Noncommutative algebra

Luka Horjak (luka1.horjak@gmail.com)

October 28, 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 $\sigma \in \mathrm{End}(R)$. 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 $xb = \sigma(b)x$ 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 $xb = bx + \sigma(b)$ 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:

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

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

iii) Same as ii). □

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 ring 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. □

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 $I \lhd R$.

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 $I \lhd J \lhd R$ 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 $I \lhd R$ and suppose that $M' \leq M$ is a submodule. It follows that M' corresponds to a left ideal J such that $I \lhd J \lhd R$. 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

$$Tv = T(p(v)) = p(T(v)) \in Dv.$$ □

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, $k(\alpha) = k$. □

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

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

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 $M' = M$. □

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 $M' \leq M$. The module M/M' is then generated by the images $\overline{M}_i$ of M_i under the quotient map. If $\overline{M}_i \neq \{0\}$, 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

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

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 $M' \leq M$ be a non-zero cyclic submodule, say $M' = Rm$ for $m \neq 0$. Suppose M' is not simple. By Zorn's lemma, there exists a maximal submodule $M'' \leq M'$ 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 $S \leq M'$. 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 $M_2 \leq M$, such that $M = M_1 \oplus M_2$. If $M_2 \neq \{0\}$, by the same argument as above, M_2 has a simple module. This is of course not possible. □

[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, $S = \mathrm{End}_R(M)$ and $p, m, n \in \mathbb{N}$. There is a canonical isomorphism of abelian groups

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

such that the composition

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

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

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

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 $\Phi \colon R \to \mathrm{End}_R(R)$ by $\Phi(r) = T_r$. As Φ is injective and $f = T_{f(1)}$, we have $\mathrm{End}_R(R) \cong R^{\mathsf{op}}$.

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

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 $\mathrm{End}_R(M)$ 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

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

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. □

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. □

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. □

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

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

It follows that

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

Definition 1.7.2. A ring is *simple* if it has no nontrivial proper two-sided ideals.

Remark 1.7.2.1. Simple rings are not necessarily semisimple.

Remark 1.7.2.2. Every semisimple ring R is isomorphic to a finite product of simple rings.

Proposition 1.7.3 (Uniqueness of the decomposition)**.** Suppose that

$$R = \prod_{i=1}^{n} R_i = \prod_{i=1}^{m} R_i'$$

for simple rings R_i and R_i'. Then, $n = m$ and R_i' are a permutation of R_i.

Proof. As $R_i \triangleleft R$, we have $R_i R = R_i$. It follows that

$$R_i = \prod_{j=1}^{m} R_i R_j'.$$

As $R_i R_j' \triangleleft R_i$ is a nontrivial ideal, we must have $R_i R_j' = R_i$. Likewise, it follows that $R_i R_j' = R_j'$. $\square$

1.8 Jacobson radical

Definition 1.8.1. The *Jacobson radical* of a ring R is the set

$$\operatorname{rad} R = \bigcap \{I \lhd R \mid I \text{ is maximal in } R\}.$$

Lemma 1.8.2. For all $y \in R$ the following statements are equivalent:

i) We have $y \in \operatorname{rad} R$.

ii) For all $x \in R$ the element $(1 - xy)$ is left invertible.

iii) For all simple R-modules M we have $yM = (0)$.

Proof. Suppose that $y \in \operatorname{rad} R$. If there exists some $x \in R$ such that $(1 - xy)$ is not left invertible. Therefore, the set $R(1 - xy)$ is a proper ideal of R. By Zorn's lemma, there exists some maximal ideal $M \lhd R$ such that $R(1 - xy) \leq M$. In particular, we have $(1 - xy) \leq M$. As $y \in M$, we have $1 \in M$, which is of course not possible.

Suppose that $(1 - xy)$ is left invertible for all $x \in R$. If we have $ym \neq 0$ for an element $m \in M$ of a simple R-module, we get $R(ym) = M$. Therefore, there exists some $x \in R$ such that $xym = m$, or, equivalently, $(1 - xy) \cdot m = 0$. This is again a contradiction.

