ASSOCIATIEVE ALGEBRA

Eric Jespers

2017–2018

webstek: http://homepages.vub.ac.be/∼efjesper
HOC: donderdag 09-11 uur, F.5.207

Contents

Chapter 1

Introduction

In earlier courses we have introduced important algebraic structures, such as semigroups, groups and rings. We have seen that via representation theory of groups and group rings there is a strong link between group and ring theory. Well known and important examples of rings are matrices $M_n(K)$ over a field K, or more generally over a division ring D. In a ring one can add, subtract and multiply elements, but in general one can not divide by an element. In a division ring every nonzero element has an inverse, and thus one can divide by nonzero elements. In some sense, division rings are the "best" possible object in ring theory. Of course from known examples of rings one can built new ones through for example direct products. Hence one obtains (finite) direct products of matrices over division rings

$$M_{n_1}(D_1) \times \cdots \times M_{N_k}(D_k).$$

In Chapter two we accomplish one of the first main aims in this course: we prove that such rings are precisely the semisimple rings. This is one of the nicest characterization theorems in algebra, it is due to Wedderburn (1982 - 1948) and Artin (1898 - 1962).

For more information on these two remarkable mathematicians we refer the reader to the websites
http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Wedderburn.html
and
http://www-groups.dcs.st-andrews.ac.uk/history/Mathematicians/Artin.html.

An interesting website for background on mathematicians is
http://www.genealogy.math.ndsu.nodak.edu/index.html.

Not all rings are semisimple and thus the Wedderburn-Artin theorem does not apply. In chapter three we introduce the notion of Jacobson radical (N. Jacobson, 1910 - 1999). This set is a measure for "obstruction" to obtaining a nice structure theorem. Properties of this set are studied and the link with other obstructions (such as nil and nilpotent ideals) is given. Also applications of ring structure to group theory are given.

In Chapter two we introduce the definition of semisimple rings and we define Artinian and Noetherian rings and modules. Next we prove the Wedderburn-Artin Theorem.

In Chapter four special classes of rings are studied, such as (semi)prime and primitive rings.

In Chapter five some algebraic structure of skew fields are studied and in the last chapter the Goldie theorems are proved. These show that some classes of rings are subrings of semisimple rings.

Chapter 2

Semisimple rings and Wedderburn Artin Theorems

In this course we concentrate on non-commutative ring theory. Some of you, in an earlier algebra course, defined semisimple rings R as finite dimensional k-algebras (k a field) that are (Von Neumann) regular. It follows that every left ideal is generated by an idempotent, and that R is the direct sum of minimal left ideals. Next we showed that R is isomorphic with a direct product of simple rings. If k is algebraically closed then these simple rings are matrix rings over fields. This structure theorem was extremely useful to deal with group representations (this via the study of the semisimple group algebra kG of a finite group G).

Wedderburn showed that an analogue description can be given for arbitrary finite dimensional algebras over an arbitrary field, this provided the largest nilpotent ideal is trivial.

In this chapter we treat this subject in an even more general context (so that also some non-finite dimensional algebras are included). We call a ring R semisimple if every R-module is semisimple, that is, every R-module is a sum of simple modules.

2.1 Introduction

We always assume that a ring has an identity element 1 and that a subring contains the same identity.

Definition 2.1.1 *A ring R is simple if $\{0\}$ and R are the only two-sided ideals.*

Examples of simple rings are skew fields and matrices over skew fields.

Definition 2.1.2 *A ring R is a domain (or a ring without zero divisors) if $R \neq \{0\}$ and, for any $r, s \in R$, $rs = 0$ implies $r = 0$ or $s = 0$.*

A ring R is reduced if R has no nonzero nilpotent elements.

The opposite ring R^{op} of a ring R is as additive subgroup the same as $(R, +)$ but the multiplication $\circ$ is defined as follows, for $r, s \in R$:

$$r \circ s = sr$$

(where the latter is the product taken in the given ring R).

2.2 Ascending and descending chain conditions

A set $\{V_i \mid i \in I\}$ of subsets V_i of a set V is said to satisfy the ascending chain condition (ACC) if there does not exist an infinite strict ascending sequence

$$V_{i_1} \subset V_{i_2} \subset \cdots$$

with all $i_j \in I$.

The following are equivalent with (ACC):

1. for every ascending sequence

   $$V_{i_1} \subseteq V_{i_2} \subseteq \cdots$$

   (each $i_j \in J$) there exists $n > 0$ so that $V_{i_n} = V_{i_{n+k}}$ for all $k \geq 0$.

2. every non-empty subset of $\{V_i \mid i \in I\}$ has a maximal element (for the inclusion relation).

Similarly, one defines the descending chain condition (DCC), that is, for any chain

$$V_{i_1} \supset V_{i_2} \supset \cdots$$

there exists $n > 0$ so that $V_{i_n} = V_{i_{n+k}}$ for any $k \geq 0$. Or equivalently, every non-empty subset of $\{V_i \mid i \in\}$ has a minimal element.

Definition 2.2.1 *Let R be a ring. A (left) R-module is said to be (left) Noetherian (respectively, left Artinian) if the set of (left) submodules of M satisfies the ascending chain condition (respectively, descending chain condition) (Noether, 1982 - 1935).*

In the previous course the following result was proved.

Proposition 2.2.2 *The following properties hold for a (left) R-module M.*

1. *M is (left) Noetherian if and only if every submodule of M is finitely generated.*

2. *Let N be a submodule of M. Then, M is Noetherian if and only if both N and M/N are Noetherian. In particular, the direct sum of two Noetherian R-modules is again Noetherian.*

In a similar fashion one proves the following result.

Proposition 2.2.3 *Let M be a (left) R-module and N a submodule. Then, M is Artinian if and only if both N and M/N are Artinian. In particular, the direct sum of two Artinian R-modules is again Artinian.*

Recall that a chain of submodules (of a module M)

$$M_0 = \{0\} \subset M_1 \subset \cdots \subset M_n = M$$

is said to be a composition series if all quotient modules M_i/M_{i-1} $(1 \leq i \leq n)$ are simple (that is, the only submodules are $\{0\}$ and the module itself). The length n of the chain and the quotients are uniquely determined (modulo a permutation).

Proposition 2.2.4 *An R-module M is Noetherian and Artinian if and only if M has a composition series.*

Proof. If M has a composition series then it follows from Propositions 2.2.2 and 2.2.3 that M is Noetherian and Artinian.

Conversely, assume that M is Noetherian and Artinian. If $M = \{0\}$, then clearly M has a composition series. Suppose $M \neq \{0\}$. Because M

is Artinian, there exists a minimal nonzero submodule M_1. If $M_1 = M$ then we get the composition series

$$\{0\} \subset M_1 = M.$$

If $M_1 \neq M$, then we repeat the previous reasoning on the Artinian module M/M_1. Because of the one-one correspondence between the submodules of M/M_1 and the submodules of M containing M_1 there exists a submodule M_2 so that

$$\{0\} \subset M_1 \subset M_2 \subseteq M$$

with M_2/M_1 simple. Now we repeat the process on M/M_2. Because M is Noetherian we get a composition series after a finite number of steps. □

Definition 2.2.5 *A ring R is left (respectively right) Noetherian if R is left (respectively right) Noetherian as a left R-module (i.e., we consider R as the regular R-module). Note that R is left Noetherian if and only if every left ideal is finitely generated. A ring R is called Noetherian if and only if R is left and right Noetherian.*

Similarly one defines (left, right) Artinian rings.

In the course "Ring and Module Theory" we proved that a finitely generated left R-module over a left Noetherian ring is left Noetherian. We also constructed some examples of left Noetherian rings that are not right Noetherian (and conversely). For example,

$$R = \begin{bmatrix} \mathbf{Q} & \mathbf{Q} \\ \{0\} & \mathbf{Z} \end{bmatrix},$$

and this ring is not right nor left Artinian.

Similarly there exist rings that are left Artinian but not right Artinian. For example,

$$R = \begin{bmatrix} \mathbf{Q}(X) & \mathbf{Q}(X) \\ \{0\} & \mathbf{Q} \end{bmatrix}$$

The properties of the previous examples follow from the following result.

Proposition 2.2.6 *Let R and S be rings and M a (R,S)-bimodule, that is, M is a left R-module and a right S-module so that, for all $r \in R$, $s \in S$ and $m \in M$:*

$$(rm)s = r(ms).$$

Then, the ring

$$\begin{bmatrix} R & M \\ \{0\} & S \end{bmatrix}$$

is left (respectively right) Noetherian if and only if R and S are left (respectively right) Noetherian, and M is left Noetherian as a left R-module (respectively, right Noetherian as a right S-module).

Later we shall prove that a left (respectively right) Artinian ring always is left (respectively right) Noetherian (this result is due to Levitzki and Hopkins). We note that this result is not true for modules. Indeed, consider the additive p-Püfer group $\mathbf{Z}_{p^\infty}$:

$$\mathbf{Z}_{p^\infty} = \left\{ \frac{z}{p^i} + \mathbf{Z} \mid z \in \mathbf{Z},\ i \in \mathbf{N} \right\}$$

where p is a prime number. Every nonzero $\frac{z}{p^i} + \mathbf{Z}$ can be written as $\frac{m}{p^j} + \mathbf{Z}$ with $(m, p^j) = 1$. Let then $\alpha, \beta \in \mathbf{Z}$ be such that $\alpha m + \beta p^j = 1$. It follows that

$$\begin{aligned} \alpha\left(\frac{m}{p^j} + \mathbf{Z}\right) &= \frac{\alpha m}{p^j} + \mathbf{Z} \\ &= \frac{\alpha m + \beta p^j}{p^j} + \mathbf{Z} \\ &= \frac{1}{p^j} + \mathbf{Z} \end{aligned}$$

So, the cyclic $\mathbf{Z}$-submodules are generated by an element of the form $\frac{1}{p^j} + \mathbf{Z}$. Because every $\mathbf{Z}$-module is generated by cyclic submodules, we get that every proper submodule is cyclic. Hence, $\mathbf{Z}_{p^\infty}$ is an Artinian $\mathbf{Z}$-module, but it is not Noetherian as a $\mathbf{Z}$-module.

Also note that the ring $\mathbf{Z}$ is Noetherian but not Artinian.

Recall also that a polynomial ring $R[X]$ over a Noetherian ring is again a Noetherian ring.

2.3 Semisimplicity

A left R-module we will often denote as ${}_RM$ and a right R module N as N_R. A (R,S)-bimodule we denote by ${}_RM_S$.

Definition 2.3.1 *Let R be a ring and ${}_RM$ an R-module.*

1. *M is simple if $M \neq \{0\}$ and $\{0\}$ and M are the only submodules.*
2. *M is semisimple if every submodule N is a direct summand, that is, there exists a submodule N' such that $M = N \oplus N'$.*

Clearly every simple module is semisimple.

Proposition 2.3.2 *Submodules and quotient modules of semisimple modules are again semisimple.*

Proof. Let ${}_RM$ be a semisimple module and N a submodule. Assume N_1 is a submodule of N. Because M is semisimple there exists a submodule of M such that

$$M = N_1 \oplus N_1'.$$

It follows that

$$N = N_1 \oplus (N_1' \cap N).$$

So N_1 is a direct summand of N and we obtain that N is semisimple.

Assume N_2 is a submodule of M such that $N \subseteq N_2$. Because M is semisimple, there exists a submodule N_2' of M so that

$$M = N_2 \oplus N_2'.$$

Hence,

$$M/N = N_2/N \oplus ((N_2' + N)/N).$$

Consequently, M/N is semisimple. □

Lemma 2.3.3 *Every non-zero semisimple module contains a simple submodule.*

Proof. Let $0 \neq m \in M$. Because of Proposition 2.3.2, Rm is a semisimple module. Using Zorn's Lemma, there exists a submodule N of Rm that is maximal with respect to the condition $m \notin N$. Write

$$Rm = N \oplus N'$$

for some submodule N' of Rm. Note that $N' \neq \{0\}$ (as $m \notin N$). We prove that N' is simple, and hence the result follows. Indeed, suppose the contrary, that is, let N'' be a non-zero submodule of N'. Because of the maximality condition on N we obtain

$$m \in N \oplus N''.$$

Hence, $Rm = N \oplus N''$ and thus

$$N \oplus N'' = N \oplus N'.$$

So $N'' = N'$. □

Theorem 2.3.4 *Let ${}_RM$ be an R-module. The following properties are equivalent:*

1. *M is semisimple,*
2. *M is a direct sum of simple submodules,*
3. *M is a sum of simple submodules.*

Proof. First we prove (1) implies (3). So assume M is semisimple. Let M_1 be the sum of all simple submodules of M. Then there exists a submodule M_2 such that $M = M_1 \oplus M_2$. If $M_2 \neq \{0\}$ then it follows from Lemma 2.3.3 that M_2 contains a simple submodule. However, this is also a submodule of M_1, a contradiction. Hence $M_2 = \{0\}$ and thus $M = M_1$

Next we prove (3) implies (1), and (3) implies (2). So, assume $M = \sum_{i \in I} M_i$, with every M_i a simple module. Let N be a submodule of M. Consider the subsets J of I such that

$$\sum_{j \in J} M_j = \oplus_{j \in J} M_j$$

and

$$N \cap \sum_{j \in J} M_j = \{0\}.$$

Because of Zorn's Lemma, there exists a maximal such subset J. We now prove that for this J,

$$M_i \subseteq M' = N \oplus (\oplus_{j \in J} M_j),$$

for all $i \in I$; and thus $M = N \oplus (\oplus_{j \in J} M_j)$. Hence the result follows.

Suppose $i \in I$ and assume $M_i \not\subseteq M'$. Because M_i is simple it follows that $M' \cap M_i = \{0\}$. But then we obtain

$$M' + M_i = N \oplus (\oplus_{j \in J} M_j) \oplus M_i.$$

But this yields a contradiction with the maximality of J. □

Theorem 2.3.5 *Let R be a ring. The following properties are equivalent:*

1. *Every short exact sequence of left R-modules splits,*
2. *every left R-module is semisimple,*
3. *every finitely generated left R-module is semisimple,*
4. *every cyclic left R-module is semisimple,*
5. *the regular left R-module R is semisimple.*

Proof. The following implications are obvious: (1) $\Leftrightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5). We now prove that (5) implies (2). Suppose thus that ${}_RR$ is semisimple and let M be a left R-module. Clearly,

$$M = \sum_{m \in M} Rm$$

and each Rm is an epimorphic image of ${}_RR$. Because of Proposition 2.3.2 and the assumption, every Rm is semisimple. Hence, by Theorem 2.3.4 each Rm and thus also M is a sum of simple modules. So, again by Theorem 2.3.4, M is a semisimple module. □

Definition 2.3.6 *A ring R satisfying the equivalent conditions of Theorem 2.3.5 is called left semisimple. Similarly one defines right semisimple rings.*

Later we will show that a ring is left semisimple if and only if it is right semisimple. We therefore will call such rings simply semisimple rings.

Corollary 2.3.7 *A left semisimple ring is left Noetherian and left Artinian.*

Proof. Let R be a left semisimple ring. Because of Theorem 2.3.4,

$$R = \oplus_{i\in I} L_i$$

a direct sum of minimal left ideals of R. Because $1 \in R$, it follows that I is a finite set. Write $I = \{1, 2, \cdots, n\}$. We obtain a composition series

$$\{0\} \subset L_1 \subset L_1 \oplus L_2 \subset \cdots \subset L_1 \oplus \cdots \oplus L_n = R.$$

Hence by Proposition 2.2.4, R is left Noetherian and left Artinian. □

Recall that a left R-module P is said to be *projective* if every diagram of module morphisms

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \psi} & & \\ M & \xrightarrow{f} & N & \longrightarrow & \{0\} \end{array}$$

can be completed to a commutative diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow{\scriptstyle \varphi} & \downarrow{\scriptstyle \psi} & & \\ M & \xrightarrow{f} & N & \longrightarrow & \{0\} \end{array}$$

We know that ${}_RP$ is projective if and only if P is a direct summand of a free R-module (or equivalently, every short exact sequence $\{0\} \to N \to M \to P \to \{0\}$ splits).

Corollary 2.3.8 *Let R be a ring. The following properties are equivalent:*

1. *R is left semisimple,*
2. *every left R-module is projective,*
3. *every finitely generated left R-module is projective,*
4. *all cyclic left R-modules are projective.*

Proof. That (1) and (2) are equivalent follows immediately from Theorem 2.3.5 and the previous remarks. Obvious are the implications: (2) $\Rightarrow$ (3) $\Rightarrow$ (4). We now prove that (4) implies (1). So, suppose that every cyclic R-module is projective. Because of Theorem 2.3.5 it is sufficient to show that every short exact sequence

$$\{0\} \to L \to R \to R/L \to \{0\}$$

splits (with L a left ideal of R). But since R/L is a cylic R-module, the latter is obvious because of the assumption. $\square$

We now define the dual notion of a projective module.

Definition 2.3.9 *Let R be a ring. A left R-module I is said to be injective if every diagram of the form*

$$\begin{array}{ccccc} & & & & I \\ & & & & \uparrow{\scriptstyle \psi} \\ \{0\} & \longrightarrow & M & \xrightarrow{f} & N \end{array}$$

where the lower sequence is exact, can be completed to a commutative diagram as follows:

$$\begin{array}{ccccc} & & & & I \\ & & & & \uparrow{\scriptstyle \psi} \quad \nwarrow{\scriptstyle \varphi} \\ \{0\} & \longrightarrow & M & \xrightarrow{f} & N \end{array}$$

One then shows the following characterisation of injective modules.

Proposition 2.3.10 *A left R-module I is injective if and only if every short exact sequence*

$$\{0\} \to I \to M \to N \to \{0\}$$

splits.

If $f : R \to {}_RI$ is a module morphism, then

$$f(r) = rf(1)$$

for all $r \in R$. Thus f is right multiplication with an element of I. Hence, if ${}_RI$ is injective and L is a left ideal of R, then every homomorphism

$$f : L \to I$$

is determined by an element of I. Indeed,

$$\begin{array}{ccccc} & & I & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle \varphi} & \\ \{0\} & \longrightarrow & L & \xrightarrow{i} & R \end{array}$$

(with $i(l) = l$ for $l \in L$). So $\varphi \circ i = f$ and consequently, for every $l \in L$,

$$f(l) = \varphi(i(l)) = \varphi(l) = l\varphi(1),$$

and $\varphi(1) \in I$.

The following criterion shows the above property characterises injective modules, that is, it is sufficient to check the required property on left ideals.

Proposition 2.3.11 *(Baer's Criterion) Let R be a ring and I a left R-module. Then, I is left injective if and only if for every left ideal L of R the diagram*

$$\begin{array}{ccccc} & & I & & \\ & & \uparrow{\scriptstyle f} & & \\ \{0\} & \longrightarrow & L & \xrightarrow{i} & R \end{array}$$

can be completed to a commutative diagram

$$\begin{array}{ccccc} & & I & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle f^e} & \\ \{0\} & \longrightarrow & L & \xrightarrow{i} & R \end{array}$$

(that is, $f^e_{|L} = f$).

Proof. One implication is clear. We prove the other one. Hence, consider a diagram

$$\begin{array}{ccccc} & & & & I \\ & & & & \uparrow f \\ \{0\} & \longrightarrow & N & \xrightarrow{i} & M \end{array}$$

We search for a map $\varphi : M \to I$ that makes the diagram commutative. For this, consider the set

$$\mathcal{L} = \{(N', f') \mid {}_RN \leq {}_RN' \leq {}_RM,\ f' : N' \to I \text{ and } f'_N = f\}$$

We define a partial order on $\mathcal{L}$ as follows:

$$(N', f') \leq (N'', f'') \text{ if } N' \leq N'' \text{ and } f''_{N'} = f'.$$

Because of Zorn's Lemma, there exists a maximal element (N_0, f_0). We claim that $N_0 = M$. Hence the result follows.

Suppose, the contrary, that is, assume $N_0 \subset M$ and let $x \in (M \setminus N_0)$. Put

$$L = \{r \in R \mid rx \in N_0\}.$$

Obviously, L is a left ideal of R. Define

$$g : L \to I : a \mapsto f_0(ax).$$

Because of the assumption, there exists

$$\varphi : R \to I$$

with

$$\varphi_{|L} = g.$$

Hence, there exists $\alpha \in I$ such that

$$g(a) = a\alpha$$

for all $a \in L$. Next define

$$f_1 : N_0 + Rx \to I : y + rx \mapsto f_0(y) + r\alpha.$$

We now show that f_1 is well defined. Indeed, if $y_1+r_1x = y_2+r_2x \in N_0+Rx$ (thus, $y_1, y_2 \in N_0$ and $r_1, r_2 \in R$), then $(r_2-r_1)x = y_1-y_2 \in N_0$. Thus $r_2 - r_1 \in L$ and

$$\begin{aligned}(f_0(y_1) + r_1\alpha) - (f_0(y_2 + r_2\alpha) &= f_0(y_1 - y_2) + (r_1 - r_2)\alpha \\ &= f_0(y_1 - y_2) + g(r_1 - r_2) \\ &= f_0(y_1 - y_2) + f_0((r_1 - r_2)x) \\ &= f_0(y_1 - y_2 + (r_1 - r_2)x) \\ &= f_0(0) \\ &= 0\end{aligned}$$

As $f_1 : N_0 + Rx \to I$ is a function and an R-module homomorphism such that $(f_1)_{|N_0} = f_0$, we obtain a contradiction with the maximality of (N_0, f_0). □

Corollary 2.3.12 *Let R be a ring. The following properties are equivalent:*

1. *R is left semisimple,*
2. *every left R-module is injective,*
3. *every finitely generated left R-module is injective,*
4. *every cyclic left R-module is injective.*

Note that $\mathbf{Q}$ is a $\mathbf{Z}$-module that is not projective, but it is injective.

One can show that every R-module M is a submodule of an injective R-module I. If I is minimal over M, then I is unique. The latter exists and is called the injective hull of M

2.4 Exercises

1. Let D be a skew field. Is the polynomial ring $D[X]$ Noetherian or Artinian?
2. Let G be a finite group and F a field. Is the group algebra $F[G]$ Artinian or Noetherian.

