# Rings and modules

Fall 2023

Lecturer: Valdis Laan

Notes: Valdis Laan, Kristo Väljako

February 6, 2024

# Contents

# Chapter 1

# Basic notions

## 1.1 Ring, subring, homomorphism

The most important notion in this course is that of a ring.

**Definition 1.1.** A **ring** is a set $R$ equipped with two binary operations $+, \cdot : R \times R \longrightarrow R$ (called **addition** and **multiplication**, respectively) such that

**R1.** $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$;

**R2.** there exists an element $0 \in R$ (called the **zero**) such that $a + 0 = a = 0 + a$ for all $a \in R$;

**R3.** for every $a \in R$ there exists an element $-a \in R$ such that $a + (-a) = 0 = (-a) + a$;

**R4.** $a + b = b + a$ for all $a, b \in R$;

**R5.** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$;

**R6.** $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$;

**R7.** $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Usually one writes $ab$ instead of $a \cdot b$.

Conditions R1–R4 say that $(R, +)$ is an abelian group (the **additive group** of the ring) and R5 says that $(R, \cdot)$ is a semigroup (the **multiplicative semigroup** of the ring). Conditions R6 ja R7 are called **distributivity laws**.

As in every abelian group, one can define the **difference** of two elements $a$ and $b$ of a ring by

$$a - b := a + (-b).$$

The following proposition is easy to verify.

**Proposition 1.2.** *Each ring $R$ has the following properties:*

1. *for every $a, b, c \in R$, if $a + b = c$, then $a = c - b$;*

2. *$0a = 0 = a0$ for all $a \in R$;*

3. $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$;

4. $a(b-c) = ab - ac$ *for all* $a, b, c \in R$;

5. $(a-b)c = ac - bc$ *for all* $a, b, c \in R$.

**Definition 1.3.** An element $e$ of a ring $R$ is called an **identity element** if $ae = a = ea$ for all $a \in R$. In such a case $R$ is called a **ring with identity** or a **unital ring**. From now on we will denote the identity element of a ring $R$ (if it exists) by the symbol 1.

**Definition 1.4.** A ring $R$ is called a **commutative ring** if $ab = ba$ for all $a, b \in R$.

**Definition 1.5.** A ring $(R, +, \cdot)$ is called

- a **division ring** if $(R \setminus \{0\}, \cdot)$ is a group;
- a **field** if $(R \setminus \{0\}, \cdot)$ is an abelian group.

So we have the following implications:

$$\text{field} \implies \text{division ring} \implies \text{ring with identity} \implies \text{ring}.$$

**Remark 1.6.** It is possible, that $1 = 0$ in a ring. In such a case the ring contains only one element, because, for every element $a$, $a = a1 = a0 = 0$. Hence, if a ring has at least two elements, then in that ring $1 \neq 0$. In particular, $1 \neq 0$ in every division ring and field.

**Example 1.7** (Rings with identity)**.**

1. The well-known number sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields with respect to usual addition and multiplication of numbers.
2. The set $\mathbb{Z}$ of all integers is a commutative ring with identity with respect to the usual addition and multiplication. This ring is not a division ring, because the integer 2 does not have a multiplicative inverse.
3. The *residue class rings* $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, where $n \in \mathbb{N}$, are commutative rings with identity $\overline{1}$. It is well known that $\mathbb{Z}_n$ is a field if and only if $n$ is a prime number.
4. One can consider the set

   $$\mathbb{H} := \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

   of *quaternions*[1]. The elements $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ are sometimes called *quaternion units*. The addition on the set $\mathbb{H}$ is defined coordinate-wise:

   $$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = (a + a') + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$$

   for every $a, a', b, b', c, c', d, d' \in \mathbb{R}$, and the multiplication is defined using the table

| $\cdot$ | 1 | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ |
|---|---|---|---|---|
| 1 | 1 | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ |
| $\mathbf{i}$ | $\mathbf{i}$ | $-1$ | $\mathbf{k}$ | $-\mathbf{j}$ |
| $\mathbf{j}$ | $\mathbf{j}$ | $-\mathbf{k}$ | $-1$ | $\mathbf{i}$ |
| $\mathbf{k}$ | $\mathbf{k}$ | $\mathbf{j}$ | $-\mathbf{i}$ | $-1$ |

[1] Quaternions were discovered by an Irish mathematician William Rowan Hamilton (1805–1865) in 1843.

and extending this to arbitrary expressions using distributivity. With these operations we obtain a ring with the identity element $1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$. This ring is not a field, because it is not commutative: $\mathbf{ij} = \mathbf{k} \neq -\mathbf{k} = \mathbf{ji}$. However, $\mathbb{H}$ is a division ring, because for every quaternion $\eta \in \mathbb{H}$ there exists a quaternion $\eta^{-1} \in \mathbb{H}$ such that $\eta\eta^{-1} = \eta^{-1}\eta = 1$.

5. Let $X$ be a nonempty set and let $\wp(X)$ denote the set of all subsets of $X$. It turns out that $(\wp(X); \Delta, \cap)$, where $\Delta$ denotes the symmetric difference, is a ring. The identity element of this ring is the set $X$ and the zero element is the set $\varnothing$.
6. Consider a singleton $\{0\}$. Define:

$$0 + 0 := 0 \quad \text{and} \quad 0 \cdot 0 := 0.$$

With these operations we obtain a ring which is called a **trivial ring**.

**Example 1.8** (Rings without identity)**.**

1. Consider the set $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$ of even integers. Equipped with the usual addition and multiplication this set is a ring without identity element.
2. Let $(A; +)$ be any abelian group. For every $a, b \in A$ we define

$$ab = 0.$$

In such a way $A$ becomes a ring, which is called a **ring with zero multiplication**. This example shows that every Abelian group can be turned into a ring, although in an uninteresting way.

Now we consider substructures of rings.

**Definition 1.9.** A nonempty subset $S$ of a ring $R$ is called a **subring** if

1. $a + b \in S$ for every $a, b \in S$ ($S$ is closed under addition),
2. $-a \in S$ for every $a \in S$ ($S$ is closed under taking additive inverses),
3. $ab \in S$ for every $a, b \in S$ ($S$ is closed under multiplication).

**Proposition 1.10.** *Every subring of a ring $R$ contains the zero element of $R$.*

*Proof.* Let $S$ be a subring of $R$ and let 0 be the zero element of $R$. Since $S$ is nonempty, it contains some element $a$. Hence it also contains $-a$ and the sum $a + (-a)$. Since the last sum is 0, $S$ must contain 0. □

The following proposition is easy to verify.

**Proposition 1.11.** *A nonempty subset $S$ of a ring $R$ is a subring if and only if*

1. *$a - b \in S$ for every $a, b \in S$,*
2. *$ab \in S$ for every $a, b \in S$.*

Every subring of a ring $R$ is also a ring with respect to the restrictions of the operations of $R$.

**Example 1.12.** 1. The subset $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\} \subseteq \mathbb{Z}$ is a subring of $\mathbb{Z}$ for every $n \in \mathbb{N}$. If $n \geq 2$, then this subring does not have an identity element.

2. The subset $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{R}\} \subset \mathbb{C}$ of *Gaussian integers* is a subring of the complex field $\mathbb{C}$. It is not a division ring.

Now we consider homomorphism of rings.

**Definition 1.13.** Let $R$ and $S$ be rings. A mapping $f : R \to S$ is called a **ring homomorphism** if

1. $f(a + b) = f(a) + f(b)$ for all $a, b \in R$ ($f$ preserves addition);
2. $f(ab) = f(a)f(b)$ for all $a, b \in R$ ($f$ preserves multiplication).

**Proposition 1.14.** *If $f : R \longrightarrow S$ is a ring homomorphism, then*

1. $f(0) = 0$;
2. $f(-a) = -f(a)$ *for all* $a \in R$.

*Proof.* 1. We know that $f(0) = f(0 + 0) = f(0) + f(0)$. Adding $-f(0)$ to both sides we obtain the equality $0 = f(0)$.

2. Since $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$, we see that $f(-a)$ is the additive inverse of $f(a)$, i.e. $f(-a) = -f(a)$. □

**Remark 1.15.** If $R$ and $S$ are rings with identity (we denote them by $1_R$ and $1_S$, respectively), then a ring homomorphism $f : R \longrightarrow S$ need not preserve the identity. For example, the constant mapping

$$R \longrightarrow S, \quad a \mapsto 0$$

is such, when $S$ has more than one element. If $f : R \longrightarrow S$ is such that $f(1_R) = 1_S$, then we say that $f$ is an **identity preserving homomorphism** between rings with identity.

**Example 1.16.** The mapping

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_n, \ a \mapsto \overline{a}$$

is a ring homomorphism which preserves identity.

**Definition 1.17.** The **kernel** of a ring homomorphism $f : R_1 \to R_2$ is the set

$$\mathrm{Ker}(f) = \{a \in R_1 \mid f(a) = 0\}.$$

Precisely as in the case of vector spaces one can prove the following result.

**Proposition 1.18.** *A ring homomorphism $f : R_1 \to R_2$ is injective if and only if* $\mathrm{Ker}(f) = \{0\}$.

**Definition 1.19.** A bijective ring homomorphism is called a **ring isomorphism**. If $f : R \longrightarrow S$ is a ring isomorphism, then $R$ and $S$ are said to be **isomorphic** rings. In such case we write $R \simeq S$.

**Example 1.20.** In the course "Algebra I", usually the following well-known isomorphism is proved: if $V$ is an $n$-dimensional vector space over a field $K$ with the basis $e$, then

$$f : \mathrm{End}(V) \longrightarrow \mathrm{Mat}_n(K), \quad \varphi \mapsto A^e_\varphi$$

is a ring isomorphism.

**Exercises 1.21.** 1. Prove that if $f : R_1 \longrightarrow R_2$ and $g : R_2 \longrightarrow R_3$ are ring homomorphisms, then the mapping $gf : R_1 \longrightarrow R_3$ is also a ring homomorphism. (This observation allows us to consider the *category* of all rings, where the morphisms are the ring homomorphisms.)

2. Prove that if $f : R \longrightarrow S$ is a ring homomorphism, then the image

$$\mathrm{Im}\,(f) = \{f(a) \mid a \in R\}$$

is a subring of $S$.

2. Prove that the relation $\simeq$ is an equivalence relation on the class of all rings.

# 1.2 New rings from old

In this section we consider some constructions, that allow to create new rings from already existing ones.

## 1.2.1 Direct product

Let $R_1$ and $R_2$ be rings. On the Cartesian product $R_1 \times R_2$ we define operations componentwise:

$$(a, b) + (a', b') := (a + a', b + b'),$$
$$(a, b) \cdot (a'b') := (aa', bb').$$

In such a way we obtain a ring which is called the **direct product** of rings $R_1$ and $R_2$. Similarly one can consider finite direct products $R_1 \times \ldots \times R_n$ and even infinite direct products $\prod_{i \in I} R_i$, where $I$ is some index set and $R_i$, $i \in I$, are rings.

## 1.2.2 Matrix rings

Let $R$ be a nontrivial ring and let $n \geq 2$ be a natural number. The set $\mathrm{Mat}_n(R)$ of all $(n \times n)$-matrices with entries from $R$ is a ring with respect to usual matrix addition and multiplication. If $R$ is a ring with identity, then $\mathrm{Mat}_n(R)$ is also a ring with identity. This ring is noncommutative and it is not a division ring.

More generally, we can consider some set $I$ (possibly infinite) and $(I \times I)$-matrices, which formally are the mappings $A : I \times I \longrightarrow R$. The element at a position $(i, j)$ is $A(i, j)$. We consider the set of all those matrices $A$ where the set

$$\{(i, j) \mid i, j \in I, A(i, j) \neq 0\}$$

is finite, that is, the matrix $A$ has finitely many nonzero entries. We can still add and multiply such matrices in a "usual way" so that the axioms of a ring are satisfied.

### 1.2.3 Polynomial rings

If $R$ is a commutative ring (for example $\mathbb{Z}$ or any field), then there exists the **ring of polynomials** $R[X]$ with respect to a variable $X$. Such rings are considered in the course "Algebra I". An element of $R[X]$ is an exprerssion

$$a_0 + a_1X + a_2X^2 + \ldots + a_nX^n,$$

where $a_i \in R$ and $n \in \mathbb{N} \cup \{0\}$.

More generally, one can consider a finite number of variables $X_1, \ldots, X_n$ and the **ring of multivariate polynomials** $R[X_1, \ldots, X_n]$. Such rings are introduced in the course "Algebra II".

### 1.2.4 Semigroup rings

Let $G$ be a (multiplicative) semigroup and $R$ a ring. Denote

$$R[G] := \{f \colon G \longrightarrow R \mid f(g) \neq 0 \text{ for finitely many } g \in G\}.$$

On the set $R[G]$ we define addition and multiplication by

$$\begin{aligned}(f+h)(g) &:= f(g) + h(g),\\ (f \cdot h)(g) &:= \sum_{g_1g_2=g} f(g_1)h(g_2).\end{aligned}$$

It turns out that the set $R[G]$ is a ring with respect to these operations. The ring $(R[G]; +, \cdot)$ is called a **semigroup ring of** $G$ **over the ring** $R$. If $G$ is a monoid, then one speaks about **monoid ring**, and if $G$ is a group, then one speaks about **group ring**.

We will show that the elements of a semigroup ring $R[G]$ can be presented in a simpler form. Let $f \in R[G]$. For every $g \in G$, denote $f_g := f(g) \in R$. Now we can write the element $f$ as a formal sum

$$f =: \sum_{g \in G} f_g g. \tag{1.1}$$

Notice that this sum contains a finite number of nonzero summands, because by the definition only finite number of the coefficients $f_g$ can be different from zero. Moreover, if $G$ is a finite semigroup, then the sum (1.1) has at most $\#(G)$ nonzero summands.[2] Addition and multiplication in the ring $R[G]$ are performed similarly to the case of ordinary polynomials, i.e.

$$\begin{aligned}f + h &= \sum_{g \in G} (f_g + h_g)g,\\ f \cdot h &= \sum_{g,x \in G} (f_g h_x)(gx).\end{aligned}$$

[2] A reader may notice that the elements of a semigroup ring are similar to polynomials, except instead of the powers of a variable there are elements of the semigroup $G$. More precisely: polynomial ring $R[X]$ is the semigroup ring of the free monoid $\{1, X, X^2, \ldots\}$ (where the multiplication is defined by $X^kX^h = X^{k+h}$) over the ring $R$.

Here the product $gx$ is computed in the semigroup $G$ and the product $f_g h_x$ is computed in the ring $R$.

We note that if $R$ and $G$ are finite, then also $R[G]$ is a finite ring and

$$\#(R[G]) = \#(R)^{\#(G)}. \tag{1.2}$$

For every semigroup ring $R[G]$ there exists a ring homomorphism

$$\eta\colon R[G] \longrightarrow R, \qquad \sum_{g\in G} f_g g \mapsto \sum_{g\in G} f_g,$$

which is called the **augmentation** of the semigroup ring $R[G]$.

**Example 1.22.** Let us consider a concrete example. Take a three element semigroup $G = \{a, b, c\}$ with the Cayley table

| $\cdot$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $c$ |
| $c$ | $a$ | $c$ | $b$ |

and the semigroup ring

$$\mathbb{Z}[G] = \{xa + yb + zc \mid x, y, z \in \mathbb{Z}\}.$$

If any of the coefficients $x, y, z$ is zero, then usually the corresponding summand is omitted. In this semigroup ring we can calculate:

$$(2a - 3b)(b + 4c) = 2ab + 8ac - 3bb - 12bc = 2a + 8a - 3b - 12c = 10a - 3b - 12c.$$

### 1.2.5 Dorroh extension

It turns out that every ring can be embedded into a ring with identity.

Before giving a construction, we recall how elements of an abelian group (in particular elements of a ring) can be multiplied by integers. Let $A$ be an abelian group, $a \in A$ and $z \in \mathbb{Z}$. Then

- $za$ is the sum of $z$ copies of $a$ if $z > 0$;
- $za = -|z|a$ if $z < 0$;
- $za = 0 \in A$ if $z = 0$.

Let $R$ be a ring with the zero element $0_R$. Consider the set $R' := R \times \mathbb{Z}$ together with addition and multiplication defined by

$$\begin{aligned}(r, z) + (s, x) &= (r + s, z + x),\\ (r, z) \cdot (s, x) &= (rs + zs + xr, zx),\end{aligned}$$

where $r, s \in R$ and $z, x \in \mathbb{Z}$. One can prove that $R'$ is a ring with respect to these operations. The pair $(0, 1)$ is its identity element, because

$$(0_R, 1)(r, z) = (0_R r + 1r + z0_R, 1z) = (r, z),$$
$$(r, z)(0_R, 1) = (r0_R + z0_R + 1r, z1) = (r, z)$$

for every $(r, z) \in R \times \mathbb{Z}$. The ring $R'$ is called the **Dorroh**[3] **extension** of the ring $R$. The mapping

$$f\colon R \longrightarrow R \times \mathbb{Z}, \qquad r \longrightarrow (r, 0)$$

is an injective ring homomorphism, because

$$f(r) + f(s) = (r, 0) + (s, 0) = (r + s, 0) = f(r + s),$$
$$f(r)f(s) = (r, 0)(s, 0) = (rs + 0s + 0r, 0 \cdot 0) = (rs + 0 + 0, 0).$$

Hence the ring $R$ is isomorphic to the subring $\mathrm{Im}\,(f) = \{(r, 0) \mid r \in R\}$ of its Dorroh extension $R \times \mathbb{Z}$.

## 1.3 Algebras over fields

Sometimes rings have richer structure — in addition to the ring structure they also have the structure of a vector space.

**Definition 1.23.** Let $K$ be a field. An **algebra over** $K$ or a $K$**-algebra** is a ring $(R, +, \cdot)$ which is also a vector space over $K$ with the same addition and which satisfies

$$k(ab) = (ka)b = a(kb)$$

for all $a, b \in R$ and $k \in K$.

**Definition 1.24.** Let $R$ and $S$ be two $K$-algebras. A mapping $\varphi : R \longrightarrow S$ is called a $K$**-algebra homomorphism** if it is both a homomorphism of rings and vector spaces, that is, it preserves addition, multiplication and scalar multiplication.

**Example 1.25.** 1. Every field $K$ is a $K$-algebra over itself in a natural way.

2. The field $\mathcal{C}$ of complex numbers is an algebra over the field of real numbers. The multiplication by scalars from $\mathbb{R}$ is defined by

$$r(a + bi) := ra + rbi.$$

3. The ring $\mathbb{H}$ of Hamiltonian quaternions is an $\mathbb{R}$-algebra if we define the multiplication by scalars as

$$r(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) := ra + rb\mathbf{i} + rc\mathbf{j} + rd\mathbf{k}.$$

This algebra is called the **algebra of quaternions**.

[3] Joe Lee Dorroh – an American mathematician. This construction first appears in his article from 1932.

4. If $K$ is any field, then the matrix ring $\mathrm{Mat}_n(K)$ is an algebra if the scalar multiplication is defined in the usual way. So we may speak about **matrix algebras**.

5. If $K$ is any field, then the polynomial ring $K[X]$ is an algebra if the multiplication by a scalar $k$ is defined by

$$k(a_0 + a_1X + \ldots + a_nX^n) := ka_0 + ka_1X + \ldots + ka_nX^n.$$

Thus we have **algebras of polynomials**.

6. The set $\mathbb{R}^{\mathbb{R}}$ of all functions $\mathbb{R} \longrightarrow \mathbb{R}$ is an algebra over $\mathbb{R}$ with respect to pointwise defined operations: for every $x \in \mathbb{R}$ put

$$\begin{aligned}(f+g)(x) &:= f(x) + g(x),\\ (fg)(x) &:= f(x)g(x),\\ (kf)(x) &:= kf(x)\end{aligned}$$

where $f, g \in \mathbb{R}^{\mathbb{R}}$, $k \in \mathbb{R}$. For example, the well-known Leibniz rule

$$(fg)' = f'g + fg'$$

is formulated using differentiation and the operations of this ring. For every $x \in \mathbb{R}$, the evaluation map

$$\mathrm{eval}_x : \mathbb{R}^{\mathbb{R}} \longrightarrow \mathbb{R}, \quad f \mapsto f(x)$$

is an $R$-algebra homomorphism, because

$$\begin{aligned}\mathrm{eval}_x(f+g) = (f+g)(x) = f(x) + g(x) = \mathrm{eval}_x(f) + \mathrm{eval}_x(g),\\ \mathrm{eval}_x(fg) = (fg)(x) = f(x)g(x) = \mathrm{eval}_x(f)\mathrm{eval}_x(g),\\ \mathrm{eval}_x(kf) = (kf)(x) = kf(x) = k\mathrm{eval}_x(f).\end{aligned}$$

7. Every Banach algebra, C*-algebra and operator algebra is (among other things) an algebra in the sense of Definition 1.23. Such algebras are studied in functional analysis.

8. Every topological algebra is an algebra in the sense of Definition 1.23. Several Estonian mathematicians have studied topological algebras.

## 1.4 Module, submodule, homomorphism

The definition of a module is similar to the definition of a vector space over a field.

**Definition 1.26.** A set $M$ together with mappings

$$\begin{aligned}M \times M \to M, \quad (a,b) \mapsto a+b,\\ R \times M \to M, \quad (r,a) \mapsto ra\end{aligned}$$

is called a **left module** over a ring $R$ if

**M1.** $(a+b)+c = a+(b+c)$ for all $a, b, c \in M$;

**M2.** there exists an element $0 \in M$ such that $a + 0 = a = 0 + a$ for all $a \in M$;

**M3.** for every element $a \in M$ there exists an element $-a \in M$ such that $a + (-a) = 0 = (-a) + a$;

**M4.** $a + b = b + a$ for all $a, b \in M$;

**M5.** $r(a + b) = ra + rb$ for all $a, b \in M$ and $r \in R$;

**M6.** $(r + s)a = ra + sa$ for all $a \in M$ and $r, s \in R$;

**M7.** $(rs)a = r(sa)$ for all $a \in M$ and $r, s \in R$.

If $M$ is a left $R$-module, then we write ${}_RM$. Dually one can define right $R$-modules. Sometimes we call the mapping $R \times M \longrightarrow M$ a **left $R$-action** on $M$. Some people also use the term **scalar multiplication**, meaning that the elements of $R$ can be considered as analogues of scalars in a vector space.

**Examples 1.27.** 1. Every vector space over a field is a module over that field.

2. Every ring $R$ can be considered as a left module ${}_RR$.

3. The direct product $\mathbb{Z}^n$ is a left $\mathbb{Z}$-module if the operations are defined componentwise. Since $\mathbb{Z}$ is not a field, this module is not a vector space.

4. Every abelian group $A$ can be considered as a $\mathbb{Z}$-module if one defines products $za$, where $z \in \mathbb{Z}$ and $a \in A$, as we did before.

5. Consider the matrix ring $R = \mathrm{Mat}_m(D)$, where $D$ is a division ring. The set $M = \mathrm{Mat}_{m,n}(D)$ is a left $R$-module if the addition is the addition of matrices and the mapping $R \times M \to M$ is defined by matrix multiplication.

**Definition 1.28.** A nonempty subset $N \subseteq M$ is called a **submodule** of a module ${}_RM$ if

1. $a + b \in N$ for all $a, b \in N$;
2. $-a \in N$ for every $a \in N$;
3. $ra \in N$ for all $a \in N$ and $r \in R$.

We write $N \leq M$.

Module homomorphisms are similar to linear mappings between vector spaces.

**Definition 1.29.** Let ${}_RM$ and ${}_RN$ be left $R$-modules. A mapping $f : M \longrightarrow N$ is called a **homomorphism of left $R$-modules** if

1. $f(a + b) = f(a) + f(b)$ for all $a, b \in M$;
2. $f(ra) = rf(a)$ for all $a \in M$ and $r \in R$.

As in the case of vector spaces we see that the following result holds.

**Proposition 1.30.** *A homomorphism of modules $f$ is injective if and only if* $\mathrm{Ker}(f) = 0$.

Let us introduce some notation. Let ${}_RM$ be a left $R$-module, $A \subseteq M$ and $S \subseteq R$. We denote

$$SA := \left\{ \sum_{k=1}^{k^*} s_k a_k \middle| k^* \in \mathbb{N}; a_1, \ldots, a_{k^*} \in A; s_1, \ldots, s_{k^*} \in S \right\} \subseteq M, \tag{1.3}$$

that is, the set $SA$ consists of all finite sums of products of the form $sa$, where $a \in A$ and $s \in S$. Analogous notation is used also for right modules and bimodules.

**Definition 1.31.** Let $R$ be a ring. A module ${}_RM$ is called **unitary** if $RM = M$, i.e. for every $m \in M$ there exist a natural number $k^* \in \mathbb{N}_1$ and elements $m_1, \ldots, m_{k^*} \in M$, $r_1, \ldots, r_{k^*} \in R$ such that

$$m = \sum_{k=1}^{k^*} r_k m_k.$$

**Remark 1.32.** By the definition of an $R$-module, the inclusion $RM \subseteq M$ always holds. Thus to prove that ${}_RM$ is unitary, it suffices to verify the inclusion $M \subseteq MR$.

If $V$ is a vector space over a field $K$, then $1v = v$ for every $v \in V$. Hence every vector space is a unitary $K$-module. This observation will be generalised in the following proposition.

**Proposition 1.33.** *Let $R$ be a ring with identity 1. A module ${}_RM$ is unitary if and only if*

$$\forall m \in M: \quad 1m = m. \tag{1.4}$$

*Proof.* NECESSITY. Assume that ${}_RM$ is unitary. Take $m \in M$. Then there exist $m_1, \ldots, m_{k^*} \in M$ and $r_1, \ldots, r_{k^*} \in R$ such that $m = r_1 m_1 + \ldots + r_{k^*} m_{k^*}$. Now

$$1m = 1 \left( \sum_{k=1}^{k^*} r_k m_k \right) = \sum_{k=1}^{k^*} 1(r_k m_k) = \sum_{k=1}^{k^*} (1r_k) m_k = \sum_{k=1}^{k^*} r_k m_k = m.$$

Hence $1m = m$ for every $m \in M$.
SUFFICIENCY. Assume that the condition (1.4) holds. Then every $m \in M$ can be presented as a sum $1m$ with one summand, thus ${}_RM$ is unitary. □

**Example 1.34.** 1. Every vector space is a unitary module.

2. Let $R$ be any ring (possibly with identity) and let $(A, +)$ be a nontrivial abelian group. Defining the scalar multiplication by

$$R \times A \longrightarrow A, \ (r, a) \mapsto 0_A$$

we obtain a left $R$-module which is not unitary.

## 1.5 Ideals

**Definition 1.35.** A nonempty subset $I$ of a ring $R$ is called a **right (left) ideal**, if

1. $a + b \in I$ for every $a, b \in I$;
2. $-a \in I$ for every $a \in I$;
3. $ar \in I$ ($ra \in I$) for every $a \in I$ and $r \in R$.

An **ideal** is a right ideal which is also a left ideal.

We write $I \trianglelefteq R$ ($I \trianglelefteq_l R$, $I \trianglelefteq_r R$) if $I$ is an ideal (resp. a left ideal, a right ideal) of $R$. If $I$ is a proper ideal of $R$, then we write $I \triangleleft R$, and similarly for proper left or right ideals.

If $R$ is a ring, then $\mathsf{Id}(R)$ ($\mathsf{Id}_l(R)$, $\mathsf{Id}_r(R)$) denotes the set of all ideals (resp. all left ideals, all right ideals) of $R$.

From the definition we see that every right ideal of a ring is a subring. Therefore each right ideal contains the zero element of $R$.

We note that every left ideal $I$ of a ring $R$ can be considered as a left $R$-module with respect to the restriction of the addition defined on $R$ and the mapping

$$R \times I \longrightarrow I, \quad (r, i) \mapsto ri.$$

If $R$ is a ring, then $R$ itself and $\{0\}$ are ideals. These are called **trivial** ideals.

**Example 1.36.** Let $S$ be a ring. In the matrix ring $R = \mathrm{Mat}_n(S)$ we consider a subset $I$ consisting of those square matrices where nonzero elements can appear only in the first row. So

$$I = \left\{ \begin{pmatrix} a_{11} & \dots & a_{1n} \\ 0 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 0 \end{pmatrix} \mid a_{11}, \dots, a_{1n} \in S \right\}.$$

It is easy to see that $I$ is a right ideal of $R$.

**Example 1.37.** Recall that the subset $I = \{(r, 0) \mid r \in R\}$ is a subring of the Dorroh extension $R \times \mathbb{Z}$ of a ring $R$. We claim that it is an ideal. If $r, s \in R$ and $x \in \mathbb{Z}$, then

$$(r, 0)(s, x) = (rs + 0s + xr, 0x) = (rs + xr, 0) \in I,$$

hence $I$ is a right ideal. Analogously one can prove that it is a left ideal.

**Proposition 1.38.** *The kernel of a ring homomorphism is an ideal.*

*Proof.* We leave the proof as an exercise for the reader. □

**Proposition 1.39.** *The intersection of left ideals of a ring is a left ideal.*

*Proof.* Let $I_k$, $k \in K$, be left ideals of a ring $R$ and put $I := \bigcap_{k \in K} I_k \subseteq R$. Since each $I_k$ contains the zero element of $R$, the set $I$ is nonempty. Take $a \in I$ and $r \in R$. Then $a \in I_k$ for every $k \in K$. Since $I_k$ is a left ideal, $ra \in I_k$ for every $k \in K$. It follows that $ra \in I$. The other conditions can be verified in a similar way. □

Clearly, similar statement holds also for right ideals and two-sided ideals. Very often we will formulate and prove a result only for left ideals, but when needed we will also use its right-sided or two-sided version.

Next we introduce some notation that is often used when dealing with different subsets of a ring. If $A, B$ are nonempty subsets of a ring $R$, then

$$A + B := \{a + b \mid a \in A, b \in B\} \subseteq R,$$
$$AB := \left\{ \sum_{k=1}^{n} a_k b_k \mid n \in \mathbb{N}, a_k \in A, b_k \in B \right\} \subseteq R.$$

Using these definitions one can form the sum and product of finitely many nonempty subsets of $R$. One can prove that

$$(A + B) + C = A + (B + C), \quad (AB)C = A(BC)$$

if $A, B, C \subseteq R$. However, in general we do not have the equality $(A + B)C = AC + BC$.

One can also speak about infinite sums of subsets. If $K$ is some index set and $A_k$, $k \in K$, are nonempty subsets of $R$, then we can define

$$\sum_{k \in K} A_k := \left\{ \sum_{k \in K} a_k \mid a_k \in A_k, a_k \neq 0 \text{ for finitely many } k \in K \right\}.$$

If a subset contains only one element, then the brackets are omitted. So instead of $\{a\} + B$ one writes

$$a + B = \{a + b \mid b \in B\}.$$

Using the introduced notation, in our next proposition we will list some basic properties of (left, right) ideals.

**Proposition 1.40.** *Let $A, B, C$ be nonempty subsets of a ring $R$.*

1. *If $A$ is a left ideal, then $AB$ is a left ideal.*
2. *If $A$ is a left ideal and $B$ is a right ideal, then $AB$ is an ideal and $BA \subseteq A \cap B$. In particular, the product of two ideals is an ideal.*
3. *If $A, B$ are right ideals, then $A + B$ is a right ideal and $(A + B)C = AC + BC$ and $C(A + B) = CA + CB$.*

*Proof.* 1. Recall that

$$AB = \left\{ \sum_{k=1}^{n} a_k b_k \mid n \in \mathbb{N}, a_k \in A, b_k \in B \right\} \subseteq R.$$

We know that $0 \in A$ and there exists some $b \in B$. Hence $0 = 0b \in AB$ and $AB$ is nonempty. Clearly $AB$ is closed under addition. If $\sum_{k=1}^{n} a_k b_k \in AB$, then also

$$-\sum_{k=1}^{n} a_k b_k = \sum_{k=1}^{n} (-a_k b_k) = \sum_{k=1}^{n} (-a_k) b_k \in AB,$$

because $-a_k \in A$ for every $k$. For every $r \in R$,

$$r\sum_{k=1}^{n} a_k b_k = \sum_{k=1}^{n} r(a_k b_k) = \sum_{k=1}^{n} (ra_k) b_k \in AB,$$

because $ra_k \in A$ for every $k$.

2. The subset $AB$ is a left ideal by the claim 1 and a right ideal by the dual of claim 1. Hence $AB$ is an ideal.

Take an element $x = \sum_{k=1}^{n} b_k a_k \in BA$. Since $A$ is a left ideal, $b_k a_k \in A$ for every $k$. As $A$ is closed under addition, we conclude that $x \in A$. Similarly we can show that $x \in B$. Hence $x \in A \cap B$ and we have proved the inclusion $BA \subseteq A \cap B$.

3. It is straightforward to show that $A + B$ is a right ideal. Let us prove the equality $(A + B)C = AC + BC$.

If $x \in (A + B)C$, then $x = \sum_{k=1}^{n} (a_k + b_k) c_k$ for some $k \in \mathbb{N}$, $a_k \in A$, $b_k \in B$ and $c_k \in C$. Hence

$$x = \sum_{k=1}^{n} a_k c_k + \sum_{k=1}^{n} b_k c_k \in AC + BC.$$

Conversely, take any $x \in AC + BC$. Then $x = y + z$ where $y \in AC$ and $z \in BC$. We can write $y = \sum_{k=1}^{n} a_k c_k$ and $z = \sum_{l=n+1}^{m} b_l c_l$ for some $n, m \in \mathbb{N}$, $a_k \in A$, $b_l \in B$ and $c_k, c_l \in C$. Now

$$x = y + z = \sum_{k=1}^{n} (a_k + 0) c_k + \sum_{l=n+1}^{m} (0 + b_l) c_l \in (A + B)C,$$

because $0 \in A$ and $0 \in B$. □

**Corollary 1.41.** *If $R$ is a ring, then the poset $(\mathsf{Id}(R), \subseteq)$ is a lattice.*

*Proof.* We need to show that every pair of ideals has a join and meet.

If $I, J \in \mathsf{Id}(R)$, then by Proposition 1.39 and Proposition 1.40 we know that $I \cap J$ and $I + J$ are also ideals in $R$. Clearly $I \cap J$ is the biggest ideal contained in $I$ and $J$, so it is the meet of $I$ and $J$.

We also observe that $I, J \subseteq I + J$. If $H$ is any ideal containing $I$ and $J$, then it must contain all sums $i + j$, where $i \in I$ and $j \in J$, because $H$ must be closed under addition. Hence $H$ contains $I + J$. We have shown that $I + J$ is the smallest ideal containing $I$ and $J$, hence it is the join of $I$ and $J$. □

**Remark 1.42.** 1. In fact, $(\mathsf{Id}(R), \subseteq)$ is a complete lattice equipped with the multiplication $(I, J) \mapsto IJ$ satisfying some further conditions, which make it a structure called *quantale*. We will not emphasize this point of view during this lecture course.