Suppose now that y annihilates all simple R-modules and let $M \lhd R$ be any maximal ideal. As R/M is a simple R-module, we get $y \cdot R/M = (0)$, therefore, $y \in M$. □

Definition 1.8.3. The *annihilator* of an R-module M is the set

$$\operatorname{ann}(M) = \{y \in R \mid y \cdot M = (0)\}.$$

Remark 1.8.3.1. We have $\operatorname{ann} M \lhd R$.

Corollary 1.8.3.2. We have

$$\operatorname{rad} R = \bigcap \{\operatorname{ann} M \mid M \text{ is a simple } R\text{-module}\}.$$

In particular, $\operatorname{rad} R \lhd R$.

Lemma 1.8.4. An element $y \in R$ is an element of the Jacobson radical if and only if $1 - xyz$ is invertible for all $x, z \in R$.

Proof. If $1 - xy \cdot 1$ is invertible, we have $y \in \operatorname{rad} R$.

Suppose now that $y \in \operatorname{rad} R$ and fix $x, z \in R$. As $yz \in \operatorname{rad} R$, the element $1 - xyz$ is left invertible with inverse $u \in R$. But as $xyz \in \operatorname{rad} R$, we also have that the element $1 + u \cdot (xyz) = u$ is left invertible. □

Proposition 1.8.5. The following statements are true:

i) The set $\operatorname{rad} R$ is the largest (left) ideal J satisfying $1 + J \subseteq R^{-1}$.

ii) The left radical is the same as the right radical.

iii) Suppose that $I \lhd R$ is an ideal with $I \subseteq \operatorname{rad} R$. Then

$$\operatorname{rad}\left(R/I\right) = \operatorname{rad} R/I.$$

Proof. Maximal left ideals in R/I correspond with maximal left ideals in R which contain I. □

Definition 1.8.6. A ring R is *J-semisimple* if $\operatorname{rad} R = (0)$.

Remark 1.8.6.1. For each ring R, the quotient $R/\operatorname{rad} R$ is J-semisimple.

Proposition 1.8.7. The following statements are true:

i) R and $R/\operatorname{rad} R$ have the same simple left modules.

ii) An element $x \in R$ is (left) invertible if and only if $x + \operatorname{rad} R$ is (left) invertible in $R/\operatorname{rad} R$.

Proof.

i) Follows from lemma 1.8.2.

ii) If x is invertible, then so is $x + \operatorname{rad} R$. Suppose now that for some $y \in R$ we have $(y + \operatorname{rad} R)(x + \operatorname{rad} R) = 1 + \operatorname{rad} R$. As $1 - yx \in \operatorname{rad} R$, we have that yx is invertible, so x has a left inverse. □

Definition 1.8.8. A one-sided or two-sided ideal $I \subseteq R$ is

i) *nil* if all its elements are nilpotent,

ii) *nilpotent* if $I^n = (0)$ for some $n \in \mathbb{N}$.

Lemma 1.8.9. If a left ideal $I \subseteq R$ is nil, then $I \subseteq \operatorname{rad} R$.

Proof. Fix an element $y \in I$. For all $x \in R$, the element $xy \in I$ is nilpotent, say $(xy)^n = 0$. As

$$(1 - xy) \cdot \sum_{k=0}^{n-1} (xy)^k = 1,$$

the element $1 - xy$ is invertible. Therefore, $y \in \operatorname{rad} R$. □

Theorem 1.8.10. Suppose that R is a left-artinian ring. Then $\operatorname{rad} R$ is the largest nilpotent left ideal.[3]

Proof. As every nilpotent ideal is contained in the radical, it suffices to show that $\operatorname{rad} R$ is nilpotent.