3. Let G be a group and F a field. Prove that the map

$$F[G] \to F[G] : \sum_{g \in G} f_g g \mapsto \sum_{g \in G} f_g g^{-1}$$

is an anti-isomorphism of order 2. Prove as a consequence that $F[G]$ is left Noetherian if and only if it is right Noetherian.

4. Give an example of an injective module. And give an example of a module that is not injective.

5. Let M be a left R-module. An element $m \in M$ is said to be divisible by $r \in R$ if there exists $m' \in M$ such that $rm' = m$. The module M is said to be divisible by $r \in R$ if every element $m \in M$ is divisible by r. The module M is said to be divisible if M is divisible by every regular element (i.e. nonzero divisor) of R.

   (a) Prove that every injective module is divisible.

   (b) Prove that every divisible module over a principal ideal domain is injective.

   (c) Prove that $\mathbf{Q}/\mathbf{Z}$ is an injective $\mathbf{Z}$-module.

   (d) Prove that an epimorphic image of a divisible module is divisible.

   (e) Prove that direct product and direct sums of divisible modules are divisible.

6. Prove that a direct product and direct sum of injective modules is injective.

7. Is a subring of a left semisimple ring itself left semisimple?

8. (a) Prove that the ring $\mathbf{Z}$ is a subring of a semisimple ring.

   (b) Prove that $\mathbf{Z}[X]$ is a subring of a semisimple ring.

   (c) Is every ring a subring of a left semisimple ring?

9. Prove that a direct product $\prod_{i \in I} R_i$ of rings is semisimple if and only if $|I| < \infty$.

10. (a) Give an example of a semisimple $\mathbf{Z}$-module.
    (b) Give an example of a $\mathbf{Z}$-module that is not semisimple.
    (c) What are the semisimple $\mathbf{Z}$-modules?

11. Let $C([0,1], \mathbf{R})$ be the ring of all continuous real functions with domain $[0,1]$. Is this ring semisimple?

12. Let M be a left semisimple module over a ring R. Prove that the following properties are equivalent:
    (a) M is finitely generated,
    (b) M is Noetherian,
    (c) M is Artinian,
    (d) M is a direct sum of finitely many simple left R-modules.

13. Let D be a skew field. Prove that $M_n(D)$ is semisimple. Is the polynomial ring $D[X]$ semisimple?

14. Let R be a domain. Prove that if $M_n(R)$ is semisimple then R is a skew field.

2.5 Structure of semisimple rings

In this section we give a complete description of semisimple rings R. (Recall that in "Ring and Module Theory" we already dealt with this topic provided that R is an algebra over an algebraically closed field).

Let S be a ring. The two-sided ideals of the matrix ring $M_n(S)$ are of the form $M_n(I)$ with I a two-sided ideal of S. Thus, if D is a skew field then $R = M_n(D)$ is a simple ring. Furthermore,

$$R = M_n(D) = C_1 \oplus \cdots \oplus C_n$$

with C_i the i-th column (that is, $C_i = \{(a_{kl}) \mid a_{kl} = 0 \text{ for } 1 \leq k, k \leq n \text{ and } l \neq i\}$.) Every C_i is a simple R-module. Thus R is a left semisimple R-module and

$$\{0\} \subset C_1 \subset C_1 \oplus \cdots \subset C_1 \oplus \cdots \oplus C_n = R$$

is a composition series of ${}_RR$. Let now V be a simple left R-module. Then

$$V \cong R/M$$

for some maximal left ideal M of R. Thus, V is a composition factor of ${}_RR$ and hence

$${}_RV \cong {}_RC_i,$$

for some C_i. As ${}_RC_1 \cong {}_RC_2 \cong \cdots {}_RC_n$ we have thus shown that (up to isomorphism) there exists a unique simple left R-module V and

$${}_RV \cong {}_RD^n \text{ and } {}_RR \cong V \oplus \cdots \oplus V$$

(n-copies of V).

Schur's Lemma yields that (with $V \cong D^n$)

$$\mathrm{End}_R(V)$$

is a skew field. We now prove that this ring is isomorphic with D. For this, define

$$\varphi : D \to \mathrm{End}_R(V) : d \mapsto \varphi_d$$

with

$$\varphi_d : V \to V : v \mapsto vd$$

(here we consider V as right D-vector space). Also V is a $(R, \mathrm{End}_R(V))$-bimodule. For the latter we write the functions in $\mathrm{End}_R(V)$ on the right hand side, i.e.

$$(v)f$$

for $v \in V$; and $f_1 \circ f_2$ means "first f_1 and then f_2".

Clearly φ is a ring homomorphism. Moreover, $\varphi_d \neq 0$ if $d \neq 0$. So φ is injective. To prove the surjectivity, let $f \in \mathrm{End}_R(V)$. Write

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} f = \begin{pmatrix} d \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

for some $d, x_2, \cdots, x_n \in D$. It follows that

$$\begin{aligned}
\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} f &= \left(\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ d_n & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right) f \\
&= \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ d_n & 0 & \cdots & 0 \end{pmatrix} \left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} f \right) \\
&= \begin{pmatrix} d_1 d \\ \vdots \\ d_n d \end{pmatrix} \\
&= \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \varphi_d
\end{aligned}$$

Thus, $f = \varphi(d)$.

Hence, we have proven the following result.

Theorem 2.5.1 *Let D be a skew field and $R = M_n(D)$. The following properties hold:*

1. *R is simple, left semisimple, left Artinian and left Noetherian,*
2. *R has a unique (up to isomorphism) simple left module M and M is a faithful left R-module such that ${}_RR \cong {}_RM \oplus \cdots {}_RM$ (n terms).*
3. *The ring $End({}_RM)$ is isomorphic with D.*

Lemma 2.5.2 *The direct product $R = R_1 \times \cdots \times R_n$ of semisimple rings is semisimple.*

Proof. Write $R_i = Ł_{i1} \oplus \cdots \oplus L_{in_i}$, a direct sum of minimal left ideals in R_i. Consider R_i as a two-sided ideal of R. It then follows that every L_{ij} is a minimal left R-ideal. So

$$_RR = {}_RR_1 \oplus \cdots \oplus {}_RR_n = \oplus_{i,j} L_{ij}$$

and thus ${}_RR$ is left semisimple. □

It follows that the direct product of matrix rings over skew fields is a semsimple ring. We shall now prove the converse. For this we first recall the following lemma (see "Ring and Module Theory").

Lemma 2.5.3 *Let R be a ring and let $I_1, I_2, \cdots, I_r, J_1, \cdots, J_s$ be nonzero ideals such that*

$$R = I_1 \oplus \cdots \oplus I_r = J_1 \oplus \cdots \oplus J_s.$$

If every ideal I_i, J_j is indecomposable as an ideal (that is, it is not a direct sum of two nonzero ideals), then $r = s$ and (after renumbering, if necessary) $I_i = J_i$, for $1 \leq i \leq r$.

Theorem 2.5.4 *(Wedderburn-Artin) Let R be a left semisimple ring. Then*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

for some skew fields $D_1, \cdots, D_r$ and $n_1, \cdots, n_r \in \mathbf{N}_0$. The number r is uniquely determined as well as the pairs $(n_1, D_1), \cdots, (n_r, D_r)$ (up to a permutation). There are precisely r non-isomorphic simple left R-modules.

Proof. Let R be a left semisimple ring. Then R is a direct sum of minimal left ideals. It follows that

$$_RR \cong n_1V_1 \oplus \cdots \oplus n_rV_r,$$

with $V_1, \cdots, V_r$ (two-by-two) non-isomorphic simple left R-modules. Note that ${}_RR$ has a composition series with quotients isomorphic to one of the modules $V_1, \cdots, V_r$. Since every simple R-module V is isomorphic to a

quotient of R it follows from the Jordan-Hölder theorem that ${}_RV \cong {}_RV_i$, for some $1 \leq i \leq r$. So $\{V_1, \cdots, V_r\}$ is a complete set of non-isomorphic simple left R-modules.

Because $\mathrm{End}_R(V_i, V_j) = \{0\}$, for $i \neq j$, we get

$$\begin{aligned} R &\cong \mathrm{End}_R(R) \\ &\cong \mathrm{End}_R(n_1V_1 \oplus \cdots \oplus n_rV_r) \\ &\cong \mathrm{End}(n_1V_1) \times \cdots \times \mathrm{End}(n_rV_r) \\ &\cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r) \end{aligned}$$

with $D_i = \mathrm{End}_R({}_RV_i)$, a skew field.

To prove the uniqueness, because of Lemma 2.5.3, we may suppose that $R \cong M_n(D)$ (thus R is simple). Hence, assume

$$R \cong M_n(D) \cong M_{n'}(D'),$$

with D' also a skew field. It then follows that

$${}_RR \cong nV \cong n'V \quad (\text{with } V \cong D^n,\ V' \cong (D')^{n'}).$$

Using the Jordan-Hölder theorem we then get that $n = n'$ and $V \cong V'$. Moreover,

$$D' \cong \mathrm{End}_R(V') \cong \mathrm{End}_R(V) \cong D.$$

□

Corollary 2.5.5 *A ring R is left semisimple if and only if it is right semisimple.*

Proof. Because a direct sum of matrix rings over skew fields is left and right semisimple. □

Note that in any ring R one can show that the sum of all minimal left ideals isomorphic (as R-modules) with a given minimal left ideal L is a two-sided ideal. Let us denote this by B_L. Further, $B_L\ B_{L'} = \{0\}$ if L and L' are two non-isomorphic minimal left ideals of R.

Corollary 2.5.6 *The following properties are equivalent for a simple ring R:*

1. *R is left Artinian,*
2. *R is (left) semisimple,*
3. *R has a minimal left ideal,*
4. *$R \cong M_n(D)$ for some skew field D and some $n \in \mathbf{N}_0$.*

Proof. That (2) and (4) are equivalent follows from Theorem 2.5.4. That (1) implies (3) and that (2) implies (1) are clear.

We now prove that (3) implies (2). So let L be a minimal left ideal of R. Then, B_L is a two-sided ideal of R. Because R is simple we get $B_L = R$. Hence ${}_RR$ is semisimple. □

Corollary 2.5.7 *Let R be a simple finite dimensional algebra over field k. Then*

$$R = M_n(D)$$

for some skew field D. Moreover, $D \cong End_R(V)$, with V the unique simple left R-module. In particular, D is a finite dimensional k-algebra.

This is the original version of the Wedderburn Theorem (1907). It also follows that if R is a semisimple finite dimensional k-algebra over an algebraically closed field k, then

$$R \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k).$$

So this yields the result proven in Ring and Module Theory.

Also note that a semisimple commutative ring is a finite direct product of fields.

2.6 Examples

Let

$$R_0 \subseteq R_1 \subseteq R_2 \subseteq$$

be an ascending chain of rings (all with the same 1). If every R_i is simple, then

$$R = \cup_{i=0}^{\infty} R_i$$

also is a simple ring. For example, let D be a skew field and

$$R_i = M_{2^i}(D).$$

Identify each R_i with a subring of R_{i+1} via the map

$$R_i \to R_{i+1} : M \mapsto \begin{bmatrix} M & 0 \\ 0 & M \end{bmatrix}$$

However, R is not (left) Artinian. To prove this, let $e_i = E_{11} \in R_i$. It follows that, $e_{i+1} = e_{i+1}e_i \in R_{i+1}$. So

$$Re_0 \supseteq Re_1 \supseteq Re_2 \supseteq \cdots,$$

a descending chain of left ideals of R. We now show that this is a strict descending chain. For this it is sufficient to show that $e_i \notin Re_{i+1}$ (for all i). Indeed, suppose the contrary, that is, assume $e_i \in Re_{i+1}$. Then $e_i \in R_j e_{i+1}$ for some $j \geq 0$. Thus

$$e_i = Me_{i+1}$$

for some $M \in M_{2^j}(D)$. However, the $(2^i + 1, 2^i + 1)$-position of Me_{i+1} is 0, while the $(2^i + 1, 2^i + 1)$-position of e_i equals 1, a contradiction.

Let D be a division ring and $V = \oplus_{i \geq 1} e_i D$, a right D-vector space of countable infinite dimension. Let $E = \mathrm{End}(V_D)$ and I the ideal of the endomorphisms of finite rank. Then $R = E/I$ is a simple ring which is not left Noetherian.

Let R be a ring and δ a differential operator on R, that is,

$$\delta(ab) = a\delta(b) + \delta(a)b,$$

and

$$\delta(a + b) = \delta(a) + \delta(b),$$

for all $a, b \in R$. Consider then the polynomial ring $R[X]$ with the usual addition, but with multiplication defined via

$$Xa = aX + \delta(a),$$

for all $a \in R$. We obtain a ring which is denoted by

$$R[X;\delta].$$

This ring is called the *differential polynomial ring*. One says δ is inner if there exists $c \in R$ so that

$$\delta(a) = ca - ac$$

for all $a \in R$.

If R is a simple k-algebra, with k a field of characteristic zero, and δ is not inner, then $R[X;\delta]$ is simple.

To prove this, suppose I is a nonzero proper ideal of $R[X;\delta]$. Let n be the minimal degree of a non-constant polynomial in I and let ℓ be the set consisting of the coefficients of X^n for $f \in I$ of degree n, together with 0. Then ℓ is a nonzero ideal of R and thus $\ell = R$. In particular, $1 \in \ell$ and hence there exists in I a polynomial

$$f = X^n + aX^{n-1} + \cdots$$

For any $r \in R$,

$$X^n r = rX^n + n\delta(r)X^{n-1} + \cdots$$

Because $rf - fr \in I$ we get $rf - fr = 0$. Hence

$$ra - n\delta(r) - ar = 0.$$

Consequently, because $0 \neq n \in k$,

$$\delta(r) = r(n^{-1}a) - (n^{-1}a)r,$$

for all $r \in R$. So δ is inner, a contradiction. This proves that indeed $R[X;\delta]$ is simple. Note that the result remains valid if R is a k-algebra that has no non-zero δ-invariant ideals.

Now consider $R = k[X]$ and δ the formal derivative on R. Since R is commutative it is clear that δ is not inner. Also R does not have non-zero ideals that are invariant under taking derivatives (for k a field of characteristic zero). It follows that the Weyl algebra

$$A_1(k) = (k[X])[Y;\delta] = k\langle X, Y\rangle/(YX - XY - 1)$$

(with k a field of characteristic zero) is a simple ring and a domain. Moreover, $A_1(k)$ is not Artinian, but it is Noetherian.

2.7 Exercises

1. Prove that $M_n(R)$ is semisimple if and only if R is semisimple.

2. Prove that the centre of a semisimple ring is a direct product of finitely many fields (and thus semisimple)

3. Let M be a finitely generated left R-module and $E = \mathrm{End}_R(M)$. If R is semisimple (respectively Artinian) then E is semisimple (respectively Artinian).

4. Let R be a simple ring and $k = Z(R)$. Assume $\dim_k(R) < \infty$. Let M be a finitely generated left R-module and $E = \mathrm{End}_R(M)$. Prove that
$$(\dim_k(M))^2 = \dim_k(R)\ \dim_k(E).$$

5. For a subset X of a ring R define
$$\mathrm{ann}_l(X) = \{r \in R \mid rX = \{0\}\}$$
and
$$\mathrm{ann}_r(X) = \{r \in R \mid Xr = \{0\}\}.$$
These are called the left (respectively right) annihilator of the set X.

   (a) Give an example where the left and right annihilator are different.

   (b) Is the annihilator a left, right, two-sided ideal?

   (c) Assume R is semisimple, I is a left ideal of R and J is a right ideal of R. Prove that
   $$\mathrm{ann}_l(\mathrm{ann}_r(I)) = I \text{ and } \mathrm{ann}_r(\mathrm{ann}_l(J) = J.$$
   (An Artinian ring that satisfies the double annihilator condition is called a quasi Frobenius ring.)

6. Let C_2 be the cyclic group of order 2 and $\mathbf{Z}_2$ the field with two elements. Why is the group ring $\mathbf{Z}_2[C_2]$ not semisimple?

Chapter 3

The Jacobson radical

We study rings that do not necessarily satisfy the descending chain condition on (one-sided) ideals. Such rings R are not necessarily semisimple and hence they could contain a nonzero nilpotent ideal. The latter ideals are an obstruction to obtain "nice" structure theorems, such as a Wedderburn-Artin theorem. It is for this reason that Jacobson (1945) defined a radical of R. This is an ideal J that "contains all obstruction" and such that R/J has "a better structure". In this chapter we give an introduction to this theory.

3.1 The Jacobson radical

Definition 3.1.1 *Let R be a ring. The Jacobson radical $J(R)$ of R is the intersection of all maximal left ideals of R. (If $R = \{0\}$ then by definition $J(R) = \{0\}$.)*

We first show that the definition of $J(R)$ is left-right symmetric, and hence the intersection of all maximal left ideals is the same as the intersection of maximal right ideals.

Lemma 3.1.2 *Let R be a ring and $r \in R$. The following are equivalent:*

1. *$r \in J(R)$,*
2. *$1 - ar$ has a left inverse for all $a \in R$,*
3. *$rM = \{0\}$ for every simple left R-module M.*

Proof. We first prove (1) implies (2). So suppose $r \in J(R)$ and $a \in R$. Then ar belongs to every left ideal L. Because $1 \notin L$, we obtain that $1 - ar$ does not belong to any maximal left ideal. Hence $1 - ar$ is left invertible.

Next we prove (2) implies (3). Suppose $1 - ar$ is left invertible for any $a \in R$. Let M be a simple left R-module. Suppose $rm \neq 0$ for some $m \in M$. Then $R(rm) = M$ and thus $m = a(rm)$ for some $a \in R$. Hence $(1 - ar)m = 0$, a contradiction. It follows that $rM = \{0\}$, as desired.

Finally we prove (3) implies (1). Suppose $r \in R$ and $rM = \{0\}$ for any simple left R-module M. Let L be a maximal left ideal of R. Then, R/L is a simple left R-module. Hence, $r(R/L) = \{0\}$, this means, $r \in L$. So, $r \in J(R)$. □

The left annihilator of a left R-module M is the twosided ideal

$$\text{ann}(M) = \{r \in R \mid rM = \{0\}\}.$$

In case $M = R/L$, with L a maximal left ideal of R, then

$$\text{ann}(R/L) = \{r \in R \mid rR \subseteq L\},$$

and this is the largest two-sided ideal contained in L (called the *kernel* of L).

Corollary 3.1.3 *Let R be a ring.*

1. *$J(R) = \cap ann(M)$, where the intersection is taken over all simple left R-modules M. So, $J(R)$ is a two-sided ideal of R.*

2. *$r \in J(R)$ if and only if $1 - arb$ is invertible in R for all $a, b \in R$.*

Proof. Part (1) is obvious.

We prove (2). Let $r \in J(R)$. Because of (1), for any $b \in R$, $rb \in J(R)$. Thus by Lemma 3.1.2, there exists $u \in R$ so that $u(1 - arb) = 1$. Also, $arb \in J(R)$ and thus the element $1 - (-u)arb$ has a left inverse. It follows that

$$u = 1 + uarb$$

has a left and right inverse. So $u \in U(R)$ and hence $1 - arb \in U(R)$.

If $1 - arb \in U(R)$ for any $a, b \in R$, then it follows from Lemma 3.1.2 that $r \in J(R)$. □

Corollary 3.1.4 *Let R be a ring.*

1. *$J(R)$ is the largest left (and two-sided) ideal L so that $1 + L \subseteq U(R)$ (the group of invertible elements of R).*
2. *$J(R)$ is the intersection of all maximal right ideals.*

Proposition 3.1.5 *Let R be a ring and I an ideal contained in $J(R)$.*

1. *$J(R/I) = J(R)/I$,*
2. *$J(R/J(R)) = \{0\}$.*

Proo.f Because $I \subseteq J(R)$ we get that I is contained in every maximal left ideal of R. Moreover, the maximal left ideals of R/I are the sets L/I with L a maximal left ideal of R that contains I. Hence (1) follows.

Part (2) is clear. □

Let M be a simple left R-module. Because of Corollary 3.1.3

$$J(R)M = \{0\}.$$

Hence, M is also a left $R/J(R)$-module for the operation

$$R/J(R) \times M \to M; (\overline{r}, m) \mapsto rm.$$

Clearly M is a simple $R/J(R)$-module.

Conversely, if N is a simple $R/J(R)$-module, then it also is an R-module for the operation

$$R \times N \to N : (r, n) \mapsto \overline{r}n.$$

Clearly N is a simple R-module.

So, the simple R-modules are the same as the simple $R/J(R)$-modules.

Note that $\overline{r} \in R/J(R)$ is left invertible if and only if $r \in R$ is left invertible. Indeed, let $\overline{u} \in \overline{R} = R/J(R)$ such that $\overline{ur} = \overline{1}$. Then, $1 - ur \in J(R)$ and thus $ur \in 1 + J(R) \subseteq U(R)$. So, there exists $v \in U(R)$ such that $vur = 1$. Hence r has a left inverse in R. The converse is obvious.

Definition 3.1.6 *A ring R is said to be semiprimitive (or J-semisimple) if $J(R) = \{0\}$.*

3.2 Nilpotent and nil ideals

Definition 3.2.1 *A (left) ideal L of a ring R is nil if all its elements are nilpotent; L is said to be nilpotent if $L^n = \{0\}$ for some $n \in \mathbf{N}_0$ (that is, $l_1 \cdots l_n = 0$ for all $l_i \in L$).*

The ideal $(\overline{6})$ of $\mathbf{Z}_{24}$ is nilpotent. In a commutative ring R, the ideal Rr is nilpotent if and only if r is a nil element. This is not true anymore in non-commutative rings. For example the elementary matrix E_{12} is a nilpotent element in $M_2(\mathbf{Z})$. But the left ideal $M_2(\mathbf{Z})E_{12}$ is not nilpotent (not even nil) as it contains the idempotent E_{22}.

Clearly a nilpotent ideal is a nil ideal. The following example shows that the converse is false. For example, let

$$R = \mathbf{Z}[X_1, X_2, \cdots]/(X_1^2, X_2^3, X_3^4, \cdots).$$

The ideal $(\overline{X_1}, \overline{X_2}, \cdots)$ is nil, but is not nilpotent.