2. In a similar manner one can show that $(\mathsf{Id}_l(R), \subseteq)$ and $(\mathsf{Id}_r(R), \subseteq)$ are lattices (or quantales).

**Definition 1.43.** An element $a$ of a ring $R$ is called

- a **left zero divisor** if $ab = 0$ for some nonzero $b \in R$;

- a **right zero divisor** if $ba = 0$ for some nonzero $b \in R$;
- a **zero divisor** if it is a left or right zero divisor;

**Definition 1.44.** An **integral domain** is a nonzero commutative ring with identity and without zero divisors.

The ring $\mathbb{Z}$ is an integral domain. Also, every field is an integral domain.

**Definition 1.45.** An integral domain $R$ is called a **Dedekind**[4] **ring** or a **Dedekind domain** if

$$(\forall I, J \in \mathsf{Id}(R))(I \subseteq J \implies (\exists H \in \mathsf{Id}(R))\, I = JH).$$

There are many other alternative definitions of Dedekind rings.

**Example 1.46.** It can be shown that every ideal of the ring $\mathbb{Z}$ has the form

$$(n) := n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$$

for some $n \in \mathbb{N} \cap \{0\}$. In particular $(0) = \{0\}$ and $(1) = \mathbb{Z}$. Note that

$$(m) \subseteq (n) \iff n \mid m.$$

We also observe that, for all $m, n \in \mathbb{N} \cap \{0\}$,

$$(m)(n) = (mn),$$

because

$$\begin{aligned}(m)(n) &= \left\{ \sum_{k=1}^{n} ma_k nb_k \mid k \in \mathbb{N}, a_k, b_k \in \mathbb{Z} \right\} \\ &= \left\{ mn \sum_{k=1}^{n} a_k b_k \mid k \in \mathbb{N}, a_k, b_k \in \mathbb{Z} \right\} \\ &= mn\mathbb{Z} \\ &= (mn).\end{aligned}$$

Now

$$\begin{aligned}(m) \subseteq (n) &\implies n \mid m \\ &\implies (\exists z \in \mathbb{Z})\, nz = m \\ &\implies (m) = (nz) = (n)(z).\end{aligned}$$

Thus $\mathbb{Z}$ is a Dedekind domain.

[4]Richard Dedekind (1831–1916) — German mathematician

## 1.6 Existence of maximal ideals

In this section we show that every nonzero ring contains a maximal ideal.

**Definition 1.47.** A right ideal $I$ of a ring $R$ is called

- **minimal** if $I \neq 0$ and it does not contain properly any nonzero right ideal of $R$;
- **maximal** if $I \neq R$ and it is not contained properly in any right ideal $\neq R$.

Similar definitions can be given for left ideals and two-sided ideals.

**Proposition 1.48.** *In a ring with identity, every proper ideal is contained in a maximal ideal.*

*Proof.* Consider a proper ideal $J$ of a ring $R$ and the poset

$$P = \{I \in \mathsf{Id}(R) \mid J \subseteq I, I \neq R\}$$

with respect to inclusion. Since $J \in P$, this poset is nonempty.

We verify the assumption of the Zorn's lemma. By that lemma we will conclude that $P$ has a maximal element $I'$, which will be a maximal ideal of $R$ containing $J$.

Suppose that $X \subseteq P$ is a nonempty chain. Consider the set

$$A := \bigcup_{I \in X} I.$$

We prove that $A \in P$.

- We show that $A$ is an ideal of $R$. Let $a, b \in A$. Then there exist $I_a, I_b \in X$ such that $a \in I_a$ and $b \in I_b$. Since $X$ is a chain, $I_a \subseteq I_b$ or $I_b \subseteq I_a$. Consider the first case, the second is analogous. Then $a, b \in I_b$, whence $a + b \in I_b \subseteq A$, because $I_b$ is an ideal. Also $-b \in I_b \subseteq A$ and $rb \in I_b \subseteq A$ for every $r \in R$.
- $J \subseteq A$. Since $X$ is nonempty, we can choose some $I_0 \in X$. Now $J \subseteq I_0 \subseteq A$, so $J \subseteq A$.
- $A \neq R$. Suppose to the contrary that $A = R$. Then $1 \in A$, hence $1 \in I$ for some $I \in X$. But then $r = 1r \in I$ for every $r \in R$, and hence $R = I$, a contradiction.

Finally, $I \subseteq A$ for every $I \in X$, so $A$ is an upper bound for $X$ in $P$. Thus the assumption of Zorn's lemma is true for $P$. □

By contrast, a ring with identity need not have any minimal ideals.

**Example 1.49.** Recall that $\mathsf{Id}(\mathbb{Z}) = \{(n) \mid n \in \mathbb{N} \cup \{0\}\}$. Maximal ideals in the ring $\mathbb{Z}$ are of the form $(p)$, where $p$ is a prime number. This ring does not have any minimal ideals.

**Definition 1.50.** A ring is called **local** if it has a unique maximal left ideal. Equivalently one could define that a ring is local if it has a unique maximal right ideal.

**Example 1.51.** 1. The ring $\mathbb{Z}_8$ has 4 ideals: $\mathbb{Z}_8$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$, $\{\overline{0}, \overline{4}\}$ and $\{\overline{0}\}$. Hence it is a local ring, because $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ is the unique maximal (right) ideal.

2. The ring $\mathbb{Z}_6$ is not local, because it has two maximal ideals.
3. The ring $\mathbb{Z}$ is not local, because it has infinitely many maximal ideals.

## 1.7 Ideals generated by a subset

Our next purpose is to explain how one can construct the smallest (left, right) ideal containing a given subset of a ring.

**Lemma 1.52.** *Let $A$ be a subset of a ring $R$. The set*

$$ {}_R(A) := \bigcap \{I \subseteq R \mid I \text{ is a left ideal}, A \subseteq I\} $$

*is the smallest left ideal of $R$ containing the set $A$.*

*Proof.* There is always at least one left ideal containing $A$ — this is $R$. According to Proposition 1.39, the intersection of $I$'s is again a left ideal. If $J$ is any left ideal such that $A \subseteq J$, then ${}_R(A) \subseteq J$. □

**Definition 1.53.** Let $A$ be a subset of a ring $R$. The left ideal ${}_R(A)$ is called the **left ideal generated by** $A$. Similarly one can define the **right ideal** $(A)_R$ **generated by** $A$ and the **ideal** $(A)$ **generated by** $A$.

**Proposition 1.54.** *If $A$ is a nonempty subset of a ring $R$, then*

1. $(A) = \mathbb{Z}A + RA + AR + RAR$;
2. ${}_R(A) = \mathbb{Z}A + RA$;
3. $(A)_R = \mathbb{Z}A + AR$.

*If $R$ has the identity element, then*

1. $(A) = RAR$;
2. ${}_R(A) = RA$;
3. $(A)_R = AR$.

*Proof.* We only prove claim 1, the proofs of 2 and 3 are similar.

First we recall that the subsets $\mathbb{Z}A, RA, AR$ and $RAR$ consist of finite sums of certain products. Adding zero summands to such sums we can present each element of the set $\mathbb{Z}A + RA + AR + RAR$ in the form of a sum

$$ \sum_{k=1}^{n} (z_k a_k + r'_k a'_k + a''_k r''_k + r_k \hat{a}_k \hat{r}_k), $$

where $a_k, a'_k, a''_k, \hat{a}_k \in A$, $r'_k, r''_k, r_k, \hat{r}_k \in R$ and $z_k \in \mathbb{Z}$. It is easy to see that adding two such sums produces a sum of the same type and taking the additive inverse also gives a

sum of the same type. Note that $(\mathbb{Z}A)R = \mathbb{Z}(AR) \subseteq AR$. If $r \in R$, then

$$\begin{aligned}\left(\sum_{k=1}^{n}(z_k a_k + r'_k a'_k + a''_k r''_k + r_k \hat{a}_k \hat{r}_k)\right) r &= \sum_{k=1}^{n}(z_k a_k + r'_k a'_k + a''_k r''_k + r_k \hat{a}_k \hat{r}_k) r \\ &= \sum_{k=1}^{n}(z_k a_k r + r'_k a'_k r + a''_k r''_k r + r_k \hat{a}_k \hat{r}_k r) \\ &= \sum_{k=1}^{n}((z_k a_k) r + a''_k (r''_k r) + r'_k a'_k r + r_k \hat{a}_k (\hat{r}_k r)) \\ &\in (\mathbb{Z}A)R + AR + RAR \\ &\subseteq \mathbb{Z}A + RA + AR + RAR.\end{aligned}$$

Thus $\mathbb{Z}A + RA + AR + RAR$ is a right ideal. Analogously one can show that it is a left ideal, hence it is an ideal.

It also contains the set $A$, because every element $a \in A$ can be written as $a = 1a + 0a + a0 + 0a0$. Hence $(A) \subseteq \mathbb{Z}A + RA + AR + RAR$, because $(A)$ is the smallest such ideal. On the other hand, every ideal $I \supseteq A$ must contain all the elements of $\mathbb{Z}A + RA + AR + RAR$, so the intersection of such $I$'s also contains them and $\mathbb{Z}A + RA + AR + RAR \subseteq (A)$. This completes the proof of the equality $\mathbb{Z}A + RA + AR + RAR = (A)$.

Suppose now that the ring $R$ has the identity element which we denote $1_R$ to distinguish it from the natural number 1. Clearly $RAR \subseteq \mathbb{Z}A + RA + AR + RAR$. The converse inclusion also holds, because

$$\sum_{k=1}^{n}(z_k a_k + r'_k a'_k + a''_k r''_k + r_k \hat{a}_k \hat{r}_k) = \sum_{k=1}^{n}(z_k 1_R a_k 1_R + r'_k a'_k 1_R + 1_R a''_k r''_k + r_k \hat{a}_k \hat{r}_k) \in RAR.$$

□

**Definition 1.55.** If a (left, right) ideal $I$ of a ring $R$ is generated by a finite subset $A \subseteq R$, then $I$ is called **finitely generated**. If $I$ is generated by a singleton $\{a\}$, then it is called a **principal (left, right) ideal**.

Thus, for example, the principal ideal $(a)$ generated by $a$ is $(a) = \mathbb{Z}a + Ra + aR + RaR$.

## 1.8 Quotient ring

Let $I$ be an ideal of a ring $R$. For every $r \in R$, the set

$$[r] := r + I = \{r + a \mid a \in I\} \subseteq R$$

is called a **coset of $I$ with respect to $r$**. Note that

- $r \in [r]$ for every $r \in R$;
- $[r] = [s]$ if and only if $r - s \in I$.

The set

$$R/I := \{[r] \mid r \in R\}$$

of all cosets is a ring with respect to operations

$$[r] + [r'] := [r + r'], \tag{1.5}$$
$$[r][r'] := [rr'], \tag{1.6}$$

where $r, r' \in R$. This ring is called the **quotient ring** (or the **factor ring**) of $R$ by ideal $I$. The zero element of this ring is the coset $[0] = 0 + I = I$.

The mapping

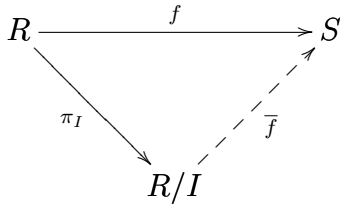
$$\pi_I : R \longrightarrow R/I, \quad r \mapsto [r]$$

is a ring homomorphism, which is called the **canonical projection** of $R$ onto quotient ring $R/I$. Note that $\operatorname{Ker} \pi_I = I$.

**Example 1.56.** Perhaps the best known example of a quotient ring is the residue class ring modulo $n \in \mathbb{N}$, which is the quotient ring of the ring $\mathbb{Z}$ by its ideal $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ of integers divisible by $n$. Shortly: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Using the construction of a quotient ring we can formulate The Homomorphism Theorem for rings. The proof is standard and we omit it.

**Theorem 1.57.** *If $f : R \longrightarrow S$ is a ring homomorphism and $I$ is an ideal with $I \subseteq \operatorname{Ker} f$, then there exists precisely one homomorphism $\overline{f} : R/I \longrightarrow S$ with $f = \pi_I \overline{f}$, i.e. the diagram*




*is commutative. If $I = \operatorname{Ker} f$, then $\overline{f}$ is injective. If $f$ is surjective, then $\overline{f}$ is also surjective.*

**Corollary 1.58.** *If $f : R \longrightarrow S$ is a surjective homomorphism of rings, then $S \simeq R/\operatorname{Ker} f$.*

Using The Homomorphism Theorem we can prove the isomorphism theorems.

**Theorem 1.59** (The First Isomorphism Theorem)**.** *If $I, J$ are ideals of a ring $R$, then*

$$I/(I \cap J) \simeq (I + J)/J.$$

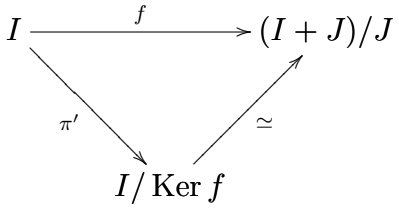
*Proof.* The sum $I + J$ of two ideals is an ideal (see Proposition 1.40), so it is also a subring and a ring. Clearly $J \subseteq I + J$, and since $J$ is an ideal in $R$, it is also an ideal in the ring $I + J$. Therefore we may form the quotient ring $(I + J)/J$. By the two-sided version of Proposition 1.39, $I \cap J$ is an ideal in $R$ and hence in the ring $I$. So we also have the quotient $I/(I \cap J)$.

Define a mapping $f : I \to (I + J)/J$ by

$$f(x) := x + J$$

for every $x \in I$. Since $f = \pi|_I$, where $\pi : I + J \to (I + J)/J$ is a natural projection, $f$ is a ring homomorphism. If $(i+j)+J \in (I+J)/J$, then $f(i) = i+J = i+(j+J) = (i+j)+J$, proving that $f$ is onto. Using Corollary 1.58 we can say that

$$I/\operatorname{Ker} f \simeq (I + J)/J.$$

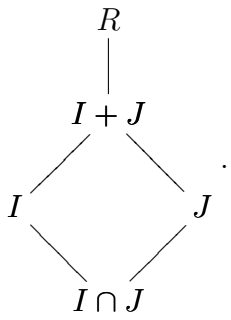



Since

$$\begin{aligned} x \in \operatorname{Ker} f &\iff x \in I \wedge f(x) = J \iff x \in I \wedge x + J = J \\ &\iff x \in I \wedge x \in J \iff x \in I \cap J, \end{aligned}$$

we have $\operatorname{Ker} f = I \cap J$. □

**Remark 1.60.** The inclusion relations between the ideals appearing in the previous theorem are illustrated by the following diagram (bigger ideals are higher):




**Theorem 1.61** (The Second Isomorphism Theorem)**.** *Let $R$ be a ring, $I, J$ ideals of a ring and $J \subseteq I$. Then*

$$(R/J)/(I/J) \simeq R/I.$$

*Proof.* Since $J$ is an ideal of $R$, it is also an ideal of $I$. Hence the quotient rings $R/J$, $I/J$ and $R/I$ exist. We need to show that $I/J$ is an ideal of $R/J$. It is clear that $I/J \subseteq R/J$. Let $i + J, i' + J \in I/J$. Since $i, i' \in I$ and $-i \in I$, we have $i + i' + J, -i + J \in I/J$, so $I/J$ is a subgroup of the additive group $(R/J, +)$. If $r \in R$, then siis $ir \in I$, because $I$ is and ideal of $R$. Hence

$$(i + J)(r + J) = ir + J \in I/J$$

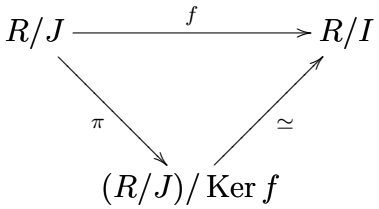
and we have shown that $I/J$ is an ideal in the ring $R/J$.

Define a mapping $f : R/J \to R/I$ by

$$f(r + J) := r + I,$$

$r \in R$. Suppose that $r_1 + J = r_2 + J$. Then $r_1 - r_2 \in J \subseteq I$. Hence $r_1 + I = r_2 + I$, which shows that $f$ is well defined. It is easy to verify that $f$ is a surjective homomorphism. By Corollary 1.58,

$$(R/J)/\operatorname{Ker} f \simeq R/I\,.$$




Since, for every coset $r + J \in R/J$,

$$r + J \in \operatorname{Ker} f \iff f(r + J) = I \iff r + I = I \iff r \in I \implies r + J \in I/J.$$

Also the converse of the last implication holds, because

$$\begin{aligned} r + J \in I/J &\implies (\exists i \in I)\, r + J = i + J \implies (\exists i \in I)\, r - i \in J \subseteq I \\ &\implies r - i \in I \implies (r - i) + i \in I \implies r \in I. \end{aligned}$$

Hence we have $\operatorname{Ker} f = I/J$ (these sets contain the same elements). This completes the proof. □

Our next purpose is to prove that the quotient by a maximal left ideal is a division ring. We will need the following lemma.

**Lemma 1.62.** *Let $R$ be a ring with identity $1 \neq 0$. If every nonzero element of $R$ is left invertible, then this ring is a division ring.*

*Proof.* Consider a ring $R$ with identity $1 \neq 0$, where all nonzero elements are left invertible. Take arbitrary $a \in R \setminus \{0\}$. We need to show that it has a two-sided inverse. By assumption we can find $b \in R$ such that $ba = 1$. If $b = 0$, then $1 = ba = 0a = 0$, a contradiction. So $b \neq 0$ and applying the assumption once more we can find $c \in R$ such that $cb = 1$. Now

$$a = 1 \cdot a = (cb)a = c(ba) = c \cdot 1 = c.$$

Hence $ba = 1$ and $ab = 1$ meaning that $a$ has a two-sided inverse $b$. □

**Theorem 1.63.** *Let $R$ be a ring with identity and let $I \subseteq R$ be an ideal of $R$. Then the following are equivalent:*

1. *$I$ is a maximal left ideal;*
2. *$I$ is a maximal right ideal;*
3. *the quotient ring $R/I$ is a division ring.*

*Proof.* We prove the equivalence of 1 and 3. The proof of 2 $\iff$ 3 is similar.

1 $\implies$ 3. Assume that $I$ is a maximal left ideal. Then $R/I$ is a ring with the identity element $1_R + I$. By Lemma 1.62 it suffices to prove that evey nonzero element of $R/I$ has a left inverse element.

Take a nonzero element $a + I \in R/I$. Then $a + I \neq I$, and hence $a \notin I$. Define a subset

$$J := \{i + ra \mid i \in I, r \in R\} \subseteq R.$$

We will prove that $J$ is a left ideal of $R$. Since $a = 0_R + 1_R \cdot a \in J$, $J$ is nonempty. Take $i + ra, i' + r'a \in J$ and $s \in R$. Then

$$\begin{aligned}(i + ra) + (i' + r'a) &= (i + i') + (r + r')a \in J,\\ -(i + ra) &= (-i) + (-r)a \in J,\\ s(i + ra) &= si + (sr)a \in J.\end{aligned}$$

Consequently, $J$ is a left ideal. Now every $i \in I$ can be written as $i = i + 0_R \cdot a$, so $I \subseteq J$. From $a \in J \setminus I$ we conclude that $I \subset J$. Since $I$ is a maximal left ideal, $J = R$. Thus $1_R \in J$ and there exist $i_0 \in I$ and $r_0 \in R$ such that $1_R = i_0 + r_0 a$. So $1_R - r_0 a = i_0 \in I$ and

$$1_R + I = r_0 a + I = (r_0 + I)(a + I).$$

This means that $r_0 + I$ is a left inverse of $a + I$.

3 $\implies$ 1. Suppose to the contrary that $J$ is a left ideal such that $I \subset J \subset R$. Let $j \in J \setminus I$. Then $j + I \neq I$, that is, $j + I$ is a nonzero element in $R/I$. As $R/I$ is a division ring, there exists $r + I \in R/I$ such that

$$1_R + I = (r + I)(j + I) = rj + I.$$

Hence $1_R - rj \in I \subset J$. Since $J$ is a left ideal, $rj \in J$. Now $1_R - rj, rj \in J$ imply $1_R = (1_R - rj) + rj \in J$, so $R = J$, a contradiction. □

## 1.9 Quotient module

Let $N$ be a submodule of a left $R$-module $M$. For every $m \in M$, the set

$$[m] := m + N = \{m + a \mid a \in N\} \subseteq M$$

is called a **coset of** $M$ **with respect to** $m$. Note that

- $m \in [m]$ for every $m \in M$;
- $[m] = [m']$ if and only if $m - m' \in N$.

The set

$$M/N := \{[m] \mid m \in M\}$$

of all cosets is a left $R$-module with respect to operations

$$[m] + [m'] := [m + m'], \tag{1.7}$$

$$r[m] := [rm], \tag{1.8}$$

where $m, m' \in M$ and $r \in R$. This module is called the **quotient module** (or the **factor module**) of $M$ by submodule $N$. The zero element of this module is the coset $[0] = 0 + N = N$.

The mapping

$$\pi_N : M \longrightarrow\!\!\!\!\!\rightarrow M/N, \;\; m \mapsto [m]$$

is a homomorphism of left $R$-modules, which is called the **canonical projection** of $M$ onto the quotient module $M/N$. Note that $\operatorname{Ker} \pi_N = N$.

Next we will prove some technical lemmas about quotient modules, which will be used several times.

**Lemma 1.64.** *If $X, N$ are submodules of a left module ${}_RM$, then*

$$\{x + N \mid x \in X\} = (X + N)/N.$$

*Proof.* The inclusion $\subseteq$ is clear, because $x + N = (x + 0) + N$ for every $x \in X$.

Conversely, any element of $(X+N)/N$ has form $(y+n)+N$, where $y \in X$ and $n \in N$. But

$$(y + n) + N = y + (n + N) = y + N \in \{x + N \mid x \in X\},$$

because $n + N = N$. □

**Lemma 1.65.** *If $N \leq X \leq {}_RM$ and $M/N = X/N$, then $M = X$.*

*Proof.* We need to show that $M \subseteq X$. Take any $m \in M$. Since $m + N \in X/N$, there exists $x \in X$ such that $m + N = x + N$. Hence $m - x \in N \subseteq X$. As $X$ is a submodule, $m = (m - x) + x \in X$. So $M \subseteq X \subseteq M$ and $M = X$. □

**Corollary 1.66.** *If $N \leq {}_RM$ and $M/N$ is a zero module, then $N = M$.*

*Proof.* We have $M/N = \{N\} = N/N$. By Lemma 1.65, $M = N$. □

## 1.10 Nakayama's Lemma

**Definition 1.67.** Let $R$ be a ring with identity. The intersection of all maximal right ideals is called the **Jacobson radical** of $R$ and it is denoted by $J(R)$. It can be shown that $J(R)$ equals also the intersection of all maximal left ideals.

**Definition 1.68.** Let $R$ be a ring with identity. A unitary module ${}_RM$ is called **finitely generated** if $M = \{0\}$ or there exist $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in M$ such that

$$M = \{r_1x_1 + \ldots + r_nx_n \mid r_1, \ldots, r_n \in R\}.$$

The set $\{x_1, \ldots, x_n\}$ is called a **set of generators** for ${}_RM$ and the expressions $r_1x_1 + \ldots + r_nx_n$ are called **linear combinations** of elements $x_1, \ldots, x_n$. If $M = \{0\}$, then we say that ${}_RM$ is generated by the empty set. A generating set is called **minimal** if no proper subset of it is a generating set. Clearly every finitely generated module has a minimal generating set.

**Example 1.69.** Let $n$ be a fixed natural number. The set

$$M = \{a_0 + a_1X + \ldots + a_nX^n \mid a_k \in \mathbb{Z}\}$$

of polynomials is a left $\mathbb{Z}$-module with respect to natural operations. It has a finite generating set

$$\{1, X, X^2, \ldots, X^n\}.$$

On the other hand, the module ${}_{\mathbb{Z}}\mathbb{Z}[X] = \langle 1, X, X^2, \ldots\rangle$ is not finitely generated.

**Example 1.70.** A minimal generating set of a module need not be a basis. For example, consider the abelian group $(\mathbb{Z}_3, +)$ as a $\mathbb{Z}$-module. Then $\{\overline{1}\}$ is a minimal generating set ($\overline{0} = 0 \cdot \overline{1}$, $\overline{1} = 1 \cdot \overline{1}$, $\overline{2} = 2 \cdot \overline{1}$). But it is not linearly independent, because $3 \cdot \overline{1} = \overline{0}$, but $3 \neq 0$ in the ring $\mathbb{Z}$.

**Theorem 1.71** (Nakayama's Lemma)**.** *Let ${}_RM$ be a finitely generated unitary module over a ring $R$ with identity and let $I \in \mathsf{Id}_r(R)$ be such that $I \subseteq J(R)$. Then*

$$IM = M \implies M = \{0\}.$$

*Proof.* We will prove the equivalent implication

$$M \neq 0 \implies IM \neq M.$$

Suppose $M \neq 0$ and let $\{x_1, \ldots, x_n\}$ be a minimal generating set for ${}_RM$. We need to find an element of $M$, which does not belong to $IM$. We claim that $x_n$ is such an element.

Suppose to the contrary that $x_n \in IM$. Then there exist $p \in \mathbb{N}$, $i_1, \ldots, i_p \in I$ and $m_1, \ldots, m_p \in M$ such that

$$x_n = i_1m_1 + \ldots + i_pm_p.$$

Since $\{x_1, \ldots, x_n\}$ is a generating set, Each $m_k$ can be written as $m_k = \sum_{l=1}^{n} r_{kl}x_l$ for some $r_{kl} \in R$. Hence

$$\begin{aligned} x_n &= \sum_{k=1}^{p} i_k m_k = \sum_{k=1}^{p} i_k \left(\sum_{l=1}^{n} r_{kl}x_l\right) = \sum_{k=1}^{p}\sum_{l=1}^{n} i_k r_{kl} x_l = \sum_{l=1}^{n}\sum_{k=1}^{p} i_k r_{kl} x_l \\ &= \sum_{l=1}^{n}\left(\sum_{k=1}^{p} i_k r_{kl}\right) x_l. \end{aligned}$$

Since $I$ is a right ideal, $c_l := \sum_{k=1}^{p} i_k r_{kl} \in I$ for every $l \in \{1, \ldots, n\}$ and

$$x_n = c_1x_1 + \ldots + c_nx_n. \tag{1.9}$$

We will prove that the element $1 - c_n$ is left invertible. Consider the principal left ideal $R(1 - c_n)$ of $R$. Suppose that $R(1 - c_n) \subset R$. Then, by the analogue of Proposition 1.48 for left ideals, there exists a maximal left ideal $J \subset R$ such that $R(1 - c_n) \subseteq J$. Therefore $1 - c_n \in J$ and $c_n \in I \subseteq J(R) \subseteq J$. (The inclusion $J(R) \subseteq J$ comes from the definition of the Jacobson radical: $J(R)$ is contained in every maximal left ideal of $R$.) It follows that

$1 = c_n + (1 - c_n) \in J$ and so $J = R$, a contradiction. Thus we must have $R(1 - c_n) = R$. From this we conclude that $1 = d(1 - c_n)$ for some $d \in R$.

For $n$ we have two possibilities.

1) $n = 1$. Then, from (1.9) we have $x_1 = c_1 x_1$ and $(1 - c_1)x_1 = 0$. Multiplying the last equality by $d$ we obtain

$$0 = d0 = d(1 - c_1)x_1 = 1x_1 = x_1,$$

where the last equality holds due to unitarity of the module ${}_RM$. Hence $M = \langle x_1 \rangle = \langle 0 \rangle = \{0\}$, a contradiction.

2) $n > 1$. From (1.9) we conclude that

$$(1 - c_n)x_n = c_1 x_1 + \ldots + c_{n-1} x_{n-1}.$$

Multiplying by $d$ we obtain

$$x_n = dc_1 x_1 + \ldots + dc_{n-1} x_{n-1}.$$

But then $\{x_1, \ldots, x_{n-1}\}$ is also a generating set, contradicting the minimality of the generating set $X$. □

**Corollary 1.72.** *Let ${}_RM$ be a finitely generated unitary module over a ring $R$ with identity, let $N \subseteq M$ be a submodule and let $I \trianglelefteq R$ such that $I \subseteq J(R)$. Then*

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

*Proof.* Since $I$ is a two-sided ideal of $R$, one can see that $IM$ is a submodule of $M$. In particular, for every $r \in R$ and $i_1 m_1 + \ldots + i_n m_n \in IM$,

$$r(i_1 m_1 + \ldots + i_n m_n) = (ri_1)m_1 + \ldots + (ri_n)m_n \in IM,$$

because $ri_1, \ldots, ri_n \in I$.

Assume that $M = IM + N$. Then

$$\begin{aligned}
I(M/N) &= \{i_1(m_1 + N) + \ldots + i_n(m_n + N) \mid n \in \mathbb{N}, i_k \in I, m_k \in M\} \\
&= \{(i_1 m_1 + N) + \ldots + (i_n m_n + N) \mid n \in \mathbb{N}, i_k \in I, m_k \in M\} \\
&= \{(i_1 m_1 + \ldots + i_n m_n) + N \mid n \in \mathbb{N}, i_k \in I, m_k \in M\} \\
&= \{x + N \mid x \in IM\} && \text{(def. of } IM\text{)} \\
&= (IM + N)/N && \text{(Lemma 1.64)} \\
&= M/N. && (IM + N = M)
\end{aligned}$$

By Nakayama's Lemma, $M/N$ is a zero module. Hence $M = N$ by Corollary 1.66. □

Recall that a ring is called local if it has a unique maximal left ideal. Consider a commutative local ring $R$ with identity and let $\mathfrak{m}$ be its unique maximal ideal. Then $\mathfrak{m} = J(R)$, the Jacobson radical of $R$. By Theorem 1.63, the quotient ring

$$F := R/\mathfrak{m}$$

is a division ring. As a quotient of a commutative ring, $F$ is also commutative, so it is actually a field, which is called **the residue field of** $R$. Let ${}_RM$ be any unitary finitely generated left $R$-module. Then the subset $\mathfrak{m}M \subseteq M$ is a submodule of $M$.

**Lemma 1.73.** *In the described situation, the abelian group $M/\mathfrak{m}M$ can be considered as a unitary $F$-module, hence a vector space over the field $F$. Moreover, this vector space is finite dimensional.*

*Proof.* We define a left $F$-action on the abelian group $M/\mathfrak{m}M$ by

$$(r+\mathfrak{m})(m+\mathfrak{m}M) := rm+\mathfrak{m}M,$$

$r \in R$, $m \in M$. We need to verify that this action is well defined. Suppose that $r+\mathfrak{m} = r'+\mathfrak{m}$ and $m+\mathfrak{m}M = m'+\mathfrak{m}M$. Then $r-r' \in \mathfrak{m}$ and $m-m' \in \mathfrak{m}M$. Hence

$$\begin{aligned} rm - r'm' &= rm - rm' + rm' - r'm' \\ &= r(m-m') + (r-r')m' \in R\cdot\mathfrak{m}M + \mathfrak{m}M \subseteq \mathfrak{m}M + \mathfrak{m}M = \mathfrak{m}M. \end{aligned}$$

Therefore $rm+\mathfrak{m}M = r'm'+\mathfrak{m}M$ and the action is well defined. It is straightforward to show that the axioms of a module are satified. This module is unitary, because, for every $m \in M$,

$$m+\mathfrak{m}M = 1m+\mathfrak{m}M = (1+\mathfrak{m})(m+\mathfrak{m}M),$$

where $1+\mathfrak{m}$ is the identity element of the field $F$.

Let ${}_RM$ be generated by elements $x_1,\ldots,x_n \in M$. If $m+\mathfrak{m}M \in M/\mathfrak{m}M$, then there exist $r_1,\ldots,r_n \in R$ such that $m = r_1x_1+\ldots+r_nx_n$. Hence

$$m+\mathfrak{m}M = (r_1x_1+\ldots+r_nx_n)+\mathfrak{m}M = (r_1+\mathfrak{m})(x_1+\mathfrak{m}M)+\ldots+(r_n+\mathfrak{m})(x_n+\mathfrak{m}M)$$

is an $F$-linear combination of the elements $x_1+\mathfrak{m}M,\ldots,x_n+\mathfrak{m}M \in M/\mathfrak{m}M$. Thus

$${}_F(M/\mathfrak{m}M) = \langle x_1+\mathfrak{m}M,\ldots,x_n+\mathfrak{m}M\rangle$$

is a finitely generated vector space over $F$. □

**Theorem 1.74.** *Let $R$ be a commutative local ring with an identity element with the unique maximal ideal $\mathfrak{m}$ and let ${}_RM$ be a finitely generated unitary module. If $x_1,\ldots,x_n \in M$ are such that*

$$\{x_1+\mathfrak{m}M,\ldots,x_n+\mathfrak{m}M\}$$

*is a basis for the vector space $M/\mathfrak{m}M$ over the field $F = R/\mathfrak{m}$, then*

$${}_RM = \langle x_1,\ldots,x_n\rangle$$

*(the $R$-module ${}_RM$ is generated by $x_1,\ldots,x_n$), where $\{x_1,\ldots,x_n\}$ is a minimal set of generators.*

Roughly saying: every basis of the quotient space $M/\mathfrak{m}M$ can be lifted to a minimal set of generators of the module ${}_RM$.

*Proof.* Consider the submodule

$$N := \langle x_1,\ldots,x_n\rangle = \{r_1x_1+\ldots+r_nx_n \mid r_k \in R\} \leq M.$$

Our aim is to show that $N = M$. We have

$$\begin{aligned} M/\mathfrak{m}M &= \langle x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M \rangle && \text{(hypothesis of the theorem)} \\ &= \{(r_1 + \mathfrak{m})(x_1 + \mathfrak{m}M) + \ldots + (r_n + \mathfrak{m})(x_n + \mathfrak{m}M) \mid r_k \in R\} \\ &= \{(r_1x_1 + \mathfrak{m}M) + \ldots + (r_nx_n + \mathfrak{m}M) \mid r_k \in R\} \\ &= \{(r_1x_1 + \ldots + r_nx_n) + \mathfrak{m}M \mid r_k \in R\} && \text{(def. of + in } M/\mathfrak{m}M) \\ &= \{y + \mathfrak{m}M \mid y \in N\} && \text{(def of } N) \\ &= (N + \mathfrak{m}M)/\mathfrak{m}M. && \text{(Lemma 1.64)} \end{aligned}$$

Since $N + \mathfrak{m}M$ is a submodule of ${}_RM$, we conclude that $M = N + \mathfrak{m}M$ by Lemma 1.65. We can apply Corollary 1.72, because $\mathfrak{m} = J(R)$. It gives $M = N$, as needed.