Consider the decreasing chain

$$R \supseteq \operatorname{rad} R \supseteq (\operatorname{rad} R)^2 \supseteq \dots$$

As R is artinian, this chain is eventually constant – call that ideal I. Assume that $I \neq (0)$. By the artinian property, there exists a minimal left ideal I_0 such that $I \cdot I_0 \neq 0$. Therefore, there exists some $a \in I_0$ such that $I \cdot a \neq (0)$. Then $I \cdot (Ia) = Ia \neq (0)$. It follows that $I \cdot a = I_0$. In particular, for some $y \in I$ we have $ya = a$, or $(1 - y)a = 0$. As $y \subseteq \operatorname{rad} R$, we get $a = 0$, which is a contradiction, therefore $I = (0)$. □

Theorem 1.8.11. For a ring R the following statements are equivalent:

[3] Also the *Wedderburn radical*.

i) The ring R is semisimple.

ii) The ring R is J-semisimple and left-artinian.

Proof. A semisimple ring is left-artinian by the Wedderburn theorem. Since R is semisimple, there exists a left R-module $I \leq R$ such that $R = \operatorname{rad} R \oplus I$. If $\operatorname{rad} R \neq (0)$, I is a proper ideal and therefore contained in a maximal ideal M. But as $\operatorname{rad} R$ is also contained in the same ideal M, it follows that $R \subseteq M$, which is impossible.

Now suppose that R is J-semisimple and left-artinian. By the artinian property, we can write $\operatorname{rad} R$ as a finite intersection of maximal submodules

$$(0) = \operatorname{rad} R = \bigcap_{i=1}^{n} M_i.$$

Consider the homomorphism

$$\varphi \colon R \to \bigoplus_{i=1}^{n} R/M_i$$

with

$$\varphi(x) = \prod_{i=1}^{n} (x + M_i).$$

As $\ker \varphi = (0)$, it is injective. We can therefore write

$$R \leq \bigoplus_{i=1}^{n} R/M_i \,,$$

so R is semisimple. □

Lemma 1.8.12 (Nakayama)**.** For a left ideal $J \leq R$ the following statements are equivalent:

i) $J \subseteq \operatorname{rad} R$

ii) The only finitely generated R-module M such that $JM = M$ is $M = (0)$.

iii) For all R-modules N and M such that $N \leq M$ and M/N is finitely generated, we have

$$N + JM = M \implies N = M.$$

Proof. Suppose that $J \subseteq \operatorname{rad} R$ and that $M \neq (0)$ is finitely generated with a minimal set of generators $\{x_1, \ldots, x_k\}$. Since $J \cdot M = M$, we can write

$$x_k = \sum_{i=1}^{k} a_i x_i$$

for some $a_i \in J$. But as $1 - a_k$ is invertible, we can express x_k as a linear combination of x_1, x_2, …, x_{k-1}, which is a contradiction.

Suppose that the second statement holds and let $N \leq M$ be modules. If $N \neq M$, it follows that $J \cdot M/N \neq M/N$, so $N + JM \neq M$.

No suppose that the third statement holds and let $y \in J \setminus \operatorname{rad} R$. Let M be a maximal submodule of R such that $y \notin M$. As $M + J = R$, it follows that $M = R$, which is a contradiction. □

1.9 Group rings and Maschke's theorem

Theorem 1.9.1 (Maschke)**.** Suppose that G is a finite group and k a field such that $\operatorname{char} k \nmid |G|$. Then kG is semisimple.

Proof. By Algebra 3, theorem 4.2.2, every submodule W of V is a direct summand, so M has the complement property. □

Proposition 1.9.2. If k is a field and G is an infinite group, then kG is not semisimple.

Proof. Consider the map $\varepsilon\colon kG \to k$ such that $\varepsilon|_k = \mathrm{id}$ and $\varepsilon(g) = 1$ for all $g \in G$. Let $I = \ker \varepsilon$ and note that $I \lhd kG$.