Lemma 3.2.2 *Let R be a ring and $L_1, L_2, \cdots, L_n$ left ideals of R.*

1. *If L_i is nil then $L_i \subseteq J(R)$.*
2. *If every L_i is nilpotent then $L_1 + \cdots + L_n$ is nilpotent.*

Proof. We first prove (1). So let L be a nil left ideal of R. Assume $l \in L$ and n a positive integer so that $l^n = 0$. Then

$$(1 - l)(1 + l + \cdots + l^{n-1}) = 1 - l^n = 1.$$

So $1 - l$ is invertible. Hence, $1 + L \subseteq U(R)$. Corollary 3.1.4 therefore yields that $L \subseteq J(R)$.

We now prove (2). By induction it is sufficient to deal with the case $n = 2$. Suppose thus that L_1 and L_2 are two nilpotent left ideals so that $L_1^n = L_2^m = \{0\}$. Consider a product

$$(a_1 + b_1)(a_2 + b_2) \cdots (a_{n+m} + b_{n+m})$$

with all $a_i \in L_1$ and all $b_i \in L_2$. This product is a sum of terms that are products of $n+m$ elements. Of the latter, either at least n factors belong to L_1, or at least m factors belong to L_2. Because L_1 and L_2 are left ideals it follows easily that all these products are zero. □

Proposition 3.2.3 *If R is a left Artinian ring, then $J(R)$ is the largest nilpotent left ideal, and the largest nilpotent right ideal. It follows that in this case every nil left ideal is nilpotent.*

Proof. Because of Lemma 3.2.2, it is sufficient to show that the ideal $J = J(R)$ is nilpotent. Clearly

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots$$

Because, by assumption, R is left Artinian, there exists a positive integer n so that $J^n = J^{n+k}$ for all $k \in \mathbf{N}$. We now claim that $J^n = \{0\}$. Suppose the contrary, then there exists a left ideal L minimal for the condition

$$J^n L \neq \{0\}.$$

Let $l \in L$ be such that $J^n l \neq \{0\}$. Then

$$J^n(J^n l) = J^{2n} l = J^n l \neq \{0\}.$$

Because of the minimality we obtain $J^n l = L$. So, there exists $r \in J^n \subseteq J(R)$ with $rl = l$. Hence $(1-r)l = 0$. Because $1 - r \in U(R)$ this yields $l = 0$, a contradiction. This proves the claim, and hence the result follows. □

Theorem 3.2.4 *The following conditions are equivalent for a ring R:*

1. *R is semisimple,*
2. *R is J-semisimple and left Artinian,*
3. *R is J-semisimple and R satisfies the descending chain condition on principal left ideals.*

Proof. We first prove (1) implies (2). So suppose R is semisimple. Let $J = J(R)$. From Corollary 2.3.7 we know that R is left Artinian. Moreover, there exists a left ideal L of R so that $R = J \oplus L$. Hence there exist idempotents $e_1, e_2 \in R$ such that $J = Re_1$ and $L = Re_2$ (and $1 = e_1 + e_2$). Because $e_1 \in J$ it follows that $e_2^2 = e_2 = 1 - e_1 \in U(R)$. Hence $e_2 = 1$ and thus $e_1 = 0$. So $J = \{0\}$.

(2) implies (3) is obvious.

To prove (3) implies (1), suppose R is J-semisimple and suppose R satisfies the descending chain condition on left principal ideals. It follows that every nonzero left ideal has a minimal left ideal. Moreover, every minimal left ideal L is a direct summand of ${}_RR$. Indeed, because $J(R) = \{0\}$ and $L \neq \{0\}$, there exists a maximal left ideal M of R so that $L \not\subseteq M$. It follows that $L + M = R$ and $L \cap M = \{0\}$. So $R = L \oplus M$. Suppose now that R is not semisimple. Let L_1 be a minimal left ideal of R and M_1 a left ideal so that

$$R = L_1 \oplus M_1.$$

Then $M_1 \neq \{0\}$ and thus there exists a minimal left ideal $L_2 \subseteq M_1$ so that

$$R = L_2 \oplus M_2'$$

for some left ideal M_2'. Put $M_2 = M_1 \cap M_2'$. Then

$$R = L_1 \oplus L_2 \oplus M_2.$$

Repeating this process we get a descending chain of left ideals

$$M_1 \supset M_2 \supset M_3 \cdots$$

Because every M_i is a direct summand of R we also know that each M_i is a principal left ideal. This yields a contradiction. □

Rings that satisfy the descending chain condition on principal left ideals are called right perfect.

3.3 Examples

Example 3.3.1 *The ring* $\mathbf{Z}$ *is semiprimitive, that is*

$$J(\mathbf{Z}) = \{0\}.$$

Proof. The ring $\mathbf{Z}$ has infinitely many maximal ideals $p\mathbf{Z}$ (p prime) and

$$J(\mathbf{Z}) = \cap_{p \text{ prime}} p\mathbf{Z} = \{0\}.$$

□

This result can be extended to any principal ideal domain with infinitely many maximal ideals. Or even more general, to any ring of integers in a number field K (thus $\dim_{\mathbf{Q}} K < \infty$)

Example 3.3.2 *For any ring R,*

$$J(M_n(R)) = M_n(J(R)).$$

Proof. First we show that $M_n(J(R)) \subseteq J(M_n(R))$. To show this inclusion it is sufficient to show that $rE_{ij} \in J(M_n(R))$ for every $r \in J(R)$. So we have to show that $B = 1 - ArE_{ij} \in U(M_n(R))$ for any $A \in M_n(R)$. Write

$$A = \sum_{k,l} a_{kl} E_{kl}$$

with all $a_{kl} \in R$. Then

$$\begin{aligned} B &= 1 - ArE_{ij} \\ &= 1 - \sum_k a_{ki} r E_{kj} \\ &= 1 - a_{ji} r E_{jj} - \sum_{k \neq j} a_{ki} r E_{kj} \end{aligned}$$

Let $\alpha = \sum_{k \neq j} a_{ki} r E_{kj}$. Then, $\alpha^2 = 0$. Because $r \in J(R)$ we know that $1 - a_{ji} r$ is invertible in R. Let its inverse be $1 - b$ with $b \in R$. So $1 - bE_{jj} = (1 - a_{ji} r E_{jj})^{-1}$. Consequently,

$$(1 - bE_{jj})B = 1 - (1 - bE_{jj}) \sum_{k \neq j} a_{ki} r E_{kj} = 1 - \sum_{k \neq j} a_{ki} r E_{kj}$$

Now,

$$\left(1 - \sum_{k \neq j} a_{ki} r E_{kj}\right)^{-1} = 1 + \sum_{k \neq j} a_{ki} r E_{kj}.$$

So $(1 - bE_{jj})B$ and thus also B is invertible.

To prove the converse inclusion, we first note that

$$J(M_n(R)) = M_n(I)$$

for some ideal I of R. Let $r \in I$ and thus $r1 \in M_n(I)$. Hence $1 - ar1 = (1 - ar)1$ is invertible for all $a \in R$. So $1 - ar \in U(R)$ for all $a \in R$, and thus $r \in J(R)$. □

Example 3.3.3 *A skew field and a simple ring are semiprimitive.*

Example 3.3.4 *Let K be a field, then*

$$J(K[[X]]) = XK[[X]].$$

Note that $K[[X]]$ is a domain.

Proof. The only maximal ideal of $K[[X]]$ is the ideal $K[[X]]X$ (because every power series with nonzero constant term is invertible). □

Example 3.3.5 *Let $UT_n(K)$ be the ring of all $n \times n$ upper triangular matrices over a field K. Then $J(UT_n(K)$ is the ideal of all strict upper triangular matrices.*

Proof. Let $R = UT_n(K)$ and let J be the ideal of all strict upper triangular matrices. Note that $J^n = \{0\}$ and

$$\begin{aligned} R/J &\cong \left\{ \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix} \mid a_{ii} \in R,\ 1 \leq i \leq n \right\} \\ &\cong K \times \cdots \times K \end{aligned}$$

Thus R/J is semisimple and $J \subseteq J(R)$. Because of Theorem 3.2.4 we know that $J(R/J) = \{0\}$ and thus by Proposition 3.1.5, $J(R) = J$. □

Also note that because of the remark before Definition 3.1.6 we obtain that (up to isomorphism) there are precisely n simple left R-modules, say $M_1, \cdots, M_n$, each one dimensional over K. Write $M_i = {}_RK$. Then, for every $d \in M_i$,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix} \cdot d = a_{ii}d$$

Theorem 3.3.6 *(Maschke) Let R be a ring and G a finite group. Then $R[G]$ is semisimple if and only if R is semisimple and $|G|1 \in U(R)$.*

Proof. The proof is similar as in the case k is a field. □

Note that the mapping

$$\omega : RG \to R : \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g$$

is a ring epimorphism. So if RG is semisimple then so is R (by Proposition 2.3.2). Conversely, if R is semisimple, then $R = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ for some division algebras $D_1, \cdots, D_k$. It follows that

$$\begin{aligned} RG &\cong M_{n_1}(D_1)G \times \cdots \times M_{n_k}(D_k)G \\ &\cong M_{n_1}(D_1G) \times \cdots \times M_{n_k}(D_kG) \end{aligned}$$

So if all D_iG are semisimple then so are all $M_{n_i}(D_iG)$ and thus also RG.

Example 3.3.7 *Let R be a nonzero ring. If G is an infinite group then $R[G]$ is not semisimple.*

Proof. Suppose RG is semisimple and let $I = \ker(\omega)$, where $\omega : RG \to R$ is the augmentation map. Then there exists a left ideal L of RG so that

$$RG = I \oplus L.$$

Hence there exist non-zero orthogonal idempotents e and f in RG so that

$$I = (RG)e \text{ and } L = (RG)f.$$

Because $g - 1 \in I$ (for any $g \in G$) we get

$$(g-1)f = (g-1)ef = 0.$$

So, $gf = f$ for all $g \in G$. Write

$$f = \sum_{h \in G} f_h h$$

(note that only a finite number of the coefficients f_h are nonzero). If $f_h \neq 0$, then

$$gf = \sum_{h \in G} f_h gh = \sum_{h \in G} f_h h.$$

Hence $f_{gh} \neq 0$ for all $g \in G$. But then infinitely many coefficients f_h are nonzero, a contradiction. □

Example 3.3.8 *If R is a ring so that $S = U(R) \cup \{0\}$ is a skew field, then $J(R) = \{0\}$. In particular the following rings are semiprimitive (D is a skew field): free algebras $D\langle x_i \mid i \in I\rangle$, polynomial rings in commuting variables $D[x_i \mid i \in I]$, skew polynomial rings $D[X, \sigma]$ (σ an automorphism of D) and a derivation ring $D[X, \delta]$.*

Proof. Indeed, $J(R) \cap S = \{0\}$. Thus, if $r \in J(R)$ then $1 + r \in U(R) \subseteq S$. Hence, $r \in S \cap J(R) = \{0\}$. So $J(R) = \{0\}$. □

If K is a field then

$$J(K[X, X^{-1}]) = \{0\}.$$

This is because the only invertible elements of $K[X, X^{-1}]$ are the polynomials of the form kX^i with $0 \neq k \in K$ and i an integer. Hence, by Theorem 3.2.4 and Example 3.3.7, we get that $K[X, X^{-1}]$ is not Artinian. Of course, the latter can be proved in a simple and direct manner.

Proposition 3.3.9 *Let K be a field and R a K-algebra.*

1. *$r \in J(R)$ is algebraic over K if and only if r is nilpotent.*
2. *If R is algebraic over K, then $J(R)$ is the largest nil ideal of R. (For example, R is a group algebra of a locally finite group G, such as for example a torsion abelian group.)*

Proof. Suppose $r \in R$ is nilpotent, that is $r^n = 0$ for some positive integer n. Of course r is then an algebraic element. Conversely, assume $r \in J(R)$ is algebraic over K. Then,

$$r^n + k_1 r^{n+1} + \cdots + k_l r^{n+l} = 0$$

for some $k_i \in K$. Because $1 + k_1 r + \cdots + k_l r^l \in 1 + J(R) \subseteq U(R)$, we get that $r^n = 0$. Hence $n \geq 1$ and r is nilpotent.

Part (2) follows from part (1) and the fact that $J(R)$ contains all nil ideals. □

3.4 Hopkins-Levitzki and Nakayama results

Theorem 3.4.1 *(Hopkins-Levitzki) Let R be a ring so that $J(R)$ is nilpotent and $\overline{R} = R/J(R)$ is semisimple (one says R is semiprimary). The following are equivalent for a left R-module M;*

1. *M is Noetherian,*
2. *M is Artinian,*
3. *M has a composition series.*

In particular, a ring R is left Artinian if and only if R is semiprimary and left Noetherian. Furthermore, it follows that every finitely generated left module over a left Artinian ring has a composition series.

Proof. We only have to prove that (1) implies (3), and (2) implies (3). So suppose ${}_R M$ is Noetherian or Artinian. Let n be a positive integer so that $J^n = \{0\}$ (with $J = J(R)$). Consider the descending chain

$$M \supseteq JM \supseteq J^2M \supseteq \cdots \supseteq J^nM = \{0\}.$$

Now, every $J^iM/J^{i+1}M$ is an $\overline{R}$-module, and its module structure is the same as that of its R-module structure. Now, every $J^iM/J^{i+1}M$ is Noetherian or Artinian as an R-module (and thus also as an $\overline{R}$-module). Since $\overline{R}$ is semisimple, each $J^iM/J^{i+1}M$ is a direct sum of simple $\overline{R}$-modules (and thus as simple R-modules). Because of the chain condition, the direct sum is a finite sum. Hence, every $J^iM/J^{i+1}M$ has a composition series. It follows that also M has a composition series. □

Theorem 3.4.2 *(Nakayama's Lemma) Let R be a ring and L a left ideal. The following are equivalent:*

1. $L \subseteq J(R)$.
2. *for every finitely generated left R-module M:*

$$\text{if } LM = M \text{ then } M = \{0\}.$$

3. *for all left R-modules $N \subseteq M$ with M/N finitely generated:*

$$\text{if } N + LM = M \text{ then } N = M.$$

Proof. First we show (1) implies (2). Suppose M is a finitely generated module and $M \neq \{0\}$. Because of Zorn's Lemma, M contains a maximal submodule M' (note that $M' \neq M$). So, M/M' is a simple module and thus $L(M/M') = \{0\}$. It follows that

$$LM \subseteq M'$$

and thus

$$LM \neq M.$$

That (2) implies (3) is obvious.

To prove (3) implies (1), suppose $L \not\subseteq J(R)$. Then there exists a maximal left ideal M of R so that $L \not\subseteq M$. It follows that

$$L + M = R$$

and thus

$$M + LR = R.$$

Because of (3) this implies $M = R$, a contradiction. □

3.5 Von Neumann Regular Rings

Theorem 3.5.1 *The following are equivalent for a ring R:*

1. *for all $r \in R$ there exists $x \in R$ so that $r = rxr$.*
2. *Every principal left ideal is generated by an idempotent.*
3. *Every principal left ideal is a direct summand of R_R.*
4. *Every finitely generated left ideal is generated by an idempotent.*
5. *Every finitely generated left ideal is a direct summand of R_R.*

A ring that satisfies these conditions is called Von Neumann regular (J. Von Neumann, 1903 - 1957) .

Proof. (1) implies (2). Let $a \in R$ and consider the principal left ideal Ra. Let $x \in R$ be such that $axa = a$. Then $e = xa$ is an idempotent. Indeed,

$$e = xa = xaxa = e^2.$$

Clearly $Re \subseteq Ra$. As $a = ae$ it follows that $Ra = Re$.

(2) implies (1). Let $a \in R$. Then $Ra = Re$ for some idempotent $e \in R$. Write $a = ye$ and $e = xa$ for some $x, y \in R$. Then,

$$axa = (ye)e = ye^2 = ye = a.$$

(2) implies (4). It is sufficient to show that for idempotents $e, f \in R$ the left ideal $L = Re + Rf$ is generated by an idempotent. Because $f = f(e + (1 - e))$ we get that

$$Rf = Rf(e + (1 - e)) \subseteq Re + Rf(1 - e) \subseteq Re + Rf.$$

Hence

$$L = Re + Rf = Re + Rf(1 - e).$$

Now, $Rf(1 - e) = Re'$ for some idempotent $e' \in R$. Note that $e'e = 0$. Consequently, $e'(e' + e) = e'$ and thus, for any $r_1, r_2 \in R$:

$$\begin{aligned} r_1e + r_2e' &= r_1(e + e') + (r_2 - r_1)e'(e' + e) \\ &= (r_1 + (r_2 - r_1)e')(e' + e) \end{aligned}$$

It follows that

$$L = Re + Rf(1-e) = Re + Re' = R(e+e')$$

and thus

$$L = Re''$$

for some idempotent $e'' \in R$.

(4) implies (2) is obvious.

That (2) and (3) are equivalent, and that (4) and (5) are equivalent is well known. □

Corollary 3.5.2 *Every semisimple ring is Von Neumann regular. Every Von Neumann regular ring is J-semisimple.*

Proof. The first part is clear. To prove the second part, suppose R is Von Neumann regular. Then for $0 \neq r \in J(R)$ there exists an idempotent $e \in R$ so that $Rr = Re$. But then $e \in J(R)$ and thus $1-e$ is invertible. Because $e(1-e) = 0$ we thus obtain that $e = 0$, a contradiction. Hence $J(R) = \{0\}$. □

Corollary 3.5.3 *A ring R is semisimple if and only if R is left Noetherian and Von Neumann regular. If these conditions are satisfied, then R is also Artinian.*

Proposition 3.5.4 *Let M be a semisimple left module over a ring R. Then $E = End_R(M)$ is Von Neumann regular.*

Proof. Let $f \in E$ and $K = \ker f$. Suppose ${}_RN \leq {}_RM$ so that

$$M = K \oplus N.$$

Then, $N \cong f(N)$ and let ${}_RN' \leq {}_RM$ so that $M = f(N) \oplus N'$. Define

$$g : M = f(N) \oplus N' \to M$$

so that $g(N') = 0$ and $g_{|f(N)} = \left(f_{|N}\right)^{-1}$. Then,

$$fgf = f.$$

□

3.6 Linear groups and the Burnside problem

In Algebra I we showed that there is a close relationship between the representation theory of a finite group G and the module and ring structure of the finite dimensional algebra kG. We proved this for an algebraically closed field k and in case $\mathrm{char}(k)$ does not divide the order of the group G. One can also show this for some fields that are not necessarily algebraically closed.

We now show that in the study of infinite groups G one can sometimes also make use of ring and module theory. We do this for linear groups G. These are by definition subgroups of $\mathrm{GL}(V)$, with V a finite dimensional vector space over a field k.

Note that V is in a natural way a right and left $k < G >$-module (here we denote by $k < G >$ the k-algebra of $\mathrm{End}(V_k)$ generated by G; this algebra is finite dimensional over k). Hence, V is in a natural way a right and left kG-module (via the epimorphism of kG onto $k < G >$). We identify $\mathrm{End}(V_k)$ with $M_n(k)$ (with $n = \dim_k V$).

Suppose G is a subgroup of $\mathrm{GL}_n(k)$ and thus k^n is a right kG-module. Let $R = k < G >$. If k is algebraically closed and k^n is a simple right kG-module, then k^n is a simple $R/J(R)$-module. Since $R/J(R)$ is semsimple (as R is finite dimensional) we know, from Corollary 2.5.7, that $R/J(R) \cong M_{n_1}(k) \oplus \cdots \oplus M_{n_l}(k)$. Moreover, there exists an i so that $n_i = n$. Hence the natural homomorphism

$$kG \to R/J(R) \to M_n(k)$$

is surjective.

Lemma 3.6.1 *(Trace Lemma) Let k be an algebraically closed field and G a subgroup of $GL_n(k)$ such that k^n is a simple kG-module. Let $tr : G \to k$ denote the trace map. If $|tr(G)| = r < \infty$ then $|G| \leq r^{(n^2)}$.*

Proof. Because $kG \to M_n(k)$ is surjective there exist $g_1, \cdots, g_{n^2} \in G$ that form a k-basis for $M_n(k)$. Define

$$T : M_n(k) \to k^{n^2} : A \mapsto (\mathrm{tr}(Ag_1), \cdots, \mathrm{tr}(Ag_{n^2})).$$

Clearly T is k-linear. We now show that it is a k-monomorphism (and thus a k-isomorphism). Suppose therefore that $A = (a_{ij}) \in M_n(k)$ and $T(A) = 0$. Then we get

$$\mathrm{tr}(AB) = 0$$

for all $B \in M_n(k)$. In particular, $a_{ji} = \mathrm{tr}(AE_{ij}) = 0$ for all $1 \leq i, j \leq n$. Hence $A = 0$.

So we get $|G| = |T(G)| \leq r^{n^2}$. $\square$

A group G is said to be of exponent $n \in \mathbf{N}_0$ if $g^n = e$ for all $g \in G$ (where e is the identity of G) and n is the smallest such number.

Theorem 3.6.2 *Let k be a field of characteristic $p \geq 0$ and let G be a subgroup of $GL_n(k)$. If G is a group of exponent N and $p \not| N$ then $|G| \leq N^{(n^3)}$.*

Proof. We may assume that k is algebraically closed. If $n = 1$, then $G \subseteq k^*$. Then, all elements of G satisfy the equation $x^N = 1$ in k^*. Hence there are at most N different such elements.

Suppose thus that $n \geq 2$. Let $g \in G$. Then $g^N = e$ and thus every eigenvalue of g is a N-th root of unity. So, $\mathrm{tr}(g)$ is a sum of N-th roots of unity and hence $\mathrm{tr}(g)$ can have at most $r = N^n$ different values in k. So $|\mathrm{tr}(G)| \leq r < \infty$.

We consider two cases. First, k^n is a non-simple kG-module. Hence, making a proper choice of a k-basis for k^n, we get that every element $g \in G$ is of the following form

$$g = \begin{pmatrix} g_1 & h \\ 0 & g_2 \end{pmatrix},$$

with $g_1 \in \mathrm{GL}_{n_1}(k)$, $g_2 \in \mathrm{GL}_{n_2}(k)$ for some $1 \leq n_1, n_2 < n$. Let G_i be the group of all such matrices g_i, $1 \leq i \leq 2$. By induction we may suppose that

$$|G_i| \leq N^{n_i^3}$$

for $1 \leq i \leq 2$. Define

$$\varphi : G \to G_1 \times G_2 : g = \begin{pmatrix} g_1 & h \\ 0 & g_2 \end{pmatrix} \mapsto (g_1, g_2).$$

We now show that the morphism φ is injective. Suppose therefore that $g = \begin{pmatrix} g_1 & h \\ 0 & g_2 \end{pmatrix} \in \ker \varphi$. Then $g_1 = I_{n_1}$ and $g_2 = I_{n_2}$ and thus

$$I = g^N = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^N = \begin{pmatrix} 1 & Nh \\ 0 & 1 \end{pmatrix}$$

Hence $Nh = 0$. Because, by assumption, p does not divide $|N|$ we get that $h = 0$ and thus $g = I$.