Suppose that $\{x_1, \ldots, x_n\}$ is not a minimal set of generators. Then one of these elements is a linear combination of the others. Without loss of generality, let $x_n = r_1x_1 + \ldots + r_{n-1}x_{n-1}$, where $r_1, \ldots, r_{n-1} \in R$. Then

$$\begin{aligned} x_n + \mathfrak{m}M &= (r_1x_1 + \ldots + r_{n-1}x_{n-1}) + \mathfrak{m}M \\ &= (r_1 + \mathfrak{m})(x_1 + \mathfrak{m}M) + \ldots + (r_{n-1} + \mathfrak{m})(x_{n-1} + \mathfrak{m}M), \end{aligned}$$

contradicting the assumption that the set $\{x_1+\mathfrak{m}M, \ldots, x_n+\mathfrak{m}M\}$ is linearly independent. □

**Remark 1.75.** Consider the same situation as in Lemma 1.73, but require that $\{x_1, \ldots, x_n\}$ is a minimal generating set for ${}_RM$. We saw that $\{x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M\}$ is a generating set for the vector space ${}_F(M/\mathfrak{m}M)$. Every generating set of a vector space contains a basis. Suppose that $\{x_1 + \mathfrak{m}M, \ldots, x_t + \mathfrak{m}M\}$, where $t \leq n$, is a basis for ${}_F(M/\mathfrak{m}M)$. By Theorem 1.74, $\{x_1, \ldots, x_t\}$ is a generating set for ${}_RM$. By minimality of $\{x_1, \ldots, x_n\}$, we must have $t = n$. Thus:

*if* ${}_RM$ *has a minimal generating set of* $n$ *elements, then* $\dim({}_F(M/\mathfrak{m}M)) = n$.

In particular, all minimal generating sets of ${}_RM$ must have the same cardinality, because all bases of ${}_F(M/\mathfrak{m}M)$ have the same number of vectors.

**Exercise 1.76.** What are the maximal ideals of the residue class ring $\mathbb{Z}_{12}$? Find the Jacobson radical of this ring.

## 1.11 Direct sums

In algebra, a typical approach is to try to prove that a given structure can be obtained from certain substructures using some construction. The hope is that those substructures have some good properties or that they are better understood. One such construction is the internal direct sum, which can be used, for example, for modules, rings, vector spaces, abelian groups etc. There is also the construction of external direct sum, which we also consider later in this section.

In this section, we will assume that all modules are left modules over a ring $R$. First we define sums of submodules of a module.

**Definition 1.77.** The **sum** of submodules $A_k$, $k \in K$, where $K \neq \emptyset$, of an $R$-module $A$ is the set of all elements of $A$ that can be presented as a finite sum of elements belonging to some submodules $A_k$.

Such a sum is denoted by $\sum_{k\in K} A_k$. The sum of finitely many submodules $A_1, \ldots, A_n$ is denoted by $A_1 + \ldots + A_n$. By the definition, the sum $\sum_{i\in I} A_i$ consists of elements

$$a_{k_1} + a_{k_2} + \ldots + a_{k_n} \in A, \tag{1.10}$$

where $n \in \mathbb{N}$, $k_1, k_2, \ldots, k_n \in K$ and $a_{k_l} \in A_{k_l}$ for every $l = 1, \ldots, n$. If $n = 1$, then the sum (1.10) equals the element $a_{k_1}$. Hence the sum $\sum_{k\in K} A_k$ contains all submodules $A_k$, $k \in K$.

**Proposition 1.78.** *The sum of submodules $A_k$, $k \in K$ of an $R$-module $A$ is the smallest submodule of $A$, which contains all submodules $A_k$, $k \in K$.*

*Proof.* It is easy to see that the set of all sums (1.10) is closed with respect to addition, taking additive inverses and $R$-action. Hence $\sum_{k\in K} A_k$ is a submodule of $A$.

If $B$ is a submodule of $A$, which also contains all submodules $A_k$, $k \in K$, then $B$ must contain all sums (1.10) (because $B$ is closed under addition), hence $\sum_{k\in K} A_k \subseteq B$. □

**Example 1.79.** Consider the module $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ over the ring $\mathbb{Z}$ with componentwise operations. Then

$$A_1 = \{(a, 0, a) \mid a \in \mathbb{Z}\},$$
$$A_2 = \{(b, b, b) \mid b \in \mathbb{Z}\}$$

are submodules of $A$. It can be shown that their sum is

$$A_1 + A_2 = \{(c, d, c) \mid c, d \in \mathbb{Z}\} \subset A\,.$$

**Definition 1.80.** The sum of submodules $A_1, \ldots, A_n$ of an $R$-module $A$ is called the **internal direct sum** if every element $a \in A_1 + \ldots + A_n$ can be expressed uniquely as a sum

$$a = a_1 + \ldots + a_n,$$

where $a_k \in A_k$ for every $k = 1, \ldots, n$. Notation: $A_1 \dot{+} \ldots \dot{+} A_n$. One says that $A$ is the **internal direct sum of its submodules** $A_1, \ldots, A_n$ if $A = A_1 + \ldots + A_n$ and this sum is an internal direct sum. In that case we write

$$A = A_1 \dot{+} \ldots \dot{+} A_n.$$

Uniqueness of the expression in the definition means that if

$$a_1 + \ldots + a_n = b_1 + \ldots + b_n,$$

where $a_k, b_k \in A_k$ for every $k = 1, \ldots, n$, then

$$a_1 = b_1, \ldots, a_n = b_n.$$

**Theorem 1.81.** *Let $A_1, \ldots, A_n$ be submodules of an $R$-module $A$. The following are equivalent:*

1. *the sum of $A_1, \ldots, A_n$ is a direct sum;*
2. *for every $k = 1, \ldots, n$,*

$$A_k \cap (A_1 + \ldots + A_{k-1} + A_{k+1} + \ldots + A_n) = \{0\}; \tag{1.11}$$

3. *if $a_1 + \ldots + a_n = 0$, where $a_k \in A_k$ for every $k = 1, \ldots, n$, then $a_1 = \ldots = a_n = 0$.*

*Proof.* 1. $\Rightarrow$ 2. Suppose that $A_1 + \ldots + A_n = A_1 \dot{+} \ldots \dot{+} A_n$. Let

$$a \in A_k \cap (A_1 + \ldots + A_{k-1} + A_{k+1} + \ldots + A_n).$$

Then there exist $a_1 \in A_1, \ldots, a_{k-1} \in A_{k-1}, a_{k+1} \in A_{k+1}, \ldots, a_n \in A_n$ such that

$$\begin{aligned} a &= a_1 + \ldots + a_{k-1} + 0 + a_{k+1} + \ldots + a_n, \\ a &= 0 \ + \ldots + \ 0 \quad + a + 0 \quad + \ldots + 0. \end{aligned}$$

Due to the uniqueness of the representation, $a = 0$. Thus we have shown that

$$A_k \cap (A_1 + \ldots + A_{k-1} + A_{k+1} + \ldots + A_n) \subseteq \{0\}.$$

The opposite inclusion is obvious.

2. $\Rightarrow$ 3. Assume that, for every $k = 1, \ldots, n$, the equality (1.11) holds and that $a_1 + \ldots + a_n = 0$, where $a_k \in A_k$ for every $k = 1, \ldots, n$. Then, for every $k = 1, \ldots, n$,

$$-a_k = a_1 + \ldots + a_{k-1} + a_{k+1} + \ldots + a_n \in A_k \cap (A_1 + \ldots + A_{k-1} + A_{k+1} + \ldots + A_n) = \{0\}$$

and hence $-a_k = 0$, which implies $a_k = 0$.

3. $\Rightarrow$ 1. Assume that condition 3 holds. Suppose that

$$a_1 + \ldots + a_n = b_1 + \ldots + b_n,$$

where $a_k, b_k \in A_k$ for every $k = 1, \ldots, n$. Then

$$(a_1 - b_1) + \ldots + (a_n - b_n) = 0,$$

where $a_k - b_k \in A_k$ for every $k = 1, \ldots, n$. By assumption,

$$a_1 - b_1 = 0, \ldots, a_n - b_n = 0$$

or $a_1 = b_1, \ldots, a_n = b_n$. □

**Example 1.82.** The sum $A_1 + A_2$ of submodules $A_1$ and $A_2$ considered in the Example 1.79 is a direct sum, because if $(x, y, z) \in A_1 \cap A_2$, then $y = 0$ and $x = y = z$, whence $x = z = 0$. Thus $A_1 \cap A_2 = \{(0, 0, 0)\}$.

**Example 1.83.** Consider again the module $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ over $\mathbb{Z}$. It is easy to see that

$$\begin{aligned} A_1 &= \{(a,0,0) \mid a \in \mathbb{Z}\}, \\ A_2 &= \{(0,b,0) \mid b \in \mathbb{Z}\}, \\ A_3 &= \{(0,0,c) \mid c \in \mathbb{Z}\} \end{aligned}$$

are submodules of $A$ and that $A = A_1 + A_2 + A_3$. It is also clear that

$$A_1 \cap (A_2 + A_3) = \{0\},\ A_2 \cap (A_1 + A_3) = \{0\},\ \text{ and }\ A_3 \cap (A_1 + A_2) = \{0\}.$$

Since condition 2 of Theorem 1.81 is satisfied, we can say that

$$A = A_1 \dot{+} A_2 \dot{+} A_3.$$

**Example 1.84.** Consider the ring $\mathbb{Z}_{12}$ as a module over itself. Then

$$\begin{aligned} \overline{2}\mathbb{Z}_{12} &= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}, \\ \overline{3}\mathbb{Z}_{12} &= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \end{aligned}$$

are submodules. Since $\overline{1} = \overline{10} + \overline{3}$, we see that every element of $\mathbb{Z}_{12}$ can be written as a sum $a + b$, where $a \in \overline{2}\mathbb{Z}_{12}$ and $b \in \overline{3}\mathbb{Z}_{12}$. Hence

$$\overline{2}\mathbb{Z}_{12} + \overline{3}\mathbb{Z}_{12} = \mathbb{Z}_{12}\,.$$

This sum is not a direct sum, because $\overline{0} \neq \overline{6} \in \overline{2}\mathbb{Z}_{12} \cap \overline{3}\mathbb{Z}_{12}$.

The internal direct sum of submodules can be defined also for infinitely many submodules.

**Definition 1.85.** The sum of submodules $A_k$, $k \in K$ of an $R$-module $A$ is called the **internal direct sum** if for every finite set of pairwise distinct indices $k_1, \ldots, k_n \in K$, the sum of submodules $A_{k_1}, \ldots, A_{k_n}$ is a direct sum. Notation: $\dot{\sum}_{k \in K} A_k$.

Theorem 1.81 can be generalized to the case where we have an arbitrary number of submodules.

**Theorem 1.86.** *Let $A_k, k \in K$, be submodules of an $R$-module $A$. The following are equivalent:*

1. *the sum of submodules $A_k, k \in K$, is a direct sum;*
2. *for every $k \in K$,*
$$A_k \cap \left( \sum_{j \in I \setminus \{k\}} A_j \right) = \{0\};$$
3. *if $a_1 + \ldots + a_n = 0$, where $a_l \in A_{k_l}$ for every $l = 1, \ldots, n$ and $k_1, \ldots, k_n \in K$ are pairwise distinct, then $a_1 = \ldots = a_n = 0$.*

We will not give the proof of this theorem in this course.

Now we consider external direct sums.

**Definition 1.87.** The **external direct sum** of $R$-modules $A_k$, $k \in K$, is the submodule $\oplus \sum_{i\in I} A_i$ of the direct product $\prod_{k\in K} A_k$, which consists of all generalized sequences $(a_k)_{k\in K}$ having only finitely many nonzero components.

Thus

$$\oplus \sum_{i\in I} A_i = \left\{ (a_i)_{i\in I} \in \prod_{i\in I} A_i \;\middle|\; |\{j \in I \mid a_j \neq 0\}| < \infty \right\}.$$

If $K = \{1, \ldots, n\}$, then instead of $\oplus \sum_{k\in K} A_k$ we write $A_1 \oplus \ldots \oplus A_n$.

It is clear that the external direct sum of finitely many $R$-modules is equal to their direct product:

$$A_1 \oplus \ldots \oplus A_n = A_1 \times \ldots \times A_n.$$

In the next theorem we describe the connections between internal and external direct sums.

**Theorem 1.88.** *If $A = \dot{\sum}_{k\in K} A_k$, where $A_k$, $k \in K$, are submodules of an $R$-module $A$, then $A \simeq \oplus \sum_{k\in K} A_k$.*

*Conversely, if $B_k$, $k \in K$, are $R$-modules and $A = \oplus \sum_{k\in K} B_k$, then there exist submodules $A_k$, $k \in K$, of the module $A$ such that $A = \dot{\sum}_{k\in K} A_k$ and $A_k \simeq B_k$ for every $k \in K$.*

*Proof.* 1) Assume that $A = \dot{\sum}_{k\in K} A_k$ and define a mapping $\varphi : \oplus \sum_{k\in K} A_k \to A$ by

$$\varphi((a_k)_{k\in K}) := \sum_{k\in K} a_k.$$

On the right hand side of this equality we take the sum of all nonzero components of the generalized sequence $(a_k)_{k\in K}$. Since there are finitely many such components, this sum exists and $\sum_{k\in K} a_k \in \dot{\sum}_{k\in K} A_k = A$.

We check that $\varphi$ is a homomorphism of modules. Indeed, for every $(a_k)_{k\in K}, (b_k)_{k\in K} \in \oplus \sum_{k\in K} A_k$ and $r \in R$,

$$\begin{aligned}
\varphi\left((a_k)_{k\in K} + (b_k)_{k\in K}\right) &= \varphi\left((a_k + b_k)_{k\in K}\right) && \text{(def. of + on the direct product)} \\
&= \sum_{k\in K} (a_k + b_k) && \text{(def. of } \varphi\text{)} \\
&= \sum_{k\in K} a_k + \sum_{k\in K} b_k && \text{(commutativity of +)} \\
&= \varphi\left((a_k)_{k\in K}\right) + \varphi\left((b_k)_{k\in K}\right), && \text{(def. of } \varphi\text{)} \\
\varphi\left(r(a_k)_{k\in K}\right) &= \varphi\left((ra_k)_{k\in K}\right) && \text{(def. of } R\text{-action on the direct product)} \\
&= \sum_{k\in K} (ra_k) && \text{(def. of } \varphi\text{)} \\
&= r \sum_{k\in K} a_k && \text{(def. of a module)} \\
&= r\varphi((a_k)_{k\in K}). && \text{(def. of } \varphi\text{)}
\end{aligned}$$

It is clear that $\varphi$ is surjective. Suppose that $\varphi((a_k)_{k\in K}) = 0 \in A$. Then $\sum_{k\in K} a_k = 0$, where the sum has finitely many nonzero summands. Since $A$ is an internal direct sum of submodules $A_k$, $k \in K$, we must have $a_k = 0$ for every $k \in K$. Hence $(a_k)_{k\in K} = (0)_{k\in K}$ and $\varphi$ is injective by Proposition 1.30. Therefore $\varphi$ is an isomorphism of modules.

2) Assume that $B_k$, $k \in K$, are $R$-modules and $A = \oplus \sum_{k\in K} B_k$. Denote

$$A_k := \{(b_l)_{l\in K} \in A \mid b_l = 0 \text{ for every } l \in K \setminus \{k\}\} .$$

Thus the elements of $A_k$ are generalized sequences that have a nonzero component (if it exists) only at the $k$-th position. It is easy to understand that $A_k$ is a submodule of the module $A$ and $A_k \simeq B_k$ for every $k \in K$. Let $(b_l)_{l\in K} \in A$ be a generalized sequence, whose nonzero components are $b_{l_1}, \ldots, b_{l_n}$. Denoting by $\beta_{l_k}$, $k = 1, \ldots, n$, the generalized sequence whose $l_k$-component is $b_{l_k}$ and all other components are 0-s, we see that

$$(b_l)_{l\in K} = \beta_{l_1} + \ldots + \beta_{l_n},$$

where $\beta_{l_k} \in A_{l_k}$ for every $k = 1, \ldots, n$. Thus $A$ is a sum of submodules $A_k$, $k \in K$.

If now $l_1, \ldots, l_n \in K$ are pairwise distinct indices, $\alpha_{l_1} \in A_{l_1}, \ldots, \alpha_{l_n} \in A_{l_n}$ and $\alpha_{l_1} + \ldots + \alpha_{l_n}$ is a generalized sequence of zeroes, then also $\alpha_{l_1}, \ldots, \alpha_{l_n}$ are zero sequences, because addition is defined componentwise. Thus, the third condition of Theorem 1.86 is satisfied and hence $A$ is an internal direct sum of its submodules $A_k$, $k \in K$. □

**Example 1.89.** In case of the module considered in Example 1.83, $A = B_1 \times B_2 \times B_3 = B_1 \oplus B_2 \oplus B_3$, where $B_1 = B_2 = B_3 = \mathbb{Z}$. The submodules $A_1, A_2, A_3$ of $A$ are constructed precisely as submodules $A_k$ in the proof of Theorem 1.88.

The definitions and theorems given in this section apply to several cases:

- abelian groups, because they are just $\mathbb{Z}$-modules;
- right $R$-modules, because we can dualize the notions and arguments;
- left ideals of $R$, because they are submodules of the module ${}_R R$.

We will also use direct sums in the case of ideals and subrings of a ring $R$. In those cases the proofs will go through without essential changes.

In particular, a ring $R$ is an internal direct sum of its ideals $I$ and $J$ if and only if $R = I + J$ and $I \cap J = 0$. Then $I$ and $J$ are called **direct summands** of $R$ and we write $R = I \dot{+} J$. We also say that $R = I \dot{+} J$ is a **decomposition** of $R$ into ideals $I$ and $J$. Analogously one can speak about direct sums of one-sided ideals.

## 1.12 Properties of elements and ideals

**Definition 1.90.** An element $a$ of a ring $R$ is called

- an **idempotent** if $a^2 = a$;
- **nilpotent** if $a^k = 0$ for some $k \in \mathbb{N}$;

- **regular** if $a = aba$ for some $b \in R$;
- **left (right) invertible** if $R$ has an identity element 1 and there exists $b \in R$ such that $ba = 1$ (resp. $ab = 1$);
- **invertible** if it is left and right invertible;
- **central** if $ab = ba$ for all $b \in R$.

**Proposition 1.91.** *Let $R$ be a ring.*

1. *Every nonzero idempotent which is not an identity element is a zero divisor.*
2. *Every nonzero nilpotent element is a zero divisor.*
3. *Every right or left invertible element is regular.*
4. *Every idempotent is regular.*
5. *If $a \in R$ is a regular element and $a = aba$, where $b \in R$, then $ab$ and $ba$ are idempotents.*
6. *If zero is the only nilpotent element in $R$, then every idempotent of $R$ is central.*
7. *The set $Z(R)$ of all central elements of $R$ is a subring, which is called the* **centre** *of $R$.*

*Proof.* 1. Suppose that $e \neq 0$ is an idempotent which is not an identity element. Then there exists $a \in R$ such that $ae \neq a$ or there exists $b \in R$ such that $eb \neq b$. In the first case $ae - a \neq 0$ and

$$(ae - a)e = aee - ae = ae - ae = 0,$$

so $e$ is a right zero divisor. In the second case we obtain $e(eb - b) = 0$.

2. Let $a \neq 0$ be a nilpotent element. Then $a^l = 0$ for some $l \in \mathbb{N}$. Let $k$ be the smallest natural number such that $a^k = 0$. Then $k \neq 1$, because $a \neq 0$. Hence $k > 1$, $a^{k-1} \neq 0$ and $a^{k-1} \cdot a = 0$, so $a$ is a zero divisor.

3. If $ab = 1$, then $aba = 1a = a$ and $bab = b1 = b$.

4. If $e^2 = e$, then $e = eee$.

5. If $aba = a$, then $(ab)(ab) = (aba)b = ab$ and $(ba)(ba) = b(aba) = ba$.

6. If $e^2 = e$, then

$$\begin{aligned}(ea - eae)^2 &= (ea - eae)(ea - eae) = eaea - eaeae - eaeea + eaeeae \\ &= eaea - eaeae - eaea + eaeae = 0\end{aligned}$$

for every $a \in R$. By assumption, $ea - eae = 0$, i.e. $ea = eae$. Similarly we can show that $ae = eae$. We conclude that $ea = ae$ for every $a \in R$.

7. This is left as an exercise. □

**Definition 1.92.** An idempotent of a ring is called **central** if it belongs to the centre of that ring.

**Definition 1.93.** Two idempotents $e, f$ of a ring $R$ are called **orthogonal** if $ef = fe = 0$. An idempotent is called **primitive** if it cannot be written as a sum of two nonzero orthogonal idempotents.

**Example 1.94.** The idempotents of the ring $\mathbb{Z}_6$ are $\overline{0}, \overline{1}, \overline{3}$ and $\overline{4}$. Since $\overline{1} = \overline{3} + \overline{4}$ and $\overline{3} \cdot \overline{4} = \overline{0}$, $\overline{1}$ is a non-primitive idempotent. The other idempotents are primitive.

**Definition 1.95.** For a nonempty subset $A$ of a ring $R$, the set

1. $\mathrm{Ann}^l_R(A) := \{b \in R \mid ba = 0 \text{ for all } a \in A\}$ is called the **left annihilator** of $A$;
2. $\mathrm{Ann}^r_R(A) := \{b \in R \mid ab = 0 \text{ for all } a \in A\}$ is called the **right annihilator** of $A$;
3. $\mathrm{Ann}_R(A) := \mathrm{Ann}^l_R(A) \cap \mathrm{Ann}^r_R(A)$ is called the **annihilator** of $A$.

If the ring is clear from the context, then we write just $\mathrm{Ann}^l(A)$, $\mathrm{Ann}^r(A)$ and $\mathrm{Ann}(A)$.

**Example 1.96.** In the ring $\mathbb{Z}_{12}$, $\mathrm{Ann}(\{\overline{4}\}) = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$.

**Proposition 1.97.** *Let $A$ be a nonempty subset of a ring $R$. Then*

1. $\mathrm{Ann}^l(A)$ *is a left ideal and* $\mathrm{Ann}^r(A)$ *is a right ideal of $R$;*
2. *if $A \subseteq Z(R)$, then* $\mathrm{Ann}^l(A) = \mathrm{Ann}^r(A)$ *is an ideal of $R$;*
3. *if $A$ is a left ideal, then* $\mathrm{Ann}^l(A)$ *is an ideal of $R$;*
4. $A \subseteq \mathrm{Ann}(\mathrm{Ann}(A))$*;*
5. $\mathrm{Ann}(A)$ *is a subring.*

*Proof.* 1. If $b, b' \in \mathrm{Ann}^l(A)$ and $r \in R$, then

$$\begin{aligned} (b+b')a &= ba + b'a = 0 + 0 = 0, \\ (-b)a &= -ba = 0, \\ (rb)a &= r(ba) = r0 = 0 \end{aligned}$$

for every $a \in A$, so $b + b', -b, rb \in \mathrm{Ann}^l(A)$ and $\mathrm{Ann}^l(A)$ is a left ideal. A similar proof shows that $\mathrm{Ann}^r(A)$ is a right ideal.

2. Assume that $A \subseteq Z(R)$. If $b \in \mathrm{Ann}^l(A)$, then $0 = ba = ab$ for every $a \in A$. So $b \in \mathrm{Ann}^r(A)$ and $\mathrm{Ann}^l(A) \subseteq \mathrm{Ann}^r(A)$. Analogously $\mathrm{Ann}^r(A) \subseteq \mathrm{Ann}^l(A)$.

3. We already know that $\mathrm{Ann}^l(A)$ is a left ideal, so it remains to prove that it is a right ideal. If $b \in \mathrm{Ann}^l(A)$ and $r \in R$, then $(br)a = b(ra) = 0$, because $ra \in A$.

4. Take an arbitrary element $a \in A$. For every $b \in \mathrm{Ann}(A)$, $ab = 0$ and $ba = 0$. Thus $a \in \mathrm{Ann}^l(\mathrm{Ann}(A)) \cap \mathrm{Ann}^r(\mathrm{Ann}(A)) = \mathrm{Ann}(\mathrm{Ann}(A))$.

5. If $x, y \in \mathrm{Ann}(A)$, then

$$\begin{aligned} (x-y)a &= xa - ya = 0 - 0 = 0, \\ a(x-y) &= ax - ay = 0 - 0 = 0, \\ a(xy) &= (ax)y = 0y = 0, \\ (xy)a &= x(ya) = x0 = 0 \end{aligned}$$

for every $a \in A$. Hence $\mathrm{Ann}(A)$ is a subring. □

**Proposition 1.98.** *Let $R$ be a ring.*

1. *For every idempotent $e \in R$,*
$$R = {}_R(e) \dotplus \mathrm{Ann}^l(e)$$
*is a decomposition of $R$ into left ideals.*

2. *For every central idempotent $f \in R$,*
$$R = (f) \dotplus \mathrm{Ann}(f)$$
*is a decomposition of $R$ into ideals.*

3. *If $R$ has an identity element $1$, then every left ideal which is a direct summand of $R$ is generated by an idempotent $e \in R$ and $\mathrm{Ann}^l(e) = R(1-e)$.*

4. *If $R$ has an identity element $1$, then every ideal which is a direct summand of $R$ is generated by a central idempotent $f \in R$ and $\mathrm{Ann}(f) = R(1-f)$.*

*Proof.* 1. Recall that ${}_R(e) = \mathbb{Z}e + Re$ is the principal left ideal of $R$ generated by $e$ (see Proposition 1.54). For every $a \in R$, we have $a = ae + (a - ae)$, where $ae \in Re \subseteq {}_R(e)$ and $a - ae \in \mathrm{Ann}^l(e)$. Thus $R = {}_R(e) + \mathrm{Ann}^l(e)$.

To prove that ${}_R(e) \cap \mathrm{Ann}^l(e) = 0$, we consider an element $b \in {}_R(e) \cap \mathrm{Ann}^l(e)$. Then $b = ze + re$ for some $z \in \mathbb{Z}$ and $r \in R$, and $be = 0$. But
$$be = (ze + re)e = zee + ree = ze + re = b,$$
so $b = 0$.

2. If $f$ is central, then $\mathrm{Ann}^l(f) = \mathrm{Ann}^r(f) = \mathrm{Ann}(f)$ is a two-sided ideal. Note that $RRf = Rf$, because the inclusion $RRf \subseteq Rf$ is clear and the converse holds because $rf = rff \in RRf$ for every $r \in R$. Therefore, using Proposition 1.54 and centrality of $f$,
$$(f) = \mathbb{Z}f + Rf + fR + RfR = \mathbb{Z}f + Rf + Rf + RRf = \mathbb{Z}f + Rf = {}_R(f).$$
The assertion follows now from claim 1.

3. Let $R = I \dotplus J$ be a decomposition of $R$ into left ideals. Then $1 = i + j$ for some $i \in I$ and $j \in J$. We have $i = i1 = i(i + j) = i^2 + ij$ and $ij = i - i^2 \in I \cap J = 0$, hence $i^2 = i$. For every $a \in I$ we get $a = ai + aj$ and hence $aj = a - ai \in I \cap J = 0$, i.e. $a = ai$. We have shown that $I = Ii \subseteq Ri \subseteq I$, so $I = Ri$, where $i$ is an idempotent.

If $r(1-i) \in R(1-i)$, then $r(1-i)i = r(i-i^2) = r0 = 0$. Thus $R(1-i) \subseteq \mathrm{Ann}^l(i)$. On the other hand, if $a \in \mathrm{Ann}^l(i)$, then $a(1-i) = a - ai = a - 0 = a$, i.e. $\mathrm{Ann}^l(i) \subseteq R(1-i)$.

4. If $I$ and $J$ are ideals, $R = I \dotplus J$ and $1 = i + j$, where $i \in I$, $j \in J$, then
$$ri + rj = r1 = 1r = ir + jr$$
for every $r \in R$. As $I$ and $J$ are ideals, $ri, ir \in I$ and $rj, jr \in J$. Since the representation is unique (see Theorem 1.81),
$$ri + rj = ir + jr \implies ri = ir \text{ and } rj = jr \implies i \in Z(R).$$
Therefore $\mathrm{Ann}(i) = \mathrm{Ann}^l(i) = R(1-i)$. □

**Lemma 1.99.** *If $e$ is an idempotent of a ring $R$, then $eRe = \{ere \mid r \in R\}$ is a subring of $R$ which has the identity element $e$.*

*Proof.* If $r, r' \in R$, then

$$\begin{aligned} ere - er'e = e(re - r'e) = e(r - r')e \in eRe, \\ (ere)(er'e) = e(rer')e \in eRe, \\ e(ere) = ere = (ere)e. \end{aligned}$$

□

Subrings $eRe$ are called **local subrings** of $R$. These play an important role in Morita theory of rings.

In the next result we will show that every idempotent of a ring gives rise to a decomposition into certain subrings. That decomposition is called the **Peirce**[5] **decomposition**.

**Theorem 1.100.** *Let $e$ be an idempotent of a ring $R$. Then*

$$R = eRe \dotplus e\operatorname{Ann}^l(e) \dotplus \operatorname{Ann}^r(e)e \dotplus \operatorname{Ann}(e)$$

*is a decomposition of $R$ as a direct sum of subrings. If $e$ is a central idempotent then*

$$R = Re \dotplus \operatorname{Ann}(e)$$

*is a decomposition of $R$ into ideals.*

*Proof.* We know that $eRe$ is a subring by Lemma 1.99 and $\operatorname{Ann}(e)$ is a subring by Proposition 1.97. It is easy to see that $e\operatorname{Ann}^l(e)$ and $\operatorname{Ann}^r(e)e$ are also subrings. For every $a \in R$ we have

$$a = eae + e(a - ae) + (a - ea)e + (a - ea - ae + eae),$$

where $eae \in eRe$, $a - ae \in \operatorname{Ann}^l(e)$ and $a - ea \in \operatorname{Ann}^r(e)$. Let us prove that $x := a - ea - ae + eae \in \operatorname{Ann}^l(e)$ (similarly $x \in \operatorname{Ann}^r(e)$). Indeed,

$$xe = ae - eae - aee + eaee = ae - eae - ae + eae = 0.$$

Thus $R$ is the sum of the claimed subrings.

We prove that this sum is an internal direct sum using condition 3 in the analogue of Theorem 1.81 for subrings. Assume that

$$0 = a_1 + a_2 + a_3 + a_4 \tag{1.12}$$

with $a_k$ in the corresponding subring. We must show that every $a_k = 0$. Observe that

$$\begin{aligned} a_1 \in eRe &\implies ea_1 = a_1 = a_1e, \\ a_2 \in e\operatorname{Ann}^l(e) &\implies a_2e = 0 \wedge ea_2 = a_2, \\ a_3 \in \operatorname{Ann}^r(e)e &\implies ea_3 = 0 \wedge a_3e = a_3, \\ a_4 \in \operatorname{Ann}(e) &\implies ea_4 = 0 = a_4e. \end{aligned}$$

[5]Benjamin Peirce (1809–1880) — American mathematician

Multiplying (1.12) by $e$ from one or both sides we obtain

$$\begin{aligned} 0 = e0e &= ea_1e + ea_2e + ea_3e + ea_4e = ea_1e = a_1, \\ 0 = e0 &= ea_1 + ea_2 + ea_3 + ea_4 = ea_2 = a_2, \\ 0 = 0e &= a_1e + a_2e + a_3e + a_4e = a_3e = a_3. \end{aligned}$$

Hence aslo $a_4 = 0$. Therefore we have a direct sum of subrings.

If $e$ is a central idempotent, then $\mathrm{Ann}(e) = \mathrm{Ann}^l(e) = \mathrm{Ann}^r(e)$ is an ideal and

$$\begin{aligned} R &= eRe + e\,\mathrm{Ann}^l(e) + \mathrm{Ann}^r(e)e + \mathrm{Ann}(e) \\ &\subseteq eeR + \mathrm{Ann}(e) + \mathrm{Ann}(e) + \mathrm{Ann}(e) = eR + \mathrm{Ann}(e) \subseteq R, \end{aligned}$$

so $R = eR + \mathrm{Ann}(e)$. Also $eR \cap \mathrm{Ann}(e) = 0$, and hence $R = eR \dotplus \mathrm{Ann}(e)$. □

**Example 1.101.** In the ring $\mathbb{Z}_{12}$, $\overline{4}$ is a central idempotent, $\mathbb{Z}_{12} \cdot \overline{4} = \{\overline{0}, \overline{4}, \overline{8}\}$ and $\mathrm{Ann}(\{\overline{4}\}) = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$. Hence

$$\mathbb{Z}_{12} = \{\overline{0}, \overline{4}, \overline{8}\} \dotplus \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}.$$

Next we define some properties of right ideals.

**Definition 1.102.** A right ideal $I$ of a ring $R$ is called

- a **nil ideal** if every element of $I$ is nilpotent;
- **nilpotent** if there is $k \in \mathbb{N}$ such that $I^k = 0$;
- **idempotent** if $I^2 = I$.

Similar definitions can be given for left ideals and two-sided ideals.

It is easy to see that every nilpotent ideal is a a nil ideal.

**Definition 1.103.** A proper ideal $I$ of a ring $R$ is called

- **prime** if, for any ideals $A, B$ of $R$,

$$AB \subseteq I \implies A \subseteq I \text{ or } B \subseteq I;$$

- **semiprime** if it is an intersection of some family of prime ideals.

In particular, every prime ideal $I$ is semiprime as it is the intersection of the family consisting of $I$. Also $R$ is a semiprime ideal, because it may be considered as the intersection of the empty family of prime ideals.

**Proposition 1.104.** *Let $n \in \mathbb{N}$, $n \geq 2$. An ideal $(n)$ of the ring $\mathbb{Z}$ is prime if and only if $n$ is a prime number.*

*Proof.* NECESSITY. Let $(n)$ be a prime ideal. Suppose that $n$ is not a prime number. Then $n = ab$, where $1 < a, b < n$. We conclude that $(n) = (a)(b)$. Hence either $(a) \subseteq (n)$ or $(b) \subseteq (n)$. Thus, $n \mid a$ or $n \mid b$, a contradiction.
SUFFICIENCY. Let $n$ be a prime number and $AB \subseteq (n)$, where $A, B \in \mathsf{Id}(\mathbb{Z})$. Then $A = (u)$ and $B = (v)$ for some $u, v \in \mathbb{N}$. Therefore $(uv) = (u)(v) \subseteq (n)$, and so $n \mid uv$. Since $n$ is a prime number, $n \mid u$ or $n \mid v$, and hence $(u) \subseteq (n)$ or $(v) \subseteq (n)$. □

**Example 1.105.** Since $(2) \cap (3) = (6)$ in the ring $\mathbb{Z}$, we see that $(6) = 6\mathbb{Z}$ is a semiprime ideal, which is not a prime ideal.