Suppose that kG is semisimple. Therefore, there exists a submodule $J \leq kG$ such that $I \oplus J = kG$. Write $1 = e + f$ where $e \in I$ and $f \in J$. As $e = e^2 + ef$, it follows that $ef = 0$ and $e = e^2$. Similarly, we have $f = f^2$. Analogously, we get that $b = be$ for all $b \in I$, so $I = (kG)e$ and $J = (kG)f$.

Note that for all $g \in G$ we have $g - 1 \in I$, so $gf = f$. It is now clear that $f \neq 0$ must have the same non-zero coefficient in front of every element $g \in G$ in its linear combination of elements of G. This is not possible, as the linear combination is finite. □

Remark 1.9.2.1. The ring $\mathbb{C}G$ is always J-semisimple.

Remark 1.9.2.2. If G is a finite group and $\operatorname{char} k \mid |G|$, the ring kG is also not semisimple.

2 Primitive rings

2.1 Density theorem

Definition 2.1.1. A ring R is *primitive* if it has a faithful[4] simple module M.

Remark 2.1.1.1. Equivalently, the representation $R \to \mathrm{End}(M)$ is injective.

Definition 2.1.2. Let V be a vector space over a division ring D, and let $R \subseteq \mathrm{End}_D(V)$ be a subring. The ring R is a *dense ring of linear transformations*[5] if for every finite set $\{v_1, \ldots, v_n\} \subseteq V$ of linearly independent vectors and any $\{w_1, \ldots, w_n\} \subseteq V$ there exists some $\phi \in R$ such that $\phi(v_i) = w_i$ for all $i \leq n$.

Theorem 2.1.3 (Density)**.** Let M be a semisimple module over a ring R. We denote $S = \mathrm{End}_R(M)$ and let $\phi \in \mathrm{End}_S(M)$. Then for any finite set $\{x_1, \ldots, x_n\} \subseteq M$ there exists an element $r \in R$ such that $\phi(x_i) = rx_i$ for all $i \leq n$.

Proof. For $n = 1$ we can write

$$M = Rx_1 \oplus M'$$

as M is semisimple. Note that $\pi \colon M \to Rx_1$ is an element of S. It follows that

$$\phi(x_1) = \phi(\pi(x_1)) = \pi(\phi(x_1)),$$

therefore $\phi(x_1) \in Rx_1$.

Consider now M^n and $\phi^{(n)} \colon M^n \to M^n$ as the point-wise application of ϕ. Observe that $\phi^{(n)} \in \mathrm{End}_{\mathrm{End}_R(M^n)}(M^n)$. As M^n is a semisimple R-module, we can apply the $n = 1$ case. □

Theorem 2.1.4 (Jacobson)**.** A ring R is primitive if and only if R is a dense ring of linear transformations on a vector space over a division ring.

Proof. Assume that R is a primitive ring and let M be a faithful and simple R-module. By Schur's lemma, $D = \mathrm{End}_R(M)$ is a division ring, therefore, M is a D-vector space. Since M is faithful, we have $R \subseteq \mathrm{End}_D(M)$, therefore R acts as a ring of linear transformations on M. By the density theorem for modules the ring R is dense.

Assume now that R is a dense ring of linear transformations on a vector space V over a division ring D. In particular, V is an R-module. By definition we have $R \subseteq \mathrm{End}_D(V)$, therefore V is a faithful R-module. It is clear that every non-zero element generates V, therefore V is simple. □

Corollary 2.1.4.1. Any simple artinian ring R is isomorphic to $M_n(D)$ for a division ring D.

Proof. As R is simple, it is primitive. Let M be a faithful and simple R-module and denote $D = \mathrm{End}_R(M)$. This is of course a division ring by Schur's lemma. By Jacobson's theorem, R is a dense subring of $\mathrm{End}_D(M)$.

[4] $\mathrm{ann}(M) = (0)$.
[5] R acts densely on V.