It follows that

$$|G| \leq |G_1|\,|G_2| \leq N^{n_1^3+n_2^3} \leq N^{(n_1+n_2)^3} = N^{n^3}.$$

In the second case we have that k^n is a simple kG-module. So by the trace lemma we get that $|G| \leq r^{n^2}$. $\square$

Note that if k has characteristic $p > 0$, then

$$G = \left\{ \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \mid h \in k \right\} \subseteq \mathrm{GL}_2(k)$$

and G has exponent p, but $|G| = |k|$ is not necessarily finite.

Definition 3.6.3 *A group is said to be periodic if all its elements have finite order.*

Lemma 3.6.4 *Let G be a group with abelian subgroup H of finite index. If G is finitely generated and periodic then G is finite.*

Proof. Because H has finite index

$$G = g_1 H \cup \cdots \cup g_m H$$

for some $g_1, \cdots, g_m \in G$. Let $g_{m+1}, \cdots, g_n \in G$ be such that $G = \langle g_1, \cdots, g_m, g_{m+1}, \cdots, g_n \rangle$ and $g_i^{-1} \in \{g_1, \cdots, g_n\}$ for all $1 \leq i \leq n$. Now, for every $1 \leq i, j \leq n$ there exist $h_{ij} \in H$ and $1 \leq r \leq m$ so that

$$g_i g_j = g_r h_{ij}.$$

Let $H_0 = \langle h_{ij} \mid 1 \leq i, j \leq n \rangle$. Because H_0 is abelian and periodic, H_0 is finite. Now, for every $1 \leq s \leq n$,

$$g_s g_i g_j = g_s g_r h_{ij} = g_t h_{s,r} h_{ij} \in g_t H_0$$

for some $t \leq m$. It follows that (note that $g_i^{-1} \in \{g_1, \cdots, g_n\}$)

$$G = \langle g_i \mid 1 \leq i \leq n \rangle \subseteq \cup_{i=1}^n g_i H_0 \subseteq G.$$

So $G = \cup_{i=1}^n g_i H_0$ is finite. □

Lemma 3.6.5 *Let k be a field and G a finitely generated periodic subgroup of $GL_n(k)$. Then G has finite exponent.*

Proof. Let $F = \mathbf{Z}_p$ if $p = \mathrm{char}(k) > 0$, otherwise let $F = \mathbf{Q}$. Because every element $g = (a_{ij}) \in \mathrm{GL}_n(k)$ and because G is finitely generated, it is sufficient to show the result assuming that k is finitely generated as a field over F. It follows that there exists a purely transcendental extension $k_0 \subseteq k$ of F such that $\dim_{k_0} k = r < \infty$. Now, as k_0-modules,

$$k^n = k_0^{rn}$$

and thus $G \subseteq U(\mathrm{End}_k(k^n)) \subseteq U(\mathrm{End}_{k_0}(k_0^{rn})) = \mathrm{GL}_{rn}(k_0)$. Hence we may assume that

$$G \subseteq \mathrm{GL}_{rn}(k_0).$$

Let $g \in G$ and let $m_g(X) \in k_0[X]$ be the polynomial of minimal degree with leading coefficient 1 such that $m_g(g) = 0$ (i.e. $m_g(X)$ is the minimal polynomial of g). We now consider separately the cases $F = \mathbf{Q}$ and $F = \mathbf{Z}_p$.

First assume $F = \mathbf{Q}$. Because g has finite order, say l, we have $g^l = 1$ and thus $m_g(X) | (X^l - 1)$. Hence the roots of $m_g(X)$ are l-th roots of unity. In particular, they are algebraic integers. Hence the coefficients of $m_g(X)$ are also algebraic integers. Because $k_0 = \mathbf{Q}(X_1, \cdots, X_n)$ the only algebraic integers in k_0 are the elements of $\mathbf{Z}$. So $m_g(X) \in \mathbf{Z}[X]$. Further, because of Hamilton's Theorem, we know that g is a root of its characteristic polynomial P (recall that we consider g as an element in $M_{rn}(k_0)$). So $m_g(X) | P(X)$ and hence $\deg(m_g(X)) \leq \deg(P(X)) = rn$. Now, one can consider the coefficients of $m_g(X)$ as elementary symmetric functions in the roots of $m_g(X)$. Because these roots are

roots of unity in $\mathbf{C}$, the norm of these elementary functions (in the roots) is bounded by 2^{rn}. Hence the coefficients of $m_g(X) \in \mathbf{Z}[X]$ are bounded by the number 2^{rn}. So, there are only finitely many possibilities for $m_g(X)$ when g runs through the group G. Because $m_g(X)$ uniquely determines the order of g, we get that G has finite exponent.

In case $F = \mathbf{Z}_p$ it is clear that there are only finitely many possible $m_g(X)$. Hence the result also follows. □

Theorem 3.6.6 *(Schur) Let k be a field. A finitely generated periodic subgroup G of $GL_n(k)$ is finite.*

Proof. Because of Lemma 3.6.5, G has finite exponent. One can now prove the result as in Theorem 3.6.2 (only in the last part does the proof differ in case k^n is not a simple kG-module). Consider again the mapping

$$\varphi : G \to G_1 \times G_2.$$

By induction the groups G_1 and G_2 are finite. Hence

$$\ker \varphi = \left\{ \begin{bmatrix} I & h \\ 0 & I \end{bmatrix} \in G \right\}$$

is of finite index in G. As $\ker \varphi$ is an abelian group, Lemma 3.6.4 the implies that G is finite. □

A group G is said to be locally finite if every finitely generated subgroup is finite.

Corollary 3.6.7 *A linear group $G \subseteq GL_n(K)$ over a field K is periodic if and only if G is locally finite.*

In 1902 Burnside posed the following problem:

(GBP) Is an arbitrary periodic group locally finite?

(RBP) Is an arbitrary periodic group of finite exponent locally finite?

We have shown that (GBP) has positive answer if G also is a linear group. In 1964, Golod constructed for every prime number p an infinite p-group generated by two elements. In 1968, Novikov and Adjan showed that (RBP) is not valid if N is odd and $N \geq 4381$. For other values of N the problem mainly remains unsolved.

In 1982, Lichtman proved that (GBP) also holds for periodic subgroups of $\mathrm{GL}_n(D)$, with D a skew field.

3.7 Exercises

1. Compute $J(\mathbf{Z}_n)$.

2. Let R be a ring. Prove that every maximal ideal of R is the annihilator of a simple left R-module. Show that the converse is false.

3. Let R be a ring and let $\mathcal{B}(R)$ denote the intersection of all maximal ideals of R (this is called the Brown-McCoy radical of R). Prove that $J(R) \subseteq \mathcal{B}(R)$. Give an example of a ring R such that $J(R)$ is strictly contained in $\mathcal{B}(R)$. Show that if R is commutative then $J(R) = \mathcal{B}(R)$.

4. Let $f : R \to S$ be a ring epimorphism. Prove that $f(J(R)) \subseteq J(S)$ and give an example where the inclusion is strict.

5. Prove that $J(R)$ is the smallest ideal I of a ring R so that R/I is J-semisimple.

6. Let R be a ring and $I = \cap_{x \in X} I_x$, where I_x is an ideal of R for each $x \in X$. Prove:

   (a) If every R/I_x is J-semisimple then R/I is J-semisimple.

   (b) If X is finite and each R/I_x is semisimple then R/I is semisimple.

7. Let $R = \prod_{i \in I} R_i$, a direct product of rings. Prove that $J(R) = \prod_{i \in I} J(R_i)$.

8. Let R be the ring of all continuous real functions on a topological space X. Prove:

   (a) the intersection of all maximal ideals is $\{0\}$, and thus $\mathcal{B}(R) = J(R) = \{0\}$.

   (b) suppose $|X| > 1$ and X is connected and compact Hausdorff. Then, the only idempotents in R are the functions 0 and 1. Prove also that if R is Von Neumann regular then R is a field.

9. For a commutative Noetherian ring R one can prove that $\cap_{n\geq 1} J(R)^n = \{0\}$ (this is Krull's Intersection Theorem). Prove that this theorem no longer holds for arbitrary non-commutative rings R.

10. Let G be a subgroup of $\mathrm{GL}_n(k)$, with k a field. Prove that G is a finite conjugacy group (that is, all conjugacy classes of G are finite) if and only if $[G : Z(G)] < \infty$. Prove then that every finite group is a linear group, but not every infinite group is linear.

Chapter 4

Prime and primitive rings

In commutative ring theory we have seen three special classes: reduced rings, domains and fields. These one also can consider in the non-commutative setting: reduced rings, domains and skew fields. The latter are defined in an elementwise manner. However, also a definition can be given using ideals. One then obtains semiprime rings, prime rings and left (respectively right) primitive rings. These will be studied in this chapter.

4.1 Prime rings

Recall that an ideal P of a ring R is said to be a *prime ideal* if $P \neq R$ and the following property holds for all ideals I and J of R:

$$\text{if } IJ \subseteq P \text{ then } I \subseteq P \text{ or } J \subseteq P.$$

Equivalent conditions are, for all $a, b \in R$:

$$\text{if } aRb \subseteq P \text{ then } a \in P \text{ or } b \in P;$$

or

$$\text{if } (a)(b) \subseteq P \text{ then } a \in P \text{ or } b \in P.$$

One more equivalent condition is, for all left ideals L_1, L_2 in R:

$$\text{if } L_1 L_2 \subseteq P \text{ then } L_1 \subseteq P \text{ or } L_2 \subseteq P.$$

Also recall that every maximal ideal is a prime ideal and that a proper ideal P in a commutative ring is prime if $R \setminus P$ is a multiplicatively closed set.

Definition 4.1.1 *An m-system in a ring R is a a non-empty subset S of R so that for every $s_1, s_2 \in S$ there exists $r \in R$ so that $s_1 r s_2 \in S$.*

Clearly an ideal P of a ring R (with $P \neq R$) is a prime ideal if and only if $R \setminus P$ is an m-system.

If R is a ring and $r \in R$ then the following sets are m-systems: $\{r, r^2, r^4, r^8, \cdots\}$ and $\{r, r^2, r^3, \cdots\}$.

Proposition 4.1.2 *Let $S \subseteq R$ be an m-system in a ring R and P an ideal of R maximal with respect to the condition $P \cap S = \emptyset$. Then P is a prime ideal of R.*

Proof. Suppose $IJ \subseteq P$ for some ideals I and J with $I \not\subseteq P$ and $J \not\subseteq P$. Because of the "maximal condition" there exist $s, s' \in S$ so that $s \in P + I$ and $s' \in P + J$. Let $r \in R$ be such that $srs' \in S$. Then

$$srs' \in (P + I)R(P + J) \subseteq P + IJ \subseteq P,$$

a contradiction. So, P is a prime ideal. □

Definition 4.1.3 *For an ideal I of R we denote*

$$\sqrt{I} = \{r \in R \mid I \cap S \neq \emptyset, \text{ for every } m - \text{system } S \text{ with } r \in S\}.$$

Because $\{r, r^2, r^3, \cdots\}$ is an m-system for every $r \in R$ we get

$$\sqrt{I} \subseteq \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}.$$

In case R is commutative then $\sqrt{I} = \{r \in R \mid r^n \in I, \text{ for some } n \geq 1\}$. Indeed, suppose $s \in R$ and $s^n \in I$ for some $n \geq 1$. Let S be an m-system so that $s \in S$. Because R is commutative and because of the definition of m-system there exists an $r \in R$ so that $s^n r \in S$. But then $s^n r \in S \cap I$ and thus $s \in \sqrt{I}$. So, for commutative rings, $\sqrt{I}$ is an ideal and $R/\sqrt{I}$ is a reduced ring. We now show that $\sqrt{I}$ always is an ideal and we will write $\sqrt{I}$ as an intersection of prime ideals.

Theorem 4.1.4 *Let I be an ideal in a ring R. Then $\sqrt{I}$ is the intersection of all prime ideals that contain I. In particular, $\sqrt{I}$ is an ideal of R.*

Proof. Let $s \in \sqrt{I}$ and let P be a prime ideal containing I. Then $S = R \setminus P$ is an m-system. As $S \cap P = \emptyset$ we get that $s \in P$. Hence $\sqrt{I} \subseteq \cap_{I \subseteq P,\, P \text{ prime}} P$. Conversely, suppose $s \notin \sqrt{I}$. Hence there exists an m-system S with $s \in S$ and $I \cap S = \emptyset$. Because of Zorn's Lemma there exists an ideal P of R, with $I \subseteq P$, and maximal with respect to the condition $P \cap S = \emptyset$. Proposition 4.1.2 yields that P is a prime ideal. So $s \notin \cap_{I \subseteq P,\, P \text{ prime}} P$. □

Also for non-commutative rings has $R/\sqrt{I}$ a property that corresponds with being reduced in the case of commutative rings. In order to state this we first give the following definition.

Definition 4.1.5 *An ideal I of a ring R is said to be semiprime if $J^2 \subseteq I$ implies $J \subseteq I$, for any ideal J of R.*

Prime ideals are semiprime ideals. In the ring $\begin{bmatrix} \mathbf{Q} & \mathbf{Q} \\ \{0\} & \mathbf{Q} \end{bmatrix}$ is $\begin{bmatrix} \{0\} & \mathbf{Q} \\ \{0\} & \{0\} \end{bmatrix}$ a semiprime ideal that is not prime.

Proposition 4.1.6 *The following conditions are equivalent for an ideal I in a ring R:*

1. *I is semiprime,*
2. *for any $r \in R$, $(RrR)^2 \subseteq I$ implies $r \in I$.*
3. *for any $r \in R$, $rRr \subseteq I$ implies $r \in I$; that is, $R \setminus I$ is an n-system.*
4. *for every left ideal L in R, $L^2 \subseteq I$ implies $L \subseteq I$.*
5. *for any right ideal V in R, $V^2 \subseteq I$ implies $V \subseteq I$.*

Proof. Exercise. □

Lemma 4.1.7 *Let $N \subseteq R$ be an n-system in a ring R and $s \in N$. Then there exists an m-system $S \subseteq N$ so that $s \in S$.*

Proof. We define $S = \{s_1, s_2, \cdots\}$ inductively as follows:

$$s_1 = s,\ s_{n+1} = s_n r_n s_n \in N \text{ (for some } r_n \in R).$$

Note that $s_{i+k} \in s_i R \cap R s_i$ for any $k \geq 0$, and any $i \geq 1$. Thus, for any i, j we get

$$s_{k+1} \in s_k R s_k \subseteq s_i R s_j$$

where $k = \max\{i, j\}$. Hence, $s_i R s_j \cap S \neq \emptyset$, and thus S is an m-system. □

Theorem 4.1.8 *The following conditions are equivalent for an ideal I in a ring R:*

1. *I is semiprime,*
2. *I is the intersection of prime ideals,*
3. *$I = \sqrt{I}$.*

Proof. First we show (1) implies (3). So, suppose I is semiprime and thus $R \setminus I$ is an n-system. So, because of Lemma 4.1.7, for every $r \in (R \setminus I)$, there exists an m-system $S \subseteq (R \setminus I)$ so that $r \in S$. Clearly $S \cap I = \emptyset$ and thus $r \notin \sqrt{I}$. It follows that $\sqrt{I} \subseteq I$ and thus $\sqrt{I} = I$.

Theorem 4.1.4 implies that (2) follows from (3).

We finish by showing that (2) implies (1). Write $I = \cap P$, where every P is a prime ideal. Let J be an ideal of R so that $J^2 \subseteq I$. Then, for every P we get $J^2 \subseteq P$. Since P is prime this yields $J \subseteq P$. Hence $J \subseteq I$. □

Note that $\sqrt{I}$ is the smallest semiprime ideal that contains I.

Definition 4.1.9 *The prime radical (or (Baer) lower nil radical, or Baer-McCoy radical) of R is*

$$\sqrt{\{0\}} = \cap_{P \text{ prime ideal}} P.$$

We denote this ideal by $B(R)$.

Proposition 4.1.10 *Let R be a ring.*

1. *$B(R)$ is a nil ideal that contains all nilpotent ideals.*
2. *$B(R) \subseteq J(R)$.*

Recall that a ring is said to be prime (respectively semiprime) if $\{0\}$ is a prime (respectively semiprime) ideal.

Proposition 4.1.11 *The following are equivalent for a ring R:*

1. *R is semiprime,*
2. *$B(R) = \{0\}$,*
3. *R has no nonzero nilpotent ideals,*
4. *R has no nonzero nilpotent left ideals.*

4.2 Examples

Example 4.2.1 *Domains and simple rings are prime.*

Example 4.2.2 *Reduced rings are semiprime.*

Example 4.2.3 *Von Neumann regular rings are J-semisimple and thus also semiprime.*

Example 4.2.4 *For any ring R, $B(M_n(R)) = M_n(B(R))$.*

Proof. The prime ideals of $M_n(R)$ are precisely the ideals $M_n(P)$ where P is a prime ideal. The result thus follows. □

Example 4.2.5 *For any ring R:*

1. *$R[X]$ is prime if and only if R is prime.*

2. *$R[X]$ is semiprime if and only if R is semiprime.*

3. *$B(R[X]) = B(R)[X]$.*

Proof. We only prove (3). If P is a prime ideal of R then $P[X]$ is an ideal of $R[X]$ and

$$R[X]/P[X] \cong (R/P)[X].$$

So, by (1), $P[X]$ is a prime ideal of $R[X]$. It follows that $B(R[X]) \subseteq B(R)[X]$. Let now P be an arbitrary prime ideal of $R[X]$. Then $R \cap P$ is a prime ideal of R. So, $B(R)[X] \subseteq (P \cap R)[X] \subseteq P$. Consequently, $B(R)[X] \subseteq B(R[X])$ and the result follows. □

Example 4.2.6 *For any ring R and any automorphism f of R:*

1. *$f(J(R)) = J(R)$ and $f(B(R)) = B(R)$,*

2. *$B(R/B(R)) = \{0\}$.*

Example 4.2.7 *If I is a nil ideal of a ring R and S/I is a nil subset of R/I, then $S + I$ is nil. Hence, every ring has a largest nil ideal (the sum of all nil ideals). This ideal is called the upper nil radical and it is denoted by*

$$Nil(T).$$

So,

$$B(R) \subseteq Nil(R) \subseteq J(R).$$

If R is commutative, then $B(R) = Nil(R)$.

Example 4.2.8 *Let R be a ring. By transfinite induction we define:*

$$\begin{aligned} N_1(R) &= \sum I, \text{ where the sum runs over all nilpotent ideals,} \\ N_\alpha(R) &= \{r \in R \mid r + N_\beta(R) \in N_1(R/N_\beta(R))\}, \text{ for } \alpha = \beta^+, \\ N_\alpha(R) &= \cup_{\beta<\alpha} N_\beta(R), \text{ for } \alpha \text{ a limit ordinal.} \end{aligned}$$

This yields an ascending chain of ideals and

$$N_\alpha(R) = N_{\alpha'}(R)$$

for all ordinals α, α' with $\alpha, \alpha' > |R|$. Now for such an ordinal α we have $N_\alpha(R) \subseteq B(R)$ and $R/N_\alpha(R)$ does not contain non-zero nilpotent ideals. Thus $B(R) = N_\alpha(R)$. Note that if $Nil(R)$ is nilpotent then $B(R) = Nil(R)$.

Example 4.2.9 *If R is a left Artinian ring, then $J(R)$ is the largest nilpotent ideal (and thus $J(R) = B(R) = Nil(R) = N_1(R)$).*

Theorem 4.2.10 *(Levitzki) If R is a left Noetherian ring, then every nil left ideal or right ideal is nilpotent.*

Proof. Let L be a nil left ideal of R. We first show that $L \subseteq B(R)$. Suppose the contrary, and choose an element $a \in L \setminus B(R)$ so that $l.ann_R(a)$ is maximal. Let $r \in R$. Suppose $ra \neq 0$. Then there exists an $n \in \mathbf{N}$ so that $(ra)^n \neq 0$ and $(ra)^{n+1} = 0$. Hence

$$(ra)^{n-1}r \notin l.ann_R(a)$$

but

$$(ra)^{n-1}r \in l.ann_R(ara).$$

Consequently

$$l.ann_R(a) \subset l.ann_R(ara),$$

a proper inclusion. However, since $ara \in L$ the maximality condition yields that

$$ara \in B(R).$$

Hence we have shown that

$$aRa \subseteq B(R).$$

Since $B(R)$ is a semiprime ideal we get that $a \in B(R)$, a contradiction.

Let N be a maximal nilpotent ideal in R. Then $N \subseteq B(R)$ and R/N does not have nonzero nilpotent ideals. So R/N is semiprime and $N = B(R)$ is nilpotent.

By the first part of the proof, every nil left ideal contained in $B(R)$, and thus it is nilpotent.

If aR is nil then so is Ra. Hence Ra is nilpotent. It follows that aR is nilpotent. This proves the result. □

Corollary 4.2.11 *If R is a left Noetherian ring, then the prime radical contains all nil left and right ideals. Thus, $B(R) = Nil(R) = N_1(R)$.*

4.3 Some properties and applications

Lemma 4.3.1 *(Brauer) Let L be a minimal left ideal in a ring R. Then either $L^2 = \{0\}$ or $L = Re$ for some idempotent $e \in L$.*

Proof. Suppose $L^2 \neq \{0\}$. Then $La \neq \{0\}$ for some $a \in L$ and thus $La = L$. Let $e \in L$ so that $a = ea$. Put

$$A = l.ann_L(a) = \{l \in L \mid la = 0\}.$$

Clearly A is a left ideal of R and $A \subset L$. Hence $A = \{0\}$. Because $e^2 - e \in L$ and $(e^2 - e)a = e(1 - e)a = e(a - ea) = 0$ we get $e^2 - e \in A = \{0\}$. So $e^2 = e$ and the result follows. □

We can now prove the analog of Theorem 3.2.4 for the prime radical.