**Proposition 1.106.** *In any ring $R$ with identity, every maximal ideal is a prime ideal.*

*Proof.* Let $I, J, \mathfrak{m} \in \mathsf{Id}(R)$, where $\mathfrak{m}$ is a maximal ideal. Suppose $IJ \subseteq \mathfrak{m}$, but $I \not\subseteq \mathfrak{m}$. Then $\mathfrak{m} + I$ is an ideal containing $\mathfrak{m}$, so $\mathfrak{m} + I = R$ by maximality of $\mathfrak{m}$. Since $R$ has an identity, we have $J = RJ$. So

$$\begin{aligned} J &= (\mathfrak{m} + I)J && (\mathfrak{m} + I = R) \\ &= \mathfrak{m}J + IJ && (\text{Proposition 1.40}) \\ &\subseteq \mathfrak{m} + IJ && (\mathfrak{m} \text{ is an ideal}) \\ &\subseteq \mathfrak{m} + \mathfrak{m} && (IJ \subseteq \mathfrak{m}) \\ &\subseteq \mathfrak{m}. && (\mathfrak{m} \text{ is an ideal}) \end{aligned}$$

□

**Proposition 1.107** (Brauer's Lemma)**.** *Let $I$ be a minimal left ideal of a ring $R$ such that $I^2 \neq 0$. Then $I = Re$ for some idempotent $e \in R$ and $eRe$ is a division ring.*

*Proof.* If $I^2 \neq 0$, then there exist $b, a \in I$ such that $ba \neq 0$, hence $Ia \neq 0$. Note that $Ia$ is a left ideal and $Ia \subseteq I$, because $a \in I$. By minimality of $I$, $Ia = I$. Now $a \in I \subseteq Ia$ means that $a = ea$ for some $e \in I$. Hence $a = ea = e^2a$ and $(e^2 - e)a = 0$. Since $\mathrm{Ann}^{\mathrm{l}}(a)$ is a left ideal, also $\mathrm{Ann}^{\mathrm{l}}(a) \cap I$ is a left ideal of $R$, which is contained in $I$. Note that $I = Ia \neq 0$. By minimality of $I$ we have two possibilities.

1) $\mathrm{Ann}^{\mathrm{l}}(a) \cap I = I$. Then $I \subseteq \mathrm{Ann}^{\mathrm{l}}(a)$ and $b \in I$ implies $ba = 0$, a contradiction.

2) $\mathrm{Ann}^{\mathrm{l}}(a) \cap I = 0$. Since $e^2 - e \in \mathrm{Ann}^{\mathrm{l}}(a) \cap I$, we conclude that $e^2 - e = 0$, or $e^2 = e$. Since $(Ie)a = I(ea) = Ia = I$, also $Ie \neq 0$ and $Re \neq 0$ is a left ideal contained in $I$. By minimality, $Re = I$.

Finally we prove that $eRe$ is a division ring. For this, it suffices to prove that every nonzero element has a left inverse. Let $0 \neq b \in eRe$. Then $0 \neq Rb \subseteq Re$, so $Rb = Re$ by minimality. Hence there exists $r \in R$ such that $e = rb$ and

$$(ere)b = er(eb) = erb = e^2 = e,$$

so $ere$ is a left inverse for $b$ in $eRe$. □

**Proposition 1.108.** *In a ring $R$ with identity, every (left) ideal generated by a regular element is idempotent.*

*Proof.* If $a \in R$ is a regular element, then $a \in aRa$ and $Ra \subseteq RaRa \subseteq Ra$, so $(Ra)^2 = Ra$, and

$$RaR \subseteq RaRaR = RaRRaR \subseteq RaR,$$

so $(RaR)^2 = RaR$. □

**Exercise 1.109.** Prove that if $e$ is an idempotent in a ring $R$, then

1. $\mathrm{Ann}^l(e) = \{x - xe \mid x \in R\}$,
2. $\mathrm{Ann}^r(e) = \{x - ex \mid x \in R\}$,
3. $\mathrm{Ann}(e) = \{x - xe - ex - exe \mid x \in R\}$.

# Chapter 2

# Projective modules

## 2.1 Exact sequences

In this section we will assume that all considered modules are left modules over a fixed ring $R$.

To speak about projectivity, we first need to consider some basic facts about exact sequences. Consider a sequence

$$\ldots \xrightarrow{f_{\alpha-1}} A_\alpha \xrightarrow{f_\alpha} A_{\alpha+1} \xrightarrow{f_{\alpha+1}} \ldots . \tag{2.1}$$

of modules $A_\alpha$ and module homomorphisms $f_\alpha$. This sequence can be finite, infinite in both directions or infinite in one direction.

As in the case of vector spaces one can show that the kernel and the image of a module homomorphism are submodules.

**Definition 2.1.** A sequence (2.1) is called **exact at** $\alpha$ if

$$\mathrm{Ker}(f_\alpha) = \mathrm{Im}(f_{\alpha-1})\,.$$

This sequence is called **exact** if it is exact at every $\alpha$.

If a sequence is exact at $\alpha$, then $f_\alpha f_{\alpha-1} = 0$, i.e. the composite of these two homomorphisms is the zero homomorphism.

**Example 2.2.** Consider abelian groups $\mathbb{Z}$ and $\mathbb{Z}_2$ as $\mathbb{Z}$-modules. Then there exists an exact sequence

$$\mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}_2,$$

where the homomorphisms $f$ and $g$ are defined by

$$f(a) := 2a,$$
$$g(a) := \overline{a}.$$

Exact sequences is an important tool in the theory of modules, because they enable to describe several properties of modules and homomorphisms. In what follows, the symbol 0 may denote the zero element of a module, a one-element module or a zero homomorphism. We hope that it will be clear from the context, which meaning is used.

**Lemma 2.3.** *A sequence of modules*

1. $0 \longrightarrow A \xrightarrow{f} B$ *is exact if and only if* $f$ *is injective;*

2. $A \xrightarrow{f} B \longrightarrow 0$ *is exact if and only if* $f$ *is surjective;*

3. $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ *is exact if and only if* $f$ *is bijective.*

*Proof.* 1. We note that there exists precisely one homomorphism $0 \longrightarrow A$, which must take the zero element to the zero element. Usually such a homomorphism is not written in the figures. The image of that homomorphism is $\{0\}$. Now

$$0 \longrightarrow A \xrightarrow{f} B \text{ is exact } \iff \ker(f) = \{0\} \iff f \text{ is injective.}$$

2. The only homomorphism $B \longrightarrow 0$ is the zero homomorphism, whose kernel is $B$. Hence

$$A \xrightarrow{f} B \longrightarrow 0 \text{ is exact } \iff \operatorname{Im}(f) = B \iff f \text{ is surjective.}$$

3. This is a direct consequence of parts 1 and 2. □

**Definition 2.4.** Exact sequences of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

are called **short exact sequences**.

We can say the following about a short exact sequence

1. $f$ is injectivne;

2. $g$ is surjective;

3. $C \cong B/\operatorname{Ker}(g) = B/\operatorname{Im}(f)$ by the analogue of Corollary 1.58 for modules;

4. if we identify $A$ and the submodule $\operatorname{Im}(f)$ of $B$, which is isomorphic to it, then we could write $C \cong B/A$.

A typical short exact sequence is

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} B/A \longrightarrow 0$$

where

- $A$ is a submodule of $B$,
- $\iota$ is the inclusion mapping,
- $\pi : b \mapsto b + A$ is the natural projection on the quotient module $B/A$.

In the next theorem we consider short exact sequences, where one of the middle homomorphisms has a one-sided inverse.

**Theorem 2.5.** *Let $R$ be a ring and let*

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

*be a short exact sequence of left $R$-modules. The following are equivalent.*

(i) *There exists a homomorphism $\varphi : B \to A$ such that $\varphi\iota = id_A$.*

(ii) *There exists an endomorphism $f : B \to B$ such that $f^2 = f$ and $\mathrm{Im}(f) = \mathrm{Im}(\iota)$.*

(iii) *There exists a submodule $H$ of $B$ such that $B = \mathrm{Im}\,\iota \dotplus H$.*

(iv) *There exists a homomorphism $\psi : C \to B$ such that $\pi\psi = id_C$.*

*Proof.* (ii) $\Rightarrow$ (iii) We show that the claim holds for $H = \mathrm{Ker}(f)$, i.e. we prove that

$$B = \mathrm{Im}(\iota) \dotplus \mathrm{Ker}(f).$$

First we show that $B = \mathrm{Im}(\iota) + \mathrm{Ker}(f)$. To this end, we observe that, for every $b \in B$, $b - f(b) \in B$ and

$$f(b - f(b)) = f(b) - f^2(b) = f(b) - f(b) = 0\,.$$

Thus $b - f(b) \in \mathrm{Ker}(f)$ and

$$b = f(b) + (b - f(b)) \in \mathrm{Im}(f) + \mathrm{Ker}(f) = \mathrm{Im}(\iota) + \mathrm{Ker}(f)\,.$$

Now let $b \in \mathrm{Im}(f) \cap \mathrm{Ker}(f)$, i.e. $f(b) = 0$ and $b = f(b')$ for some $b' \in B$. Then $b = f(b') = f^2(b') = f(f(b')) = f(b) = 0$. Therefore $\mathrm{Im}(f) \cap \mathrm{Ker}(f) = 0$ and $B = \mathrm{Im}(\iota) \dotplus \mathrm{Ker}(f)$, i.e. the module $B$ is a direct sum of its submodules $\mathrm{Im}\,(\iota)$ and $\mathrm{Ker}(f)$.

(iii) $\Rightarrow$ (i) Let $B = \mathrm{Im}\,\iota \dotplus H$, where $H$ is a submodule of $B$. Then every $b \in B$ can be uniquely presented as a sum $b = \iota(x) + y$, where $x \in A$, $y \in H$. Since $\iota$ is injective, not only $\iota(x)$ is unique, but also $x$ is unique. Thus we can define a mapping $\varphi : B \to A$ by

$$\varphi(b) = \varphi(\iota(x) + y) = x\,.$$

It is not difficult to check that $\varphi$ is a homomorphism of modules. Moreover,

$$(\varphi\iota)(a) = \varphi(\iota(a) + 0) = a = id_A(a)$$

for every $a \in A$. We have proved that $\varphi\iota = id_A$.

(i) $\Rightarrow$ (iv) We define the mapping $\psi : C \to B$ by

$$\psi(c) = b - (\iota\varphi)(b)\,,$$

where $b \in B$ is one of the elements satisfying $\pi(b) = c$ (recall that $\pi$ is surjective). We will show that the preceding definition does not depend upon the choice of $b$. Suppose

that $b' \in B$ is also such that $\pi(b') = c$. Then $\pi(b - b') = 0$ and $b - b' \in \mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$. Hence there exists $a \in A$ such that $b - b' = \iota(a)$. Now

$$\begin{aligned}(\iota\varphi)(b) - (\iota\varphi)(b') = (\iota\varphi)(b - b') &= (\iota\varphi)(\iota(a)) \\ &= (\iota(\varphi\iota))(a) = (\iota id_A)(a) = \iota(a) = b - b',\end{aligned}$$

whence

$$\psi(c) = b - (\iota\varphi)(b) = b' - (\iota\varphi)(b')\,.$$

This means that $\psi$ is well defined. It is not difficult to show that $\psi$ is a homomorphism.

Finally, for every $c \in C$,

$$(\pi\psi)(c) = \pi(b - (\iota\varphi)(b)) = \pi(b) - (\pi\iota)(\varphi(b)) = \pi(b) - 0 = c = id_C(c)\,,$$

where we used that $\pi\iota$ is the zero mapping. Thus $\pi\psi = id_C$, as needed.

(iv) $\Rightarrow$ (ii) We define a mapping $f : B \to B$ by

$$f = id_B - \psi\pi\,.$$

As $f$ is the difference of endomorphisms $id_B$ and $\psi\pi$ of $B$, it is an endomorphism of $B$. Also,

$$\begin{aligned}f^2 &= (id_B - \psi\pi)(id_B - \psi\pi) = id_B - \psi\pi - \psi\pi + \psi(\pi\psi)\pi \\ &= id_B - \psi\pi - \psi\pi + \psi(id_C)\pi = id_B - \psi\pi = f\,.\end{aligned}$$

It remains to show that $\mathrm{Im}(\iota) = \mathrm{Im}(f)$. For every $a \in A$,

$$\begin{aligned}f(\iota(a)) = (id_B - \psi\pi)(\iota(a)) &= id_B(\iota(a)) - (\psi\pi)(\iota(a)) \\ &= \iota(a) - \psi((\pi\iota)(a)) = \iota(a) - \psi(0) = \iota(a)\,,\end{aligned}$$

which implies $\mathrm{Im}(\iota) \subseteq \mathrm{Im}(f)$. Conversely, if $b \in B$, then

$$\pi(f(b)) = \pi(b - (\psi\pi)(b)) = \pi(b) - (\pi\psi\pi)(b) = \pi(b) - (id_C\pi)(b) = 0\,,$$

and hence $f(b) \in \mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$. Therefore $\mathrm{Im}(f) \subseteq \mathrm{Im}(\iota)$. We conclude that $\mathrm{Im}(f) = \mathrm{Im}(\iota)$. □

**Example 2.6.** Let us consider the following two homomorphisms of left $\mathbb{Z}$-modules: $\iota : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, $a \mapsto (a, 0)$, and $\pi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(a, b) \mapsto b$. Then

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \times \mathbb{Z} \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0$$

is a short exact sequence, because $\iota$ is injective, $\pi$ is surjective and we have $\mathrm{Im}\,(\iota) = \{(a, 0) \mid a \in \mathbb{Z}\} = \mathrm{Ker}(\pi)$. This sequence also satisfies the conditions of Theorem 2.5, because we may take $\varphi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(a, b) \mapsto a$.

## 2.2 Free modules

**Definition 2.7.** A module is called **free** if it has a basis, i.e. a linearly independent set of generators.

Linear independence in the case of modules is defined in the same way as it is defined in the case of vector spaces.

**Example 2.8.** For example, ${}_{\mathbb{Z}}F = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ is a free $\mathbb{Z}$-module. One of its bases is $\{(1,0,0),(0,1,0),(0,0,1)\}$. For instance, an element $(5,-2,3)$ is a linear combination

$$(5,-2,3) = 5(1,0,0) - 2(0,1,0) + 3(0,0,1).$$

Every basis of a unitary module ${}_RM$ over a ring with identity $1 \neq 0$ is a minimal generating set. Let us prove this fact. If $X$ is a basis then it certainly is a generating set. Let us prove its minimality. Suppose to the contrary that $Y \subset X$ is also a generating set. Choose $x \in X \setminus Y$. Then $x = r_1y_1 + \ldots + r_ny_n$, where $r_1, \ldots, r_n \in R$ and $y_1, \ldots, y_n \in Y$. We see that

$$1_Rx - r_1y_1 - \ldots - r_ny_n$$

is a nontrivial linear combination of elements of $X$, which equals 0, a contradiction.

On the other hand, a minimal generating set of a module need not be a basis, see Example 1.70. This is an important difference between modules and vector spaces: in a vector space, the bases are precisely the minimal generating sets.

In the next result we show that there exist free modules with bases of any cardinality.

**Proposition 2.9.** *For every nonempty set $X$ and every ring $R$ with identity $1_R \neq 0_R$ there exists a unitary free left $R$-module $R^{(X)}$ and an injective mapping $\iota : X \longrightarrow R^{(X)}$ such that $\iota(X)$ is a basis for $R^{(X)}$.*

*Proof.* We define $R^{(X)}$ as the external direct sum of copies of the module ${}_RR$ indexed by the set $X$:

$$R^{(X)} := \oplus \sum_{x \in X} R.$$

We may think of the elements of $R^{(X)}$ in two ways:

a) they are generalized sequences $a = (a_x)_{x \in X}$ having finitely many nonzero components with componentwise operations, or, equivalently,

b) they are mappings $a : X \longrightarrow R, x \mapsto a_x$, such that $a(x) \neq 0$ for all but finitely many $x \in X$, with pointwise operations.

We will use the first approach here. For every $y \in X$, let $\delta_x = (\delta_{x,y})_{y \in X}$, where

$$\delta_{x,y} = \begin{cases} 1_R, & \text{if } x = y \\ 0_R, & \text{if } x \neq y \end{cases}$$

(this is a version of the Kronecker delta). Then each nonzero element of $R^{(X)}$ can be wrtitten as a finite sum

$$a = \sum_{x \in X} a_x \delta_x$$

of those terms, where $a_x \neq 0$. Two such sums are equal if the coefficients of $\delta_x$ are equal in both sums for every $x \in X$. It is easy to see that $\{\delta_x \mid x \in X\}$ is a basis of the module $R^{(X)}$ and the mapping

$$\iota : X \longrightarrow R^{(X)}, \quad x \mapsto \delta_x$$

is injective. Hence $R^{(X)}$ is a free left $R$-module. Obviously, it is unitary. □

**Proposition 2.10** (The Universal Property)**.** *Let $X$ and $R$ be as in Proposition 2.9. For every mapping $g : X \longrightarrow {}_RM$, where ${}_RM$ is a unitary left $R$-module, there exists a unique mapping $\overline{g} : R^{(X)} \longrightarrow {}_RM$ such that $g = \overline{g}\iota$.*

*Proof.* The mapping $\overline{g}$ is defined by

$$\overline{g}\left(\sum_{x\in X} a_x\delta_x\right) := \sum_{x\in X} a_x g(x),$$

where both sums are finite. A straightforward verification shows that $\overline{g}$ is a homomorphism of left $R$-modules. Now $g = \overline{g}\iota$, because, for every $x \in X$,

$$(\overline{g}\iota)(x) = \overline{g}(\delta_x) = \overline{g}(1_R\delta_x) = 1_R \cdot g(x) = g(x).$$

If $h : R^{(X)} \longrightarrow {}_RM$ is another homomorphism such that $g = h\iota$, then, for every $\sum_{x\in X} a_x\delta_x \in R^{(X)}$,

$$\begin{aligned}
h\left(\sum_{x\in X} a_x\delta_x\right) &= \sum_{x\in X} a_x h(\delta_x) && (h \text{ is a homomorphism})\\
&= \sum_{x\in X} a_x (h\iota)(x), && (\text{def. of } \iota)\\
&= \sum_{x\in X} a_x g(x) && (h\iota = g)\\
&= \overline{g}\left(\sum_{x\in X} a_x\delta_x\right). && (\text{def. of } \overline{g})
\end{aligned}$$

Hence $h = \overline{g}$, proving the uniqueness of $\overline{g}$. □

**Theorem 2.11.** *Let $R$ be a ring with identity $1_R \neq 0_R$. A unitary left $R$-module ${}_RF$ is free if and only if there exists a set $X \neq \emptyset$ such that ${}_RF \simeq R^{(X)}$.*

*Proof.* Necessity. Suppose that ${}_RF$ is a free module with a basis $\{e_x \mid x \in X\}$, where $X \neq \emptyset$ is some index set. Then every element of $F$ can be uniquely expressed as a linear combination

$$r_1e_{x_1} + \ldots + r_ne_{x_n},$$

where $n \in \mathbb{N}$ and $r_1, \ldots, r_n \in R$. We consider the map

$$\varphi : F \longrightarrow R^{(X)}, \quad r_1e_{x_1} + \ldots + r_ne_{x_n} \mapsto r_1\delta_{x_1} + \ldots + r_n\delta_{x_n}.$$

Note that $r_1\delta_{x_1} + \ldots + r_n\delta_{x_n}$ is a generalized sequence, whose $x_i$-component is $r_i$ for every $i = 1, \ldots, n$, and which has zeroes elsewhere. It is straightforward to show that $\varphi$ is a homomorphism of left $R$-modules. It is also clear that $\varphi$ is surjective. If $f = r_1e_{x_1} + \ldots + r_ne_{x_n} \in \mathrm{Ker}(\varphi)$, then $\varphi(f) = r_1\delta_{x_1} + \ldots + r_n\delta_{x_n}$ is the zero sequence, hence $r_1 = \ldots = r_n = 0$ and therefore $f = 0$. Thus $\mathrm{Ker}(\varphi) = 0$ and $\varphi$ is injective. We have shown that $\varphi$ is an isomorphism.
SUFFICIENCY. This follows from Proposition 2.9. □

A module $A$ is called an **epimorphic image** of a module $B$, if there exists a surjective homomorphism $B \longrightarrow A$. In such a case, $A$ is isomorphic to a quotient module of $B$ due to The Homomorphism Theorem.

**Proposition 2.12.** *Every unitary left module over a ring $R$ with identity $1_R \neq 0_R$ is an epimorphic image of a free module.*

*Proof.* Let $A$ be a left $R$-module. Consider $A$ as a set of indices. By Theorem 2.11, $F := R^{(A)}$ is a free module. For an element $x = (x_a)_{a\in A} \in F$, we define

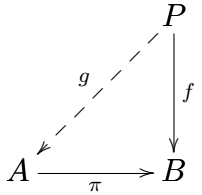
$$f(x) := \sum_{a\in A} x_a a\,.$$

Note that the sum is finite, because the generalized sequence $(x_a)_{a\in A}$ has a finite number of nonzero elements. Hence we obtain a mapping $f : F \longrightarrow A$. It is easy to verify that $f$ is a homomorphism of left modules.

In addition, $f(\delta_a) = 1_R \cdot a = a$, showing that $f$ is surjective. □

## 2.3 Projective modules

**Definition 2.13.** Let $R$ be a ring. A module ${}_RP$ is called **projective** if for evey surjective module homomorphism $\pi : {}_RA \to {}_RB$ and every module homomorphism $f : {}_RP \to {}_RB$ there exists a module homomorphism $g : {}_RP \to {}_RA$ such that $f = \pi g$.




**Proposition 2.14.** *Every free module over a ring is projective.*

*Proof.* Let $F$ be a free left $R$-module with a basis $\{e_i \mid i \in I\}$. We will show that $F$ is projective. Let $A, B$ be modules, $f : F \longrightarrow B$ a homomorphism and $\pi : A \longrightarrow B$ a surjective homomorphism. Denote $b_i := f(e_i)$ for every $i \in I$. Since $\pi$ is surjective, for every $i \in I$ we can choose an element $a_i \in A$ such that $\pi(a_i) = b_i$.

Now we define a mapping $g : F \longrightarrow A$. Every nonzero element $x \in F$ can be presented uniquely as a linear combination

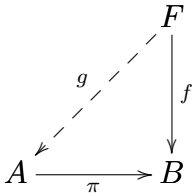
$$x = r_{i_1} e_{i_1} + \ldots + r_{i_n} e_{i_n} = \sum_{k=1}^{n} r_{i_k} e_{i_k},$$

where $n \in \mathbb{N}$, $i_1, \ldots, i_n \in I$ and $r_{i_1}, \ldots, r_{i_n} \in R$. We define

$$g(x) := \sum_{k=1}^{n} r_{i_k} a_{i_k}$$

and $g(0) := 0$. Because of the uniqueness of the representation, $g$ is well defined. It is easy to check that $g$ is a module homomorphism.

To complete the proof, we verify that the triangle




is commutative. Clearly, $(\pi g)(0) = 0 = f(0)$. If an element $x \in F \setminus \{0\}$ is given as before, then

$$\begin{aligned}
(\pi g)(x) &= \pi \left( \sum_{k=1}^{n} r_{i_k} a_{i_k} \right) && \text{(def. of } g\text{)} \\
&= \sum_{k=1}^{n} r_{i_k} \pi(a_{i_k}) && (\pi \text{ is a homomorphism}) \\
&= \sum_{k=1}^{n} r_{i_k} b_{i_k} && (\pi(a_{i_k}) = b_{i_k}) \\
&= \sum_{k=1}^{n} r_{i_k} f(e_{i_k}) && (f(e_{i_k}) = b_{i_k}) \\
&= f \left( \sum_{k=1}^{n} r_{i_k} e_{i_k} \right) && (f \text{ is a homomorphism}) \\
&= f(x)\,.
\end{aligned}$$

Thus $\pi g = f$. □

Every idempotent gives rise to a projective module which, in general, is not free.

**Proposition 2.15.** *If $e$ is an idempotent in a ring $R$, then $Re$ is a projective left $R$-module.*

*Proof.* Let $f : Re \longrightarrow {}_RB$ be a homomorphism and $\pi : {}_RA \longrightarrow {}_RB$ a surjective homomorphism. Denote $b := f(e) \in B$. Choose $a \in A$ such that $\pi(a) = b$. Then $eb = ef(e) = f(ee) = f(e) = b$. Define $g : Re \longrightarrow A$ by

$$g(re) := rea.$$

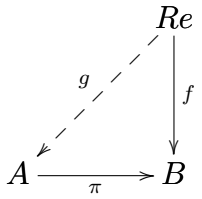
Then

$$\begin{aligned} g(re + r'e) = g((r + r')e) = (r + r')ea = rea + r'ea = g(re) + g(r'e), \\ g(s(re)) = g((sr)e) = (sr)ea = s(re)a = sg(re) \end{aligned}$$

for every $r, r', s \in R$, proving that $g$ is a homomorphism of left $R$-modules. In addition, for every $r \in R$,

$$(\pi g)(re) = \pi(rea) = re\pi(a) = reb = rb = rf(e) = f(re).$$

Thus $\pi g = f$.

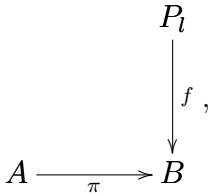



□

**Corollary 2.16.** *A one-element module is projective.*

**Proposition 2.17.** *Let $P_k$, $k \in K$, be left modules over a ring $R$. Then $\oplus \sum_{k\in K} P_k$ is projective if and only if $P_k$ is projective for every $k \in K$.*

*Proof.* NECESSITY. Assume that $\oplus \sum_{k\in K} P_k$ is projective. We fix $l \in K$ and prove that $P_l$ is projective. Consider the diagram




where $f$ and $\pi$ are homomorphisms and $\pi$ is surjective. Let $\pi_l : \oplus \sum_{k\in K} P_k \longrightarrow P_l$ be the projection on the $l$-th direct summand $P_l$ and let $\iota : P_l \longrightarrow \oplus \sum_{k\in K} P_k$ be a mapping that takes $x \in P_l$ to a generalized sequence whose $l$-component is $x$ and other components are zeroes. Since $\oplus \sum_{k\in K} P_k$ is projective, there exists a homomorphism $g : \oplus \sum_{k\in K} P_k \longrightarrow A$ such that $\pi g = f\pi_l$. Then

$$\pi(g\iota_l) = (\pi g)\iota_l = f\pi_l\iota_l = fid_{P_l} = f.$$

SUFFICIENCY. Assume that modules $P_k$, $k \in K$, are projective. Consider a diagram

$$\begin{array}{ccc} & & \oplus \sum_{k\in K} P_k \\ & & \downarrow f \\ A & \xrightarrow[\pi]{} & B \end{array} ,$$

where $\pi$ is surjective. Now, for every $l \in K$, there exists a homomorphism $g_l : P_l \longrightarrow A$ such that $\pi g_l = f\iota_l$.

$$\begin{array}{ccc} & & P_l \\ & \overset{g_l}{\swarrow} & \downarrow f\iota_l \\ A & \xrightarrow[\pi]{} & B \end{array}$$

Define

$$g\left((a_k)_{k\in K}\right) := \sum_{k\in K} g_k(a_k),$$

where the last sum is finite. Let us show that $g$ is a homomorphism. For any sequences $(a_k)_{k\in K}, (b_k)_{k\in K} \in \oplus \sum_{k\in K} P_k$,

$$\begin{aligned} g\left((a_k)_{k\in K} - (b_k)_{k\in K}\right) &= g\left((a_k - b_k)_{k\in K}\right) && \text{(addition in direct sum)} \\ &= \sum_{k\in K} g_k(a_k - b_k) && \text{(def. of } g\text{)} \\ &= \sum_{k\in K} (g_k(a_k) - g_k(b_k)) && (g_k \text{ is a homomorphism}) \\ &= \sum_{k\in K} g_k(a_k) - \sum_{k\in K} g_k(b_k) && \text{(addition is commutative)} \\ &= g\left((a_k)_{k\in K}\right) - g\left((b_k)_{k\in K}\right) && \text{(def. of } g\text{)} \end{aligned}$$

and, similarly $g\left(r(a_k)_{k\in K}\right) = rg\left((a_k)_{k\in K}\right)$ if $r \in R$.

Finally,

$$\begin{aligned} (\pi g)\left((a_k)_{k\in K}\right) &= \pi\left(\sum_{k\in K} g_k(a_k)\right) && \text{(def. of } g\text{)} \\ &= \sum_{k\in K} (\pi g_k)(a_k) && (\pi \text{ is a homomorphism}) \\ &= \sum_{k\in K} (f\iota_k)(a_k) && (\pi g_k = f\iota_k) \\ &= f\left(\sum_{k\in K} \iota_k(a_k)\right) && (f \text{ is a homomorphism}) \\ &= f\left((a_k)_{k\in K}\right), && \text{(def. of } \iota_k\text{)} \end{aligned}$$

so $\pi g = f$. □

**Corollary 2.18.** *If $e_k$, $k \in K$, are idempotents in a ring $R$, then the external direct sum $\oplus \sum_{k\in K} Re_k$ is a projective left $R$-module.*

*Proof.* This follows from Proposition 2.15 and Proposition 2.17. □

Among other things we will show in the next theorem that, up to isomorphism, projective modules are direct summands of free modules.

**Theorem 2.19.** *Let $R$ be a ring with identity $1 \neq 0$. The following assertions about a unitary left $R$-module $P$ are equivalent.*

(i) *The module $P$ is projective.*

(ii) *For every short exact sequence*

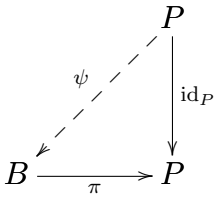
$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} P \longrightarrow 0$$

*there exists a homomorphism $\psi : P \to B$ such that $\pi\psi = \mathrm{id}_P$ and*

$$B = \mathrm{Ker}(\pi) \dotplus \psi(P).$$

(iii) *There exists a free module $F$ and submodules $A, B$ such that $F = A \dotplus B$, where one of the direct summands is isomorphic to the module $P$.*

*Proof.* (i) ⇒ (ii) We apply projectivity of $P$ for homomorphisms $\pi : B \to P$ and $\mathrm{id}_P : P \to P$. Then there exists a homomorphism $\psi : P \to B$ such that $\pi\psi = \mathrm{id}_P$, as needed.




Let us prove the equality $B = \mathrm{Ker}(\pi) \dotplus \psi(P)$. Every element $b \in B$ can be presented as a sum

$$b = (b - \psi(\pi(b))) + \psi(\pi(b)),$$

where $\psi(\pi(b)) \in \psi(P)$ and $b - \psi(\pi(b)) \in \mathrm{Ker}(\pi)$, because

$$\pi(b - \psi(\pi(b))) = \pi(b) - (\pi\psi\pi)(b) = \pi(b) - (\mathrm{id}_P\,\pi)(b) = 0.$$

Hence $B = \mathrm{Ker}(\pi) + \psi(P)$. If $\psi(p) \in \mathrm{Ker}(\pi) \cap \psi(P)$, then

$$p = \mathrm{id}_P(p) = (\pi\psi)(p) = \pi(\psi(p)) = 0,$$

hence also $\psi(p) = 0$, proving that $\mathrm{Ker}(\pi) \cap \psi(P) = 0$. So $B = \mathrm{Ker}(\pi) \dotplus \psi(P)$ follows.

(ii) ⇒ (iii) By Proposition 2.12, there exists a short exact sequence

$$0 \longrightarrow \mathrm{Ker}(\pi) \xrightarrow{\iota} F \xrightarrow{\pi} P \longrightarrow 0\,,$$

where $F$ is a free module and $\iota$ is the inclusion. By (ii), there exists a homomorphism $\psi : P \to F$ such that $\pi\psi = \mathrm{id}_P$ and $F = \mathrm{Ker}(\pi) \dotplus \psi(P)$. The equality $\pi\psi = \mathrm{id}_P$ implies that $\psi$ is injective. Hence the mapping

$$P \longrightarrow \psi(P), \quad p \mapsto \psi(p),$$

is an isomorphism of modules.

(iii) $\Rightarrow$ (i) The free module $F = A \dotplus P \cong A \oplus P = A \times P$ is projective by Proposition 2.14. Now Proposition 2.17 implies that both $A$ and $P$ are projective. □

**Remark 2.20.** If $e$ is an idempotent in a ring $R$, then by Proposition 1.98 we have

$$R = Re \dotplus \mathrm{Ann}(e) \simeq Re \times \mathrm{Ann}(e) = Re \oplus \mathrm{Ann}(e),$$

which means that $Re$ is a direct summand of the free module ${}_RR$. Thus, if $R$ has an identity element, then the projectivity of $Re$ follows from Theorem 2.19.

## 2.4 Projective modules over local rings

In this section, our aim is to prove that, over local rings, finitely generated projective and free modules coincide. Before going to the main result we prove some results about the structure of local rings. Recall that those are rings having a unique maximal left ideal.

**Lemma 2.21.** *If $R$ is a local ring with identity, then $0$ and $1$ are its only idempotents.*

*Proof.* Let $\mathfrak{m}$ be the unique maximal left ideal and suppose that $e \in R$ is an idempotent. For the principal left ideals $Re$ and $R(1-e)$ we have three possibilities.

1) $Re = R$. Then $1 = re$ for some $r \in R$, which implies $e = ree = re = 1$.

2) $R(1-e) = R$. Then $1 = r(1-e)$ for some $r \in R$. Hence

$$e = r(1-e)e = r(e-e^2) = r(e-e) = r0 = 0.$$

3) $Re$ and $R(1-e)$ are proper left ideals. Then they must be contained in $\mathfrak{m}$. Hence also $e, 1-e \in \mathfrak{m}$. Since $\mathfrak{m}$ is closed under addition, $1 = e + (1-e) \in \mathfrak{m}$, yielding $R = \mathfrak{m}$, a contradiction. □

Note that if $R$ is a local ring with identity, then $0 \neq 1$, because otherwise there are no proper ideals and hence no maximal left ideal.

**Proposition 2.22.** *If $R$ is a local ring with identity, then its unique maximal left ideal is also a right ideal.*

*Proof.* Let $\mathfrak{m}$ be the unique maximal left ideal of $R$. We will prove that it is a right ideal. Take any $r \in R$. Suppose that $xr = 1$ for some $x \in \mathfrak{m}$. Then $(rx)^2 = rxrx = r1x = rx$, so $rx$ is an idempotent. Therefore $rx \in \{0, 1\}$ by Lemma 2.21. We have two cases.

a) $rx = 0$. Then $x = 1x = xrx = x0 = 0$, so $1 = xr = 0$, a contradiction.

b) $rx = 1$. Then $1 \in \mathfrak{m}$, because $x \in \mathfrak{m}$ and $\mathfrak{m}$ is a left ideal. Hence $\mathfrak{m} = R$, a contradiction. So

$$(\forall x \in \mathfrak{m})\ xr \neq 1,$$

meaning that $\mathfrak{m}r \subset R$ is a proper left ideal of $R$. Hence $\mathfrak{m}r \subseteq \mathfrak{m}$ for every $r \in R$, proving that $\mathfrak{m}$ is a right ideal. Therefore $\mathfrak{m}$ is also an ideal. □

**Lemma 2.23.** *If $r$ and $s$ are elements in a ring $R$ with identity $1 \neq 0$ such that $rs = 1$ but $sr \neq 1$, then neither $sr$ nor $1 - sr$ is either left or right invertible.*

*Proof.* If $rs = 1$, then

$$sr(1 - sr) = sr - srsr = sr - sr = 0 = (1 - sr)sr.$$

Suppose that $sr$ is left invertible, i.e. $usr = 1$ for some $u \in R$. Then $1-sr = usr(1-sr) = u0 = 0$, contradicting the assumption $sr \neq 1$. Similarly, if $1 - sr$ has a left inverse $v \in R$, then $sr = v(1 - sr)sr = v0 = 0$. But then $1 = 1^2 = rsrs = 0$, a contradiction.