Assume that $\dim_D M = \infty$ and let $(v_n)_n$ be an infinite sequence of linearly independent vectors in M. Let

$$I_n = \{r \in R \mid \forall i \leq n \colon rv_i = 0\}$$

be a submodule of R. Note that these submodules form a strictly decreasing chain, which is impossible.

As $\dim_D M < \infty$, we know that $R = \mathrm{End}_D(M) \cong M_{\dim_D M}(D)$. □

Theorem 2.1.5 (Structure)**.** Let R be a primitive ring with a faithful simple module M and denote $D = \mathrm{End}_R(M)$. Then either

i) $R \cong M_n(D)$ for some $n \in \mathbb{N}$ or

ii) for all $m \in \mathbb{N}$ there exists a subring $R_m \subseteq R$ and an endomorphism $R_m \to M_m(D)$.

Proof. If $\dim_D M < \infty$, we have $R = \mathrm{End}_D(M) = M_n(D)$ for $n = \dim_D M$. Now assume that $\dim_D M = \infty$. If $(v_n)_n$ is an infinite sequence of linearly independent vectors in M, form $V_m = \mathrm{Lin}_D \{v_i \mid i \leq m\}$. Now set

$$R_m = \{r \in R \mid r \cdot V_m \subseteq V_m\}.$$

Note that

$$I_m = \{r \in R \mid rV_m = 0\}$$

is an ideal in R_m. By Jacobson's theorem we have $R_m/I_m \cong M_m(D)$. □

Remark 2.1.5.1. In the case of finite-dimensional algebras the notions of primitive and simple coincide.

Remark 2.1.5.2. The free algebra is primitive. Every algebra is the image of some primitive algebra.

2.2 An application of primitive rings

Proposition 2.2.1. Suppose that R is a ring in which $x^3 = x$ holds for all $x \in R$. Then R is commutative.

Proof. Note that if $ab = 0$, we also have $ba = (ba)^3 = 0$. Let $e \in R$ be an idempotent. Note that for all $x \in R$ we have $e(x - ex) = 0$, therefore $xe = exe$. Similarly, we have $(x - xe)e = 0$, therefore $ex = exe$. This implies that $e \in Z(R)$.

Let $x \in R$ and note that $(x^2)^2 = x^2$. Therefore, x^2 is an idempotent and we have $x^2 \in Z(R)$. Also note that for all $c \in R$ such that $c^2 = 2c$ we have $c = 2c^2 \in Z(R)$.

Now let $x \in R$. Note that

$$(x^2 + x)^2 = x^4 + 2x^3 + x^2 = 2(x^2 + x),$$

therefore, we have both $x^2 + x \in Z(R)$ and $x = (x^2 + x) - x^2 \in Z(R)$. □

Theorem 2.2.2 (Jacobson)**.** Suppose that R is a ring such that for all x there exists an $n > 1$ such that $x^n = x$. Then R is commutative.

Theorem 2.2.3 (Jacobson-Herstein)**.** A ring R is commutative if and only if for all $x, y \in R$ there exists an $n > 1$ such that

$$(xy - yx)^n = xy - yx.$$

Proposition 2.2.4. A ring R is J-semisimple if and only if it has a faithful semisimple module M.

Proof. Suppose that R has a faithful semisimple module M. Recall that the radical is the set of all elements that act trivially on all simple R-modules. It follows that $\operatorname{rad} R \cdot M = 0$, whence $\operatorname{rad} R = (0)$ as M is faithful.

Suppose now that R is J-semisimple. Let $(M_i)_{i \in I}$ be all non-isomorphic simple R-modules and

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

Note that

$$\operatorname{ann}(M) = \bigcap_{i \in I} \operatorname{ann}(M_i) = \operatorname{rad}(R) = (0).$$ □

Corollary 2.2.4.1. Every J-semisimple ring R is a subdirect product of primitive rings.

Proof. The inclusion

$$R \hookrightarrow \textstyle\prod_{i \in I} R \big/ \operatorname{ann} M_i$$

is the desired representation. □

Index