Theorem 4.3.2 *Let R be a ring. The following are equivalent:*

1. *R is semisimple,*

2. *R is semiprime and left Artinian,*

3. *R is semiprime and satisfies the descending chain condition on principal left ideals.*

Proof. We only prove that (3) implies (1) (the other implications are clear). Because of Brauer's Lemma and condition (3) we obtain that every left ideal of R contains a direct summand of R (a minimal left ideal). One can then continue reasoning as in the proof of Theorem 3.2.4. □

Often one would like to know whether a particular nil subset of a ring is nilpotent. We deal with this question using the structure theorems.

Definition 4.3.3 *A subset S of a ring R is called weakly closed if for any $s_1, s_2 \in S$ there exists $v \in \mathbf{Z}$ so that*

$$s_1 s_2 + v s_2 s_1 \in S.$$

One calls, $s_1 s_2 + v s_2 s_1$ a weak product of s_1 and s_2 in S.

If $v = 0$ then S is multiplicatively closed. If $v = -1$ then this is the Lie product in R. If $v = +1$ then this is the Jordan product.

Proposition 4.3.4 *(Jacobson) Let D be a skew field and $R = M_n(D)$. If S is a nil and weakly closed subset of R, then $S^n = \{0\}$.*

Proof. Note that from the assumptions it follows that $0 \in S$. Let L be a minimal left ideal of R. Then $\dim_D(L) = n$ (here we consider L as a right D-vector space). The result is clear if $n = 1$.

We claim that $S_0^n = \{0\}$ for every nilpotent subset S_0 of R. Indeed, suppose the contrary, then

$$S_0^n L \neq \{0\}$$

(because $LR = R$). It follows that $L \supset S_0 L \supset S_0^2 L \supset \cdots \supset S_0^n L \neq \{0\}$, because if $S_0^i L = S_0^{i+1} L$ then $S_0^{i+k} L = S_0^{i+k+1} L$ for any positive k. Hence $S_0^i L = S_0^{i+k} L$ for all such k and thus is impossible as S_0 is nilpotent. It follows that $\dim_D S_0^n L = 0$ and thus $S_0^n L = \{0\}$, a contradiction.

Because every element of S is nilpotent it follows from the claim that the set of nilpotent subsets of S has a maximal element (Zorn's

Lemma is applicable because S has a subset that is nilpotent). Let S_0 be such a set. Note that $0 \in S_0$. Then $S_0^n = \{0\}$. Put $V = S_0L \subset L$ and $m = \dim_D V$. So $0 < m < n$. Let

$$S_1 = \{s \in S \mid sV \subseteq V\}.$$

Note that $S_0 \subseteq S_1$. So S_1 is a nil and weakly closed subset of $\mathrm{End}(V_D) \cong M_m(D)$. By induction we know that $S_1^m V = \{0\}$.

Also S_1 acts on the quotient space L/V as follows:

$$s(a + V) = sa + V.$$

Because $\dim_D(L/V) = n - m < n$ we get (again from the induction hypothesis) that

$$S_1^{n-m} L \subseteq V.$$

Hence

$$S_1^n L = S_1^m(S_1^{n-m} L) \subseteq S_1^m V = \{0\}.$$

So $S_1^n = \{0\}$. Because $S_0 \subseteq S_1$ we obtain from the maximality of S_0 that $S_0 = S_1$. Hence

$$sS_0L = sV \not\subseteq S_0L = V$$

for all $s \in (S \setminus S_0)$.

We now show that $S = S_0$ (and hence the result follows).

Denote by $s_1 \circ s_2$ the weak product $s_1s_2 + vs_2s_1$ (where v is dependent of s_1 and s_2). Suppose $s \in (S \setminus S_0)$ and $s \circ S_0 \subseteq S_0$. It follows that for every $s_0 \in S_0$ and $a \in L$,

$$s(s_0a) = (s \circ s_0)a - vs_0(sa) \in S_0L$$

for some $v \in \mathbf{Z}$. So $s \in S_1 \setminus S_0$, a contradiction. Hence we may suppose that

$$s \circ S_0 \not\subseteq S_0$$

for all $s \in S \setminus S_0$. Suppose thus that $s_1 \in S \setminus S_0$ and $s_{01} \in S_0$ is such that $s_2 = s_1 \circ s_{01} \notin S_0$. Inductively, let $s_i \in S \setminus S_0$ and take $s_{0i} \in S_0$ such that

$$s_{i+1} = s_i \circ s_{0i} \notin S_0.$$

Then, s_{2n+1} is a sum of usual products of length $2n+1$ of permutations of $s_1 \in S \setminus S_0, s_{01}, s_{02}, \cdots, s_{0,2n}$. So every term contains a product of

elements of S_0 of length n and thus is 0. So $s_{2n+1} = 0$, in contradiction with $s_{2n+1} \notin S_0$. $\square$

Note that the restriction on the nil set S is necessary. Indeed, in $M_2(D)$ is $\{e_{12}, e_{21}\}$ a nil subset but $e_{12}e_{21} = e_{11}$ is not nilpotent.

Theorem 4.3.5 *(Jacobson) Let N be a nilpotent ideal in a ring R and assume R/N is semisimple. If S is a nil and weakly closed subset of R, then there exists n so that $S^n = \{0\}$.*

Proof. Clearly $N = J(R)$ and

$$R/N \cong \prod_{i=1}^{k} M_{n_i}(D_i)$$

for some skew fields D_i. Let S_i denote the natural image of S in $M_{n_i}(D_i)$ and $n = \max\{n_1, \cdots, n_k\}$. Then $S_i^n = \{0\}$ for all $1 \leq i \leq k$. It follows that $S^n \subseteq N$, as desired. $\square$

The result shows the potential interest in finding a criterion for a ring to be contained in an Artinian ring.

As an application one can show the following result.

Proposition 4.3.6 *Let F be a field and let R be a finite dimensional algebra over F. Assume S is a subset such that every $s \in S$ is a sum of nilpotent elements. If S is multiplicatively closed then S is nilpotent.*

4.4 Primitive rings

We define a new class of rings: the left primitive rings. Within the class of Artinian rings it will yield a new approach to the Wedderburn-Artin theorems. Within the class of non-Artinian rings we obtain a structure theorem that can be considered as a generalisation of the Wedderburn-Artin theorems.

Proposition 4.4.1 *A ring R is J-semisimple (or semiprimitive) if and only if R has a faithful semisimple left R-module.*

Proof. Suppose M is a faithful semisimple left R-module. So, $M = \sum_{i\in I} M_i$, where each M_i is a simple left R-module and $\text{ann}_R(M) = \{r \in R \mid rM = \{0\}\} = \{0\}$. Because of Corollary 3.1.3, $J(R)M = \{0\}$. Hence $J(R) \subseteq \text{ann}_R(M) = \{0\}$ and thus $J(R) = \{0\}$.

Conversely, suppose $J(R) = \{0\}$. Let $\{M_i \mid i \in I\}$ be a set of two-by-two non-isomorphic simple left R-modules so that this set contains a representative of every isomorphism class of the simple left R-modules. Then, $M = \sum_{i\in I} M_i$ is a semisimple left R-module and

$$\text{ann}_R(M) = \cap_{i\in I}\text{ann}_R(M_i) = J(R) = \{0\}.$$

So, M is a faithful simple left R-module. □

Definition 4.4.2 *A ring R is left (respectively right) primitive if R has a faithful simple left (respectively right) module.*

There exists examples (due to Bergman and Jategaonkar) of left primitive rings that are not right primitive.

Definition 4.4.3 *An ideal I of a ring R is left (respectively right) primitive if the quotient ring R/I is left (respectively right) primitive.*

Proposition 4.4.4 *An ideal I in a ring R is left primitive if and only if $I = ann_l(M)$ for some simple left R-module.*

Proof. Suppose I is a left primitive ideal of a ring R and suppose M is a faithful simple left R/I-module. Then, as an R-module, M is simple and

$$\text{ann}_R(M) = I.$$

Conversely, let $I = \text{ann}_R(M)$ where M is a simple left R-module. Then, one can consider M as a left R/I-module. The latter is still simple and it is faithful. □

Corollary 4.4.5 *The Jacobson radical of a ring R is the intersection of all left (respectively right) primitive ideals in R.*

4.5 Examples of primitive rings

Proposition 4.5.1 *Let R be a ring.*

1. *If R is simple, then R is left and right primitive.*
2. *If R is left primitive, then R is semiprimitive (i.e. $J(R) = \{0\}$) and prime.*

Proof. To prove part one, assume R is simple and let M be a non-zero left R-module. Because $\mathrm{ann}_R(M)$ is a two-sided ideal of R we get that $\mathrm{ann}_R(M) = \{0\}$. So, every left (and right) R-module is faithful. It follows that R has a faithful simple left R-module. So R is left primitive.

To prove part two, assume R is left primitive. Because of Proposition 4.4.1, $J(R) = \{0\}$. Let M be a faithful simple left R-module. Then, for every non-zero ideal I of R, the set IM is a non-zero submodule of M. As M is simple we get $IM = M$. In particular, for any two non-zero ideals J and I of M,

$$IJM = IM = M.$$

Hence $IJ \neq \{0\}$. So we get that R is prime. □

So we have introduced several classes of rings that are linked as follows:

$$\begin{array}{rcccc} \text{semisimple} & \Rightarrow & \text{semiprimitive} & \Rightarrow & \text{semiprime} \\ & & \Uparrow & & \Uparrow \\ \text{simple} & \Rightarrow & \text{left primitive} & \Rightarrow & \text{prime} \end{array}$$

In general, none of the converse implications is valid. In case R is Artinian, then simple rings are semisimple and all horizontal implications can be reversed.

Proposition 4.5.2 *Let R be a left Artinian ring. Then,*

1. *R is semisimple if and only if R is semiprimitive if and only if R is semiprime.*
2. *R is simple if and only if R is left (respectively right) primitive if and only if R is prime.*

Proof. Part one follows at once from Theorem 3.2.4 and Theorem 4.3.2.

To prove part two it is sufficient to show that a prime ring R is simple provided R is left Artinian. So, suppose R is prime and left Artinian. Then R is semiprime, and thus by part one, R is semisimple. Hence, R is a direct product of simple rings. But R being prime then implies that R is simple. □

Proposition 4.5.3 *A commutative ring R is (left) primitive if and only if R is a field.*

Proof. Suppose R is a field. Then ${}_RR$ is a faithful and simple R-module, and thus R is primitive.

Conversely, suppose R is a commutative and primitive ring. Let M be a faithful simple (left) R-module. Then, $M \cong R/I$ (an isomorphism as R-modules) for some maximal ideal I of R (here we use that R is commutative). Clearly, $IM = \{0\}$ and thus, because M is faithful, $I = \{0\}$. So R is a field. □

It is now easy to construct left primitive rings. Indeed for any ring R and for any simple left R-module M we get that $R/\mathrm{ann}_R(M)$ is a left primitive ring. We give some concrete examples. Let D be a skew field, V_D a right D vector space and $E = \mathrm{End}(V_D)$. As left E-module we get that V is faithful and simple. So E is left primitive. If $\dim_D(V) < \infty$ then $E \cong M_n(D)$ and thus E is a simple Artinian ring. If $\dim_D(V) = \infty$ then E is not simple, not commutative, not-Artinian, but it is left primitive. Later we shall show that any left primitive ring is closely related to such a ring.

We now will show that any prime ring is left and right primitive if the ring contains a minimal left ideal (for example, if the ring is left Artinian). To prove this result we first need to show the following lemma.

Lemma 4.5.4 *Let R be a semiprime ring and $r \in R$. Then, Rr is a minimal left ideal if and only if rR is a minimal right ideal.*

Proof. Suppose Rr is a minimal left ideal. To prove rR is a minimal right ideal, it is sufficient to show that if $0 \neq rr' \in rR$ then $r \in rr'R$. Since, R is semiprime we know

$$rr'Rrr' \neq \{0\}$$

and thus $rr'arr' \neq 0$ for some $a \in R$. Define

$$\varphi : Rr \to Rr : x \mapsto xr'ar.$$

Clearly φ is an R-module homomorphism. Furthermore, $\varphi(r) = rr'ar \neq 0$. Hence φ is bijective and thus φ is a module isomorphism. We get

$$r = \varphi^{-1}(\varphi(r)) = \varphi^{-1}(rr'ar) = rr'\varphi^{-1}(ar) \in rr'R,$$

as desired.

The converse is shown in a similar manner. □

If R is not semiprime, then the Lemma no longer holds in general. Indeed, let

$$R = \begin{bmatrix} \mathbf{Q} & \mathbf{Q} \\ \{0\} & \mathbf{Q} \end{bmatrix}.$$

Then $RE_{11} = \begin{bmatrix} \mathbf{Q} & \{0\} \\ \{0\} & \{0\} \end{bmatrix}$ is a minimal left ideal, but $E_{11}R = \begin{bmatrix} \mathbf{Q} & \mathbf{Q} \\ \{0\} & \{0\} \end{bmatrix}$ is not a minimal right ideal as it contains the right ideal $\begin{bmatrix} \{0\} & \mathbf{Q} \\ \{0\} & \{0\} \end{bmatrix}$.

Theorem 4.5.5 *Let R be a ring with a minimal left ideal L. The following are equivalent:*

1. *R is prime,*
2. *R is left primitive,*
3. *R is right primitive.*

If these conditions are satisfied, then R has a minimal right ideal V. Every faithful simple left (respectively right) R-module is isomorphic with ${}_RL$ (respectively V_R).

Proof. We already know that (1) follows from (2) (and from (3)).

Suppose thus that (1) holds, that is, suppose R is a prime ring. We claim that

$$\mathrm{ann}_R(L) = \{0\}.$$

Indeed, let $r \in \mathrm{ann}_R(L)$. Then, $rL = RrL = \{0\}$. Because R is prime it follows that $r = 0$. From the claim we get that L is a faithful simple

left R-module and thus (2) follows. Because of Lemma 4.5.4 we also get that $V = rR$ is a minimal right ideal. It follows that V_R is a faithful simple right R-module and (3) follows.

Now, let M be an arbitrary faithful simple left R-module. Then $Lm \neq \{0\}$ for some $m \in M$. Thus, because M is simple, $M = Lm$. The mapping

$$L \to Lm = M : l \mapsto lm$$

is an R-module isomorphism. □

We consider an example. Let D be a skew field and V a non-zero right D-vector space. Let $0 \neq v \in V$ and let $L = vD$. Let $e : V \to L$ be a natural projection. Clearly $e = e^2 \in E = \mathrm{End}(V_D)$. We already know that V is a faithful and simple left E-module. So, by Theorem 4.5.5, the ring E has a "unique" minimal and faithful right E-module (and E is right primitive).

We now show that

$$eE$$

is the unique (up to isomorphism) faithful and simple right E-module. Indeed, consider the mapping

$$\varphi : {}_EE \to {}_EV : g \mapsto g(v).$$

This is an E-epimorphism and

$$\ker \varphi = E(1 - e).$$

To prove the latter first note that

$$(E(1 - e))(v) = E(v - ev) = E(v - v) = \{0\}$$

and thus $E(1 - e) \subseteq \ker \varphi$. Conversely, if $g \in \ker \varphi$ then

$$(ge)(V) = g(vD) = g(v)D = \{0\}$$

and thus $0 = ge = g - g(1 - e)$. So $g = g(1 - e)$ and hence $\ker \varphi \subseteq E(1 - e)$.

So φ induces an E-isomorphism $Ee \to V$. Thus Ee is a minimal and faithful left E-module. Lemma 4.5.4 then implies that indeed eE is a minimal and faithful right E-module.

Now, if $\dim_D(V) = \infty$ then E is neither left nor right Artinian. So, Corollary 2.5.6 then yields that E is not a simple ring.

The sum of all minimal left ideals of a ring R is called the *left socle* of R and is denoted by

$$\mathrm{soc}({}_R R).$$

(In case no minimal left ideals exist then the socle is by definition the zero module.) Similarly one defines the right socle

$$\mathrm{soc}(R_R).$$

In case R is semiprime, then, by Lemma 4.5.4, $\mathrm{soc}({}_R R) = \mathrm{soc}(R_R)$, and this is is an ideal. One can actually show that always both socles are twosided ideals. In general these are different ideals.

We finish this section with an example of a left primitive ring that has infinitely many non-isomorphic faithful simple left modules.

Let $R = D[X, \sigma]$, a skew polynomial ring, with σ an endomorphism of the skew field D. Note that for all $f(X), g(X) \in D[X, \sigma]$, with $f(X) \neq 0$, there exist $q(X), r(X) \in D[X, \sigma]$ so that

$$g(X) = q(X)f(X) + r(X),$$

with $r(X) = 0$ or $\deg(r(X)) < \deg(f(X))$. That is, the Euclidean algorithm is valid in $D[X, \sigma]$. It follows that every non-zero left ideal L of R is generated by an arbitrary polynomial of L of minimal degree. We now describe the ideals of R, provided that σ is not an automorphism of finite order modulo the inner automorphisms.

Proposition 4.5.6 *Let D be a skew field and let σ be an automorphism of D that is not of finite inner order (that is, the natural image of σ in the group $Aut(D)/Inn(D)$ is of infinite order). Then the non-zero ideals of $R = D[X, \sigma]$ are all ideals of the form RX^m, with $m \geq 0$.*

Proof. Because, for every $d \in D$

$$Xd = \sigma(d)X$$

we get that RX^m is an ideal of R.

Conversely, let I be a nonzero ideal of R. Then $I = Rf$ with $f = X^m + d_{m-1}X^{m-1} + \cdots + d_nX^n$, with each $d_i \in D$, $d_n \neq 0$ and $m \geq n \geq 0$. Note that

$$fX - Xf = (d_{m-1} - \sigma(d_{m-1}))X^m + \cdots + (d_n - \sigma(d_n))X^{n+1} \in Rf.$$

So, $fX - Xf = df$ for some $d \in D$. Comparing the coefficients of X^n we get

$$dd_n = 0$$

and thus $d = 0$. Hence $\sigma(d_i) = d_i$ for all i. Furthermore, for any $r \in D$,

$$fr - \sigma^m(r)f \in I$$

and

$$\deg(fr - \sigma^m(r)f) < m.$$

So, $fr - \sigma^m(r)f = 0$. Again comparing coefficients of X^n we obtain

$$d_n\sigma^n(r) - \sigma^m(r)d_n = 0.$$

Hence,

$$\sigma^n(d_nr) = \sigma^m(rd_n).$$

Because σ is injective this yields

$$d_nr = \sigma^{m-n}(rd_n) = \sigma^{m-n}(r)d_n.$$

So, if $k = m - n > 0$, then

$$\sigma^k(r) = d_nrd_n^{-1},$$

in particular, σ^k is an inner automorphism, a contradiction. Hence $m = n$ and $f = X^m$. $\square$

Proposition 4.5.7 *Let σ be an automorphism of a skew field D. Assume that σ is not an automorphism of finite inner order. Then, for any $0 \neq d \in D$,*

$$M_d = R/R(X - d)$$

is a faithful simple left $R = D[X, \sigma]$-module. Thus R is left primitive. Moreover,

$$M_d \cong M_{d'} \text{ if and only if } d = \sigma(c)d'c^{-1}$$

for some $0 \neq c \in D$. (One says d is σ-conjugated to d'.)

Proof. Clearly, as left R-modules,

$$M_d = R/R(X-d) \cong D,$$

with R-action on D defined as follows: $Xr = \sigma(r)d$ (because $Xr = \sigma(r)(X-d) + \sigma(r)d$). Hence M_d is a simple left R-module. Also, $X^m \notin R(X-d)$, for any $0 \neq d \in D$ and $m \geq 0$. Hence, Proposition 4.5.6 yields that $R(X-d)$ does not contain any nonzero twosided ideal. So $\operatorname{ann}(M_d) = \{0\}$ and thus M_d is a faithful R-module.

Suppose now that

$$f : M_d \to M_{d'}$$

is an R-isomorphism. Then, there exists $0 \neq c \in D$ so that

$$f(b) = bc$$

for all $b \in D = M_d$. Because

$$f(Xb) = Xf(b)$$

we obtain

$$\sigma(b)dc = \sigma(bc)d'.$$

So

$$d = \sigma(c)d'\sigma(d').$$

Hence we have shown that $M_d \cong M_{d'}$ implies $d = \sigma(c)d'c^{-1}$ for some $0 \neq c \in D$. The converse is an easy exercise. □

So the isomorphism classes of the faithful simple left R-modules of the form M_d are in a one-to-one correspondence with the σ-conjugacy classes of $D \setminus \{0\}$.

Consider now $D = \mathbf{R}(t)$ and $R = D[X, \sigma]$ with σ the $\mathbf{R}$-automorphism defined by $\sigma(t) = t + 1$. Define

$$\deg(f/g) = \deg(f) - \deg(g)$$

for $f, g \in \mathrm{R}[t]$ and $0 \neq g$. Then, for every $c = c(t) \in \mathbf{R}(t)$,

$$\deg(\sigma(c)c^{-1}) = \deg(c(t+1)/c(t)) = 0.$$

So, if $d(t)$ and $d'(t)$ are σ-conjugated, then $\deg(d(t)) = \deg(d'(t))$. Hence

$$M_1,\ M_t,\ M_{t^2},\ \cdots$$

are non-isomorphic faithful simple left R-modules.

4.6 Density Theorem

Let R and k be rings and ${}_RV_k$ an (R,k)-bimodule. Put $E = \mathrm{End}(V_k)$. Then V is a left E-module. One says that the action of R on V_k is *dense* if for all $f \in E$ and for all $v_1, \cdots, v_n \in V$ there exists $r \in R$ so that

$$rv_i = f(v_i)$$

for all $1 \leq i \leq n$.

The name "dense" has a topological meaning. Indeed, consider the sets of the type

$$\{g \in E \mid g(v_i) = v_i',\ 1 \leq i \leq n\}$$

where $v_1, \cdots, v_n, v_1', \cdots, v_n' \in V$ and $n \in \mathbf{N}_0$. Consider the topology τ with these sets as a basis. It follows that the action of R on V_k is dense if and only if the image of the natural map $R \to E$ is a dense subring of E (this with respect to the topology τ).