Thus neither $sr$ nor $1 - sr$ can be left invertible. A similar argument shows that they are not right invertible. □

**Lemma 2.24.** *For a local ring $R$ with identity and with the maximal left ideal $\mathfrak{m}$, the following are equivalent:*

1. *$x$ has a left inverse,*
2. *$x$ has a right inverse,*
3. *$x$ is invertible,*
4. *$x \notin \mathfrak{m}$.*

*Proof.* 1 $\implies$ 4. Suppose that $x$ is left invertible: $yx = 1$ for some $y \in R$. If $x \in \mathfrak{m}$, then also $1 \in \mathfrak{m}$, and hence $R = \mathfrak{m}$, a contradiction. Therefore $x \notin \mathfrak{m}$.

4 $\implies$ 1. Suppose that $x \notin \mathfrak{m}$. Consider the left ideal $Rx$. If $Rx$ is proper, then it is contained in a maximal left ideal, i.e. in $\mathfrak{m}$. So $x \in \mathfrak{m}$, a contradiction. Therefore $Rx$ cannot be a proper left ideal. We conclude that $Rx = R$, so the element 1 can be written as $1 = yx$ for some $y \in R$.

2 $\implies$ 4. This is similar to 1 $\implies$ 4, because $\mathfrak{m}$ is a right ideal by Proposition 2.22.

4 $\implies$ 2. Assume that $x \notin \mathfrak{m}$. Since 4 $\iff$ 1, there exists $y \in R$ such that $yx = 1$. If $xy = 1$, then $x$ is right invertible and we are done. Suppose, to the contrary, that $xy \neq 1$. By Lemma 2.23, $xy$ is not left invertible. Using condition 1, we conclude that $xy \in \mathfrak{m}$. From Proposition 2.22 we know that $\mathfrak{m}$ is a right ideal. Hence $x = x \cdot 1 = x(yx) = (xy)x \in \mathfrak{m}$, a contradiction.

1 $\implies$ 3. We have shown that 1 and 2 are equivalent, hence every left invertible element is invertible.

3 $\implies$ 1. This is obvious. □

So $\mathfrak{m}$ is precisely the set of all non-invertible elements of $R$ and every element of $R \setminus \mathfrak{m}$ is invertible.

**Proposition 2.25.** *If $R$ is a local ring $R$ with identity, then its unique maximal left ideal is also the unique maximal right ideal.*

*Proof.* Let $I$ be an arbitrary proper right ideal. If there exists $x \in I$ such that $x \notin \mathfrak{m}$, then by Lemma 2.24 we can conclude that there exists $y \in R$ such that $xy = 1$. Since $x \in I$ and $I$ is a right ideal, we have $xy \in I$ and hence also $1 \in I$, which implies that $I = R$, a contradiction. Therefore, $I \subseteq \mathfrak{m}$. Since $\mathfrak{m}$ is a proper right ideal and every proper right ideal is contained in $\mathfrak{m}$, we conclude that $\mathfrak{m}$ is the greatest proper right ideal and hence the unique maximal right ideal. □

**Proposition 2.26.** *A ring with identity $1 \neq 0$ is local if and only if the sum of any two non-invertible elements of $R$ is non-invertible.*

*Proof.* NECESSITY. If $R$ is local with $\mathfrak{m}$ the unique maximal left ideal of $R$, then from Lemma 2.24 it follows that if $r$ and $s$ are non-invertible elements of $R$, then $r, s \in \mathfrak{m}$ and hence also $r + s \in \mathfrak{m}$, because $\mathfrak{m}$ is closed under addition. Using Lemma 2.24 again, we conclude that $r + s$ is non-invertible as well.
SUFFICIENCY. Let

$$I = \{a \in R \mid a \text{ is not invertible}\} \supseteq \{a \in R \mid a \text{ is not left invertible}\}.$$

By assumption, $I$ is closed under addition. First we claim that every left invertible element $r \in R$ is invertible. Indeed, if $sr = 1$ but $rs \neq 1$, then by Lemma 2.23 $rs \in I$ and $1 - rs \in I$. But then $1 = rs + (1 - rs) \in I$, which is impossible, as 1 is invertible. Thus

$$I = \{a \in R \mid a \text{ is not left invertible}\}.$$

We note that $I$ is a left ideal: if $a \in I$ and $r \in R$, then $ra$ cannot be left invertible, so $ra \in I$. By hypothesis, $I$ is also closed under addition.

The ideal $I$ is proper, because $1 \notin I$. Let $J$ be some proper left ideal. Then no element of $J$ can be left invertible (otherwise $1 \in J$ and $J = R$, a contradiction). We conclude that $J \subseteq I$. Thus $I$ is the unique maximal left ideal and $R$ is a local ring. □

Let ${}_RM$ be a module, $A \subseteq R$ and $B \subseteq M$. We denote

$$AB := \left\{ \sum_{k=1}^{k^*} a_k b_k \middle| k^* \in \mathbb{N}, a_k \in A, b_k \in B \right\}.$$

**Theorem 2.27** (Kaplansky)**.** *Every nonzero finitely generated unitary projective module over a local ring $R$ with identity is free.*

*Proof.* Let $\mathfrak{m}$ be the unique maximal left ideal of $R$. Consider a finitely generated unitary projective module ${}_RP$ with a minimal set of generators $\{x_1, \ldots, x_n\}$. We also consider the free left $R$-module $F = {}_RR^n$. Then the mapping

$$\varphi : R^n \longrightarrow P, \quad (r_1, \ldots, r_n) \mapsto r_1x_1 + \ldots + r_nx_n$$

is a surjective homomorphism of left modules. Denote $K := \mathrm{Ker}(\varphi) \leq R^n$. If we manage to show that $K = 0$, then $\varphi$ will be an isomorphism and ${}_RP$ will be free.

Note that $\mathfrak{m}^n$ is a submodule of ${}_RR^n$, because $\mathfrak{m}$ is a left ideal. We claim that

$$K \subseteq \mathfrak{m}F.$$

Indeed, let $(r_1, \ldots, r_n) \in \mathrm{Ker}(\varphi)$. Then $r_1x_1 + \ldots + r_nx_n = 0$ in $P$. Suppose that some of the elements $r_1, \ldots, r_n$, say $r_1$, is not in $\mathfrak{m}$. Then $r_1$ is invertible by Lemma 2.24, and hence

$$x_1 = -r_1^{-1}r_2x_2 - \ldots - r_1^{-1}r_nx_n$$

in $P$, contradicting the minimality of the generating set $\{x_2, \ldots, x_n\}$. Thus $r_1, \ldots, r_n \in \mathfrak{m}$ and

$$(r_1, \ldots, r_n) = r_1(1, 0, \ldots, 0) + \ldots + r_n(0, \ldots, 0, 1) \in \mathfrak{m}F.$$

Since ${}_RP$ is projective, considering the short exact sequence

$$0 \longrightarrow K \xrightarrow{\iota} F \xrightarrow{\varphi} P \longrightarrow 0\,,$$

and using Theorem 2.19 we know that there exists a homomorphism $\psi : {}_RP \longrightarrow {}_RF$ such that

$$F = \psi(P) \dotplus K.$$

We claim that

$$K = \mathfrak{m}K.$$

Since $\mathfrak{m}K \subseteq K$, we actually need to show that $K \subseteq \mathfrak{m}K$. Observe that

$$K = K \cap \mathfrak{m}F = K \cap \mathfrak{m}(\psi(P) + K) = K \cap (\mathfrak{m}\psi(P) + \mathfrak{m}K).$$

Now $K \cap \psi(P) = 0$ (because $F = \psi(P) \dotplus K$) and $\mathfrak{m}\psi(P) \subseteq \psi(P)$, hence $K \cap \mathfrak{m}\psi(P) = 0$. If now $k \in K$, then $k \in K \cap (\mathfrak{m}\psi(P) + \mathfrak{m}K)$, so $k = x + y$, where $x \in \mathfrak{m}\psi(P)$ and $y \in \mathfrak{m}K \subseteq K$ ($K$ is a left $R$-module). So $x = k - y \in K \cap \mathfrak{m}\psi(P) = 0$, hence $x = 0$ and $k = 0 + y = y \in \mathfrak{m}K$. We have shown that $K \subseteq \mathfrak{m}K$, as needed.

The mapping

$$f : F = \psi(P) \dotplus K \longrightarrow K, \;\; \psi(p) + k \mapsto k$$

is clearly a surjective module homomorphism with the kernel $\psi(P)$. The Homomorphism Theorem gives an isomorphism $K \simeq F/\psi(P)$. Since ${}_RF$ is finitely generated and unitary, also ${}_RK$ is a unitary finitely generated module. So $K = \mathfrak{m}K$ implies $K = 0$ by Nakayama's Lemma (Theorem 1.71). Thus $\varphi$ is an isomorphism and ${}_RP$ is free. □

# Chapter 3

# Radicals of rings

## 3.1 Definition of a radical

**Definition 3.1.** A mapping $\tau$ from the class of all rings to the class of all rings is called a **radical** if

**Rad1.** $\tau(R)$ is an ideal in a ring $R$;

**Rad2.** $\tau(\tau(R)) = \tau(R)$;

**Rad3.** if $f : R \longrightarrow\!\!\!\!\!\rightarrow R'$ is a surjective homomorphism of rings, then $f(\tau(R)) \subseteq \tau(R')$;

**Rad4.** $\tau(R/\tau(R)) = 0$.

The ideal $\tau(R)$ is called the **radical** of a ring $R$.

There exist several different radicals for rings. In the next sections we will consider some of them.

## 3.2 Jacobson radical

Earlier we defined the Jacobson radical for rings with identity as the intersection of all maximal right ideals. In this section we will show how to construct Jacobson radical for arbitrary rings in a series of lemmas, and then we prove that, for rings with identity, the two notions coincide.

On a ring $R$ we define a new operation $\circ$ by

$$a \circ b := a + b + ab.$$

We call it "a new multiplication".

**Lemma 3.2.** $(R, \circ)$ *is a monoid with identity element* $0$.

*Proof.* For every $a, b, c \in R$,

$$\begin{aligned}(a \circ b) \circ c &= (a + b + ab) \circ c = a + b + ab + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc = a + b + c + ab + ac + bc + abc\end{aligned}$$

and, similarly, $a \circ (b \circ c) = a + b + c + ab + ac + bc + abc$. Also, for every $a \in R$,

$$a \circ 0 = a + 0 + a0 = a = 0 + a + 0a = 0 \circ a.$$

□

**Definition 3.3.** An element $a \in R$ is called **quasiregular** if it is invertible in the monoid $(R, \circ)$, that is,

$$a \circ b = 0 = b \circ a$$

for some $b \in R$.

**Definition 3.4.** A right ideal of $R$ is called **quasiregular** if all its elements are quasiregular.

In particular, $\{0\}$ is a quasiregular right ideal.

Let $J(R)$ be the sum of all quasiregular right ideals of $R$. Then $J(R)$ is a right ideal of $R$. We will prove that the mapping

$$R \mapsto J(R)$$

is a radical. This radical is called the **Jacobson radical**.

It turns out that a right ideal is quasiregular whenever each of its elements has a right inverse element with respect to $\circ$.

**Lemma 3.5.** *Let $I \subseteq R$ be a right ideal such that*

$$(\forall a \in I)(\exists x \in R)\ a \circ x = 0.$$

*Then $I$ is quasiregular.*

*Proof.* Let $a \in I$. Then there exists $x \in R$ such that $a \circ x = 0$. It suffices to prove that $x \circ a = 0$. From $a + x + ax = 0$ we obtain $x = -a - ax$. Since $a \in I$ and $I$ is a right ideal, also $x \in I$. Therefore $x \circ y = 0$ for some $y \in R$. Thus

$$y = 0 \circ y = (a \circ x) \circ y = a \circ (x \circ y) = a \circ 0 = a$$

and $x \circ a = 0$. □

**Lemma 3.6.** *If $x, y, z \in R$ and $xy \circ z = 0$, then there exists $u \in R$ such that $yx \circ u = 0$.*

*Proof.* Let $xy \circ z = 0$. Putting $u := -yx - yzx$ we have

$$\begin{aligned}yx \circ u &= yx + u + yxu \\ &= yx - yx - yzx - yxyx - yxyzx \\ &= -y(z + xy + xyz)x \\ &= -y(xy \circ z)x \\ &= (-y) \cdot 0 \cdot x \\ &= 0.\end{aligned}$$

□

**Lemma 3.7.** *If $I$ and $J$ are quasiregular right ideals of $R$, then $I + J$ is a quasiregular right ideal.*

*Proof.* An arbitrary element of $I + J$ has form $a + b$, where $a \in I$ and $b \in J$. By quasiregularity of $J$, there exists $y \in R$ such that $b \circ y = 0$. Since $a + ay \in I$ and $I$ is quasiregular, there exists $z \in R$ such that $(a + ay) \circ z = 0$. Now

$$\begin{aligned}(a+b)\circ(y\circ z) &= ((a+b)\circ y)\circ z\\ &= (a+b+y+ay+by)\circ z\\ &= a+b+y+ay+by+z+az+bz+yz+ayz+byz\\ &= (b+y+by)+(a+ay+z+az+ayz)+(b+y+by)z\\ &= b\circ y+(a+ay)\circ z+(b\circ y)z\\ &= 0+0+0z=0.\end{aligned}$$

By Lemma 3.5, $I + J$ is quasiregular. □

**Lemma 3.8.** *$J(R)$ is a quasiregular right ideal.*

*Proof.* Every element $a$ of $J(R)$ is a finite sum of elements belonging to some quasiregular right ideals $I_1, \ldots, I_n$. The sum $I_1 + \ldots + I_n$ is a quasiregular right ideal by Lemma 3.7, hence $a$ is a quasiregular element. □

**Lemma 3.9.** *$J(R)$ is an ideal.*

*Proof.* We know that $J(R)$ is a right ideal. So it remains to prove that $ra \in J(R)$ for every $r \in R$ and $a \in J(R)$. In other words, we need to prove the inclusion $rJ(R) \subseteq J(R)$.

Clearly $rJ(R)$ is a right ideal. We will show that it is quasiregular. This will suffice, because each quasiregular right ideal is contained in $J(R)$.

Let $ra \in rJ(R)$, where $a \in J(R)$. As $ar \in J(R)$ and $J(R)$ is quasiregular, we can find $z \in R$ such that $ar \circ z = 0$. By Lemma 3.6, there exists $u \in R$ such that $ra \circ u = 0$. Hence $u$ is a right inverse element of $ra$ in the monoid $(R, \circ)$. Now $rJ(R)$ is quasiregular by Lemma 3.5. □

**Lemma 3.10.** *$J(J(R)) = J(R)$.*

*Proof.* Note that $J(R)$, being an ideal of $R$, is also a subring of $R$. Hence we can consider its Jacobson radical $J(J(R))$.

Let $a \in J(R)$. Due to Lemma 3.8 there exists $a' \in R$ such that $a \circ a' = 0 = a' \circ a$. Then $a + a' + aa' = 0$, which implies $a' = -a - aa' \in J(R)$, because $J(R)$ is a right ideal. Thus all elements of the ring $J(R)$ are quasiregular. This means that $J(R)$ itself is one of the quasiregular right ideals of $J(R)$. We conclude that $J(J(R)) = J(R)$. □

**Lemma 3.11.** *If $f : R \longrightarrow R'$ is a surjective homomorphism of rings, then $f(J(R)) \subseteq J(R')$.*

*Proof.* We will prove that if $I$ is a quasiregular right ideal, then $f(I)$ is also a quasiregular right ideal. Since $J(R)$ is a quasiregular right ideal by Lemma 3.8, it follows that $f(J(R))$ is also a quasiregular right ideal and hence $f(J(R)) \subseteq J(R')$ by the definition of $J(R')$.

Let $I$ be quasiregular. Surjectivity of $f$ implies easily that $f(I)$ is a right ideal. Let now $b \in f(I)$. Then there exists $a \in I$ such that $f(a) = b$. Since $I$ is quasiregular, there exists $a' \in R$ such that $a + a' + aa' = a \circ a' = 0$. As $f$ is a ring homomorphism, we have $f(a) + f(a') + f(a)f(a') = 0$. Hence $b \circ f(a') = 0$. By Lemma 3.5, $f(I)$ is a quasiregular right ideal. □

**Lemma 3.12.** *Let $f : R \longrightarrow R'$ be a homomorphism of rings. If $J$ is an ideal in $R'$, then*

$$I := f^{-1}(J) = \{r \in R \mid f(r) \in J\}$$

*is an ideal in $R$.*

*Proof.* Clearly, $0_R \in I$. If $r, r' \in I$ and $s \in R$, then

$$\begin{aligned} f(r - r') &= f(r) - f(r') \in J, \\ f(rs) &= f(r)f(s) \in J, \\ f(sr) &= f(s)f(r) \in J, \end{aligned}$$

because $J$ is an ideal. Hence $r - r', rs, sr \in I$. □

**Lemma 3.13.** $J(R/J(R)) = 0$.

*Proof.* Denote $J := J(R/J(R))$. By Lemma 3.9, this is an ideal in the quotient ring $R/J(R)$. Let

$$\pi : R \longrightarrow R/J(R), \quad r \mapsto r + J(R)$$

be the natural projection and put

$$I := \pi^{-1}(J) = \{r \in R \mid \pi(r) \in J\}.$$

By Lemma 3.12, $I$ is an ideal in $R$.

We will use Lemma 3.5 to show that $I$ is a quasiregular right ideal. Let $a \in I$ be an arbitrary element. Then $\pi(a) \in J$. Using the fact that $J$ is quasiregular, we can find $u \in J$ such that $\pi(a) \circ u = 0$. Since $J \subseteq R/J(R)$, there exists $x \in R$ such that $u = x + J(R) = \pi(x)$. Now

$$0 = \pi(a) \circ \pi(x) = \pi(a) + \pi(x) + \pi(a)\pi(x) = \pi(a + x + ax) = \pi(a \circ x).$$

The equality $\pi(a \circ x) = 0$ means in fact that $a \circ x + J(R) = \pi(a \circ x) = J(R)$. This implies $a \circ x \in J(R)$. Since $J(R)$ is quasiregular, there exists an element $y \in J(R)$ such that $(a \circ x) \circ y = 0$. Then also $a \circ (x \circ y) = 0$, which means that $x \circ y$ is a right inverse of $a$ with respect to $\circ$. Thus $I$ is quasiregular by Lemma 3.5. It follows that $I \subseteq J(R)$ and hence

$$J = \pi(I) = \{\pi(a) \mid a \in I\} = \{a + J(R) \mid a \in I\} = \{J(R) \mid a \in I\} = \{J(R)\},$$

where the coset $J(R)$ is the zero element of the quotient ring $R/J(R)$. □

**Theorem 3.14.** *Let $R$ be a ring with identity element $1 \neq 0$. Then its Jacobson radical is equal to the intersection of all maximal right ideals of $R$.*

*Proof.* Note that $\{0\}$ is a proper right ideal of $R$. By the analogue of Proposition 1.48 for right ideals, it is contained in a maximal right ideal of $R$. Therefore there exists at least one maximal right ideal in $R$. Let $I$ be the intersection of all maximal right ideals of $R$. We will prove that $I = J(R)$.

First we show that $J(R) \subseteq I$. Suppose to the contrary that $J(R) \not\subseteq I$. Then there exist a maximal right ideal $M$ such that $J(R) \not\subseteq M$. Consider the right ideal $J(R) + M$. Since $M \subset J(R) + M$, we must have $J(R) + M = R$ due to maximality of $M$. Hence there exist $x \in J(R)$ and $y \in M$ such that $1 = x + y$. Since $J(R)$ is quasiregular, there exists an element $z \in R$ such that $0 = (-x) \circ z = -x + z - xz$. We conclude that

$$x = z - xz = (1 - x)z = yz \in M,$$

because $M$ is a right ideal. Therefore $1 = x+y \in M$, so $R = M$, contradicting maximality of $M$.

Finally, we show that $I \subseteq J(R)$. For this we show that $I$ is quasiregular using Lemma 3.5. Let $i \in I$. The set $(1+i)R$ is a right ideal of $R$. We will prove that it equals $R$. Suppose to the contrary that $(1 + i)R \neq R$. By the analogue of Proposition 1.48 for right ideals, there exists a maximal right ideal $M$ such that $(1 + i)R \subseteq M$. Then $1 + i \in M$. Since $I \subseteq M$ (by the definition of $I$), also $1 = (1 + i) - i \in M$, again contradicting maximality of $M$. Hence $(1 + i)R = R$. Therefore $1 = (1 + i)r$ for some $r \in R$. This implies

$$0 = r + ir - 1 = i + r - 1 + ir - i = i \circ (r - 1).$$

We have found a right inverse for $i$ with respect to $\circ$. By Lemma 3.5, $I$ is a quasiregular right ideal. □

**Definition 3.15.** A ring $R$ is called **semiprimitive** or **Jacobson semisimple** if $J(R) = 0$.

**Example 3.16.** The ring $\mathbb{Z}$ is semiprimitive.

## 3.3 Nilradical

Recall that an ideal $I$ of a ring $R$ is called a **nil ideal** if all elements of $I$ are nilpotent.

**Lemma 3.17.** *The sum of nil ideals of a ring is a nil ideal.*

*Proof.* First we consider the sum of two nil ideals $I$ and $J$. Let $x = a + b \in I + J$, where $a \in I$ and $b \in J$. Then there exists $n \in \mathbb{N}$ such that $a^n = 0$. Hence

$$x^n = (a + b) \dots (a + b) = a^n + c = 0 + c = c,$$

where $c$ is a sum of products, each ofwhich contains $b$ as a factor. Since $J$ is a two-sided ideal, $c \in J$. Therefore $c^m = 0$ for some $m \in \mathbb{N}$. We conclude that $x^{nm} = c^m = 0$. Hence $I + J$ is a nil ideal.

If now $I_k$, $k \in K$, are nil ideals, then an element $x \in \sum_{k\in K} I_k$ has form $x = a_{k_1} + \dots + a_{k_n}$, where $k_1, \dots, k_n \in K$ and $a_{k_1} \in I_{k_1}, \dots, a_{k_n} \in I_{k_n}$. Using the above argument we see that $x^m = 0$ for some $m \in \mathbb{N}$. □

For a ring $R$, define the **nil radical** of $R$ as

$$\mathsf{N}(R) := \text{ the sum of all nil ideals of } R.$$

Note that in general $\mathsf{N}(R)$ does not contain all nilpotent elements of $R$. This happens, however, for commutative rings.

**Theorem 3.18.** *The mapping $R \mapsto \mathsf{N}(R)$ is a radical.*

*Proof.* We will verify the conditions of Definition 3.1.

Rad1. The sum of ideals is an ideal, so $\mathsf{N}(R)$ is an ideal of $R$.

Rad2. By Lemma 3.17, $\mathsf{N}(R)$ is a nil ideal. Hence $\mathsf{N}(\mathsf{N}(R)) = \mathsf{N}(R)$.

Rad3. Let $f : R \longrightarrow\!\!\!\!\!\rightarrow R'$ be a surjective homomorphism of rings. To prove the inclusion

$$f(\mathsf{N}(R)) \subseteq \mathsf{N}(R'),$$

it suffices to show that $f(I)$ is a nil ideal whenever $I$ is a nil ideal.

Let $I$ be a nil ideal and let $f(a) \in f(I)$. Then $a^n = 0$ for some $n \in \mathbb{N}$. Hence $f(a)^n = f(a^n) = f(0) = 0$. We conclude that $f(I)$ is a nil ideal.

Rad4. Let $J := \mathsf{N}(R/\mathsf{N}(R))$. Then $J$ is an ideal in the quotient ring $R/\mathsf{N}(R)$. Put

$$I := \pi^{-1}(J) = \{r \in R \mid \pi(r) \in J\},$$

where $\pi : R \longrightarrow\!\!\!\!\!\rightarrow R/\mathsf{N}(R)$ is the natural projection. By Lemma 3.12, $I$ is an ideal in $R$. We will prove that $I$ is a nil ideal.

Take $r \in I$. Then $\pi(r) = r + \mathsf{N}(R) \in J$. Since $J$ is a nil ideal, there exists $n \in \mathbb{N}$ such that

$$\mathsf{N}(R) = (r + \mathsf{N}(R))^n = r^n + \mathsf{N}(R).$$

Hence $r^n \in \mathsf{N}(R)$ and we can find $m \in \mathbb{N}$ such that $r^{nm} = (r^n)^m = 0$. Thus $I$ is a nil ideal and $I \subseteq \mathsf{N}(R)$. Therefore

$$J = \pi(I) = \{\pi(a) \mid a \in I\} = \{a + \mathsf{N}(R) \mid a \in I\} = \{\mathsf{N}(R) \mid a \in I\} = \{\mathsf{N}(R)\},$$

as needed. □

The nilradical of a commutative ring has a simpler description.

**Theorem 3.19.** *If $R$ is a commutative ring, then*

$$\mathsf{N}(R) = \{r \in R \mid r \textit{ is nilpotent}\}$$

*and the quotient ring $R/\mathsf{N}(R)$ has no nonzero nilpotent elements.*

*Proof.* 1) We denote

$$A := \{r \in R \mid r \text{ is nilpotent}\}$$

and prove that $A$ is an ideal of $R$. Then every nil ideal $I$ of $R$ is contained in $A$ and therefore $\mathsf{N}(R) \subseteq A$. But $A$ itself is also a nil ideal, so $A \subseteq N(R)$, yielding $A = N(R)$, as desired.

Let $a, b \in A$ and $r \in R$. Then $a^m = 0$ and $b^n = 0$, where $m, n \in \mathbb{N}$. Using commutativity we see that

$$(ar)^m = a^m r^m = 0 \cdot r^m = 0,$$
$$(-a)^m = \pm a^m = 0.$$

Hence $ar, -a \in A$. Also,

$$(a+b)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} a^i b^{m+n-1-i},$$

where $\binom{m+n-1}{i}$ is the usual binomial coefficient. We observe the following.

If $i \geq m$, then $a^i = 0$.

If $i < m$, then $m + n - 1 - i = n + (m - i - 1) \geq n$, hence $b^{m+n-1-i} = 0$.

Thus all summands are zeroes and $(a+b)^{m+n-1} = 0$, proving that $a + b \in A$. We have shown that $A$ is an ideal.

2) Suppose that $r + \mathsf{N}(R)$ is a nilpotent element of the quotient ring $R/\mathsf{N}(R)$. Then there exists $n \in \mathbb{N}$ such that

$$\mathsf{N}(R) = (r + \mathsf{N}(R))^n = r^n + \mathsf{N}(R).$$

Hence $r^n \in \mathsf{N}(R)$ and there exists $m \in \mathbb{N}$ such that $0 = (r^n)^m = r^{nm}$. We see that $r \in \mathsf{N}(R)$, so $r + \mathsf{N}(R) = \mathsf{N}(R)$, which is the zero element of $R/\mathsf{N}(R)$. □

Next we consider prime ideals in commutative rings. For this we need the following result about principal ideals.

**Lemma 3.20.** *If $R$ is a commutative ring, then*

$$(a)(b) = (ab)$$

*for every $a, b \in R$.*

*Proof.* From Proposition 1.54 it follows that

$$(a) = \mathbb{Z}a + Ra + aR + RaR = \mathbb{Z}a + Ra.$$

If $x \in (a)(b)$, then $x = x_1y_1 + \ldots + x_ny_n$ for some $x_1, \ldots, x_n \in (a) = \mathbb{Z}a + Ra$ and $y_1, \ldots, y_n \in (b) = \mathbb{Z}b + Rb$. Hence, for every $i \in \{1, \ldots, n\}$,

$$x_i = u_i a + r_i a \quad \text{and} \quad y_i = v_i a + s_i a,$$

where $u_i, v_i \in \mathbb{Z}$ and $r_i, s_i \in R$. Now

$$\begin{aligned} x_i y_i &= (u_i a + r_i a)(v_i a + s_i a) = (u_i v_i)ab + (u_i s_i)ab + (v_i r_i)ab + (r_i s_i)ab \\ &= (u_i v_i)ab + (u_i s_i + v_i r_i + r_i s_i)ab \in \mathbb{Z}ab + Rab = (ab). \end{aligned}$$

Therefore $x \in (ab)$. We have shown that $(a)(b) \subseteq (ab)$. Conversely,

$$ab = (1 \cdot a + 0 \cdot a)(1 \cdot b + 0 \cdot b) \in (a)(b),$$

hence $(ab) \subseteq (a)(b)$. □

**Proposition 3.21.** *A proper ideal $P$ of a commutative ring $R$ is prime if and only if*

$$(\forall a, b \in R)(ab \in P \implies (a \in P \text{ or } b \in P)).$$

*Proof.* NECESSITY. Let $P$ be a prime ideal of $R$ and let $ab \in P$, $a, b \in R$. By Lemma 3.20,

$$(a)(b) = (ab) \subseteq P,$$

which implies $(a) \subseteq P$ or $(b) \subseteq P$. Hence $a \in P$ or $b \in P$.
SUFFICIENCY. Assume that the implication in the formulation of this lemma holds. Let $AB \subseteq P$ for some ideals $A, B$ in $R$. Suppose that $A \not\subseteq P$. Then there exists $a \in A \setminus P$. For every $b \in B$, $ab \in AB \subseteq P$, hence we must have $b \in P$. Thus $B \subseteq P$. □

**Theorem 3.22.** *Let $R$ be a commutative ring with identity $1 \neq 0$ and $I \trianglelefteq R$. Then $I$ is a prime ideal if and only if the quotient ring $R/I$ is an integral domain.*

*Proof.* NECESSITY. Clearly, $R/I$ is a commutative ring with identity. We need to prove that it does not have zero divisors. Indeed, for every $a, b \in R$,

$$\begin{aligned}
(a+I)(b+I) = I &\implies ab + I = I && \text{(multiplication in } R/I) \\
&\implies ab \in I && \text{(equality of cosets)} \\
&\implies a \in I \text{ or } b \in I && (I \text{ is prime}) \\
&\implies a + I = I \text{ or } b + I = I. && \text{(equality of cosets)}
\end{aligned}$$

SUFFICIENCY. Assume that $R/I$ is an integral domain. Let $a, b \in R$ be such that $ab \in I$. Then

$$\begin{aligned}
ab \in I &\implies ab + I = I && \text{(equality of cosets)} \\
&\implies (a+I)(b+I) = I && \text{(multiplication in } R/I) \\
&\implies a + I = I \text{ or } b + I = I && (R/I \text{ has no zero divisors}) \\
&\implies a \in I \text{ or } b \in I. && \text{(equality of cosets)}
\end{aligned}$$

□

**Theorem 3.23.** *The nilradical of a commutative ring with identity $1 \neq 0$ is the intersection of all prime ideals of the ring.*

*Proof.* Let $R$ be a commutative ring and put

$$J := \text{ the intersection of all prime ideals of } R.$$

We wish to show that $N(R) = J$.

First we prove $N(R) \subseteq J$. Let $P$ be any prime ideal of $R$. Take an arbitrary $a \in N(R)$. Then there exists $n \in \mathbb{N}$ such that $a^n = 0 \in P$. Since $aa^{n-1} \in P$, either $a \in P$ or $a^{n-1} \in P$. By a simple induction we see that $a \in P$. Thus $N(R) \subseteq P$ for every prime ideal $P$. Consequently, $N(R) \subseteq J$.

Now we show that $J \subseteq N(R)$. Suppose to the contrary that there is an element $a \in J \setminus N(R)$, so $a$ is not nilpotent. Put

$$\Sigma := \{I \lhd R \mid (\forall n \in \mathbb{N})\ a^n \notin I\}$$

and consider it as a poset with respect to inclusion. Since $a$ is not nilpotent, $\{0\} \in \Sigma$, so $\Sigma$ is a nonempty poset. Suppose $X \subseteq \Sigma$ is a nonempty chain. Then

$$A := \bigcup_{I \in X} I$$

is an upper bound of $X$. Note that $A \in \Sigma$, because $a^n \in A$ would imply that $a^n \in I$ for some $I \in X$, which cannot happen. The rest can be shown precisely as in the proof of Proposition 1.48. Applying Zorn's lemma we conclude that $\Sigma$ has a maximal element $P$. We will prove that $P$ is a prime ideal.

Let $b, c \in R$ and $bc \in P$. Suppose to the contrary that $b, c \notin P$. Then

$$P \subset P + bR \trianglelefteq R \quad \text{and} \quad P \subset P + cR \trianglelefteq R.$$

Since $P$ is a maximal element of the poset $\Sigma$, we conclude that $P + bR, P + cR \notin \Sigma$. Hence there exist $m, n \in \mathbb{N}$ such that $a^m \in P + bR$ and $a^n \in P + cR$, which implies

$$a^{m+n} = a^m a^n \in P + bcR \trianglelefteq R.$$

So $P + bcR \notin \Sigma$. But $bc \in P$, so $P + bcR = P \in \Sigma$, a contradiction. Thus $b \in P$ or $c \in P$, and $P$ is a prime ideal.

In particular, $a \notin P$ (because $P \in \Sigma$), so $a \notin J$ (because $J$ is the intersection of prime ideals), a contradiction. Hence $J \subseteq N(R)$.

The proof is complete. □

**Corollary 3.24.** *If $R$ is a commutative ring with identity $1 \neq 0$, then*

$$N(R) \subseteq J(R).$$

*Proof.* This holds because every maximal ideal is a prime ideal by Proposition 1.106. □

**Exercise 3.25.** Find the nilradical of the ring $\mathbb{Z}_{12}$.

## 3.4 More on Jacobson radicals

The next result helps to decide whether an element of a ring belongs to the Jacobson radical or not.

**Theorem 3.26.** *Let $R$ be a ring with identity element $1 \neq 0$ and let $a \in R$. The following are equivalent:*

1. *$a \in J(R)$;*
2. *for all $b \in R$, $1 - ab$ is right invertible in $R$;*

*3. for all $b \in R$, $1 - ba$ is left invertible in $R$.*

*Proof.* 1. $\implies$ 2. Suppose that there exists $b \in R$ such that $1 - ab$ is not right invertible. Then $(1 - ab)R$ is a proper right ideal of $R$ which is contained in some maximal right ideal $M$ by Proposition 1.48. In particular, $1 - ab \in M$.

