus M',$$

we can write

$$M' = \bigoplus_{i \in I \setminus I'} M_i.$$ $\square$

Proposition 1.4.3. Let M be a module such that every submodule of M is a direct summand.[2] Then M is semisimple.

Proof. Let $M' \le M$ be a non-zero cyclic submodule, say $M' = Rm$ for $m \ne 0$. Suppose M' is not simple. By Zorn's lemma, there exists a maximal submodule $M'' \le M'$ with $m \notin M''$. The module M'/M'' is therefore simple. As M' also has the complement property, we can write $M' = M'' \oplus S$ for some $S \le M'$. Since $S \cong M'/M''$, it is a simple submodule. In both cases, we have found a simple submodule of M.

Let M_1 be the sum of all simple submodules of M. Then there exists a submodule $M_2 \le M$, such that $M = M_1 \oplus M_2$. If $M_2 \ne \{0\}$, by the same argument as above, M_2 has a simple module. This is of course not possible. $\square$

---

[2] We call this the *complement property*.

1.5   Endomorphism ring of a semisimple module

Proposition 1.5.1. Let M be an R-module, $S = \operatorname{End}_R(M)$ and $p, m, n \in \mathbb{N}$. There is a canonical isomorphism of abelian groups

$$\operatorname{Hom}_R(M^n, M^m) \cong S^{m \times n},$$

such that the composition

$$\operatorname{Hom}_R(M^n, M^m) \times \operatorname{Hom}_R(M^p, M^n) \to \operatorname{Hom}_R(M^p, M^m)$$

corresponds to matrix multiplication. In particular, $\operatorname{End}_R(M^n) \cong S^{n \times n} = M_n(S)$ is an isomorphism of rings.

Proof. The isomorphism is given by the map $f \mapsto [\pi_i \circ f \circ \iota_j]_{i,j}$. $\qquad\qquad\square$

Remark 1.5.1.1. For $r \in R$ the map $T_r \colon R \to R$ given by $T_r(x) = xr$ is R-linear. We can therefore define a homomorphism $\Phi \colon R \to \operatorname{End}_R(R)$ by $\Phi(r) = T_r$. As Φ is injective and $f = T_{f(1)}$, we have $\operatorname{End}_R(R) \cong R^{\mathsf{op}}$.

Corollary 1.5.1.2. For a division ring D, we have $\operatorname{End}_D(D^n) = M_n(D^{\mathsf{op}})$.

Definition 1.5.2. A semisimple module has *finite length* if it is a finite direct sum of simple modules.

Proposition 1.5.3. If M is a semisimple R-module of finite length, then $\operatorname{End}_R(M)$ is isomorphic to a finite product of matrix rings over division rings.

Proof. Let

$$M \cong \bigoplus_{i=1}^{k} M_i^{n_i}$$

for distinct simple modules M_i. By Schur's lemma, we can write

$$\operatorname{End}_R(M) = \operatorname{End}_R\left(\bigoplus_{i=1}^{k} M_i\right) = \prod_{i=1}^{k} \operatorname{End}_R\left(M_i^{n_i}\right) = \prod_{i=1}^{k} M_{n_i}\left(\operatorname{End}_R(M_i)\right). \qquad\square$$

1.6   Semisimple rings

Definition 1.6.1. A ring R is *semisimple* if it is a semisimple left R-module.

Theorem 1.6.2. Let R be a ring. The following statements are equivalent:

i) The ring R is semisimple.

ii) Every R-module is semisimple.

iii) Every short exact sequence of R-modules split.

Proof. Suppose that R is semisimple. As all R-modules are quotients of a free module R^I, which is semisimple, all R-modules are semisimple.

Suppose that every R-module is semisimple. As those have the complement property, every short exact sequence splits.

Suppose that every short exact sequence splits and let $I \leq R$ be a submodule over R. As

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

is a short exact sequence, it splits, so I is a direct summand of R. It follows that R has the complement property, therefore, it is semisimple. $\qquad\square$

Corollary 1.6.2.1. Suppose that R is a semisimple ring. Then R as an R-module has finite length and any simple R-module is isomorphic to a simple component of R.

Proof. We can write

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

for simple R-modules M_i. By considering $1 \in R$, we see that I is a finite set.

Let M be a simple R-module. As we have $M = R \cdot m$, there exist maps $M_i \to M$. As $R \to M$ is surjective, at least one of those maps is non-zero and therefore an isomorphism by Schur's lemma. $\qquad\square$

Proposition 1.6.3. Let D be a division ring and V be an n-dimensional vector space over D. Then $R = \mathrm{End}_D(V)$ is semisimple.

Proof. The map $f \mapsto (f(e_1), f(e_2), \ldots, f(e_n))$ is an isomorphism of R-modules R and V^n. As V is simple by corollary 1.3.2.1, R is semisimple. $\qquad\square$

1.7   Wedderburn structure theorem

Theorem 1.7.1 (Wedderburn)**.** Every semisimple ring R is isomorphic to a finite product of matrix rings over division rings. If R is also commutative, it is a finite direct products of fields.

Proof. By proposition 1.5.3, we can write

$$R^{\mathsf{op}} \cong \operatorname{End}_R(R) \cong \prod_{i=1}^{k} M_{n_i}(D_i).$$

It follows that

$$R \cong \left(\prod_{i=1}^{k} M_{n_i}(D_i)\right)^{\mathsf{op}} = \prod_{i=1}^{k} M_{n_i}\left(D_i^{\mathsf{op}}\right). \qquad \square$$

Index