Lemma 4.6.1 *Suppose that ${}_RV$ is a semisimple R-module, $k = End_R(V)$ and $E = End(V_k)$. Then, every R-submodule W of V is an E-submodule.*

Proof. Because ${}_RV$ is a semisimple R-module, there exists an R-submodule W' so that $V = W \oplus W'$. Let $e : V \to W$ be the projection on W. So $e \in \mathrm{End}({}_RV) = k$. Then, for any $f \in E$,

$$f(W) = f(We) = (f(W))e \subseteq W.$$

Hence W is an E-submodule of V. □

Theorem 4.6.2 *(Density theorem of Jacobson and Chevalley) Let R be a ring and V a semisimple left R-module. Put $k = End_R(V)$ and let $E = End(V_k)$. Then, the action of R on V_k is dense.*

Proof. Let $v_1, \cdots, v_n \in V$ and $f \in E$. We have to prove that there exists an $r \in R$ so that $rv_i = f(v_i)$ for all $1 \leq i \leq n$.

Apply Lemma 4.6.1 on the semisimple left R-module $\overline{V} = V \oplus \cdots \oplus V = V^n$. Put $\overline{k} = \mathrm{End}({}_R\overline{V}) = \mathrm{End}({}_RV^n)$. Then

$$\overline{k} = M_n(\mathrm{End}({}_RV)) = M_n(k).$$

Define

$$\overline{f} : \overline{V} \to \overline{V} : (a_1, \cdots, a_n) \mapsto (f(a_1), \cdots, f(a_n)).$$

We now show that

$$\overline{f} \in \mathrm{End}(\overline{V}_{\overline{k}}).$$

Indeed, let $\overline{e} = (e_{ij}) \in M_n(k)$ (hence each $e_{ij} \in k$). Then, for any $(w_1, \cdots, w_n) \in \overline{V}$,

$$\begin{aligned}
\overline{f}((w_1, \cdots, w_n)\overline{e}) &= \overline{f}(\sum w_i e_{i1}, \cdots, \sum w_i e_{in}) \\
&= (f(\sum w_i e_{i1}), \cdots, f(\sum w_i e_{in})) \\
&= (\sum f(w_i) e_{i1}, \cdots, \sum f(w_i) e_{in}) \\
&= (f(w_1), \cdots, f(w_n))\overline{e} \\
&= \left(\overline{f}(w_1, \cdots, w_n)\right) \overline{e}.
\end{aligned}$$

Let now $\overline{W}$ be the cyclic R-submodule of $\overline{V}$ generated by the element $(v_1, \cdots, v_n) \in \overline{V}$. Because of Lemma 4.6.1 it follows that $\overline{W}$ is a left $\mathrm{End}(\overline{V}_{\overline{k}})$-submodule. So, in particular,

$$\overline{f}(v_1, \cdots, v_n) = (f(v_1), \cdots, f(v_n)) \in \overline{W}.$$

Hence there exists an $r \in R$ so that

$$f(v_i) = rv_i$$

for all $1 \leq i \leq n$. □

Corollary 4.6.3 *Let R be a ring and V a semisimple left R-module. Put $k = End_R(V)$. If V_k is finitely generated as a right k-module, then the natural map*

$$\rho : R \to E$$

is surjective.

Proof. Put $V = v_1k + \cdots + v_nk$, and let $f \in E = \mathrm{End}(V_k)$. Because of the density theorem there exists an $r \in R$ so that $rv_i = f(v_i)$ for all $1 \leq i \leq n$. Let now $v \in V$ be an arbitrary element in V. Then there exist $a_1, \cdots, a_n \in k$ so that

$$v = v_1a_1 + \cdots + v_na_n.$$

Hence

$$\begin{aligned} rv &= \sum r(v_i a_i) \\ &= \sum (rv_i)a_i \\ &= \sum f(v_i)a_i \\ &= \sum f(v_i a_i) \\ &= f(\sum v_i a_i) \\ &= f(v) \end{aligned}$$

Consequently, $f = \rho(r)$. □

Definition 4.6.4 *Let D be a skew field and V_D a right D-module. Put $E = End(V_D)$. A subset $S \subseteq E$ is said to be m-transitive on V if for any set $v_1, \ldots, v_n \in V$ of $n \leq m$ linear independent vectors and any set of n vectors $v'_1, \cdots, v'_n \in V$ there exists $s \in S$ so that*

$$s(v_i) = v'_i$$

for all $1 \leq i \leq n$.

One calls S a dense set of linear transformations on V_k if S is m-transitive for any $m \in \mathbf{N}_0$.

Proposition 4.6.5 *Let D be a skew field and R a ring. Assume V is an (R, D)-bimodule. Put $E = End(V_D)$ and let $\rho : R \to E$ be the natural map. Then, the action of R on V_D is dense if and only if $\rho(R)$ is a dense subring of linear transformations on V.*

Proof. Exercise. □

The following theorem is a generalisation of the Wedderburn-Artin theorem (recall that a left Artinian ring is left primitive if and only if the ring is simple).

Theorem 4.6.6 *(Structure theorem of left primitive rings) Let R be a left primitive ring and V a faithful simple left R-module. Let $D = End_R(V)$ (a skew field). Then R is isomorphic with a dense ring of linear transformations on V_D. Moreover,*

1. *if R is left Artinian, then $dim_D(V) = n < \infty$ and $R \cong M_n(D)$.*

2. *if R is not left Artinian, then $dim_D(V) = \infty$, and for every $n \in \mathbf{N}_0$ there exists a subring R_n of R so that $M_n(D)$ is an epimorphic image of R_n.*

Proof. Put $E = \mathrm{End}(V_D)$ and let $\rho : R \to E$ be the natural mapping. Because ${}_RV$ is a faithful left R-module, the mapping ρ is injective. The density theorem yields that $\rho(R)$ is a dense ring of linear transformations on V_D.

Suppose now that $\dim_D(V) = n < \infty$. Because of the density theorem we then get that ρ is surjective, and hence is a bijection. So $R \cong M_n(D)$ and thus R is left Artinian.

Next suppose that $\dim_D(V)$ is infinite. Let $v_1, v_2, v_3, \cdots$ be a collection of D independent vectors in V. Put

$$V_n = \mathrm{vect}_D\{v_1, \cdots, v_n\},$$

with $n \in \mathbf{N}_0$. Define

$$R_n = \{r \in R \mid rV_n \subseteq V_n\}$$

and

$$U_n = \{r \in R \mid rV_n = \{0\}\}.$$

Then, R_n is a subring of R and U_n is an ideal of R_n and a left ideal of R. Clearly V_n is a left R_n/U_n-module. Because of the n-transitivity of R on V we get that every D-endomorphism on V_n is given by left multiplication by an element $r \in R_n$. Hence the natural map

$$R_n/U_n \to \mathrm{End}((V_n)_D)$$

is an isomorphism and thus

$$R_n/U_n \cong M_n(D).$$

The $n+1$-transitivity yields the existence of an element $a \in R$ so that

$$av_1 = \cdots = av_n = 0 \text{ and } av_{n+1} \neq 0.$$

It follows that

$$U_{n+1} \subset U_n$$

for any $n \in \mathbf{N}_0$. Hence we obtain a strict descending chain of left ideals of R:

$$U_1 \supset U_2 \supset U_3 \supset \cdots$$

So, R is not left Artinian and the result follows. □

Theorem 4.6.7 *Let D be a skew field and let R be a ring of linear transformations on a nonzero right D vector space V. Then,*

1. *R is 1-transitive if and only if ${}_RV$ is a simple R-module. In this case R is left primitive.*

2. *The following are equivalent:*

   (a) *R is 2-transitive,*

   (b) *R is 1-transitive and $End_R(V) = D$,*

   (c) *R is dense in $End(V_D)$.*

Proof. Part (1) in obvious.

So we prove part (2). That (b) implies (c) follows from (1) and the density theorem. That (c) implies (a) is also obvious. So we now prove that (a) implies (b). So suppose that R is 2-transitive. So clearly R is 1-transitive. Let $f \in \mathrm{End}({}_RV)$ and $0 \neq v \in V$. We claim that v and $(v)f$ are D-linearly dependent.

Suppose the contrary. Because of the 2-transitivity there exists an $r \in R$ so that $rv = 0$ and $r(vf) \neq 0$. But, since f is R-linear, we get $0 \neq r(vf) = (rv)f = (0)f = 0$, a contradiction.

Let thus $d \in D$ so that $(v)f = vd$. Because R is 1-transitive, there exists for every $w \in V$ an $r' \in R$ so that $w = r'v$. It follows that

$$(w)f = (r'v)f = r'(vf) = r'(vd) = (r'v)d = wd.$$

Thus $f = d \in D$ and so $\mathrm{End}({}_RV) = D$. □

We give an example of a 1-transitive ring that is not 2-transitive. Let k be a field that is not algebraically closed. Let $k \subset R$ be a field extension of finite degree (and $k \neq R$). We consider R as a k-vector space V, and we consider R as a subring of $E = \mathrm{End}(V_k)$ (by identifying $r \in R$ with the left multiplication by r). Because R is a field it is clear that ${}_RV$ is a simple module and thus R is 1-transitive on V. However R is not 2-transitive. Indeed, let $0 \neq v_1 \in k$ and $v_2 \in (R \setminus k)$. Let f be a k-linear transformation so that $f(v_2) = v_1$ and $f(v_1) = v_2$. If there exists $r \in R$ so that $rv_2 = v_1 = f(v_2)$ and $rv_1 = v_2 = f(v_1)$, then $v_1 = rv_2 = r^2v_1$. Hence $r = \pm 1$ and thus $v_2 \in k$, a contradiction.

Suppose k is an algebraically closed field and $\dim({}_kV) < \infty$. Let R be a k-subalgebra of $E = \mathrm{End}(V_k)$. If R is 1-transitive on V, then ${}_RV$ is simple and $\mathrm{End}({}_RV)$ is a skew field that is finite dimensional over k. So $E = k$. The previous Theorem then yields that R is 2-transitive (and thus dense).

We now give another example of dense subrings of linear transformations, and thus we provide examples of left primitive rings. First note that the centre $Z(R)$ of a left primitive ring is a domain (because a left primitive ring is prime). The following example (due to I. Kaplansky, 1917-) shows that $Z(R)$ can be an arbitrary domain.

Let A be an arbitrary domain and k its field of fractions. Let

$$V_k = \oplus_{i=1}^{\infty} e_i k,$$

a right k-vector space of infinite countable dimension. The elements of $E = \mathrm{End}(V_k)$ have a matrix representation (it are the column finite matrices). Let R be the subring of E consisting of the matrices that are of the following form:

$$\begin{pmatrix} M & 0 \\ 0 & aI \end{pmatrix}$$

where $M \in M_n(k)$ for some $n \in \mathbf{N}_0$, $a \in A$ and I the identity matrix. This ring is dense in E and thus it is left primitive. It is easily verified that

$$Z(R) = \{aI \mid a \in A\} \cong A.$$

To construct another example, define $f \in E$ as follows

$$f(e_1) = 0, \quad f(e_i) = e_{i-1} \text{ for } i \geq 2.$$

Let $g \in E$ be an endomorphism so that, for all $m \geq 1$,

$$g^m e_1 = e_{r(m)}$$

and

$$\lim_{m \to \infty} r(m) = \infty.$$

Let R be the k-subalgebra of E generated by f and g (note that $k \subseteq Z(E)$). We claim that V is a simple left R-module; and hence R is

left primitive. Indeed, suppose W is a non-zero submodule of V. Let $0 \neq w \in W$ be an element that is a linear combination of a minimal number of the basis elements e_i. Write

$$w = e_{i_1}a_1 + e_{i_2}a_2 + \cdots + e_{i_n}a_n$$

with $i_1 < i_2 < \cdots < i_n$ and each $a_i \neq 0$. It follows that $f^{i_1}(w) \in W$ has less nonzero terms, except of $n = 1$. Thus $e_{i_1} \in W$ and hence $f^{i_1-1}(e_{i_1}) = e_1 \in W$. The definition of f and g then yields that each $e_j \in W$. So $W = V$, and this proves the claim.

Next we claim that R is dense in E. Because of the density theorem it is sufficient to show that $\mathrm{End}({}_RV) = k$. So let $\lambda \in \mathrm{End}({}_RV)$. Because $f(e_1\lambda) = (fe_1)\lambda = 0$ and because $\ker f = e_1k$ it follows that

$$e_1\lambda = e_1a$$

for some $a \in k$. Now, for any j there exist $s, t \in \mathbf{N}$ so that

$$e_j = f^s g^t e_1.$$

Thus

$$e_j\lambda = (f^s g^t e_1)\lambda = f^s g^t(e_1a) = e_ja.$$

Hence $\lambda = a \in k$.

Now choose for g the following endomorphism

$$g(e_i) = e_{i+1} \quad (i \geq 1).$$

Then, all relations between f and g are the consequence of $fg = 1$. So

$$k\langle x, y\rangle \to R : x \mapsto f,\ y \mapsto g$$

is a ring epimorphism with kernel $(xy - 1)$. Therefore,

$$R \cong k\langle x, y\rangle/(xy - 1)$$

is a left primitive ring. By making another choice for g we obtain the following proposition.

Proposition 4.6.8 *(Samuel) For $i \geq 1$, define $g(e_i) = e_{i^2+1}$. Then the map*

$$\psi : k\langle x, y\rangle \to R : \begin{cases} x & \mapsto & f \\ y & \mapsto & g \end{cases}$$

defines a k-algebra automorphism. So, the free k-algebra $k\langle x, y\rangle$ is left primitive.

Note that if k is a field, then $k[X]$ nor $k[X,Y]$ are left primitive. The reason being that a commutative ring is primitive if and only if it is a field.

Proof. It is sufficient to show that ψ is an isomorphism. Obviously the ψ is surjective. So we need only show that ψ is injective. Now, via the k-homomorphism ψ we get that V is a left $A = k\langle x, y\rangle$-module. It is now sufficient to show that V is faithful left A-module.

We will show the following: if $a \in A$ and $ae_i = 0$ for sufficiently large i (we say that a is "eventually" 0), then $a = 0$.

Let M be a monomial in x and y. For i sufficiently large we get

$$Me_i = e_{m(i)}$$

with m a uniquely determined monic polynomial in $\mathbf{Z}[t]$ of degree $\deg(m) = 2^d$, with $d = \deg_y(M)$. We now first show the following claim: if M and M' are different monomials in x and y, then $m \neq m'$ in $\mathbf{Z}[t]$.

Indeed, if M and M' finish in the same letter (either x or y) then the result follows by induction on the length of the monomial. If they finish in a different letter then we may suppose that $M = M_1 x$ and $M' = M_1' y$. It follows that the polynomial m' (associated with M') only has even powers in t. On the other hand, the polynomial m (associated with M) is of the form (because the polynomial associated with x is $t - 1$):

$$t^{2^k} - nt^{2^k - 1} + \cdots,$$

with $k = \deg_y(M_1)$ and $n \in \mathbf{N}_0$. Thus $m(t) \neq m'(t)$.

Suppose now that $a = \sum_{j=1}^{n} k_k M_j \in A$ with $k_j \in k$ and $M_1, \cdots M_n$ distinct monomials. It follows that for sufficiently large i:

$$ae_i = \left(\sum_j k_j M_j\right) a_i = \sum_j a_j e_{m_j(i)}.$$

Because of the previous claim we know that all m_j's are different. So $a \neq 0$ and a is not eventually zero. □

As an application one can show the following result.

Proposition 4.6.9 *For any field k is the free k-algebra in finitely many or a countable number of variables a left primitive ring.*

Formanek extended this result to any free k-algebra (without any restriction on the variables).

We have encountered many type of ring structures that are closely related. Sometimes one can show results by first proving them for skew fields. Next one shows them for matrices over skew fields, and then for left primitive rings and more general for semiprimitive rings. Finally one would like then to "lift" the knowledge to non-semiprimitive rings. Using this method we prove the following result (Herstein, 1923 - 1988).

Theorem 4.6.10 *(Jacobson-Herstein) A ring R is commutative if and only if for any $a, b \in R$ there exists $n = n(a,b) > 1$ so that $(ab - ba)^{n(a,b)} = ab - ba$.*

Proof. Let R be a ring so that for any $a, b \in R$ there exists $n = n(a,b) > 1$ with $(ab - ba)^{n(a,b)} = ab - ba$.

Step 1.
In the next chapter we shall prove the result for skew fields.

Step 2.: The result holds for left primitive rings R.
Because of the structure theorem for left primitive rings there exists a skew field D so that $R \cong M_m(D)$ for some $m \in \mathbf{N}_0$, or (for every m) R contains a subring R_m such that $M_m(D)$ is an epimorphic image of R_m If $m \geq 2$, then

$$E_{11}E_{12} - E_{12}E_{11} = E_{12}$$

and thus

$$(E_{11}E_{12} - E_{12}E_{11})^n = E_{12}^n = 0 \neq E_{11}E_{12} - E_{12}E_{11}$$

for every $n \geq 2$. So $R \cong D$, a skew field and the result follows from Step 1.

Step 3: The result holds for semiprimitive rings R.
Because $J(R) = \{0\}$ we get that there exist primitive rings $R_i = R/M_i$ (with M_i a primitive ideal of R) so that the natural map

$$R \to \prod R_i,$$

is injective and every projection $R \to R_i$ is surjective (one says that R is a subdirect product of left primitive rings). As an epimorphic image,

R_i also satisfies the assumption of the theorem. So by Step 2, each R_i is commutative. It follows that R is commutative.

Step 4: The result holds for any ring R.
Because of Step 3, $R/J(R)$ is commutative. Let $a, b \in R$ and $n > 1$ so that $(ab - ba)^n = ab - ba$. Then

$$(ab - ba)(1 - (ab - ba)^{n-1}) = 0.$$

Because $(ab-ba)^{n-1} \in J(R)$ we know that $1-(ab-ba)^{n-1} \in U(R)$. So we get $ab - ba = 0$. Because a and b are arbitrary we showed that R is commutative. □

4.7 Exercises

1. (a) Prove that the centre of a prime ring is a domain and that it has characteristic a prime number or zero.

   (b) Every commutative domain is the centre of some prime ring.

2. Prove that a ring R is a domain if and only if R is prime and reduced.

3. Let $R = UT_3(D)$ be the ring of the upper triangular matrices over a skew field.

   (a) Compute $J(R)$, $B(R)$ and $\mathcal{B}(R)$.

   (b) Compute all prime ideals.

   (c) Compute all semiprime ideals.

   Do the same for the ring $UT_3(\mathbf{Z})$.

4. Prove that in a right Artinian ring every prime ideal is maximal.

5. Prove that the following are equivalent for a ring R:

   (a) all ideals (different from R) are prime,

   (b) every ideal I of R is idempotent (that is, $I^2 = I$) and, moreover, all ideals are linearly ordered.

6. Let n be a nonzero integer. Prove that $R = \begin{bmatrix} \mathbf{Z} & n\mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} \end{bmatrix}$ is a prime ring, while $R' = \begin{bmatrix} \mathbf{Z} & n\mathbf{Z} \\ \{0\} & \mathbf{Z} \end{bmatrix}$ is nor prime.

7. Prove that a homomorphic image of a left primitive ring is not necessarily left primitive.

8. Let R be a left primitive ring and $e = e^2 \in R$. Prove that eRe is also a left primitive ring.

9. Prove that a ring R is left primitive if and only if $M_n(R)$ is left primitive.

10. Give an example of a left primitive ring so that $R[X]$ is not left primitive.

11. (a) Prove that a ring R is semiprime if and only if for all ideals I, J, $IJ = \{0\}$ implies $I \cap J = \{0\}$.

    (b) Let I and J be ideals in a semiprime ring R. Prove that $IJ = \{0\}$ if and only if $JI = \{0\}$.

12. Let I be a nonzero left ideal in a ring R so that there exists $n \in \mathbf{N}_0$ with $x^n = 0$ for all $x \in I$.

    (a) Prove that I contains a nonzero nilpotent left ideal of R.

    (b) Prove that $I \subseteq B(R)$.

Chapter 5

Skew fields

A skew field is a ring in which every nonzero element is invertible. In the previous chapter we have shown that these form an important class of rings. In this chapter we mainly give attention to the noncommutative skew fields.

5.1 Wedderburn's Theorem

We first show that there do not exist finite noncommutative skew fields.

Theorem 5.1.1 *(Wedderburn) Every finite skew field is commutative.*

Proof. Let F be the centre of a finite skew field D. So F is a finite field. Let $\mathrm{char}(F) = p > 0$ and thus $|F| = q = p^m \geq 2$, for some $m \in \mathbf{N}$. It is sufficient to prove that $\dim_F(D) = n = 1$. Suppose that $n > 1$ and let $D^* = D \setminus \{0\}$. The class equation yields:

$$|D^*| = q^n - 1 = q - 1 + \sum_d [D^* : C_{D^*}(d)],$$

with $C_{D^*}(d)$ the centraliser of $d \in D^*$, and where the sum runs through one representative of each conjugacy class with more than one element.

Now $C_{D^*}(d) = C_D(d) \setminus \{0\}$, with $C_D(d)$ the centraliser of $d \in D$. Clearly, $C_D(d)$ is a skew field containing F. Put

$$r = r(d) = \dim_F(C_D(d)).$$

Then $1 \leq r < n$. Because

$$\dim_F(D) = \dim_{C_D(d)} D \cdot \dim_F C_D(d)$$

we get that $r|n$. It follows that

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^r - 1}.$$

Because $r|n$,

$$X^n - 1 = \Phi_n(X)(X^r - 1)h(X),$$

with $h(X) \in \mathbf{Z}[X]$ and $\Phi_n(X) = \prod_\xi (X - \xi)$, where the latter product runs through all the primitive n-th roots of unity. It is well known that $\Phi_n(X) \in \mathbf{Z}[X]$ (it is called the n-th cyclotomic polynomial). It follows that

$$\frac{q^n - 1}{q^r - 1} = \Phi_n(q)h(q) \in \mathbf{Z}.$$

Hence

$$\Phi_n(q)|(q - 1).$$

In particular,

$$q - 1 \geq |\Phi_n(q)| = \prod_\xi |q - \xi|.$$

Because $n > 1$ and $q \geq 2$ we obtain

$$|q - \xi| > q - 1 \geq 1$$

for every ξ. So

$$q - 1 > (q - 1)^{\phi(n)},$$

a contradiction. □

Corollary 5.1.2 *Let D be a skew field.*

1. *If R is a finite subring of D, then R is a field.*
2. *If $char(D) = p > 0$ and G is a finite subgroup of D^*, then G is cyclic.*

Proof. To prove part (1), assume R is a finite subring of D. Let $0 \neq r \in R$. Then, because R is finite, there exist positive integers $m > n$ so that $r^n = r^m$. Hence, $1 = r^{m-n}$ and thus $r^{-1} = r^{m-n-1} \in R$. So we have shown that R is a skew field. Because of Theorem 5.1.1 we thus have that R is a field.