If $a \in J(R)$, then $a \in M$, because $J(R)$ is the intersection of all maximal right ideals. Hence

$$1 = (1 - ab) + ab \in M,$$

which gives a contradiction $R = M$. Thus $a \notin J(R)$.

2. $\implies$ 1. Suppose that $a \notin J(R)$. Then there exists a maximal right ideal $M$ such that $a \notin M$. Now

$$M \subset M + aR \trianglelefteq_r R.$$

By maximality of $M$, $M + aR = R$. In particular, $1 = m + ar$ for some $m \in M$ and $r \in R$. So $1 - ar = m \in M$. If $1 - ar$ is right invertible, then $R = M$. But $R \neq M$, so $1 - ar$ is not right invertible.

The proof of 1 $\iff$ 3 is analogous. □

The next result characterizes local rings in terms of its Jacobson radical.

**Proposition 3.27.** *For a ring $R$ with identity element $1 \neq 0$, the following are equivalent:*

*1. $R$ is a local ring;*

*2. the set of all non-invertible elements of $R$ is closed under addition;*

*3. the set of all elements of $R$ without right inverses is closed under addition;*

*4. $J(R) = \{x \in R \mid xR \neq R\}$;*

*5. $R/J(R)$ is a division ring;*

*6. $J(R) = \{x \in R \mid x$ is not invertible$\}$;*

*7. if $x \in R$, then either $x$ or $1 - x$ is invertible.*

*Proof.* Recall that in a ring with identity, $J(R)$ is the intersection of all maximal right ideals.

1. $\iff$ 2. This is proved in Proposition 2.26.

1. $\implies$ 3. Let $R$ be a local ring. Then it has the unique maximal right ideal, which must be $J(R)$. Let $x, y \in R$ be elements without right inverses. Then $xR, yR$ are proper right ideals, which must be contained in the maximal right ideal $J(R)$. Therefore $x, y \in J(R)$, yielding $x + y \in J(R)$, because $J(R)$ is closed under addition. Now $x + y$ cannot be right invertible, because $J(R)$ is a proper right ideal.

3. $\implies$ 4. Assume that 3 holds. Since $J(R)$ is a proper ideal,

$$J(R) \subseteq \{x \in R \mid xR \neq R\}.$$

Let us prove the converse. Assume that $x \in R$ and $xR \neq R$. Then, for every $r \in R$, $xr$ does not have a right inverse and

$$1 = xr + (1 - xr).$$

Now condition 3 implies that $1 - xr$ must have a right inverse. Thus $x \in J(R)$ by Theorem 3.26.

4. $\Longrightarrow$ 5. Assume that 4 holds. Since $1 \notin J(R)$, $1 + J(R) \neq J(R)$. In other words: the identity element of the quotient ring $R/J(R)$ is different from the zero element of $R/J(R)$. We show that every nonzero element of $R/J(R)$ has a right inverse. Indeed, for $a \in R$,

$$\begin{aligned} a + J(R) \text{ is nonzero} &\iff a + J(R) \neq J(R) \\ &\iff a \notin J(R) \\ &\iff aR = R \\ &\iff (\exists b \in R)\ ab = 1 \\ &\Longrightarrow (a + J(R))(b + J(R)) = 1 + J(R) \\ &\Longrightarrow a + J(R) \text{ is invertible in } R/J(R). \end{aligned}$$

Then also every nonzero element in $R/J(R)$ has a two-sided inverse, which means that $R/J(R)$ is a division ring.

5. $\Longrightarrow$ 1. If $R/J(R)$ is a division ring, then $J(R)$ is a maximal right ideal of $R$ by Theoprem 1.63. Now, if $J$ is any other maximal right ideal, then $J(R) \subseteq J \subset R$ implies $J(R) = J$, so $J(R)$ is the only maximal right ideal. It follows that $R$ is a local ring.

2. $\Longrightarrow$ 7. If we suppose that $x$ and $1 - x$ are non-invertible elements, then $1 = x + (1 - x)$ is non-invertible, a contradiction. Hence either $x$ or $1 - x$ must be invertible.

7. $\Longrightarrow$ 6. Assume 7. Suppose $x \in R$ is non-invertible. We have two possibilities.

1) $x$ does not have a left inverse. Then

$$\begin{aligned} (\forall r \in R)\ rx \text{ is not left invertible} &\Longrightarrow (\forall r \in R)\ rx \text{ is not invertible} \\ &\Longrightarrow (\forall r \in R)\ 1 - rx \text{ is invertible} \\ &\Longrightarrow x \in J(R). \qquad \text{(Theorem 3.26)} \end{aligned}$$

2) $x$ does not have a right inverse. Then

$$\begin{aligned} (\forall r \in R)\ xr \text{ is not right invertible} &\Longrightarrow (\forall r \in R)\ xr \text{ is not invertible} \\ &\Longrightarrow (\forall r \in R)\ 1 - xr \text{ is invertible} \\ &\Longrightarrow x \in J(R). \qquad \text{(Theorem 3.26)} \end{aligned}$$

Thus

$$\{x \in R \mid x \text{ is not invertible}\} \subseteq J(R).$$

Conversely, if $a \in J(R)$, then it cannot be invertible, because otherwise $J(R) = R$, a contradiction.

6. $\Longrightarrow$ 2. This holds because $J(R)$ is an ideal. $\square$

## 3.5 Subdirect products

Subdirect products is a general construction that can be used for universal algebras of any type. We consider it for rings.

**Definition 3.28.** Let $\{R_k \mid k \in K\}$ be a family of rings and consider the direct product

$$R = \prod_{k\in K} R_k = \{(r_k)_{k\in K} \mid r_k \in R_k \text{ for every } k \in K\}$$

with the componentwise operations. A ring $S$ is called a **subdirect product** of this family if there is an injective ring homomorphism

$$\iota : S \longrightarrow R$$

such that $\pi_k\iota : S \longrightarrow R_k$ is surjective for every $k \in K$, where $\pi_k : R \longrightarrow R_k, (r_l)_{l\in K} \mapsto r_k$, is the $k$th projection.

Roughly saying, subdirect products are "close" to direct products.

It is clear that if $S' \simeq S$, then also the ring $S'$ is a subdirect product of the family $\{R_k \mid k \in K\}$.

**Proposition 3.29.** *Let $R$ be a ring, let $\{I_k \mid k \in K\}$ be a family of ideals of $R$, and let*

$$I := \bigcap_{k\in K} I_k.$$

*Then $I \trianglelefteq R$ and $R/I$ is a subdirect product of the family $\{R/I_k \mid k \in K\}$.*

*Proof.* Consider the mapping

$$\iota : R/I \longrightarrow \prod_{k\in K} R/I_k, \quad r + I \mapsto (r + I_k)_{k\in K}.$$

It is well defined and injective, because

$$\begin{aligned} r + I = r' + I &\iff r - r' \in I \iff (\forall k \in K)\ r - r' \in I_k \\ &\iff (\forall k \in K)\ r + I_k = r' + I_k \\ &\iff (r + I_k)_{k\in K} = (r' + I_k)_{k\in K} \\ &\iff \iota(r + I) = \iota(r' + I) \end{aligned}$$

for every $r, r' \in R$. Straightforward calculations show that $\iota$ is a ring homomorphism. The composite

$$R/I \xrightarrow{\ \iota\ } \prod_{l\in K} R/I_l \xrightarrow{\ \rho_k\ } R/I_k,$$

where $\rho_k$ is the $k$th projection, is surjective for every $k \in K$, because

$$r + I_k = \rho_k((r + I_l)_{l\in K}) = (\rho_k\iota)(r + I)$$

for every $r \in R$. Thus $R/I$ is a subdirect product of the family $\{R/I_k \mid k \in K\}$. □

**Corollary 3.30.** *If $R$ is a commutative ring with identity $1 \neq 0$, then $R/N(R)$ is a subdirect product of integral domains. In particular, if $N(R) = 0$, then $R$ is a subdirect product of integral domains.*

*Proof.* Let $\{I_k \mid k \in I\}$ be the family of all prime ideals of $R$. By Theorem 3.23,

$$N(R) = \bigcap_{k \in K} I_k.$$

Proposition 3.29 implies that $R/N(R)$ is a subdirect product of the family $\{R/I_k \mid k \in K\}$, where each member is an integral domain by Theorem 3.22. □

**Corollary 3.31.** *If $R$ is a commutative ring with identity $1 \neq 0$, then $R/J(R)$ is a subdirect product of fields.*

*Proof.* Let $\{I_k \mid k \in I\}$ be the family of all maximal ideals of $R$. Then

$$J(R) = \bigcap_{k \in K} I_k.$$

Proposition 3.29 implies that $R/J(R)$ is a subdirect product of the family $\{R/I_k \mid k \in K\}$, where each member is a field by Theorem 1.63. □

# Chapter 4

# Semisimple modules and rings

## 4.1 Semisimple modules

**Definition 4.1.** A left module $M$ over a ring $R$ is called

- **simple** if $M \neq 0$ and $M$ has no submodules other than $\{0\}$ and $M$;
- **semisimple** if it is an internal direct sum of simple submodules.

**Remark 4.2.** By convention, the sum of the empty family of submodules of a module is the zero submodule. Thus every one-element left $R$-module is left semisimple.

**Example 4.3.** Every simple module is semisimple, but the converse is not true. For example, $\mathbb{Z}_6$ as a left $\mathbb{Z}$-module is not simple, because it has a nontrivial submodule $\{\overline{0}, \overline{3}\}$, but it is semisimple, because

$$\mathbb{Z}_6 = \{\overline{0}, \overline{3}\} \dot{+} \{\overline{0}, \overline{2}, \overline{4}\},$$

where the direct summands are simple modules.

**Example 4.4.** Consider a matrix ring $R = \mathrm{Mat}_m(D)$, where $D$ is a division ring. The set $M = \mathrm{Mat}_{mn}(D)$ is a left $R$-module with respect to usual matrix operations. Denote by $M^k$, $k \in \{1, \ldots, n\}$, the subset of $M$ consisting of all matrices that have zeroes outside the $k$th column. It can be shown that

- $M^k$ is a submodule of $M$;
- $M^k$ is simple;
- $M = M^1 \dot{+} M^2 \dot{+} \ldots \dot{+} M^n$.

Thus $M$ is a left semisimple $R$-module.

Our aim is to prove some alternative descriptions of semisimple modules. For this we will need some lemmas.

**Lemma 4.5.** *If $L$ is a maximal left ideal of a ring $R$, then $R/L$ is a simple left $R$-module.*

*Proof.* Suppose that $\{L\} \neq B \subseteq R/L$ is a submodule of the quotient module $R/L$. The set

$$\{r \in R \mid r + L \in B\} \subseteq R$$

is a left ideal of $R$. It contains $L$, but is strictly bigger, because there exists $r_0 + L \in B$ such that $r_0 + L \neq L$, so $r_0 \notin L$. By maximality of $L$, $\{r \in R \mid r + L \in B\} = R$, which means that $R/L = B$. We have shown that $R/L$ is simple. □

**Lemma 4.6.** *If $f : M \longrightarrow N$ and $g : N \longrightarrow M$ are homomorphisms of left $R$-modules such that $fg = id_N$, then $g(N)$ is a direct summand of the module $M$.*

*Proof.* We have a short exact sequence

$$0 \longrightarrow N \xrightarrow{g} M \xrightarrow{\pi} M/g(N) \longrightarrow 0,$$

where $g$ is a left invertible homomorphism. By Theorem 2.5, $g(N)$ is a direct summand of $M$. □

**Definition 4.7.** A homomorphism $f : M \longrightarrow N$ of left $R$-modules is called a **split epimorphism** if it is right invertible, that is, $fg = id_N$ for some homomorphism $g : N \longrightarrow M$. Note that in that case $f$ is surjective and $g$ is injective. We say that an epimorphism **splits** if it is a split epimorphism.

There are several equivalent conditions to semisimplicity.

**Theorem 4.8.** *For a unitary left module $M$ over a ring $R$ with identity $1 \neq 0$, the following are equivalent.*

1. *$M$ is semisimple.*
2. *$M$ is a sum of a family of simple submodules.*
3. *Every epimorphism $M \longrightarrow L$ of left $R$-modules splits.*
4. *Every submodule of $M$ is a direct summand of $M$.*

*Proof.* It is easy to see that all the statements are valid for a one-element module $M = \{0\}$. So from now on we will assume that $M \neq \{0\}$.

2. $\implies$ 1. Assume that $M = \sum_{k \in K} M_k$, where $M_k$, $k \in K$, are simple submodules of $M$. Consider the set

$$P = \{J \subseteq K \mid \sum_{j \in J} M_j \text{ is a direct sum}\}$$

as a poset with respect to inclusion. It certainly contains all singletons $\{k\}$, $k \in K$, so $P$ is nonempty. It can be shown that $P$ satisfies the assumption of Zorn's lemma. Hence $P$ contains a maximal element $J_0$. If $J_0 = K$, then we are done.

If $J_0 \subset K$, then we denote

$$M' := \sum_{j \in J_0} M_j.$$

If $k \in K \setminus J_0$, then $M_k \cap M'$ is a submodule of $M_k$, so simplicity of $M_k$ implies

$$M_k \cap M' = 0 \quad \text{or} \quad M_k \cap M' = M_k.$$

If $M_k \cap M' = 0$, then the sum $M' + M_k$ is a direct sum, which contradicts the maximality of $J_0$. Hence

$$\begin{aligned}(\forall k \in K \setminus J_0)\ M_k \cap M' = M_k &\implies (\forall k \in K \setminus J_0)\ M_k \subseteq M' \\ &\implies (\forall k \in K)\ M_k \subseteq M' \\ &\implies M = \sum_{k \in K} M_k \subseteq M' \\ &\implies M = M'.\end{aligned}$$

Since $M'$ is a direct sum of simple submodules, we are done.

1. $\implies$ 4. Assume that

$$M = \dot{\sum_{k \in K}} M_k,$$

where each $M_k$ is a simple submodule of $M$. Let $N$ be any submodule of $M$. Using Zorn's lemma again, we can find a maximal subset $J_0 \subseteq K$ such that the sum

$$M' = N + \sum_{j \in J_0} M_j$$

is a direct sum. As above, if $M_k \cap M' = 0$, where $k \in K \setminus J_0$, then

$$M' + M_k = N + \sum_{j \in J_0} M_j + M_k$$

is a direct sum, a contradiction. Thus $M_k \subseteq M'$, hence $M \subseteq M'$, and we conclude that $M = M'$.

3. $\implies$ 4. Let $N$ be a submodule of $M$ and $\iota : N \longrightarrow M$ the inclusion mapping. Then the sequence

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0,$$

where $\pi$ is the natural projection, is exact. By assumption, there exists a homomorphism $\psi : M/N \longrightarrow M$ such that $\pi\psi = id_{M/N}$. By Theorem 2.5, $\mathrm{Im}(\iota) = N$ is a direct summand of $M$.

4. $\implies$ 3. Consider an epimorphism $\pi : M \longrightarrow L$ of left $R$-modules. Then the sequence

$$0 \longrightarrow \mathrm{Ker}(\pi) \xrightarrow{\iota} M \xrightarrow{\pi} L \longrightarrow 0,$$

where $\iota$ is the inclusion, is exact. By assumption, $\mathrm{Ker}(\pi)$ is a direct summand of $M$, so

$$M = \mathrm{Ker}(\pi) \dotplus H = \mathrm{Im}(\iota) \dotplus H$$

for some submodule $H$ of $M$. By Theorem 2.5, there exists a homomorphism $\psi : L \longrightarrow M$ such that $\pi\psi = id_L$.

3. and 4. $\implies$ 2. First we prove that *if $M$ satisfies condition 4, then every submodule $N \leq M$ also satisfies 4.* Let $T$ be a submodule of $N$. Then it is also a submodule of $M$. By assumption, there exists $N' \leq M$ such that

$$M = T \dotplus N'.$$

We prove that

$$(T + N') \cap N = T + (N' \cap N).$$

If $t + n' = n \in (T + N') \cap N$, where $t \in T \subseteq N$, $n' \in N'$ and $n \in N$, then $n' = n - t \in N$, so $t + n' \in T + (N' \cap N)$. Conversely, if $t + x \in T + (N' \cap N)$, where $t \in T \subseteq N$ and $x \in N' \cap N$, then $t + x \in T + N'$ and $t + x \in N$.

Now

$$N = M \cap N = (T + N') \cap N = T + (N' \cap N)$$

and

$$T \cap (N' \cap N) \subseteq T \cap N' = 0.$$

We have shown that $N = T \dotplus (N' \cap N)$, thus $N$ satisfies condition 4.

Next we prove that 3 and 4 together imply that $M$ has at least one simple submodule. Choose an element $0 \neq m \in M$ and consider the homomorphism

$$g : R \longrightarrow M, \quad r \mapsto rm$$

of left $R$-modules. Then $\operatorname{Ker}(g)$ is a left ideal of $R$. Since $1 \cdot m = m \neq 0$ (because ${}_RM$ is unitary), we have $1 \notin \operatorname{Ker}(g)$, so $\operatorname{Ker}(g)$ is a proper left ideal. By the left-sided version of Proposition 1.48, $\operatorname{Ker}(g)$ is contained in a maximal left ideal $L$ of $R$. Due to The Homomorphism Theorem,

$$R/\operatorname{Ker}(g) \simeq \operatorname{Im}(g) = Rm,$$

which is a submodule of $M$. As we have seen above, $R/\operatorname{Ker}(g)$ also satisfies condition 4, and hence condition 3. Consequently, the epimorphism

$$R/\operatorname{Ker}(g) \longrightarrow R/L, \quad r + \operatorname{Ker}(g) \mapsto r + L,$$

splits. By Lemma 4.6, the module $R/\operatorname{Ker}(g)$ has a direct summand, say $B$, which is isomorphic to the module $R/L$. Since $R/\operatorname{Ker}(g)$ is isomorphic to a submodule $Rm$ of $M$, we see that $M$ has a submodule isomorphic to $R/L$, which is a simple left $R$-module due to Lemma 4.5.

Finally, let $N$ be the sum of all simple submodules of $M$. It is a submodule of $M$ (which is called the **socle** of $M$). By condition 4,

$$M = N \dotplus M'$$

for some submodule $M'$ of $M$. Suppose that $M' \neq 0$. Again using our earlier observation, we can say that $M'$ satisfies conditions 3 and 4, and hence contains a simple submodule $P$. Since $P \neq 0$, there exists $0 \neq p_0 \in P$. If $p_0 \in N$, then $p_0 \in N \cap M' = 0$, a contradiction. Thus $p_0 \in P \setminus N$. The last contradicts the definition of $N$. We conclude that $M' = 0$, so $M = N$. The proof is complete. $\square$

In the proof of implication 1 $\implies$ 4 of Theorem 4.8 we have shown the following.

**Corollary 4.9.** *Let $R$ be a ring with identity $1 \neq 0$. If $N$ is a submodule of a unitary semisimple module ${}_RM = \sum_{k\in K} M_k$, where $M_k$, $k \in K$, are simple submodules of $M$, then there exists a subset $J_0 \subseteq K$ such that*

$$M = N \dot{+} \sum_{j\in J_0} M_j.$$

In the proof of the last implication in Theorem 4.8 we have also verified the following fact.

**Corollary 4.10.** *Every submodule of a unitary semisimple module over a ring with identity $1 \neq 0$ is left semisimple.*

**Corollary 4.11.** *Every epimorphic image of a unitary semisimple module over a ring with identity $1 \neq 0$ is left semisimple.*

*Proof.* Let $M$ be unitary semisimple module and let $f : M \longrightarrow N$ be an epimorphism. We will prove that $N$ is semisimple. Take an arbitrary epimorphism $g : N \longrightarrow L$. Then also $gf : M \longrightarrow L$ is an epimorphism. By Theorem 4.8(3), there exists a homomorphism $\pi : L \longrightarrow M$ such that $gf\psi = id_L$. But then also $g$ is a split epimorphism. Using Theorem 4.8(3) again, we conclude that $N$ is semisimple. □

**Proposition 4.12.** *Any external direct sum of left semisimple modules over a ring $R$ with identity $1 \neq 0$ is left semisimple.*

*Proof.* Let $M = \oplus \sum_{k\in K} M_k$, where each $M_k$ is a semisimple left $R$-module. By Theorem 1.88, for each $k \in K$, there exists a submodule $M'_k \leq M$ such that $M'_k \simeq M_k$ and $M = \dot{\sum}_{k\in K} M'_k$. Then also each $M'_k$ is semisimple, hence it can be written as

$$M'_k = \dot{\sum_{h\in H_k}} M_{hk},$$

where each $M_{hk}$ is a simple submodule of $M'_k$. Consequently,

$$M = \sum_{k\in K} M'_k = \sum_{k\in K} \sum_{h\in H_k} M_{hk}$$

is a sum of simple submodules of $M$. Now $M$ satisfies condition 2 in Theorem 4.8, so it is left semisimple. □

**Corollary 4.13.** *Every finite direct product of unitary left semisimple modules over a ring with identity $1 \neq 0$ is left semisimple.*

*Proof.* Finite direct product is an external direct sum, so the previous proposition applies. □

## 4.2 Left semisimple rings

**Definition 4.14.** A ring $R$ is called **left semisimple** if it is semisimple as a left module over itself. Since the simple submodules of the module ${}_RR$ are the minimal left ideals of $R$, we can say that $R$ is left semisimple if it is an internal direct sum of a family of its minimal left ideals.

If $R$ has an identity element, then the module ${}_RR$ is unitary. We have the following result.

**Theorem 4.15.** *For a ring $R$ with identity $1 \neq 0$, the following are equivalent.*

1. *$R$ is left semisimple.*
2. *$R$ is a sum of a family of minimal left ideals.*
3. *Every epimorphism $R \longrightarrow\!\!\!\!\!\rightarrow L$ of left $R$-modules splits.*
4. *Every left ideal of $R$ is a direct summand of $R$.*
5. *$R$ is a finite direct sum of minimal left ideals.*

*Proof.* The equivalence of conditions 1–4 follows directly from Theorem 4.8. The implication $5 \implies 1$ is obvious. We will show that $1 \implies 5$.

Assume that

$$R = \dot{\sum_{k \in K}} I_k,$$

where $I_k$, $k \in K$, are minimal left ideals. Then there exist $n \in \mathbb{N}$, $k_1, \ldots, k_n \in K$ and $i_1 \in I_{k_1}, \ldots, i_n \in I_{k_n}$ such that

$$1 = i_1 + \ldots + i_n.$$

Hence, for every $r \in R$,

$$r = r1 = ri_1 + \ldots + ri_n \in I_{k_1} + \ldots + I_{k_n}.$$

We conclude that $R = I_{k_1} + \ldots + I_{k_n}$ and this sum is a direct sum. □

Left semisimple rings have rather good properties.

**Proposition 4.16.** *If $R$ is a left semisimple ring with identity $1 \neq 0$, then*

1. *every unitary left $R$-module is semisimple;*
2. *every short exact sequence*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0 \tag{4.1}$$

*of unitary left $R$-modules splits, that is, $g$ is a split epimorphism.*

*Proof.* 1. If ${}_RM$ is a unitary left $R$-module, then, by Proposition 2.12, there exists a free left $R$-module $F$ and an epimorphism $f : F \longrightarrow\!\!\!\!\rightarrow M$. By Theorem 2.11, $F$ is isomorphic to an external direct sum $R^{(X)}$ of copies of the module ${}_RR$. Hence $F$ is a semisimple module by Proposition 4.12. Therefore also $M$ is semisimple due to Corollary 4.11.

2. If (4.1) is a short exact sequence, then $g$ is an epimorphism and $M$ is semisimple (because of 1). By Theorem 4.8(3), there exists $\psi : M'' \longrightarrow\!\!\!\!\rightarrow M$ such that $g\psi = id_{M''}$, which means that the sequence splits. □

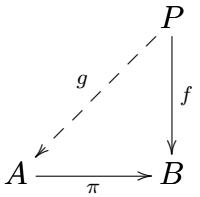
Semisimplicity of a ring can be described in terms of projective modules over it.

**Proposition 4.17.** *A ring $R$ with identity $1 \neq 0$ is left semisimple if and only if every unitary left $R$-module is projective.*

*Proof.* NECESSITY. Assume that $R$ is left semisimple. For a unitary left $R$-module $P$, consider a homomorphism $f : P \longrightarrow B$ and an epimorphism $\pi : A \longrightarrow\!\!\!\!\rightarrow B$. By Proposition 4.16, the short exact sequence

$$0 \longrightarrow \mathrm{Ker}(\pi) \xrightarrow{\iota} A \xrightarrow{\pi} B \longrightarrow 0$$

splits, so there exists a homomorphism $\psi : B \longrightarrow A$ such that $\pi\psi = id_B$. Now $g := \psi f : P \longrightarrow A$ is a homomorphism such that $\pi g = \pi\psi f = f$. Thus $P$ is projective.




SUFFICIENCY. Assume that all unitary left $R$-modules are projective. Consider an epimorphism $f : R \longrightarrow\!\!\!\!\rightarrow M$ of left $R$-modules. Since ${}_RM$ is projective, this epimorphism splits by Theorem 2.19. Hence ${}_RR$ is semisimple by Theorem 4.15. □

## 4.3 Semiprime and left artinian rings

**Definition 4.18.** A ring $R$ is called **semiprime** if, for every ideal $I$,

$$I \neq 0 \implies I^2 \neq 0.$$

**Definition 4.19.** A ring $R$ is called **left artinian** if it satisfies the descending chain condition on left ideals, i.e., if

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$$

is a descending chain of left ideals, then there exists $n \in \mathbb{N}$ such that

$$I_n = I_{n+1} = I_{n+2} = \dots.$$

Clearly, every finite ring is left artinian.

**Proposition 4.20.** *Every nonzero left ideal of a semiprime, left artinian ring $R$ with identity $1 \neq 0$ contains a nonzero idempotent.*

*Proof.* Let $I \neq 0$ be a left ideal of $R$. If $I$ is not a minimal left ideal, then it contains properly a left ideal $I_1 \neq 0$. If $I_1$ is not a minimal left ideal, then there exists a left ideal $I_2 \neq 0$ such that

$$I \supset I_1 \supset I_2.$$

Since $R$ is left artinian, we cannot continue this process infinitely, so after a finite number of steps we will get a minimal left ideal $J$ such that $I \supseteq J \neq 0$. If $j$ is a nonzero element of $J$, then $0 \neq j = j1 \in JR$. Since $0 \neq JR$ is a two-sided ideal and $R$ is semiprime, we have

$$0 \neq (JR)^2 = JRJR \subseteq JJR,$$

which implies $J^2 \neq 0$. Using Proposition 1.107, we can find a nonzero idempotent $e \in J \subseteq I$. □

**Definition 4.21.** Let $E(R)$ denote the set of all idempotents of $R$. Defining

$$e \leq f \iff ef = e = fe$$

for all $e, f \in E(R)$ we obtain a partial order relation on $E(R)$, called the **natural partial order of idempotents**.

The next result gives some properties of $\leq$.

**Lemma 4.22.** *For idempotents $e, f$ of a ring $R$ with identity $1 \neq 0$, the following are equivalent:*

1. $e \leq f$,
2. $eRe \subseteq fRf$,
3. $1 - f \leq 1 - e$.

*Proof.* 1. $\implies$ 2. If $e \leq f$, then $ere = feref \in fRf$ for every $r \in R$.

2. $\implies$ 1. If $eRe \subseteq fRf$, then $e = frf$ for some $r \in R$, and hence

$$ef = frff = frf = e = fe.$$

1. $\iff$ 3. It is easy to see that $1 - e$ and $1 - f$ are idempotents. Let $e \leq f$. Then $ef = e = fe$. Hence

$$(1 - e)(1 - f) = 1 - e - f + ef = 1 - f,$$
$$(1 - f)(1 - e) = 1 - f - e + fe = 1 - f,$$

which means that $1 - f \leq 1 - e$.

Assuming $1 - f \leq 1 - e$, we have $e = 1 - (1 - e) \leq 1 - (1 - f) = f$. □

**Lemma 4.23.** *Let $R$ be a left artinian ring with identity $1 \neq 0$. Then every nonempty subset of $E(R)$ contains a maximal element with respect to the natural partial order.*

*Proof.* Let $\emptyset \neq A \subseteq E(R)$. Take $e_1 \in A$. If $e_1$ is not a maximal element, then there exists $e_2 \in A$ such that $e_2 > e_1$. Hence $e_1e_2 = e_1 = e_2e_1$. By Lemma 4.22, we have $1 - e_2 \leq 1 - e_1$, in particular $1 - e_2 = (1 - e_2)(1 - e_1)$, so

$$R(1 - e_1) \supseteq R(1 - e_2).$$

Suppose that we have an equality here. Then $1 - e_1 = r(1 - e_2)$ for some $r \in R$. Hence

$$1 - e_2 = (1 - e_1)(1 - e_2) = r(1 - e_2)^2 = r(1 - e_2) = 1 - e_1,$$

which gives $e_1 = e_2$, a contradiction. Thus

$$R(1 - e_1) \supset R(1 - e_2).$$

If $A$ does not have a maximal element, then there is an infinite sequence

$$e_1 < e_2 < e_3 < \dots$$

of elements of $A$, which produces an infinite descending sequence

$$R(1 - e_1) \supset R(1 - e_2) \supset R(1 - e_3) \supset \dots$$

of left ideals, a contradiction. Thus $A$ must have a maximal element. □

## 4.4 Artin-Molien-Wedderburn theorem

The aim of this section is to prove a famous theorem stating that every left semisimple ring with identity is a finite direct product of matrix rings over division rings. Three mathematicians have contributed to this theorem: Artin[1], Molien[2] and Wedderburn[3].

The following lemma will be needed.

**Lemma 4.24.** *Let $I$ and $J$ be ideals in a ring $R$ with identity $1 \neq 0$, and let $R = I \dotplus J$. Then*

1. *$I$ and $J$ are rings with identity,*
2. *every left ideal of $I$ is a left ideal of $R$,*
3. *every ideal of $I$ is an ideal of $R$.*

*Proof.* 1. We will prove the claim for $I$. Since $R = I + J$, $1 = i + j$ for some $i \in I$ and $j \in J$. For every $a \in I$, $a = ai + aj$. Hence

$$aj = a - ai \in I \cap J = 0,$$

so $ai = a$. Similarly $a = ia$, and we see that $i$ is the identity element for $I$.

[1] Emil Artin (1898–1962) — an Austrian mathematician
[2] Theodor Molien (1861–1941) — a mathematician of Baltic German origin
[3] Joseph Wedderburn (1882–1948) — a Scottish mathematician

2. Let $A$ be a left ideal of $I$. Then it is closed under subtraction. Let $a \in A$ and $r \in R$. Then $r = i + j$, where $i \in I$ and $j \in J$. Now $ra = ia + ja$, where $ja \in J \cap I = 0$, so

$$ra = ia + 0 = ia \in A,$$

because $A$ is a left ideal in $I$.

3. This is similar to 2. □

By $M_n(S)$ we denote the ring of $n \times n$ matrices over a ring $S$. Recall that a ring $R$ is called **simple** if 0 and $R$ are its only ideals.

**Theorem 4.25** (Molien-Wedderburn)**.** *A ring $R$ with identity $1 \neq 0$ is simple and has a minimal left ideal if and only if $R \simeq M_n(D)$ for some $n \in \mathbb{N}$ and some division ring $D$.*

We will not give a proof of this theorem in this course. The full proof is given in the course "Introduction to Algebraic Structures" and it can be found in the book "Algebra II" by Mati Kilp.

**Theorem 4.26** (Artin-Molien-Wedderburn theorem)**.** *Let $R$ be a ring with identity $1 \neq 0$. The following are equivalent.*

1. *$R$ is left semisimple.*
2. *$R$ is semiprime and left artinian.*
3. *There exist $s, n_1, \ldots, n_s \in \mathbb{N}$ and division rings $D_1, \ldots, D_s$ such that*

$$R \simeq M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s).$$

*Proof.* 1. $\implies$ 2. First we prove that $R$ is semiprime. Assume that $A$ is an ideal of $R$ such that $A^2 = 0$. Since $R$ is left semisimple, there exists a left ideal $B$ such that $R = A \dotplus B$. Now $1 = a_0 + b_0$ for some $a_0 \in A$ and $b_0 \in B$. Hence, for every $a \in A$,

$$a = aa_0 + ab_0 = 0 + ab_0 = ab_0 \in A \cap B = 0.$$

We see that $A = 0$, so $R$ is semiprime.

Next we show that $R$ is left artinian. Consider a descending chain

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$$

of left ideals of $R$. We must prove that it stabilizes. Since $R$ is left semisimple, Theorem 4.15(5) implies that

$$R = L_1 \dotplus \ldots \dotplus L_n,$$

where $L_1, \ldots, L_n$ are minimal left ideals.

By Theorem 4.15, $I_1$ is a direct summand of $R$, so $R = I_1 \dotplus A$ for some left ideal $A$. More precisely, by Corollary 4.9, this $A$ must be a direct sum of some $L_i$'s, so let $A = L_1 \dotplus \ldots \dotplus L_{k_1}$, $k_1 \leq n$, where we have renumerated $L$'s if necessary. Thus

$$R = I_1 \dotplus (L_1 \dotplus \ldots \dotplus L_{k_1}).$$

Then $I_1 \supseteq I_2$ implies

$$I_2 \cap (L_1 \dot{+} \ldots \dot{+} L_{k_1}) = 0.$$

Suppose that $I_1 \supset I_2$. If $I_2 \dot{+} (L_1 \dot{+} \ldots \dot{+} L_{k_1}) = R = I_1 \dot{+} (L_1 \dot{+} \ldots \dot{+} L_{k_1})$, then, for every $a \in I_1$,

$$\begin{aligned}(\exists b \in I_2)(\exists c \in L_1 \dot{+} \ldots \dot{+} L_{k_1})\ a = b + c &\implies c = a - b \in I_1 \cap (L_1 \dot{+} \ldots \dot{+} L_{k_1}) = 0 \\ &\implies c = 0 \\ &\implies a = b \in I_2,\end{aligned}$$

thus $I_1 = I_2$, a contradiction. Hence

$$I_2 \dot{+} (L_1 \dot{+} \ldots \dot{+} L_{k_1}) \lhd_l R$$

is a proper left ideal of $R$. By Theorem 4.15(5),

$$I_2 \dot{+} (L_1 \dot{+} \ldots \dot{+} L_{k_1}) \dot{+} B = R$$

for some nonzero left ideal $B$ of $R$. This $B$ must be a sum of some left ideals in $\{L_{k_1+1}, \ldots, L_n\}$. After renumerating these left ideals (if necessary), we can assume that $B = L_{k_1+1} \dot{+} \ldots \dot{+} L_{k_2}$, where $k_2 > k_1$. Now

$$R = I_2 \dot{+} (L_1 \dot{+} \ldots \dot{+} L_{k_2}).$$

If $I_2 = 0$, then we are done. Otherwise we repeat the process. Since $k_1 < k_2 < k_3 \leq \ldots \leq n$, after a finite number, say $r$, steps we reach $I_r = 0$.

2. $\implies$ 3. Let $R$ be a semirpime, left artinian ring. Then it contains a minimal left ideal $L$. Define

$$\begin{aligned}I &:= LR \subseteq R, \\ J &:= \mathrm{Ann}^r(I) = \{a \in R \mid Ia = 0\} \subseteq R.\end{aligned}$$

It is easy to see that $I$ is an ideal of $R$. By the dual of Proposition 1.97(3), $J$ is also an ideal of $R$. We claim that $R$ is an internal direct sum of these ideals:

$$R = I \dot{+} J. \tag{4.2}$$

1) We have $I \cap J = 0$, because $R$ is semiprime and

$$(I \cap J)^2 \subseteq IJ = 0 \implies I \cap J = 0.$$

2) We prove that $R = I + J$. The set $I \cap E(R)$ is nonempty, because it contains 0. Since $R$ is left artinian, Lemma 4.23 implies that the subset $I \cap E(R) \subseteq E(R)$ contains a maximal idempotent $e$. Since $1 = e + (1 - e)$, it suffices to prove that $1 - e \in J$. Suppose to the contrary that $1 - e \notin J$. Then $I(1 - e) \neq 0$ and $I(1 - e)$ is a left ideal of $R$. By Proposition 4.20, there exists a nonzero idempotent $f \in I(1 - e) \subseteq I$. Hence $f = i(1 - e)$ for some $i \in I$ and

$$fe = i(1 - e)e = i(e - e^2) = 0.$$

Define

$$g := e + f - ef.$$

Then

$$\begin{aligned} g^2 &= (e+f-ef)(e+f-ef) \\ &= e^2 + ef - e^2f + fe + f^2 - fef - efe - ef^2 + efef \\ &= e + ef - ef + f - ef \\ &= e + f - ef = g, \\ ge &= e^2 + fe - efe = e, \\ eg &= e^2 + ef - e^2f = e. \end{aligned}$$

Thus $e \leq g$. Since $e, f \in I$, also $g \in I$. The maximality of $e$ yields $e = g$, so $f = ef$. Hence $f = f^2 = fef = 0f = 0$, a contradiction. Consequently, $1 - e \in J$.

By Lemma 4.24, $I$ and $J$ are rings with identity, which are both semiprime and left artinian. We will prove that $I$ is a simple ring. Condsider an ideal $0 \neq A \trianglelefteq I$. Suppose that $A \cap L = 0$. Then

$$A^2 \subseteq AI = ALR \subseteq (A \cap L)R = 0,$$

contradicting the fact that $I$ is a semiprime ring. Thus $0 \neq A \cap L \subseteq L$. The minimality of $L$ implies $A \cap L = L$, whence $L \subseteq A$ and $I = LR \subseteq AR \subseteq A$ (the last inclusion comes from Lemma 4.24). Thus $A = I$.

We also note that $L$ is a minimal left ideal of the ring $I$. Indeed, if $B$ is a left ideal of $I$ such that $0 \neq B \subseteq L$, then $B$ is a left ideal of $R$ by Lemma 4.24, so $B = L$ by the minimality of $L$ in $R$.

If $J = 0$, then $R = I$ and the proof is complete due to Theorem 4.25. Otherwise we repeat the argument with $R$ replaced by $J$ to obtain a direct sum

$$R = I \dotplus I_1 \dotplus J_1,$$

where $I_1$ is a simple ring with a minimal left ideal $L_1$. This cannot continue infinitely, because that would give an infinte descending chain of ideals

$$R \supset I_1 + I_2 + \ldots \supset I_2 + I_3 + \ldots.$$

Thus

$$R = I \dotplus I_1 \dotplus \ldots \dotplus I_n$$

for some $n \in \mathbb{N}$, where $I, I_1, \ldots, I_n$ are simple rings, which have a minimal left ideal. Again, we use Theorem 4.25 to get the desired matrix rings.

3. $\Longrightarrow$ 1. Similarly to Example 4.4 we can see that matrix rings over division rings are left semisimple. Similarly to Corollary 4.13 one can show that their finite direct product is left semisimple. □

Matrix rings are left-right symmetric. So an analogous proof will give us the following result.

**Corollary 4.27.** *A ring with identity $1 \neq 0$ is left semisimple if and only if it is right semisimple.*

Since left semisimple and right semisimple rings are the same, one usually speaks about *semisimple rings* without specifying the side.

**Remark 4.28.** Theorem 4.26 in that formulation was first proved by Emil Artin in 1927. He generalized a result of Joseph Wedderburn from 1907 stating that *every finite-dimensional simple algebra over a field $K$ is isomorphic to a matrix ring $M_n(D)$, where $D$ is a finite-dimensional division algebra over $K$ and both $n$ and $D$ are uniquely determined.*

Wedderburn's result generalized a theorem of Theodor Molien, which states (in modern terms) that: *every simple associative algebra over the field $\mathbb{C}$ is isomorphic to the algebra $M_n(\mathbb{C})$ for some $n \in \mathbb{N}$.* This was one of the main results in his doctoral thesis "Über Systeme höherer komplexer Zahlen" which he defended in 1892 at the University of Tartu. Molien worked as a docent of pure mathematics at the University of Tartu from 1885 to 1900, after that he worked as a professor in Tomsk, Russia.

## 4.5 A characterization of regular rings

Recall that a ring $R$ is called regular if, for every $a \in R$, there exists $b \in R$ such that $a = aba$.

**Theorem 4.29.** *For a ring $R$ with identity $1 \neq 0$, the following are equivalent.*

1. *$R$ is regular.*
2. *Every principal left ideal of $R$ is generated by an idempotent.*
3. *Every principal left ideal of $R$ is a direct summand in $R$.*
4. *Every finitely generated left ideal is a direct summand in $R$.*

*Proof.* 1. $\implies$ 2. Let $a \in R$. Then there exists $b \in R$ such that $a = aba$. Clearly $e := ba$ is an idempotent and $Re \subseteq Ra$. But $a = ae$ implies also $Ra \subseteq Re$. Thus $Ra = Re$.

2. $\implies$ 1. Take $a \in R$. Then $Ra = Re$ for some idempotent $e \in R$. In particular, there exists $u, v \in R$ with $e = ua$ and $ve = a$. Now $a = ae = aua$, so $a$ is a regular element.

2. $\iff$ 3. This is shown in Proposition 1.98.

4. $\implies$ 3. This is clear.

1. $\implies$ 4. A finitely generated left ideal $I$ of $R$ has form $I = Ra_1 + \ldots + Ra_n$, where $a_1, \ldots, a_n \in R$. Since we have proved that conditions 1 and 2 are equivalent, for every $i \in \{1, \ldots, n\}$ we can find an idempotent $e_i \in R$ such that $Ra_i = Re_i$. Hence $I = Re_1 + \ldots + Re_n$, where $e_1, \ldots, e_n$ are idempotents. So it suffices to prove that, for any two idempotents $e, f \in R$, the left ideal $Re + Rf$ is generated by an idempotent.

Note that

$$Re + Rf = Re + R(f - fe),$$

because, for every $a, b \in R$,

$$\begin{aligned} ae + bf &= ae + b(f - fe) + bfe = (a + bf)e + b(f - fe), \\ ae + b(f - fe) &= ae + bf - bfe = (a - bf)e + bf. \end{aligned}$$

Since $R$ is regular, there exists $x \in R$ such that

$$f - fe = (f - fe)x(f - fe).$$

Then $g := x(f - fe)$ is an idempotent such that $ge = 0$ and we have equalities

$$Re + Rf = Re + R(f - fe) = Re + Rx(f - fe) = Re + Rg = R(e + g - eg).$$

For the last equality we notice that, for every $a, b, c \in R$,

$$\begin{aligned} ae + bg &= ae + aeg - aeg + bge + bg - bgeg = (ae + bg)(e + g - eg), \\ c(e + g - eg) &= ce + cg - ceg = ce + (c - ce)g. \end{aligned}$$

Also, $e + g - eg$ is an idempotent, because

$$(e + g - eg)(e + g - eg) = e + eg - eg + ge + g - geg - ege - eg + egeg = e + g - eg.$$

□

**Corollary 4.30.** *Every semisimple ring $R$ with identity $1 \neq 0$ is regular.*

*Proof.* Compare Theorem 4.29(3) to Theorem 4.15(4). □

# Chapter 5

# Basics of category theory

## 5.1 The definition of a category

**Definition 5.1. A category** $\mathcal{C}$ consists of the following things:

D1. a class $\mathrm{Ob}(\mathcal{C})$, whose elements are called the **objects** of this category;

D2. for every pair $(A, B)$ of objects there is a set $\mathrm{Mor}_{\mathcal{C}}(A, B)$, whose elements are called **morphisms** from the object $A$ to the object $B$; the class of all morphisms in the category $\mathcal{C}$ is denoted by $\mathrm{Mor}(\mathcal{C})$;

D3. for every triple $(A, B, C)$ of objects there exists a mapping (**composition**)

$$\circ\colon \ \mathrm{Mor}_{\mathcal{C}}(A, B) \times \mathrm{Mor}_{\mathcal{C}}(B, C) \longrightarrow \mathrm{Mor}_{\mathcal{C}}(A, C);$$

the image of a pair $(f, g)$ of morphisms is denoted by $g \circ f$ and called the **composite of** $f$ **and** $g$;

D4. for every object $A$ there exists a morphism $\mathrm{id}_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$, which is called the **identity morphism** of the object $A$.

These data must satisfy the following axioms.

A1. If $(A, B) \neq (A', B')$, then $\mathrm{Mor}_{\mathcal{C}}(A, B) \cap \mathrm{Mor}_{\mathcal{C}}(A', B') = \varnothing$.

A2. *Associativity axiom:* for any morphisms $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$, $g \in \mathrm{Mor}_{\mathcal{C}}(B, C)$, $h \in \mathrm{Mor}_{\mathcal{C}}(C, D)$,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

A3. *Identity axiom:* for any morphisms $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$, $g \in \mathrm{Mor}_{\mathcal{C}}(B, C)$,

$$\mathrm{id}_B \circ f = f \quad \text{and} \quad g \circ \mathrm{id}_B = g.$$

We will introduce some further terminology and notation. Let $\mathcal{C}$ be a category. For a morphism $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ we often use the notation

$$f\colon A \longrightarrow\!\!\!\!\!\rightarrow B;$$

the uniquely determined object $A$ is called the **domain** of the morphism $f$ (notation: $\mathrm{dom}\, f := A$) and the object $B$ is called the **codomain** of the morphism $f$ (notation: $\mathrm{cod}\, f := B$).

**Definition 5.2.** A morphism $f\colon A \longrightarrow B$ is called an **isomorphism** if there exists a morphism $g\colon B \longrightarrow A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. If $f$ is an isomorphism, then the morphism $g$ is unique and it is called the **inverse** of $f$ and denoted by $f^{-1}$. If there exists an isomorphism $f\colon A \longrightarrow B$, then the objects $A$ and $B$ are called **isomorphic** and the notation $A \simeq B$ or $A \cong B$ is used.

**Definition 5.3.** A morphism $f\colon A \longrightarrow B$ is called a **split epimorphism** (a **split monomorphism**), if it is right (left) invertible, i.e. there exists a morphism $g\colon B \longrightarrow A$ such that $f \circ g = \mathrm{id}_B$ ($g \circ f = \mathrm{id}_A$).

Note that a morphism $f$ is an isomorphism if and only if $f$ is both a split epimorphism and a split monomorphism. Indeed, if $g, h\colon B \longrightarrow A$ are such that $f \circ g = \mathrm{id}_B$ and $h \circ f = \mathrm{id}_A$, then

$$g = \mathrm{id}_A \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ \mathrm{id}_B = h.$$

**Example 5.4** (Examples of categories)**.**
1. *The category* $\mathsf{Set}$ *of all sets.* The objects of the category $\mathsf{Set}$ are all sets and the morphisms are the mappings between sets, that is, $\mathrm{Mor}_{\mathsf{Set}}(A, B) = B^A := \{f \mid f\colon A \longrightarrow B\}$, where $A$ and $B$ are sets. The composition is just the usual composition of mappings and the identity morphisms are the identity transformations of sets. The isomorphisms in $\mathsf{Set}$ are the bijective mappings.
2. *The category* $\mathsf{Ab}$ *of abelian groups.* The objects are all abelian groups, the morphisms are the group homomorphisms and the isomorphisms are the bijective group homomorphisms.
3. *The category* ${}_R\mathsf{Mod}$ *of left modules over a ring* $R$. The objects are all left modules over $R$, the morphisms are the homomorphisms of modules and the isomorphisms are the bijective homomorphisms of modules.

**Definition 5.5.** A category $\mathcal{B}$ is called a **subcategory** of a category $\mathcal{A}$ if
1. the class $\mathrm{Ob}(\mathcal{B})$ is a subclass of the class $\mathrm{Ob}(\mathcal{A})$;
2. for every pair $(B, B') \in \mathrm{Ob}(\mathcal{B}) \times \mathrm{Ob}(\mathcal{B})$, $\mathrm{Mor}_{\mathcal{B}}(B, B') \subseteq \mathrm{Mor}_{\mathcal{A}}(B, B')$ such that
   (a) if $f \in \mathrm{Mor}_{\mathcal{B}}(B, B')$ and $g \in \mathrm{Mor}_{\mathcal{B}}(B', B'')$, then $g \circ f \in \mathrm{Mor}_{\mathcal{B}}(B, B'')$, and it is the composite of $g$ and $f$ in $\mathcal{B}$,
   (b) for every $B \in \mathrm{Ob}(\mathcal{B})$, the identity morphism of $B$ in $\mathcal{B}$ is the same as the identity morphism of $B$ in $\mathcal{A}$.

If $\mathcal{B}$ is a subcategory of a category $\mathcal{A}$, then we write $\mathcal{B} \subseteq \mathcal{A}$.

**Definition 5.6.** A subcategory $\mathcal{B}$ of a category $\mathcal{A}$ is called a **full subcategory** if, for any $B, B' \in \mathrm{Ob}(\mathcal{B})$, $\mathcal{B}$ contains all morphisms from $B$ to $B'$ that exist in $\mathcal{A}$, that is,

$$B, B' \in \mathrm{Ob}(\mathcal{B}) \quad \Longrightarrow \quad \mathrm{Mor}_{\mathcal{B}}(B, B') = \mathrm{Mor}_{\mathcal{A}}(B, B').$$

**Example 5.7.** Let $R$ be a ring. Then we can consider the full subcategory ${}_R\mathsf{UMod}$ of ${}_R\mathsf{Mod}$ whose objects are all unitary left $R$-modules.

## 5.2 Mono- and epimorphisms

**Definition 5.8.** A morphism $f\colon A \longrightarrow B$ in a category $\mathcal{A}$ is called

- a **monomorphism** if, for all $g, h \in \mathrm{Mor}_{\mathcal{A}}(C, A)$,
$$f \circ g = f \circ h \implies g = h;$$
- an **epimorphism** if, for all $g, h \in \mathrm{Mor}_{\mathcal{A}}(B, C)$,
$$g \circ f = h \circ f \implies g = h.$$

**Definition 5.9.** A **concrete category** is a category, where

- objects are sets (usually with some structure),
- morphisms are mappings (usually preserving that structure),
- composition is the composition of mappings,
- identity morphisms are identity mappings.

All categories in Example 5.4 are concrete categories.

**Proposition 5.10.** *In a concree category $\mathcal{A}$,*

1. *every split epimorphism (split monomorphism) is surjective (injective);*
2. *every surjective (injective) morphism is an epimorphism (a monomorphism).*

*Proof.* Let $\mathcal{A}$ be a concrete category. We will give a proof for epimorphisms (the reader may think about the case of monomorphisms). Let $f\colon A \longrightarrow A'$ be a split epimorphism, that is, there exists a morphism $g\colon A' \longrightarrow A$ such that $f \circ g = \mathrm{id}_{A'}$. If $a' \in A'$, then
$$a' = \mathrm{id}_{A'}(a') = (f \circ g)(a') = f(g(a')).$$
Hence $g(a') \in A$ is a preimage of $a'$. We have shown that $f$ is surjective.

Now let $f\colon A \longrightarrow A'$ be a surjective morphism in the category $\mathcal{A}$. Assume that $g, h : A' \longrightarrow A''$ are such that $g \circ f = h \circ f$. Let $a' \in A'$. Since $f$ is surjective, there exists $a \in A$ such that $f(a) = a'$. Hence
$$g(a') = g(f(a)) = (g \circ f)(a) = (h \circ f)(a) = h(f(a)) = h(a').$$
Thus $g = h$, and we have proved that $f$ is an epimorphism in $\mathcal{A}$. □

In many concrete categories (including $\mathsf{Set}$), the monomorphisms are precisely the injective morphisms and the epimorphisms are precisely the surjective morphisms. However, there exist examples of categories where this is not true.

**Proposition 5.11.** *Let $R$ be a ring. Epimorphisms in the category ${}_R\mathsf{Mod}$ are precisely the surjective homomorphisms.*

*Proof.* By Proposition 5.10 we know that every surjective homomorphism of $R$-modules is an epimorphism in ${}_R\mathsf{Mod}$.

Conversely, let $f\colon M \longrightarrow M'$ be an epimorphism in ${}_R\mathsf{Mod}$. Consider its cokernel $\operatorname{Coker} f = M'/\operatorname{Im} f$, the zero mapping $\mathbf{0}\colon M' \longrightarrow \operatorname{Coker} f$ and the canonical projection $\kappa\colon M' \twoheadrightarrow \operatorname{Coker} f$. For every $m \in M$,

$$(\kappa \circ f)(m) = \kappa(f(m)) = f(m) + \operatorname{Im} f = \operatorname{Im} f = 0 + \operatorname{Im} f = \mathbf{0}(f(m)) = (\mathbf{0} \circ f)(m).$$

Hence $\kappa \circ f = \mathbf{0} \circ f$, which implies $\kappa = \mathbf{0}$, as $f$ is an epimorphism. But now, for every $m' \in M'$, $m' + \operatorname{Im} f = \kappa(m') = 0 + \operatorname{Im} f = \operatorname{Im} f$, whence $m' \in \operatorname{Im} f$. Thus $\operatorname{Im} f = M'$ and therefore $f$ is surjective. □

Analogously, the following result can be proved.

**Proposition 5.12.** *Let $R$ be a ring. Monomorphisms in the category ${}_R\mathsf{Mod}$ are precisely the injective homomorphisms.*

In the categories of modules or abelian groups, there is one more simple description of monomorphisms.

**Proposition 5.13.** *Let $R$ be a ring, $\mathcal{A} \in \{\mathsf{Mod}_R, {}_R\mathsf{Mod}, \mathsf{Ab}\}$ and let $\mathcal{C} \subseteq \mathcal{A}$ be a full subcategory. A morphism $f \in \operatorname{Mor}_{\mathcal{C}}(A, B)$ is a monomorphism in $\mathcal{C}$ if and only if, for every $u \in \operatorname{Mor}_{\mathcal{C}}(D, A)$,*

$$f \circ u = \mathbf{0} \implies u = \mathbf{0}. \tag{5.1}$$

*Proof.* Necessity. Let $f$ be a monomorphism in $\mathcal{C}$. By the definition of a monomorphism, $f \circ u = \mathbf{0} = f \circ \mathbf{0}$ implies $u = \mathbf{0}$.
Sufficiency. Assume that, for every $u \in \operatorname{Mor}_{\mathcal{C}}(D, A)$, condition (5.1) holds. Let $g, h \in \operatorname{Mor}_{\mathcal{C}}(D, A)$ be such that $f \circ g = f \circ h$. Then

$$f \circ g - f \circ h = \mathbf{0}.$$

Note that, for every $d \in D$,

$$\begin{aligned}(f \circ g - f \circ h)(d) &= f(g(d)) - f(h(d)) = f(g(d) - h(d)) \\ &= f((g - h)(d)) = (f \circ (g - h))(d).\end{aligned}$$

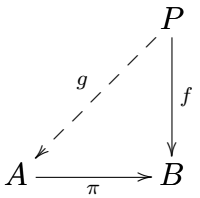
Consequently,

$$f \circ (g - h) = \mathbf{0} \implies g - h = \mathbf{0} \implies g = h.$$

Thus $f$ is a monomorphism in $\mathcal{C}$. □

Using epimorphisms, one can define projective objects.

**Definition 5.14.** An object $P$ of a category $\mathcal{A}$ is called **projective** if for every epimorphism $\pi : A \to B$ and every morphism $f : P \to B$ there exists a morphism $g : P \to A$ such that $f = \pi g$.




Definition 2.13 is a special case of this.

## 5.3 Functors

Now we will consider functors. While a category is a generalization of a monoid, we may think of functors as generalizations of monoid homomorphisms.

**Definition 5.15.** A **functor** from a category $\mathcal{A}$ to a category $\mathcal{B}$ is a mapping which

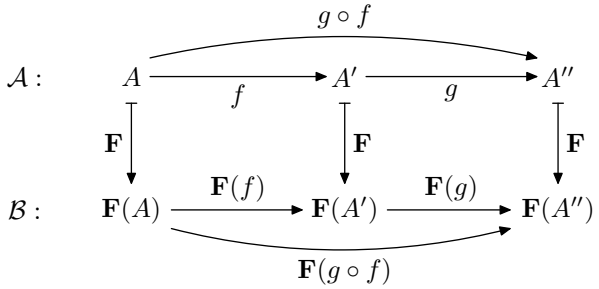
1. maps each object $A \in \mathrm{Ob}(\mathcal{A})$ to an object $\mathbf{F}(A) \in \mathrm{Ob}(\mathcal{B})$;
2. maps each morphism $f \in \mathrm{Mor}_{\mathcal{A}}(A, A')$ to a morphism $\mathbf{F}(f) \in \mathrm{Mor}_{\mathcal{B}}(\mathbf{F}(A), \mathbf{F}(A'))$;

so that

1. for every pair $g, f$ of composable morphisms in $\mathcal{A}$,
$$\mathbf{F}(g \circ f) = \mathbf{F}(g) \circ \mathbf{F}(f);$$
2. for every $A \in \mathrm{Ob}(\mathcal{A})$, $\mathbf{F}(\mathrm{id}_A) = \mathrm{id}_{\mathbf{F}(A)}$.

We write $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$.

The following diagram illustrates the definition of a functor.




**Example 5.16** (Functors)**.**

1. Let $\mathcal{A}$ be a category. The **identity functor** $\mathrm{id}_{\mathcal{A}}\colon \mathcal{A} \longrightarrow \mathcal{A}$ is defined by
$$\mathrm{id}_{\mathcal{A}}(A) := A,$$
$$\mathrm{id}_{\mathcal{A}}(f) := f,$$
where $A \in \mathrm{Ob}(\mathcal{A})$ and $f \in \mathrm{Mor}(\mathcal{A})$.
2. Let $\mathcal{B}$ be a subcategory of a category $\mathcal{A}$. There exists a functor $\mathbf{J}_{\mathcal{B}}\colon \mathcal{B} \longrightarrow \mathcal{A}$, which coincides on the objects and morphisms of $\mathcal{B}$ with the identity functor of $\mathcal{B}$. The functor $\mathbf{J}_{\mathcal{B}}$ is called the **inclusion functor** of the category $\mathcal{B}$ into the category $\mathcal{A}$.

3. Let $\mathcal{A}$ be a category and $C \in \mathrm{Ob}(\mathcal{A})$. There exists a functor $\mathrm{Mor}_{\mathcal{A}}(C, \_)\colon \mathcal{A} \longrightarrow \mathsf{Set}$, which is defined by

$$A \mapsto \mathrm{Mor}_{\mathcal{A}}(C, A),$$
$$f \mapsto (g \mapsto f \circ g),$$

where $A \in \mathrm{Ob}(\mathcal{A})$ and $f \in \mathrm{Mor}(\mathcal{A})$. We use notations

$$\mathrm{Mor}_{\mathcal{A}}(C, \_)(f) =: \mathrm{Mor}_{\mathcal{A}}(C, f) =: f \circ \_.$$

$$\begin{array}{ccccc} A & \longmapsto & \mathrm{Mor}_{\mathcal{A}}(C, A) & \ni & g \\ \downarrow f & & \downarrow \mathrm{Mor}_{\mathcal{A}}(C, f) = f \circ \_ & & \downarrow \\ A' & \longmapsto & \mathrm{Mor}_{\mathcal{A}}(C, A') & \ni & f \circ g \end{array}$$

Let us verify that $\mathrm{Mor}_{\mathcal{A}}(C, \_)$ is indeed a functor. For this, we consider morphisms $f \in \mathrm{Mor}_{\mathcal{A}}(A, A')$ and $g \in \mathrm{Mor}_{\mathcal{A}}(A', A'')$. Note that

$$\begin{aligned} \mathrm{Mor}_{\mathcal{A}}(C, g \circ f)(h) &= (g \circ f) \circ h = g \circ (f \circ h) = \mathrm{Mor}_{\mathcal{A}}(C, g)(f \circ h) \\ &= \mathrm{Mor}_{\mathcal{A}}(C, g)(\mathrm{Mor}_{\mathcal{A}}(C, f)(h)) \\ &= (\mathrm{Mor}_{\mathcal{A}}(C, g) \circ \mathrm{Mor}_{\mathcal{A}}(C, f))(h), \end{aligned}$$

for every $h \in \mathrm{Mor}_{\mathcal{A}}(C, A)$. In addition,

$$\mathrm{Mor}_{\mathcal{A}}(C, \mathrm{id}_A)(k) = \mathrm{id}_A \circ k = k = \mathrm{id}_{\mathrm{Mor}_{\mathcal{A}}(C,A)}(k),$$

for every $k \in \mathrm{Mor}_{\mathcal{A}}(A, A)$. Thus $\mathrm{Mor}_{\mathcal{A}}(C, \_)$ is a functor.
The functor $\mathrm{Mor}_{\mathcal{A}}(C, \_)\colon \mathcal{A} \longrightarrow \mathsf{Set}$ is called a **covariant mor-functor** (or **hom-functor**) induced by the object $C$ of $\mathcal{A}$.

Let $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ and $\mathbf{G}\colon \mathcal{B} \longrightarrow \mathcal{C}$ be functors. We define a new functor $\mathbf{G} \circ \mathbf{F} : \mathcal{A} \longrightarrow \mathcal{C}$ by

$$(\mathbf{G} \circ \mathbf{F})(A) := \mathbf{G}(\mathbf{F}(A)),$$
$$(\mathbf{G} \circ \mathbf{F})(f) := \mathbf{G}(\mathbf{F}(f)),$$

where $A \in \mathrm{Ob}(\mathcal{A})$ and $f \in \mathrm{Mor}(\mathcal{A})$. The functor $\mathbf{G} \circ \mathbf{F}$ is called the **composite** of the functors $\mathbf{F}$ and $\mathbf{G}$. The composition of functors is illustrated by the following figure.

$$\mathcal{A} \xrightarrow{\mathbf{F}} \mathcal{B} \xrightarrow{\mathbf{G}} \mathcal{C}, \qquad \mathcal{A} \xrightarrow{\mathbf{G} \circ \mathbf{F}} \mathcal{C}$$

**Lemma 5.17.** *Every functor preserves isomorphisms, split epimorphisms and split monomorphisms. If $f$ is an isomorphism and $\mathbf{F}$ is a functor, then $\mathbf{F}(f^{-1}) = \mathbf{F}(f)^{-1}$.*

*Proof.* Let $\mathcal{A}, \mathcal{B}$ be categories, $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ a functor and $f \in \mathrm{Mor}_{\mathcal{A}}(A, A')$ a split monomorphism. Then there exists a morphism $g \in \mathrm{Mor}_{\mathcal{A}}(A', A)$ such that $g \circ f = \mathrm{id}_A$. Observe that

$$\mathrm{id}_{\mathbf{F}(A)} = \mathbf{F}(\mathrm{id}_A) = \mathbf{F}(g \circ f) = \mathbf{F}(g) \circ \mathbf{F}(f).$$

We conclude that the morphism $\mathbf{F}(f) \in \mathrm{Mor}_{\mathcal{B}}(\mathbf{F}(A), \mathbf{F}(A'))$ is a split monomorphism.

Analogously, if $f$ is a split epimorphism, then also $\mathbf{F}(f)$ is a split epimorphism. Hence, if $f$ is an isomorphism, then also $\mathbf{F}(f)$ is an isomorphism. Moreover, we see that $\mathbf{F}(f)^{-1} = \mathbf{F}(f^{-1})$. □

Next we define two important types of functors.

**Definition 5.18.** Let $\mathbf{F}\colon \mathcal{A} \to \mathcal{B}$ be a functor. For every pair $A, A' \in \mathrm{Ob}(\mathcal{A})$ of objects we consider the mapping

$$\mathbf{F}_1^{A,A'} : \mathrm{Mor}_{\mathcal{A}}(A, A') \to \mathrm{Mor}_{\mathcal{B}}(\mathbf{F}(A), \mathbf{F}(A')), \quad f \mapsto \mathbf{F}(f).$$

The functor $\mathbf{F}$ is called

- **faithful** if the mapping $\mathbf{F}_1^{A,A'}$ is injective for every $A, A' \in \mathrm{Ob}(\mathcal{A})$;
- **full** if the mapping $\mathbf{F}_1^{A,A'}$ is surjective for every $A, A' \in \mathrm{Ob}(\mathcal{A})$.

Thus, a functor $\mathbf{F}\colon \mathcal{A} \to \mathcal{B}$ is full and faithful if and only if the mapping $\mathbf{F}_1^{A,A'}$ is bijective for every $A, A' \in \mathrm{Ob}(\mathcal{A})$.

**Proposition 5.19.** *A faithful functor $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ reflects monomorphisms and epimorphisms, i.e. if $\mathbf{F}(f)\colon \mathbf{F}(A) \longrightarrow \mathbf{F}(A')$ is a monomorphism (epimorphism), then $f\colon A \longrightarrow A'$ is a monomorphism (epimorphism).*

*Proof.* Let $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ be a faithful functor. We prove the claim for epimorphisms, for the case of monomorphisms, the proof is analogous. Let $\mathbf{F}(f)$ be an epimorphism and $g \circ f = h \circ f$ for some $g, h : A' \longrightarrow A''$. Then

$$g \circ f = h \circ f \Longrightarrow \mathbf{F}(g) \circ \mathbf{F}(f) = \mathbf{F}(h) \circ \mathbf{F}(f) \Longrightarrow \mathbf{F}(g) = \mathbf{F}(h) \Longrightarrow g = h.$$

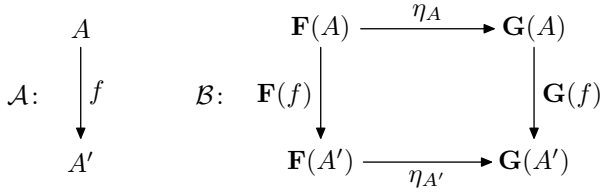
Hence $\mathbf{F}$ reflects epimorphisms. □

## 5.4 Natural transformations

**Definition 5.20.** Let $\mathbf{F}, \mathbf{G}\colon \mathcal{A} \longrightarrow \mathcal{B}$ be two functors from a category $\mathcal{A}$ to a category $\mathcal{B}$. A **natural transformation** $\eta\colon \mathbf{F} \Rightarrow \mathbf{G}$ from the functor $\mathbf{F}$ to the functor $\mathbf{G}$ is a family $(\eta_A\colon \mathbf{F}(A) \longrightarrow \mathbf{G}(A))_{A \in \mathrm{Ob}(\mathcal{A})}$ of morphisms in $\mathcal{B}$, indexed by the objects of $\mathcal{A}$, which satisfies

$$\eta_{A'} \circ \mathbf{F}(f) = \mathbf{G}(f) \circ \eta_A$$

for every morphism $f\colon A \longrightarrow A'$ in $\mathcal{A}$.




**Example 5.21** (Natural identity transformation)**.** Let $\mathcal{A}$ and $\mathcal{B}$ be categories and let $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ be a functor. There exists a natural transformation $\mathrm{id}_{\mathbf{F}}\colon \mathbf{F} \Rightarrow \mathbf{F}$, defined by

$$(\mathrm{id}_{\mathbf{F}})_A := \mathrm{id}_{\mathbf{F}(A)},$$

where $A \in \mathrm{Ob}(\mathcal{A})$. This natural transformation $\mathrm{id}_{\mathbf{F}}$ is called the **natural identity transformation**.

Let $\mathbf{F}, \mathbf{G}, \mathbf{H}\colon \mathcal{A} \longrightarrow \mathcal{B}$ be functors and let $\eta\colon \mathbf{F} \Rightarrow \mathbf{G}$ and $\zeta\colon \mathbf{G} \Rightarrow \mathbf{H}$ be natural transformations. We define a natural transformation $\zeta \circ \eta\colon \mathbf{F} \Rightarrow \mathbf{H}$ by

$$(\zeta \circ \eta)_A := \zeta_A \circ \eta_A,$$

where $A \in \mathrm{Ob}(\mathcal{A})$. Then $\zeta \circ \eta$ is called the **(vertical) composite** of the natural transformations $\eta$ and $\zeta$.

Let $\mathbf{F}, \mathbf{G}\colon \mathcal{A} \longrightarrow \mathcal{B}$ be functors. A natural transformation $\eta\colon \mathbf{F} \Rightarrow \mathbf{G}$ is called a **natural isomorphism** if $\eta_A$ is an isomorphism for every $A \in \mathrm{Ob}(\mathcal{A})$. The functors $\mathbf{F}, \mathbf{G}\colon \mathcal{A} \longrightarrow \mathcal{B}$ are called **isomorphic** (written $\mathbf{F} \cong \mathbf{G}$) if there exists a natural isomorphism $\eta\colon \mathbf{F} \Rightarrow \mathbf{G}$.

It is easy to see that a natural transformation $\eta\colon \mathbf{F} \Rightarrow \mathbf{G}$ is a natural isomorphism if and only if $\eta$ is invertible, that is, there exists (a unique) natural transformation $\eta^{-1}\colon \mathbf{G} \Rightarrow \mathbf{F}$ such that $\eta \circ \eta^{-1} = \mathrm{id}_{\mathbf{G}}$ and $\eta^{-1} \circ \eta = \mathrm{id}_{\mathbf{F}}$.

## 5.5 Equivalence of categories

Let $\mathcal{A}$ and $\mathcal{B}$ be categories. A functor $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ is called an **isomorphism** if there exists a functor $\mathbf{G}\colon \mathcal{B} \longrightarrow \mathcal{A}$ such that $\mathbf{F} \circ \mathbf{G} = \mathrm{id}_{\mathcal{B}}$ and $\mathbf{G} \circ \mathbf{F} = \mathrm{id}_{\mathcal{A}}$. If $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ is an isomorphism of categories, then the categories $\mathcal{A}$ and $\mathcal{B}$ are **isomorphic** and we write $\mathcal{A} \cong \mathcal{B}$.