To prove part (2), let $F_p = \{0, 1, \cdots, p-1\}$ be the prime subfield of D. Consider the F_p-subalgebra K of D generated by G. So

$$K = \{\sum_{i=1}^{n} f_i g_i \mid n \in \mathbf{N}_0,\ f_i \in F_p\}.$$

Clearly K is a finite subring of D. By part (1), it is a field. It is well known that a finite subgroup of a field is cyclic. So G is cyclic. □

In case $\mathrm{char}(D) = 0$ then part (2) of the corollary is not true in general. Indeed, consider the real quaternion algebra $\mathbf{H}(\mathbf{R})$. It contains the quaternion group Q_8 of order 8.

In 1955, Amitsur classified the finite subgroups of skew fields of characteristic zero. Note that $\mathbf{H}(\mathbf{R})$ also contains the following subgroup of order 24:

$$\{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}.$$

5.2 Additive commutators

Let D be a skew field. If $a, b \in D$ then $[a, b] = ab - ba$ is called the additive commutator of a and b. If $a, b \in D^*$, then $(a, b) = a^{-1}b^{-1}ab$ is called the multiplicative commutator of a and b.

Proposition 5.2.1 *Let D be a skew field and $d \in D$. If d commutes with all additive commutators in D then $d \in Z(D)$.*

Proof. Suppose the result is false, that is, suppose $d \in D$ commutes with all additive commutators but $d \notin Z(D)$. Hence there exists $a \in D$ so that $ad - da \neq 0$. Now,

$$\begin{aligned} [a, ad] &= a(ad) - (ad)a \\ &= a(ad - da) \\ &= a[a, d] \end{aligned}$$

Because of the assumption d commutes with $[a, ad]$. So

$$d(a[a, d]) - (a[a, d])d = 0.$$

Also, d commutes with $[a, d]$. Hence

$$da[a, d] - ad[a, d] = 0$$

and thus

$$(da - ad)[a, d] = 0.$$

Because $[a, d] \neq 0$ we get

$$da - ad = 0,$$

a contradiction. □

Corollary 5.2.2 *A skew field is generated by its centre and all additive commutators. In particular, a skew field is commutative if and only if all additive commutators are central.*

Proof. If $D = Z(D)$ then the result is obvious. So assume $D \neq Z(D)$. Let $a \in (D \setminus Z(D))$. Then there exists $b \in D$ so that $[a, b] \neq 0$. So

$$[a, ab] = a(ab - ba) = a[a, b]$$

and thus

$$a = [a, ab][a, b]^{-1}.$$

So the $Z(D)$-algebra generated by the additive commutators of D contains the element a. Hence the result follows. □

Let D be a ring and $a \in D$. The mapping

$$\delta_a : D \to D : x \mapsto [a, x] = ax - xa$$

is called the *inner derivation* of D associated with a. This mapping satisfies the following properties (for all $x, y \in D$):

$$\begin{aligned} \delta_a(x + y) &= \delta_a(x) + \delta_a(y), \\ \delta_a(xy) &= x\delta_a(y) + \delta_a(x)y \end{aligned}$$

An additive subgroup I of D is called a Lie ideal if it is invariant under all δ_a (with $a \in D$), that is,

$$\delta_a(I) \subseteq I.$$

Proposition 5.2.3 *Let K and D be skew fields so that K is properly contained in D. If K is a Lie ideal in D and $char(K) \neq 2$ then $K \subseteq Z(D)$.*

Proof. Let $c \in K$. We first prove that c commutes with an arbitrary element $a \in (D \setminus K)$. Indeed, from

$$\begin{aligned} \delta_a^2(c) &= \delta_a(ac - ca) \\ &= a^2c - aca - aca + ca^2 \\ &= ca^2 - 2aca + a^2c \in K \end{aligned}$$

and

$$\delta_{a^2}(c) = a^2c - ca^2 \in K$$

it follows that

$$2(a^2c - aca) = 2a\delta_a(c) \in K.$$

If $\delta_a(c) \neq 0$ then (because $\mathrm{char}(K) \neq 2$ and $2\delta_a(c) \in K^*$) $a \in K^*$, a contradiction. So $\delta_a(c) = 0$, i.e. $ac = ca$, as desired.

Next we show that c also commutes with $c' \in K^*$. Now, $a, ac' \in (D \setminus K)$. So by the previous, $ac = ca$ and $(ac')c = c(ac')$. So c commutes with a^{-1} and also with ac'. Therefore it commutes with $c' = a^{-1}(ac')$. □

One can show all the previous also for multiplicative commutators. For this one first shows the following.

Theorem 5.2.4 *(Cartan-Brauer-Hua) Let K and D be skew fields so that K is properly contained in D. If $dKd^{-1} \subseteq K$ for all $d \in D^*$ (one says K is normal in D) then $K \subseteq Z(D)$.*

As an application one then obtains

Corollary 5.2.5 *Every non-commutative skew field is generated by all its multiplicative commutators.*

5.3 Commutativity Theorems

Theorem 5.3.1 *(Herstein) Let D be a skew field and assume char$(D) = p > 0$. Suppose a is a non-central element in D^* and assume a is periodic. Then there exists $b \in D^*$ so that*

$$bab^{-1} = a^i \neq a$$

for some $i > 0$. Furthermore, b can be chosen to be an additive commutator.

Proof. Let $F = F_p$ be the prime subfield of D and let

$$K = F[a] = \left\{ \sum_{i=0}^{n} f_i a^i \mid n \in \mathbf{N}\ f_i \in F \right\}.$$

It is easily verified that K is a finite subfield of D (use for this that a is periodic). Let $n = \dim_F(K)$. Then $|K| = p^n$ for some n. So $|K^*| = p^n - 1$ and thus $a^{p^n-1} = 1$. Hence

$$a^{p^n} = a$$

(note that the latter holds for any element of K). Because, by assumption, a is not central we have that $\delta = \delta_a \neq 0$. However, for $k \in K$, $\delta(k) = 0$. So

$$\delta(kd) = k\delta(d) + \delta(k)d = k\delta(d)$$

for all $k \in K$ and $d \in D$. Hence, δ is a K-linear mapping of the K-vector space ${}_KD$.

We now prove that δ has an eigenvector in ${}_KD$. Now,

$$\delta = \lambda - \rho$$

with

$$\lambda : D \to D : x \mapsto ax$$

and

$$\rho : D \to D : x \mapsto xa$$

Because $\lambda\rho = \rho\lambda$ and because char(End$({}_KD)) = p$ we get that

$$\delta^{p^n} = (\lambda - \rho)^{p^n} = \lambda^{p^n} - \rho^{p^n}.$$

So, for all $x \in D$,

$$\delta^{p^n}(x) = a^{p^n}x - xa^{p^n} = ax - xa = \delta(x).$$

Therefore, $\delta^{p^n} = \delta \in E = \mathrm{End}({}_K D)$. Because any element $b \in K$ satisfies $b^{p^n} = b$ we obtain

$$t^{p^n} - t = \prod_{b \in K}(t - b) \in K[t].$$

Now, $\delta \in E$ and thus

$$0 = \delta^{p^n} - \delta = \left(\prod_{b \in K^*}(\delta - b)\right)\delta.$$

Because $\delta \neq 0$, there exists $b_0 \in K^*$ so that

$$\delta - b_0$$

is not a monomorphism. Hence

$$(\delta - b_0)(d) = 0$$

for some $d \in D^*$. So

$$\delta(d) = b_0 d,$$

i.e. d is an eigenvector with eigenvalue $b_0 \in K^*$.

Also it follows from

$$\delta(d) = ad - da = b_0 d$$

that

$$dad^{-1} = a - b_0 \in K \setminus \{a\}.$$

Now K^* is a cyclic group containing the elements a and dad^{-1}. Since they both have the same order, they generate the same subgroup of K^*. Hence

$$dad^{-1} = a^i \ (\neq a)$$

fors some $i > 0$. Put $d' = \delta(d) = ad - da \neq 0$. Then

$$d'a = (ad - da)a = aa^i d - a^i da = a^i d'$$

and thus

$$d'a(d')^{-1} = a^i.$$

□

Theorem 5.3.2 *Let D be a skew field. If for any $a, b \in D$ there exists $n = n(a,b) > 1$ so that $(ab - ba)^n = ab - ba$ then D is a field.*

Proof. Let $F = Z(D)$. Suppose $F \neq D$. Because of Corollary 5.2.2 we get that not every additive commutator is central. So there exist $b, b' \in D$ with

$$a = bb' - b'b \notin F.$$

Let $c \in F^*$. Then

$$ca = (cb)b' - b'(cb) = [cb, b'] \notin F^*.$$

Since ca is an additive commutator, the assumptions in the Theorem imply that there exists $k > 0$ so that

$$1 = a^k = (ca)^k = c^k a^k$$

and hence

$$c^k = 1.$$

So any element of F^* is periodic. Hence $\mathrm{char}(F) = \mathrm{char}(D) > 0$. Because a is not central and periodic it follows from Theorem 5.3.1 that there exists an additive commutator $y \in D^*$ so that

$$yay^{-1} = a^i \neq a \ \ (i > 0).$$

Because of the assumptions in the Theorem, also y is periodic. It follows that

$$\langle a, y \rangle = \langle a \rangle \ \langle y \rangle$$

is a finite periodic subgroup of D^*. Corollary 5.1.2 yields that this group is cyclic. But then $yay^{-1} = a$, a contradiction. □

5.4 Algebraic Skew Fields

An algebra A over a field F is said to be algebraic if every element of A is algebraic over F. Note that such an algebra is a skew field provided it is a domain.

Clearly finite dimensional algebras are algebraic algebras.

Theorem 5.4.1 *(Jacobson) If a skew field D is algebraic over a finite field F then D is a field.*

Proof. Let $p = \mathrm{char}(F)$. Let $d \in D$. Then $F[d]$ is algebraic extension of F. Since $F[d]$ also is a finite ring, it is a field. So $|F[d]| = p^n$ for some n. Hence $d^{p^n} = d$. Theorem 5.3.2 then implies that D is a field. □

Theorem 5.4.2 *(Frobenius) Suppose D is an $\mathbf{R}$-algebra. If D is a skew field which is algebraic over $\mathbf{R}$, then D is isomorphic (as an $\mathbf{R}$-algebra) with either $\mathbf{R}$, $\mathbf{C}$ or $\mathbf{H}(\mathbf{R})$.*

Proof. If $\dim_{\mathbf{R}} D = 1$ then $D = \mathbf{R}$. Suppose thus that $\dim_{\mathbf{R}} D \geq 2$. Choose $\alpha \in (D \setminus \mathbf{R})$. Then $\mathbf{R} \subseteq \mathbf{R}[\alpha]$ and α is algebraic over $\mathbf{R}$. So $\mathbf{R}[\alpha] \cong \mathbf{C}$. So D has a subfield isomorphic with $\mathbf{C}$ and D becomes a left $\mathbf{C}$-vector space. Let $i \in \mathbf{C}$ so that $i^2 = -1$. Put

$$D^+ = \{d \in D \mid di = id\}$$

and

$$D^- = \{d \in D \mid di = -id\}.$$

Clearly D^+ and D^- are $\mathbf{C}$-subspaces of ${}_{\mathbf{C}}D$. Moreover,

$$D^+ \cap D^- = \{0\}.$$

We now show that

$$D = D^+ + D^-.$$

Indeed, let $d \in D$, then

$$d^+ = id + di \in D^+$$

and

$$d^- = id - di \in D^-.$$

Because

$$d^+ + d^- = 2id$$

we get that

$$d = (2i)^{-1}(d^+ + d^-) \in D^+ + D^-.$$

Note that for all $d^+ \in D^+$, $\mathbf{C}[d^+]$ is an algebraic field extension of $\mathbf{C}$. Hence $\mathbf{C}[d^+] = \mathbf{C}$. So, if $D^- = \{0\}$ then $D = \mathbf{C}$.

Suppose thus that $D^- \neq \{0\}$ and choose $0 \neq z \in D^-$. Consider the map

$$f : D^- \to D^+ : x \mapsto xz.$$

Clearly f is $\mathbf{C}$-linear and injective. Because $\dim_{\mathbf{C}} D^+ = 1$ it follows that $\dim_{\mathbf{C}} D^- = 1$ and thus

$$\dim_{\mathbf{R}} D = 2\dim_{\mathbf{C}} D = 4.$$

Because z is algebraic over $\mathbf{R}$ it must be a root of a quadratic real polynomial. Hence

$$z^2 \in \mathbf{R} + \mathbf{R}z.$$

Furthermore, $z^2 = f(z) \in D^+ = \mathbf{C}$. Consequently,

$$z^2 \in \mathbf{C} \cap (\mathbf{R} + \mathbf{R}z) = \mathbf{R}.$$

If $z^2 > 0$ (in $\mathbf{R}$), then $z^2 = r^2$ for some $r \in \mathbf{R}$. But then $z = \pm r \in \mathbf{R}$, a contradiction.

So, $z^2 < 0$. It follows that $z^2 = -r^2$ for some $r \in \mathbf{R}^+$. Put $j = r^{-1}z$. Then, $j^2 = -1 = i^2$ and $ji = -ij$. So

$$D = \mathbf{C} + \mathbf{C}j = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}ij = \mathbf{H}(\mathbf{R}).$$

□

The previous theorem is not valid if one replaces $\mathbf{R}$ by $\mathbf{Q}$. Over $\mathbf{Q}$ there exist many skew fields.

5.5 Exercises

1. Let R be a domain and D a subring of R which is a division ring. If R is finite dimensional as a right D-vector space, prove that R is a division ring as well.

2. Prove that any finite prime ring is a matrix ring over a field.

3. Show that a nonzero ring R is a division ring if and only if, for any $1 \neq a \in R$ there exists $b \in R$ so that $a + b = ab$ (or equivalently, any $1 \neq a \in R$ is right quasi regular

Chapter 6

Goldie Theorems

In this chapter we prove some theorems that show that some rings can be embedded in "nicer rings", such as, semisimple rings or simple Artinian rings. In the commutative case it is well known that every domain is a subring of a field. The smallest such field is the field of fractions; this is obtained by inverting the nonzero elements (i.e. by localizing with respect to the multiplicatively closed set of nonzero elements). We begin this chapter with considering localisations within noncommutative rings.

6.1 Ore Localisations

Recall that an element s in a ring R is called regular (or a nonzero divisor) if $rs \neq 0$ and $sr \neq 0$ for any $0 \neq r \in R$. A subset S of R is said to be *regular* if every element of S is regular in R.

Definition 6.1.1 *Let S be (multiplicative) submonoid of a ring R. A ring Q is said to be a left ring of quotients (or a left localisation) of R with respect to S if the following conditions are satisfied:*

1. *there exists a ring homomorphism*

$$f : R \to Q$$

so that $f(s)$ is invertible in Q for any $s \in S$, and

$$\ker(f) = \{r \in R \mid sr = 0 \text{ for some } s \in S\},$$

2. *every element of Q can be written in the form*

$$(f(s))^{-1}\,(f(r))$$

for some $s \in S$ and $r \in R$. (Abusing notation, we often will simply write the element $(f(s))^{-1}\,(f(r))$ as $s^{-1}r$.)

If S is the submonoid of R consisting of all regular elements and $f : R \to Q$ is injective, then Q is said to be the classical ring of left quotients of R, and R is called an order in Q.

We first will determine necessary and sufficient conditions for the classical ring of quotients to exist.

Definition 6.1.2 *A left Ore set in a ring R is a submonoid S that satisfies the following conditions:*

1. *for any $s_1 \in S$ and for any $r_1 \in R$ there exist $s_2 \in S$ and $r_2 \in R$ so that*

$$s_2 r_1 = r_2 s_1,$$

and

2. *for any $r \in R$ and $s \in S$:*

$$rs = 0 \text{ implies } s'r = 0 \text{ for some } s' \in S.$$

Proposition 6.1.3 *If a ring R has a ring of left quotients with respect to a submonoid S then S is a left Ore subset.*

Proof. Suppose R has a ring of left quotients and let

$$f : R \to Q$$

be the homomorphism mentioned in Definition 6.1.1. Suppose $s_1 \in S$ and $r_1 \in R$. Then there exist $s \in S$ and $r \in R$ so that

$$f(r_1)f(s_1)^{-1} = f(s)^{-1}f(r),$$

Hence

$$f(sr_1) = f(rs_1),$$

that is,

$$f(sr_1 - rs_1) = 0$$

and thus $sr_1 - rs_1 \in \ker(f)$. So, there exists $s' \in S$ with

$$0 = s'(sr_1 - rs_1) = ((s's)r_1 - (s'r)s_1.$$

Put $s_2 = s's$ and $r_2 = s'r$ then we obtain

$$s_2r_1 = r_2s_1.$$

This proves part (1) of the definition of a left Ore set.

Suppose now that $r \in R$ and $s \in S$ are such that $rs = 0$. Then

$$0 = f(rs)f(s)^{-1} = f(r).$$

Hence there exists $s' \in S$ with $s'r = 0$. This also proves part (2) of the definition of left Ore set. □

If the set of all regular elements is a left Ore set in a ring R then R is called a left Ore ring.

Proposition 6.1.4 *Let S be a left Ore set in a ring R.*

1. *The following defines an equivalence relation $\sim$ on the set $S \times R$:*

   $$(s_1, r_1) \sim (s_2, r_2) \text{ if and only if } rr_1 = r'r_2 \text{ and } rs_1 = r's_2 \in S$$

   for some $r, r' \in R$. The equivalence class of (s, r) is denoted by $s^{-1}r$. The set of all equivalence classes is denoted by $S^{-1}R$.

2. *If $s \in S$ and $as \in S$, for some $a \in R$, then $(as)^{-1}(ar) = s^{-1}r$ in $S^{-1}R$.*

3. *A map g with domain $S^{-1}R$ is well defined if and only if $g(s_1^{-1}r_1) = g((rs_1)^{-1}(rr_1))$ for any $rs_1 \in S$.*

4. *$S^{-1}R$ has a natural ring structure. Moreover, $S^{-1}R$ is a ring of left quotients of R with respect to S*

Proof (1) Clearly $\sim$ is reflexive and symmetric. Before proving the transitivity we first prove the following claim:

if $(s_1, r_1) \sim (s_2, r_2)$ and $as_1 = a's_2 \in S$ (with $a, a' \in R$)
then there exists $b \in R$ so that $bar_1 = ba'r_2$ and $bas_1 = ba's_2 \in S$

Indeed, because $(s_1, r_1) \sim (s_2, r_2)$ there exist $r, r' \in R$ so that $rr_1 = r'r_2$ and $rs_1 = r's_2 \in S$. Because S is a left Ore set and $as_1 \in S$ there exist $r'' \in R$ and $s'' \in S$ so that

$$s''(rs_1) = r''(as_1).$$

Hence

$$(s''r - r''a)s_1 = 0.$$

Hence there exists $s_1' \in S$ so that

$$s_1'(s''r - r''a) = 0,$$

or equivalently

$$s_1's''r = s_1'r''a.$$

Now, because $as_1 = a's_2$, we get

$$s_1'r''(a's_2) = s_1'r''(as_1) = s_1's''rs_1 = s_1's''r's_2,$$

and thus

$$(s_1'r''a' - s_1's''r')s_2 = 0.$$

Hence, for some $s_2' \in S$,

$$s_2's_1'r''a' = s_2's_1's''r'.$$

Let $b = s_2's_1'r''$ and $s = s_2's_1's''$. So

$$ba' = sr'$$

and

$$ba = s_2'(s_1'r''a) = s_2'(s_1's''r) = sr.$$

So

$$bar_1 = srr_1 = sr'r_2 = ba'r_2.$$

Also, because $as_1 = a's_2 \in S$,

$$bas_1 = ba's_2$$

and

$$bas_1 = s_2's_1'r''(as_1) = s_2's_1's''(rs_1) \in S.$$

This proves the claim.

We now prove the transitivity of $\sim$. Hence, suppose $(s_1, r_1) \sim (s_2, r_2)$ and $(s_2, r_2) \sim (s_3, r_3)$. Let $a_i, a_i' \in R$ be such that. for $i = 1, 2$,

$$a_i r_i = a_i' r_{i+1}$$

and

$$a_i s_i = a_i' s_{i+1} \in S.$$

Also, there exist $s \in S$ and $a \in R$ such that

$$s(a_2 s_2) = a(a_1' s_2).$$

We obtain

$$(aa_1)s_1 = (aa_1')s_2 = s(a_2 s_2) \in S.$$

We now apply the mentioned claim on the elements aa_1 and sa_2. So we obtain an element $b \in R$ with

$$b(aa_1)r_1 = b(sa_2)r_2$$

and

$$b(aa_1)s_1 = b(sa_2)s_2 \in S.$$

We get

$$(baa_1)r_1 = bsa_2 r_2 = (bsa_2')r_3$$

and

$$(baa_1)s_1 = bsa_2 s_2 = (bsa_2')s_3 \in S.$$

So

$$(s_1, r_1) \sim (s_3, r_3).$$

(2) and (3) are obvious.

(4) We define an addition and multiplication as follows:

$$(s_1^{-1}r_1)(s_2^{-1}r_2) = (as_1)^{-1}(rr_2)$$

where $r, a \in R$ are such that $as_1 \in S$ and $ar_1 = rs_2$, and

$$(s_1^{-1}r_1) + (s_2^{-1}r_2) = (as_1)^{-1}(ar_1 + rr_2)$$

where $r, a \in R$ are such that $as_1 \in R$ and $as_1 = rs_2$. Of course we have to show that these operations are well defined. This is done in three steps:

(i) independence of r and a,

(ii) independence in the first term (resp. factor),

(iii) independence in the second term (resp. factor).

We give the prove for the multiplication.

(i) Because S is a left Ore set, there exist $r_0 \in R$ and $s_0 \in S$ so that $s_0r_1 = r_0s_2$. We prove that for every choice of r and a,

$$(as_1)^{-1}(rr_2) = (s_0s_1)^{-1}(r_0r_2).$$

Indeed, let $r' \in R$ and $s' \in S$ be such that

$$r's_0 = s'a.$$

Then we obtain

$$\begin{aligned} s'(rs_2) &= s'(ar_1) \\ &= (s'a)r_1 \\ &= (r's_0)r_1 \\ &= r'r_0s_2 \end{aligned}$$

So,

$$(s'r - r'r_0)s_2 = 0,$$

and therefore there exists $s \in S$ with

$$ss'r = sr'r_0.$$

Also

$$sr's_0s_1 = ss'as_1 \in S.$$

Moreover, by part (2) of the proposition,

$$\begin{aligned}(s_0s_1)^{-1}(r_0r_2) &= (sr's_0s_1)^{-1}sr'r_0r_2\\ &= (ss'as_1)^{-1}ss'rr_2\\ &= (as_1)^{-1}rr_2\end{aligned}$$

(ii) To prove the independence of the first factor it is sufficient (because of part (2)) to show that

$$\left((bs_1)^{-1}br_1\right)\ (s_2^{-1}r_2) = (s_1^{-1}r_1)(s_2^{-1}r_2),$$

whenever $bs_1 \in S$. To prove this let $r \in R$ and $s \in S$ be so that

$$s(br_1) = rs_2.$$

Then

$$s(bs_1) \in S,$$

and thus (because of the definition),

$$\begin{aligned}\left((bs_1)^{-1}br_1\right)(s_2^{-1}r_2) &= (sbs_1)^{-1}rr_2\\ &= ((sb)s_1)^{-1}(rr_2\end{aligned}$$

Because $(sb)r_1 = rs_2$ and $(sb)s_1 \in S$ we get

$$\left((bs_1)^{-1}br_1\right)\ (s_2^{-1}r_2) = (s_1^{-1}r_1)(s_2^{-1}r_2).$$

(iii) We now prove the independence in the second factor. It is sufficient to show that

$$(s_1^{-1}r_1)((bs_2)^{-1}br_2) = (s_1^{-1}r_1)(s_2^{-1}r_2),$$

for all $b \in R$ with $bs_2 \in S$. Well, let $r \in R$ and $s \in S$ be so that $sr_1 = rbs_2$ (note that $ss_1 \in S$). Then

$$\begin{aligned}(s_1^{-1}r_1)((bs_2)^{-1}br_2) &= (ss_1)^{-1}rbs_2\\ &= (s_1^{-1}r_1)(s_2^{-1}r_2)\end{aligned}$$

(the latter equality holds because $sr_1 = (rb)s_2$).

Hence we have proved that the operations are indeed well defined.

Let $f : R \to S^{-1}R : r \mapsto 1^{-1}r$. Clearly $r_1 \in \ker f$ if and only if $1^{-1}r_1 = 1^{-1}0$. The latter holds precisely when there exist $r, r' \in R$ so that

$$rr_1 = r'0 \text{ and } r = r' \in S.$$

So, $\ker f = \{r_1 \in R \mid rr_1 = 0 \text{ for some } r \in S\}$. Also, $f(s)(s^{-1}1) = 1 = (s^{-1}1)f(s)$. Hence $f(s)$ is invertible for any $s \in S$. This proves the result. □

6.2 Properties of Localisations

If S is a left Ore set consisting of regular elements then $\ker f = \{0\}$ and hence we can identify R with its image in $S^{-1}R$.

Theorem 6.2.1 *Let S be a left Ore set in a ring R. If $g : R \to T$ is a ring homomorphism so that $g(s)$ is invertible for any $s \in S$, then there exists a unique ring homomorphism*

$$\overline{g} : S^{-1}R \to T$$

so that $\overline{g}(1^{-1}r) = g(r)$, for any $r \in R$. Moreover,

1. *$\overline{g}(s^{-1}r) = g(s)^{-1}g(r)$, for any $r \in R$ and $s \in S$,*
2. *$\ker \overline{g} = S^{-1}(\ker g)$.*

Proof. Exercise.

We verify that $\overline{g}$ a homomorphism is for the multiplication. So, let $s_1^{-1}r_1, s_2^{-1}r_2 \in S^{-1}R$. Then

$$(s_1^{-1}r_1)(s_2^{-1}r_2) = (as_1)^{-1}(rr_2)$$

where $r, a \in R$ are such that $as_1 \in S$ and $ar_1 = rs_2$. Then, $\overline{g}(s_1^{-1}r_1) = g(s_1)^{-1}g(r_1)$, $\overline{g}(s_2^{-1}r_2) = g(s_2)^{-1}g(r_2)$ and $\overline{g}(s_1^{-1}r_1)(s_2^{-1}r_2) = (g(as_1))^{-1}g(rr_2)$. So, we need to verify that $g(s_1)^{-1}g(r_1)g(s_2)^{-1}g(r_2) = (g(as_1))^{-1}g(rr_2)$, or equivalently, $g(a)g(s_1)g(s_1)^{-1}g(r_1)g(s_2)^{-1}g(r_2) = g(rr_2)$. This on its turn is equivalent with proving that $g(a)g(r_1)g(s_2)^{-1}g(r_2) = g(rr_2)$. Now, $ar_1 = rs_2$ yields that $g(a)g(r_1) = g(r)g(s_2)$. Hence we need to show that $g(r)g(s_2)g(s_2)^{-1}g(r_2) = g(rr_2)$ and this clearly holds because g is a homomorphism.

□

Corollary 6.2.2 *A ring R is an order in a skew field if and only if R is an Ore domain.*

Proof. Suppose R is an order in a skew field. Thus $R \subseteq S^{-1}R$, with S the set of all regular elements of R, and $S^{-1}R$ is a skew field. Clearly R is a domain and because of Proposition 6.1.3 we get that $S = R \setminus \{0\}$ is an Ore set.

Conversely, suppose R is an Ore domain. So $S = R \setminus \{0\}$ is an Ore set and R is a domain. Because of Proposition 6.1.4 we get that $S^{-1}R$ is a ring that contains R. Clearly $S^{-1}R$ is a skew field and R is an order in $S^{-1}R$. □

Note that in a left Artinian ring A every regular element is invertible. Hence A equals its classical ring of quotients.

Lemma 6.2.3 *Let S be an Ore set in a ring R.*

1. *for any $s \in S$, $r_1, r_2 \in R$:*

$$s^{-1}r_1 + s^{-1}r_2 = s^{-1}(r_1 + r_2),$$

2. *for any $q_1, \ldots, q_n \in S^{-1}R$, there exist $r_1, \cdots, r_n \in R$, $s \in S$ so that $q_i = s^{-1}r_i$.*

Proof. The first part is easy. We prove the second part by induction on n. So suppose that there exist $r_1, \cdots, r_{n-1} \in R$ and $s \in S$ so that

$$q_i = s^{-1}r_i$$

for $1 \leq i \leq n-1$. Write $q_n = s_n^{-1}r_n$ with $s_n \in S$ and $r_n \in R$. Let $r' \in R$ and $s' \in S$ so that

$$s's_n = r's.$$

Then,

$$(s's_n)^{-1}(s'r_n) = q_n$$

and

$$(s's_n)^{-1}(r'r_i) = (r's)^{-1}r'r_i = s^{-1}r_i = q_i$$

for $1 \leq i \leq n$. □

Lemma 6.2.4 *Let S be a left Ore set in a ring R.*

1. *If L is a left ideal in R then*

$$(S^{-1}R)L = S^{-1}L$$

and

$$L \cap S \neq \emptyset \text{ if and only if } (S^{-1}R)L = S^{-1}R.$$

2. *If R is left Noetherian then $S^{-1}R$ is left Noetherian.*

3. *If S is regular and R is (semi)prime then $S^{-1}R$ is (semi)prime.*

4. *If I is a nilpotent (two-sided) ideal and $S^{-1}I$ is an ideal of $S^{-1}R$ then $S^{-1}I$ is nilpotent.*

Proof. Exercise. □

6.3 Annihilators

A subset L of a ring R is said to be a *left annihilator* if

$$L = \text{ann}_l(S) = \{r \in R \mid rS = \{0\}\}$$

for some subset S of R.

We already know the following properties:

1. $S \subseteq \text{ann}_l(\text{ann}_r(S))$ and $S \subseteq \text{ann}_r(\text{ann}_l(S))$.

2. $\text{ann}_l(\text{ann}_r(\text{ann}_l(S))) = \text{ann}_l(S)$ and $\text{ann}_r(\text{ann}_l(\text{ann}_r(S))) = \text{ann}_r(S)$.

3. $\cap_i \text{ann}_l(S_i) = \text{ann}_l(\sum_i S_i)$.

4. $\sum_i \text{ann}_l(S_i) \subseteq \text{ann}_l(\cap_i S_i)$.

5. $\sum_i \text{ann}_l(S_i) = \text{ann}_l(\cap_i S_i)$ if every S_i is a right annihilator.

6. if R is a subring of T and $S \subseteq R$ then $\text{ann}_{l,R}(S) = R \cap \text{ann}_{l,T}(S)$.

7. if $\text{ann}_l(x) = \text{ann}_l(x^2)$ then $Rx \cap \text{ann}_l(x) = \{0\}$.

One says that a ring satisfies the ascending chain condition on left annihilators if every ascending chain left annihilators stabilizes. We denote this property by ACC(Ann_l). Note that if a ring T satisfies ACC(Ann_l) then so does any subring R.

Lemma 6.3.1 *Let R be a ring satisfying the ascending chain condition on left annihilators. Then,*

1. *every non-zero nil right ideal of R contains a non-zero nilpotent right ideal.*

2. *if, moreover, R is semiprime then R does not contain a non-zero nil left or right ideal.*

Proof. To prove the first part, let L be a nil right ideal and let $0 \leq l \in L$ be so that $\text{ann}_l(l)$ is maximal. Suppose $r \in R$ so that $lr \neq 0$ (if this is always zero then the result follows). Then $lr \in L$ and thus for some $n > 0$,

$$(lr)^n \neq 0 \text{ and } (lr)^{n+1} = 0.$$

Because of the maximality,

$$\text{ann}_l((lr)^n) = \text{ann}_l(l).$$

So $lr \in \text{ann}_l((lr)^n) = \text{ann}_l(l)$ and hence

$$lrl = 0.$$

It follows that

$$lRl = \{0\}$$

and thus lR is nilpotent.

To prove the second part, suppose that R contains a nonzero nil left or right ideal L. Let $0 \neq l \in L$. Then Rl or lR is nil. It follows that lR is nil. By the first part lR contains a nilpotent right ideal. However, because by assumption R is semiprime, this is impossible. □

A left ideal L of a ring R is said to be *left essential* if $L \cap X \neq \{0\}$ for any nonzero left ideal X of R.

Lemma 6.3.2 *Let R be a semiprime ring and $0 \neq r \in R$. If R satisfies the ascending chain condition on left annihilators then $ann_l(r)$ is not essential in R.*

Proof. Let $J = \{r \in R \mid \text{ann}_l(r) \text{ is essential}\}$. Because, for all $a \in R$,

$$\text{ann}_l(r) \subseteq \text{ann}_l(ra)$$

we get that J is a right ideal in R. We have to prove that $J = \{0\}$. Because of Lemma 6.3.1 it is sufficient to show that J is nil. To prove this, let $r \in J$. Then

$$\text{ann}_l(r) \subseteq \text{ann}_l(r^2) \subseteq \text{ann}_l(r^3) \subseteq \cdots$$

The condition ACC(ann_l) yields that for some n,

$$\text{ann}_l(r^n) = \text{ann}_l(r^{n+1}) = \cdots$$

Hence

$$\text{ann}_l(r^n) = \text{ann}_l(r^{2n}).$$

Consequently,

$$Rr^n \cap \text{ann}_l(r^n) = \{0\}.$$

Because $r^n \in J$, it follows that $Rr^n = \{0\}$ and thus $r^n = 0$. □

Lemma 6.3.3 *Let R be a semiprime ring satisfying the ascending chain condition on left annihilators. If Rr is essential then $ann_r(r) = \{0\}$.*

Proof. If $a \in \text{ann}_r(r)$ then

$$Rr \subseteq \text{ann}_l(a).$$

So $\text{ann}_l(a)$ is essential. Because of Lemma 6.3.2, we get that $a = 0$. □

6.4 Goldie rings

A ring is said to satisfy the ascending chain condition on direct summands (of left ideals) if there do not exist strict ascending chains of the form

$$L_1 \subset L_1 \oplus L_2 \subset L_1 \oplus L_2 \oplus L_3 \subset \cdots$$

with every L_i a left ideal of R. We denote this condition by AAC$\oplus$.

Definition 6.4.1 *A ring R is (left) Goldie if R satisfies both the ascending chain condition on left annihilators and the ascending chain condition on direct summands of left ideals.*

Examples of left Goldie rings are semisimple Artinian rings.

Lemma 6.4.2 *Let R be a ring and $r \in R$ so that $ann_l(r) = \{0\}$.*

1. *If L is a left ideal of R and $L \cap Rr = \{0\}$ then $\sum_{i\in\mathbf{N}} Lr^i = \oplus_{i\in\mathbf{N}} Lr^i$.*
2. *If R satisfies the ascending chain condition on direct summands of left ideals then Rr is essential in R.*

Proof. To prove part one, assume that $\sum_{i\in\mathbf{N}} Lr^i$ is not a direct sum. Then

$$\sum_{i=m}^{n} a_i r^i = 0$$

for some $a_i \in L$ and $a_m \neq 0$. Because, by assumption, $\mathrm{ann}_l(r^m) = (0)$ we get that $m = 0$. Thus

$$a_m = -\sum_{i=1}^{n-m} a_{i+m} r^i \in L \cap Rr = (0),$$

a contradiction.

The second part now follows easily as, by part one, $L \cap Rr \neq (0)$ for all nonzero left ideals L of R. □

Proposition 6.4.3 *Let R be a semiprime Goldie ring. An element $r \in R$ is regular if and only if $ann_l(r) = \{0\}$.*

Proof. If r is regular then, of course, $\mathrm{ann}_l(r) = (0)$. Conversely, suppose $\mathrm{ann}_l(r) = (0)$. Because of Lemma 6.4.2 we then get that Rr is an essential left ideal of R. Hence, by Lemma 6.3.3, $\mathrm{ann}_r(r) = (0)$. Thus r is regular. □

Proposition 6.4.4 *An essential left ideal L of a semiprime Goldie ring contains a regular element.*

Proof. Because of Proposition 6.4.3 it is sufficient to show that there exists an element $r \in L$ so that $\text{ann}_l(r) = (0)$.

Because of Lemma 6.3.1, there exists $r_1 \in L$ so that r_1 is not nilpotent and $\text{ann}_l(r_1)$ is maximal (among $\text{ann}_l(r)$ with $r \in L$ not nilpotent). Then

$$\text{ann}_l(r_1^2) = \text{ann}_l(r_1)$$

and thus

$$Rr_1 \cap \text{ann}_l(r_1) = (0).$$

We repeat this process. Hence, suppose that we already have found $r_1, \cdots, r_k \in L$ so that the left ideal generated by $Rr_1, \cdots, Rr_k$ and $A_k = L \cap \text{ann}_l(r_1) \cap \cdots \text{ann}_k(r_k)$ generate a direct sum. If $A_k \neq (0)$, then A_k is not nil and hence there exists $r_{k+1} \in A_k$ with $\text{ann}_l(r_{k+1})$ maximal (among the left annihilators of this form). It follows that

$$Rr_{k+1} \cap \text{ann}_l(r_{k+1}) = (0)$$

and thus

$$Rr_1, \cdots, Rr_{k+1}, A_{k+1} = L \cap \text{ann}_l(r_1) \cap \cdots \text{ann}_l(r_{k+1})$$

generate a direct sum. Because of the ascending chain condition on direct summands we get that

$$A_k = (0)$$

for some k. Because L is essential this implies

$$\text{ann}_l(r_1) \cap \cdots \cap \text{ann}_l(r_k) = (0).$$

Put $r = r_1 + \cdots + r_k$. Hence, if $a \in R$ and $0 = ar = a(r_1 + \cdots + r_k)$ then $ar_i = 0$ for each i (because of the direct sum). So $a \in \cap_{i=1}^k \text{ann}_l(r_i) = (0)$. This proves that $\text{ann}_l(r) = 0$. Because of Proposition 6.4.3, $r \in L$ is regular. □

Lemma 6.4.5 *Let L be an essential left ideal in a ring R. If $r \in R$ then*

$$Lr^{-1} = \{a \in R \mid ar \in L\}$$

also is an essential left ideal in R.

Proof. Let L' be a left ideal of R and suppose $L' \cap Lr^{-1} = (0)$. Then

$$(L' \cap Lr^{-1})r = (0).$$

Now

$$L'r \cap L \subseteq (L' \cap Lr^{-1})r.$$

Thus

$$L'r \cap L = (0).$$

Because L is essential it follows that $L'r = (0)$. But then

$$L' \subseteq Lr^{-1}$$

and therefore $L' = L' \cap Lr^{-1} = (0)$. □

Theorem 6.4.6 *(Second Goldie Theorem) The following are equivalent for a ring R:*

1. *R is semiprime Goldie,*
2. *A left ideal is essential if and only if it contains a regular element.*
3. *R is an Ore ring and its classical ring of quotients is semisimple Artinian.*

Proof. That (1) implies (2) follows from Lemma 6.4.2 and Proposition 6.4.4.

To prove that (2) implies (3) we first show that R is a left Ore ring. Suppose thus that $a, r \in R$ and a is regular. Because of the assumption, Ra is essential and thus, by Lemma 6.4.5, $(Ra)r^{-1}$ also is essential. So, again by the assumption, $(Ra)r^{-1}$ contains a regular element a', say. But then $a'r \in Ra$ and thus $a'r = r'a$ for some $a' \in R$.

Let Q be the ring of left quotients of R. To prove that Q is semisimple Artinian it is sufficient to show that the only nonzero essential left ideal of Q is Q itself. Indeed, let L be an arbitrary left ideal of Q, then (using Zorn's lemma) there exists a left ideal L' of Q so that $L \oplus L'$ is an essential left ideal of Q. Hence, $L \oplus L' = Q$. It follows that every left ideal of Q is a direct summand of Q, and thus Q is semisimple.

So, let L be an essential left ideal of Q and suppose $L \neq Q$. Then $L \cap R$ is essential in R. Hence, by the assumptions, L contains a regular

element. Because this regular element is invertible in Q we get that $L = Q$.

We now prove that (3) implies (1). Because Q satisfies the ascending chain condition on left ideals, it clearly satisfies ACC(ann_l). Hence also the subring R satisfies ACC(ann_l).

We now first show that if L is an essential left ideal of R then L contains a regular element. Indeed, let $Q = S^{-1}R$ be the classical ring of left quotients. Then QL is essential in Q. So $QL = Q$ and hence $L \cap S \neq \emptyset$. So, L contains a regular element.

Next we show that R is semiprime. Suppose N is an ideal of R with $N^2 = (0)$. Let L be a left ideal of R so that $N + L$ is essential in R and $N \cap L = (0)$. Hence, by the previous, $L + N$ contains a regular element s. Also

$$Ns \subseteq N(L + N) \subseteq NL \subseteq L \cap N = \{0\}.$$

Because s is regular this yields $N = \{0\}$.

Finally we show that ACC$\oplus$ holds in R. Suppose therefore that $\{L_i \mid i \in I\}$ is a set of nonzero left ideals of R so that $\sum_{i\in I} L_i = \oplus_{i\in I} L_i$. Then, if $q_i \in QL_i$ and $\sum_{i=1}^{t} q_i = 0$ (write $q_i = s^{-1}r_i$, with s regular and $r_i \in R$) then

$$\sum_{i=1}^{t} r_i = 0.$$

So $r_i = 0$ and thus $q_i = 0$ (for all $1 \leq i \leq t$). Thus

$$\sum_{i\in I} QL_i = \oplus_{i\in I} QL_i.$$

Because Q does not contain infinite direct sums we get that $|I| < \infty$. This proves the result. □

Corollary 6.4.7 *(First Goldie Theorem) A ring R is prime Goldie if and only if R is an order in a simple Artinian ring Q*

6.5 Exercises

1. Let L be a left ideal in a ring R. Prove that there exists a left ideal L' of R so that $L + L' = L \oplus L'$ and $L \oplus L'$ is an essential left ideal in R.

2. Let R be a semiprime Goldie ring with classical ring of left quotients Q. Prove that for a left ideal L of R, L is essential in R if and only if QL is an essential left ideal in Q.

3. A ring R is said to have (left) uniform (Goldie) dimension n ($\neq 0$) if there is no set of nonzero left ideals $L_1, \cdots, L_n$ of R so that $L_1 + \cdots + L_n = L_1 \oplus \cdots \oplus L_n$, with n minimal possible. A ring R satisfies $\mathrm{ACC}_n(\mathrm{Ann})$ if every chain of left annihilators has length less than or equal to n. One says that R has Goldie rank n if R has uniform dimension n and satisfies $\mathrm{ACC}_n(\mathrm{Ann})$. Prove

   (a) that if R satisfies $\mathrm{ACC}_n(\mathrm{Ann})$ then any subring T of R satisfies $\mathrm{ACC}_n(\mathrm{Ann})$.

   (b) a semiprime Goldie ring has (finite) Goldie rank.

4. Prove that a ring R is semiprime Goldie if and only if R the matrix ring $M_n(R)$ is semiprime Goldie.

5. Prove that a ring R is semiprime Goldie if and only if the polynomial ring $R[X]$ is semiprime Goldie.

Bibliography

[1] I. Martin Isaacs, Algebra, A graduate course, Brooks/Cole Publshing Company, Pacific Grove, California, 1994. ISBN: 0-534-19002-2

[2] T.Y. Lam, A first course in noncommutative rings, Springer-Verlag, Graduate Texts in Mathematics 131, 1991. (ISBN: 0-387-97523-3)

[3] D.S. Passman, A course in ring theory, Wdasworth & Brooks/Cole, 1991. (ISBN: 0-534-13776-8)

[4] L.H. Rowen, Ring Theory, Academic Press, 1991. (ISBN: 0-12-599840-6)

Index