**Definition 5.22.** Let $\mathcal{A}$ and $\mathcal{B}$ be categories and $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ a functor. The functor $\mathbf{F}$ is called an **equivalence functor** if there exists a functor $\mathbf{G}\colon \mathcal{B} \longrightarrow \mathcal{A}$ and natural isomorphisms $\mathbf{F} \circ \mathbf{G} \Rightarrow \mathrm{id}_{\mathcal{B}}$ and $\mathrm{id}_{\mathcal{A}} \Rightarrow \mathbf{G} \circ \mathbf{F}$.

If $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ is an equivalence functor, then the categories $\mathcal{A}$ and $\mathcal{B}$ are called **equivalent** and the notation $\mathcal{A} \approx \mathcal{B}$ is used. Equivalence functors $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ and $\mathbf{G}\colon \mathcal{B} \longrightarrow \mathcal{A}$ from Definition 5.22 are called **inverse** to each other. It can be shown that if $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ is an equivalence functor, then its inverse functor $\mathbf{G}\colon \mathcal{B} \longrightarrow \mathcal{A}$ is unique up to a natural isomorphism.

The following result can be proved.

**Proposition 5.23.** *The relation $\approx$ is an equivalence relation on the class of all categories.*

A functor $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ is called **dense** if for every object $B \in \mathrm{Ob}(\mathcal{B})$ there exists an object $A \in \mathrm{Ob}(\mathcal{A})$ such that $B \cong \mathbf{F}(A)$.

**Theorem 5.24.** *A functor $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ is an equivalence functor if and only if $\mathbf{F}$ is full, faithful and dense.*

We will not give a proof of this theorem in our course.

**Proposition 5.25.** *An equivalence functor preserves monomorphisms and epimorphisms.*

*Proof.* Let $\mathcal{A}$ and $\mathcal{B}$ be categories and $\mathbf{F}\colon \mathcal{A} \longrightarrow \mathcal{B}$ an equivalence functor. Consider an epimorphism $f \in \mathrm{Mor}_{\mathcal{A}}(A, A')$. Let $g, h \in \mathrm{Mor}_{\mathcal{B}}(\mathbf{F}(A'), B)$ be such that $g \circ \mathbf{F}(f) = h \circ \mathbf{F}(f)$. Since the functor $\mathbf{F}$ is dense by Theorem 5.24, there exists an object $A'' \in \mathrm{Ob}(\mathcal{A})$ and an isomorphism $k : B \longrightarrow F(A'')$. Now $k \circ g, k \circ h$ are morphisms $F(A') \longrightarrow F(A'')$. Since $\mathbf{F}$ is full, there exist $\hat{g}, \hat{h} \in \mathrm{Mor}_{\mathcal{A}}(A', A'')$ such that $\mathbf{F}(\hat{g}) = k \circ g$ and $\mathbf{F}(\hat{h}) = k \circ h$. We have

$$\mathbf{F}(\hat{g} \circ f) = \mathbf{F}(\hat{g}) \circ \mathbf{F}(f) = k \circ g \circ \mathbf{F}(f) = k \circ h \circ \mathbf{F}(f) = \mathbf{F}(\hat{h}) \circ \mathbf{F}(f) = \mathbf{F}(\hat{h} \circ f).$$

Since $\mathbf{F}$ is faithful, $\hat{g} \circ f = \hat{h} \circ f$. As $f$ is an epimorphism, we conclude that $\hat{g} = \hat{h}$. But then $k \circ g = \mathbf{F}(\hat{g}) = \mathbf{F}(\hat{h}) = k \circ h$. Multiplying the equality $k \circ g = k \circ h$ by $k^{-1}$ from the left (recall that $k$ is an isomorphism), we obtain $g = h$. We have shown that $\mathbf{F}(f)$ is an epimorphism.

Analogously one can prove that $\mathbf{F}$ preserves monomorphisms. □

**Exercise 5.26.** Prove that if $\mathcal{A}$ and $\mathcal{B}$ are equivalent categories and all objects in $\mathcal{A}$ are projective, then also all objects in $\mathcal{B}$ are projective.

# Chapter 6

# Tensor product of modules

## 6.1 Definition and construction of the tensor product

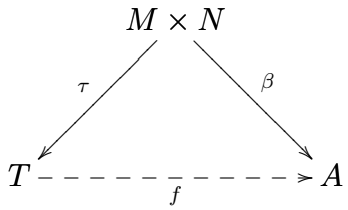
To define tensor product of modules we first need to introduce the notion of an $R$-balanced mapping.

**Definition 6.1.** Let $R$ be a ring, $M_R$ a right $R$-module, ${}_RN$ a left $R$-module and $A$ an abelian group. A mapping $\beta\colon M \times N \longrightarrow A$ is called **$R$-balanced** (or **$R$-tensorial**) if

1. $\forall m_1, m_2 \in M\, \forall n \in N\colon \quad \beta(m_1 + m_2, n) = \beta(m_1, n) + \beta(m_2, n)$;
2. $\forall m \in M\, \forall n_1, n_2 \in N\colon \quad \beta(m, n_1 + n_2) = \beta(m, n_1) + \beta(m, n_2)$;
3. $\forall m \in M\, \forall n \in N\, \forall r \in R\colon \quad \beta(mr, n) = \beta(m, rn)$.

If $\beta$ satisfies condition 1 or 2, then it is called **additive** in the first or in the second argument, respectively.

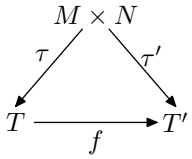
**Definition 6.2.** Let $T$ be an abelian group and $\tau\colon M \times N \longrightarrow T$ an $R$-balanced mapping. The pair $(T, \tau)$ is called a **tensor product** of modules $M_R$ and ${}_RN$ if, for every abelian group $A$ and every $R$-balanced mapping $\beta\colon M \times N \longrightarrow A$, there exists a unique group homomorphism $f\colon T \longrightarrow A$ such that $\beta = f \circ \tau$.

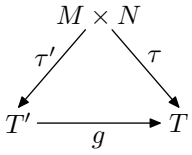



It turns out that the tensor product of two modules is unique up to isomorphism.

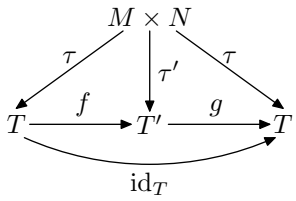
**Proposition 6.3.** *If $(T, \tau)$ and $(T', \tau')$ are tensor products of modules $M_R$ and ${}_RN$, then there exists a group isomorphism $f\colon T \longrightarrow T'$ such that $\tau' = f \circ \tau$.*

*Proof.* Let $(T, \tau)$ and $(T', \tau')$ be tensor products of modules $M_R$ and ${}_RN$. Then there exist unique group homomorphisms $f$ and $g$ such that the diagrams




commute. In the diagram




we have

$$(g \circ f) \circ \tau = g \circ (f \circ \tau) = g \circ \tau' = \tau,$$
$$\mathrm{id}_T \circ \tau = \tau.$$

By uniqueness, $g \circ f = \mathrm{id}_T$. Analogously, $f \circ g = \mathrm{id}_{T'}$. Hence the abelian groups $T$ and $T'$ are isomorphic. □

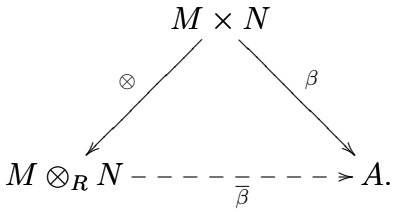
Next we introduce some notation. Let $(T, \tau)$ be the tensor product of $R$-modules $M_R$ and ${}_RN$. We denote

$$M \otimes_R N := T, \qquad \otimes := \tau \colon M \times N \longrightarrow M \otimes_R N, \quad \tau(m,n) =: m \otimes n,$$

for every $m \in M$ and $n \in N$.

With these new notations we can reformulate the definition of the tensor product as a property, which is usually called the *universal property* of tensor product. In what follows, we usually call the abelian group $M \otimes_R N$ the tensor product of $M_R$ and ${}_RN$, without specifically mentioning the mapping $\otimes$.

**The universal property of the tensor product.** For every abelian group $A$ and an $R$-balanced mapping $\beta \colon M \times N \longrightarrow A$ there exists a unique group homomorphism $\overline{\beta} \colon M \otimes_R N \longrightarrow A$ such that the following diagram commutes:




This property is often used to define mappings from a tensor product to an abelian group.

## The construction of the tensor product

Note that, although Proposition 6.3 says that the tensor product is unique, it does not say anything about the existence of the tensor product. In this section we will show that it is always possible to construct the tensor product of two modules over the same ring. Let $R$ be a ring, $M_R$ a right $R$-module and ${}_RN$ a left $R$-module. Consider the set

$$\mathbb{Z}^{(M\times N)} := \{f\colon M\times N \longrightarrow \mathbb{Z} \mid f(m,n)\neq 0 \text{ for finitely many pairs } (m,n)\in M\times N\}.$$

The set $\mathbb{Z}^{(M\times N)}$ is an abelian group with respect to the pointwise addition

$$(f+g)(m,n) := f(m,n)+g(m,n), \quad (m,n)\in M\times N.$$

It is the **free abelian group** on the set $M\times N$. The zero element in this abelian group is the zero mapping

$$\mathbf{0}\colon\ M\times N\longrightarrow\mathbb{Z}, \quad (m,n)\mapsto 0.$$

For every pair $(m,n)\in M\times N$ we consider the mapping $x_{(m,n)}\colon M\times N\longrightarrow\mathbb{Z}$ defined by

$$x_{(m,n)}(m',n') := \begin{cases} 1, & \text{if } (m',n')=(m,n),\\ 0, & \text{if } (m',n')\neq(m,n).\end{cases}$$

Clearly, $x_{(m,n)}\in\mathbb{Z}^{(M\times N)}$ for every $(m,n)\in M\times N$. The set

$$\mathcal{B} := \{x_{(m,n)} \mid (m,n)\in M\times N\}$$

is a basis in the abelian group $\mathbb{Z}^{(M\times N)}$.

For every integer $z$ and every $x_{(m,n)}\in\mathcal{B}$, the element $zx_{(m,n)}$ is defined as in the beginning of subsection 1.2.5. For every basis element $x_{(m,n)}$, the set

$$\mathbb{Z}x_{(m,n)} = \left\{zx_{(m,n)}\middle| z\in\mathbb{Z}\right\}$$

is a subgroup of the abelian group $\mathbb{Z}^{(M\times N)}$. Moreover, $\mathbb{Z}^{(M\times N)}$ is an internal direct sum of these subgroups, that is,

$$\mathbb{Z}^{(M\times N)} = \dot{\sum_{(m,n)\in M\times N}}\mathbb{Z}x_{(m,n)} = \left\{\sum_{k=1}^{k^*} z_k x_{(m_k,n_k)}\middle| k^*\in\mathbb{N}, z_k\in\mathbb{Z}, (m_k,n_k)\in M\times N\right\}. \tag{6.1}$$

Hence the set $\mathbb{Z}^{(M\times N)}$ consists of finite sums, which are *linear combinations* of basis elements. Consider the subgroup $H$ of $\mathbb{Z}^{(M\times N)}$, which is generated by the following elements:

$$\begin{gathered} x_{(m_1+m_2,n)} - x_{(m_1,n)} - x_{(m_2,n)},\\ x_{(m,n_1+n_2)} - x_{(m,n_1)} - x_{(m,n_2)},\\ x_{(mr,n)} - x_{(m,rn)},\end{gathered} \tag{6.2}$$

where $m_1,m_2,m\in M$, $n_1,n_2,n\in N$ and $r\in R$. If $\hat{H}$ is the set of all the elements given in (6.2), then it can be shown that

$$H = \{\pm a_1\pm a_2\pm\ldots\pm a_k \mid k\in\mathbb{N}, a_1,\ldots,a_k\in\hat{H}\}.$$

For every $f \in \mathbb{Z}^{(M\times N)}$, we write

$$[f] := f + H = \{f + g \mid g \in H\}.$$

Form the quotient group

$$T := \mathbb{Z}^{(M\times N)}/H = \big\{[f]\big|f \in \mathbb{Z}^{(M\times N)}\big\}$$

with the addition

$$[f_1] + [f_2] = [f_1 + f_2], \tag{6.3}$$

where $f_1, f_2 \in \mathbb{Z}^{(M\times N)}$. We have the natural projection

$$\kappa_H \colon \mathbb{Z}^{(M\times N)} \longrightarrow T, \quad f \mapsto [f].$$

Define also a mapping $\tau \colon\ M \times N \longrightarrow T$ by

$$\tau(m, n) := [x_{(m,n)}] = x_{(m,n)} + H.$$

We will prove that we have constructed the tensor product of the modules $M_R$ and ${}_RN$.

**Proposition 6.4.** *The above constructed pair $(T, \tau)$ is the tensor product of modules $M_R$ and ${}_RN$.*

*Proof.* The mapping $\tau$ is $R$-balanced, because, for every $m_1, m_2 \in M$ and $n \in N$,

$$\begin{aligned}
\tau(m_1 + m_2, n) &= [x_{(m_1+m_2,n)}] && \text{(def. of } \tau) \\
&= [x_{(m_1,n)} + x_{(m_2,n)}] && \text{(def, of } H) \\
&= [x_{(m_1,n)}] + [x_{(m_2,n)}] && \text{(by (6.3))} \\
&= \tau(m_1, n) + \tau(m_2, n), && \text{(def. of } \tau)
\end{aligned}$$

and the other two conditions can be verified analogously.

Let $A$ be an abelian group and $\beta \colon M \times N \longrightarrow A$ an $R$-balanced mapping. Define a mapping

$$\iota \colon M \times N \longrightarrow \mathbb{Z}^{(M\times N)}, \qquad (m, n) \mapsto x_{(m,n)}.$$

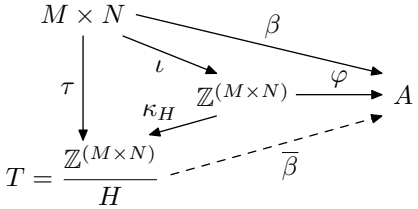
Obviously, $\iota$ is injective. We also define a mapping

$$\overline{\varphi} \colon \mathcal{B} \longrightarrow A, \qquad x_{(m,n)} \mapsto \beta(m, n).$$

We can extend it uniquely to a group homomorphism

$$\varphi \colon \mathbb{Z}^{(M\times N)} \longrightarrow A,$$

because each element of $\mathbb{Z}^{(M\times N)}$ can be expressed uniquley as a linear combination of basis elements. The upper triangle in the diagram



commutes, because

$$(\varphi \circ \iota)(m,n) = \varphi(\iota(m,n)) = \varphi(x_{(m,n)}) = \overline{\varphi}(x_{(m,n)}) = \beta(m,n)$$

for every $(m,n) \in M \times N$. Also the left triangle commutes.

Consider now the generators of $H$ from the lines (6.2) and note that, for every $m_1, m_2, m \in M$, $n_1, n_2, n \in N$ and $r \in R$,

$$\begin{aligned}
\varphi(x_{(m_1+m_2,n)} - x_{(m_1,n)} - x_{(m_2,n)}) &= \varphi(x_{(m_1+m_2,n)}) - \varphi(x_{(m_1,n)}) - \varphi(x_{(m_2,n)}) \\
&= \beta(m_1+m_2,n) - (\beta(m_1,n) + \beta(m_2,n)) \\
&= \beta(m_1+m_2,n) - \beta(m_1+m_2,n) = 0, \\
\varphi(x_{(m,n_1+n_2)} - x_{(m,n_1)} - x_{(m,n_2)}) &= 0, \\
\varphi(x_{(mr,n)} - x_{(m,rn)}) &= \beta(mr,n) - \beta(m,nr) = 0.
\end{aligned}$$

Thus $\varphi(a) = 0$ for every $a \in \hat{H}$. Now any element $b$ of the subgroup $H$ is of the form $b = \pm a_1 \pm a_2 \pm \ldots \pm a_k$, where $a_1, \ldots, a_k \in \hat{H}$. Since $\varphi$ is a group homomorphism, $\varphi(b) = 0$. We have shown that $H \subseteq \operatorname{Ker}\varphi$. By The Homomorphism Theorem for abelian groups, there exists a group homomorphism $\overline{\beta}\colon T \longrightarrow A$ such that the lower triangle in the above diagram commutes. Consequently, the whole diagramm commutes, yielding $\overline{\beta} \circ \tau = \beta$.

Finally, we must check that the homomorphism $\overline{\beta}$ is unique with the property $\overline{\beta} \circ \tau = \beta$. Let $\beta'\colon T \longrightarrow A$ be a group homomorphism such that $\beta = \beta' \circ \tau$. For every $\sum_{k=1}^{k^*} z_k x_{(m_k,n_k)} \in \mathbb{Z}^{(M\times N)}$, we have

$$\begin{aligned}
\beta'\left(\left[\sum_{k=1}^{k^*} z_k x_{(m_k,n_k)}\right]\right) &= \beta'\left(\sum_{k=1}^{k^*} z_k \left[x_{(m_k,n_k)}\right]\right) && \text{(by (6.3))} \\
&= \sum_{k=1}^{k^*} z_k \beta'\left(\left[x_{(m_k,n_k)}\right]\right) && (\beta' \text{ is a group homomorphism}) \\
&= \sum_{k=1}^{k^*} z_k (\beta' \circ \tau)(m_k,n_k) && \text{(def. of } \tau) \\
&= \sum_{k=1}^{k^*} z_k \beta(m_k,n_k) && (\beta' \circ \tau = \beta) \\
&= \sum_{k=1}^{k^*} z_k (\overline{\beta} \circ \tau)(m_k,n_k) && (\beta = \overline{\beta} \circ \tau) \\
&= \overline{\beta}\left(\left[\sum_{k=1}^{k^*} z_k x_{(m_k,n_k)}\right]\right). && (\overline{\beta} \text{ is a group homomorphism})
\end{aligned}$$

Hence $\beta' = \overline{\beta}$, meaning that $\overline{\beta}$ is unique. This completes the proof. □

In what follows, we will assume that the tensor product $M \otimes_R N$ of $M_R$ and ${}_RN$ is always obtained using the construction in this section.

## 6.2 Properties of tensor products

The next result gives a way of expressing an arbitrary element of the tensor product.

**Proposition 6.5.** *Let $R$ be a ring, $M_R$ a right $R$-module and ${}_RN$ a left $R$-module. Any element $\nu \in M \otimes_R N$ can be expressed as a finite sum*

$$\nu = \sum_{k=1}^{k^*} m_k \otimes n_k, \quad (k^* \in \mathbb{N},\ m_k \in M,\ n_k \in N). \tag{6.4}$$

*Moreover,*

1. $\forall m_1, m_2 \in M\, \forall n \in N\colon \quad (m_1 + m_2) \otimes n = (m_1 \otimes n) + (m_2 \otimes n)$;
2. $\forall m \in M\, \forall n_1, n_2 \in N\colon \quad m \otimes (n_1 + n_2) = (m \otimes n_1) + (m \otimes n_2)$;
3. $\forall m \in M\, \forall n \in N\, \forall r \in R\colon \quad mr \otimes n = m \otimes rn$;
4. *for every $m \in M$ and $n \in N$, $0 \otimes 0 = m \otimes 0 = 0 \otimes n$ is the zero element of the abelian group $M \otimes_R N$;*
5. $\forall m \in M\, \forall n \in N\colon \quad -(m \otimes n) = (-m) \otimes n = m \otimes (-n)$.

*Proof.* Consider the tensor product $M \otimes_R N$, obtained using the above construction. Thus $M \otimes_R N$ is the quotient group $\mathbb{Z}^{(M\times N)}/H$ by the subgroup $H$ described above. Therefore, every element $\nu$ is a coset

$$\nu = \left[\sum_{k=1}^{k^*} z_k x_{(m_k,n_k)}\right] = \sum_{k=1}^{k^*} z_k [x_{(m_k,n_k)}] = \sum_{k=1}^{k^*} z_k \tau(m_k, n_k) = \sum_{k=1}^{k^*} z_k (m_k \otimes n_k),$$

where $k^* \in \mathbb{N}$, $z_k \in \mathbb{Z}$ and $(m_k, n_k) \in M \times N$. Moreover, if, for some $k \in \{1, \dots, k^*\}$, $z_k \neq 1$, then we may add the summand $m_k \otimes n_k$ in the sum $|z_k|$ times and, if necessary, take the minus sign into the summand $m_k \otimes n_k$ (using the property 5, which we will prove soon).

In the proof of Proposition 6.4 we showed that the mapping $\tau = \otimes\colon M \times N \longrightarrow M \otimes_R N$ is $R$-balanced. Hence the properties 1, 2 and 3 hold.

Consider property 4. Let $m \in M$ and $n \in N$. Then

$$\begin{aligned} m \otimes n + 0 \otimes 0 &= m \otimes n + 0 \otimes (0n) = m \otimes n + (0 \cdot 0) \otimes n = m \otimes n + 0 \otimes n \\ &= (m + 0) \otimes n = m \otimes n. \end{aligned}$$

It follows that $0 \otimes 0$ is the zero element of the abelian group $M \otimes_R N$. Also,

$$m \otimes 0 = m \otimes 0 \cdot 0 = m0 \otimes 0 = 0 \otimes 0$$

and, analogously, $0 \otimes n = 0 \otimes 0$.

Consider property 5. If $m \in M$ and $n \in N$, then

$$\begin{aligned} m \otimes n + (-m) \otimes n &= (m + (-m)) \otimes n && \text{(property 1)} \\ &= 0 \otimes n && (M \text{ is an abelian group}) \\ &= 0 \otimes 0. && \text{(property 4)} \end{aligned}$$

Hence $-(m \otimes n) = (-m) \otimes n$. Analogously, $-(m \otimes n) = m \otimes (-n)$. □

Although every element of the tensor product $M \otimes_R N$ can be expressed as a sum (6.4), this expression is not unique. Sometimes the elements of the tensor product $M \otimes_R N$ are called **tensors**. From (6.4) it is clear that the set

$$\{m \otimes n \mid m \in M, n \in N\} \subseteq M \otimes_R N$$

is a set of generators of the abelian group $M \otimes_R N$. The elements $m \otimes n$ from that set are called **elementary tensors**. Thus, *every element of $M \otimes_R N$ is a finite sum of elementary tensors.*

Knowing how the elements of the tensor product can be presented, we can say more precisely, how the homomorphism $\overline{\beta}$ is defined.

**Lemma 6.6.** *Let $R$ be a ring, $M_R$ and ${}_RN$ be $R$-modules, $A$ an abelian group and $\beta : M \times N \longrightarrow A$ an $R$-balanced mapping. The assignment*

$$\overline{\beta}\colon M \otimes_R N \longrightarrow A, \qquad \sum_{k=1}^{k^*} m_k \otimes n_k \mapsto \sum_{k=1}^{k^*} \beta(m_k, n_k) \tag{6.5}$$

*is a homomorphism of abelian groups.*

*Proof.* By the universal property of the tensor product there exists a unique group homomorphism $\overline{\beta}\colon M \otimes_R N \longrightarrow A$ such that $\beta = \overline{\beta} \circ \otimes$. Since $\overline{\beta}$ is a homomorphism, for any element $\sum_{k=1}^{k^*} m_k \otimes n_k \in M \otimes_R N$ we have

$$\overline{\beta}\left(\sum_{k=1}^{k^*} m_k \otimes n_k\right) = \sum_{k=1}^{k^*} \overline{\beta}(m_k \otimes n_k) = \sum_{k=1}^{k^*} (\overline{\beta} \circ \otimes)(m_k, n_k) = \sum_{k=1}^{k^*} \beta(m_k, n_k).$$

Thus the homomorphism $\overline{\beta}$ has the form (6.5). □

Often tensor products are formed between bimodules, so let us consider that notion.

**Definition 6.7.** Let $R$ and $S$ be rings. A quadruple $(M; +, \cdot_S, \cdot_R)$ is called an **$(S, R)$-bimodule** if $M$ is a set, ${}_SM = (M; +, \cdot_S)$ is a left $S$-module, $M_R = (M; +, \cdot_R)$ is a right $R$-module and the following condition is satisfied:

$$\forall m \in M\, \forall s \in S\, \forall r \in R\colon \quad (s \cdot_S m) \cdot_R r = s \cdot_S (m \cdot_R r).$$

An $(S, R)$-bimodule $(M; +, \cdot_S, \cdot_R)$ is usually denoted as ${}_SM_R$ and we abbreviate $smr := s \cdot_S m \cdot_R r$.

**Example 6.8** (Bimodules)**.**

1. Any ring $R$ can be conisdered as an $(R, R)$-bimodule, where both $R$-actions are defined using the multiplication of $R$. A one-element abelian group $\{0\}$ can be conisdered as an $(S, R)$-bimodule over arbitrary rings $S$ and $R$.
2. Let $R$ be a ring. The set $\mathrm{Mat}_{m,n}(R)$ can be considered as a $(\mathrm{Mat}_m(R), \mathrm{Mat}_n(R))$-bimodule, where the addition is the usual addition of matrices and both actions are defined using matrix multiplication.

3. Let $R$ be a ring. Every ideal $I \trianglelefteq R$ can be considered as an $(R,R)$-bimodule, where both $R$-actions are defined using the multiplication of $R$.

**Definition 6.9.** Let $S$ and $R$ be rings and let ${}_SM_R$ and ${}_SN_R$ be $(S,R)$-bimodules. A mapping $f\colon M \longrightarrow N$ is called a **homomorphism of bimodules** if $f\colon {}_SM \longrightarrow {}_SN$ is a homomorphism of left $S$-modules and $f\colon M_R \longrightarrow N_R$ is a homomorphism of right $R$-modules.

Bimodules with bimodule homomorphisms form a category ${}_S\mathsf{Mod}_R$, whose objects are $(S,R)$-bimodules and morphisms are bimodule homomorphisms. We write

$$ {}_S\mathrm{Hom}_R(M,N) := \mathrm{Mor}_{{}_S\mathsf{Mod}_R}(M,N), $$

where $M, N \in \mathrm{Ob}({}_S\mathsf{Mod}_R)$.

If in the tensor product one of the modules is a bimodule, then the tensor product can be equipped with the structure of a module.

**Proposition 6.10.** *Let $R$ and $S$ be rings, $M_R$ a right $R$-module and ${}_RN_S$ an $(R,S)$-bimodule. The tensor product $M \otimes_R N$ can be turned (in a canonical way) into a right $S$-module defining the $S$-action by*

$$ (M \otimes_R N) \times S \longrightarrow M \otimes_R N, \qquad \left(\sum_{k=1}^{k^*} m_k \otimes n_k\right) s := \sum_{k=1}^{k^*} m_k \otimes n_k s. $$

*Proof.* We know that $(M \otimes_R N; +)$ is an abelian group. For any $s \in S$ consider the mapping

$$ \beta_s\colon\ M \times N \longrightarrow M \otimes_R N, \quad \beta_s(m,n) = m \otimes ns. $$

If $m, m' \in M$, $n, n' \in N$ and $r \in R$, then

$$ \begin{aligned} \beta_s(m+m',n) &= (m+m') \otimes ns = m \otimes ns + m' \otimes ns = \beta_s(m,n) + \beta_s(m',n), \\ \beta_s(m,n+n') &= m \otimes (n+n')s = m \otimes (ns + n's) = m \otimes ns + m \otimes n's \\ &= \beta_s(m,n) + \beta_s(m,n'), \\ \beta_s(mr,n) &= mr \otimes ns = m \otimes r(ns) = m \otimes (rn)s = \beta_s(m,rn). \end{aligned} $$

Hence the mapping $\beta$ is $R$-balanced. By Lemma 6.6, there exists a well-defined group homomorphism

$$ \overline{\beta_s}\colon M \otimes_R N \longrightarrow M \otimes_R N, \quad \sum_{k=1}^{k^*} m_k \otimes n_k \mapsto \sum_{k=1}^{k^*} m_k \otimes n_k s. $$

Now define a mapping

$$ (M \otimes_R N) \times S \longrightarrow M \otimes_R N, \qquad \left(\sum_{k=1}^{k^*} m_k \otimes n_k, s\right) \mapsto \overline{\beta_s}\left(\sum_{k=1}^{k^*} m_k \otimes n_k\right). $$

Note that this mapping coincides with the $S$-action given in the formulation of the proposition. Condition M5 in the definition of a module holds, because $\overline{\beta_s}$ is a group homomorphism for every $s \in S$. Let $\nu = \sum_{k=1}^{k^*} m_k \otimes n_k \in M \otimes_R N$ and $s, s' \in S$. Then

$$\begin{aligned}
\nu(s+s') &= \left(\sum_{k=1}^{k^*} m_k \otimes n_k\right)(s+s') = \sum_{k=1}^{k^*}(m_k \otimes n_k(s+s')) \\
&= \sum_{k=1}^{k^*} m_k \otimes (n_k s + n_k s') = \sum_{k=1}^{k^*}(m_k \otimes n_k s + m_k \otimes n_k s') \\
&= \left(\sum_{k=1}^{k^*} m_k \otimes n_k\right) s + \left(\sum_{k=1}^{k^*} m_k \otimes n_k\right) s' = \nu s + \nu s', \\
\nu(ss') &= \left(\sum_{k=1}^{k^*} m_k \otimes n_k\right)(ss') = \sum_{k=1}^{k^*} m_k \otimes n_k(ss') = \sum_{k=1}^{k^*} m_k \otimes (n_k s)s' \\
&= \left(\sum_{k=1}^{k^*} m_k \otimes n_k s\right) s' = (\nu s)s'.
\end{aligned}$$

We conclude that $M \otimes_R N$ is a right $S$-module. □

Analogously one can prove the following proposition.

**Proposition 6.11.** *Let $R$ and $S$ be rings, ${}_RN$ a left $R$-module and ${}_SM_R$ an $(S,R)$-bimodule. The tensor product $M \otimes_R N$ can be turned into a left $S$-module defining the $S$-action by*

$$S \times (M \otimes_R N) \longrightarrow M \otimes_R N, \qquad s\left(\sum_{k=1}^{k^*} m_k \otimes n_k\right) := \sum_{k=1}^{k^*} sm_k \otimes n_k.$$

**Corollary 6.12.** *Let $R$, $S$ and $T$ be rings, and ${}_SM_R$, ${}_RN_T$ bimodules. The tensor product $M \otimes_R N$ can be conisdered as an $(S,T)$-bimodule.*

*Proof.* By Proposition 6.10 and Proposition 6.11, $M \otimes_R N$ is a right $T$-module and a left $S$-module. Let $s \in S$, $t \in T$ and $\sum_{k=1}^{k^*} m_k \otimes n_k \in M \otimes_R N$. Then

$$\left(s\left(\sum_{k=1}^{k^*} m_k \otimes n_k\right)\right) t = \left(\sum_{k=1}^{k^*} sm_k \otimes n_k\right) t = \sum_{k=1}^{k^*} sm_k \otimes n_k t = s\left(\left(\sum_{k=1}^{k^*} m_k \otimes n_k\right) t\right),$$

which proves that $M \otimes_R N$ is an $(S,T)$-bimodule. □

Next we prove that tensoring by a unitary module produces a unitary module.

**Lemma 6.13.** *Let $R$ and $S$ be rings and ${}_RN_S \in \mathrm{Ob}({}_R\mathsf{Mod}_S)$ such that $N_S$ is a unitary module. For every $R$-module $M_R$, $M \otimes_R N$ is a unitary $S$-module.*

*Proof.* Let $\sum_{k=1}^{k^*} m_k \otimes n_k \in M \otimes_R N$. Since $N_S$ is unitary, there exists $h^* \in \mathbb{N}$ and, for every $k \in \{0, \ldots, k^*\}$, there exist $n_{k1}, \ldots, n_{kh^*} \in N$ and $s_{k1}, \ldots, s_{kh^*} \in S$ such that $n_k = n_{k1}s_{k1} + \ldots + n_{kh^*}s_{kh^*}$. Now

$$\sum_{k=1}^{k^*} m_k \otimes n_k = \sum_{k=1}^{k^*} m_k \otimes \left( \sum_{h=1}^{h^*} n_{kh} s_{kh} \right) = \sum_{h=1}^{h^*} \left( \sum_{k=1}^{k^*} m_k \otimes n_{kh} \right) s_{kh} \in (M \otimes_R N)S.$$

Hene $M \otimes_R N$ is a unitary right $S$-module. □

Next we will show that the tensor multiplication is associative up to isomorphism.

**Proposition 6.14.** *Let $R$ and $S$ be rings, $M_R$ a right $R$-module, ${}_RN_S$ a bimodule and ${}_SP$ a left $S$-module. Then there exists a group isomorphism*

$$\alpha\colon\ (M \otimes_R N) \otimes_S P \longrightarrow M \otimes_R (N \otimes_S P), \qquad (m \otimes n) \otimes p \mapsto m \otimes (n \otimes p).$$

We omit the proof of this proposition.

**Corollary 6.15.** *If ${}_SM_R$ and ${}_RN_T$ are bimodules, then the mapping $\alpha$ from Proposition 6.14 is an isomorphism of bimodules.*

**Exercise 6.16.** Consider the abelian group $(\mathbb{Z}_n, +)$ as a right $\mathbb{Z}$-module (in a natural way) and the abelian group $(\mathbb{Q}, +)$ as a left $\mathbb{Z}$-module. Prove that

$$\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}.$$

## 6.3 Tensor product of homomorphisms of modules

Let $R$ be a ring and let $f\colon M_R \longrightarrow M'_R$ and $g\colon {}_RN \longrightarrow {}_RN'$ be homomorphisms of $R$-modules. Define a mapping $(f;g)\colon M \times N \longrightarrow M' \otimes_R N'$ by

$$(f;g)(m,n) := f(m) \otimes g(n).$$

We show that $(f;g)$ is $R$-balanced. If $m, m' \in M$, $n, n' \in N$ and $r \in R$, then

$$\begin{aligned}
(f;g)(m+m',n) &= f(m+m') \otimes g(n) = (f(m) + f(m')) \otimes g(n) \\
&= f(m) \otimes g(n) + f(m') \otimes g(n) = (f;g)(m,n) + (f;g)(m',n), \\
(f;g)(m,n+n') &= (f;g)(m,n) + (f;g)(m,n'), \\
(f;g)(mr,n) &= f(mr) \otimes g(n) = f(m)r \otimes g(n) = f(m) \otimes rg(n) \\
&= f(m) \otimes g(rn) = (f;g)(m,rn).
\end{aligned}$$

Since $(f;g)$ is $R$-balanced, by the universal property there exists a group homomorphism $\overline{(f;g)}\colon M \otimes_R N \longrightarrow M' \otimes_R N'$ such that $\overline{(f;g)} \circ \otimes = (f;g)$. Consequently,

$$\overline{(f;g)}(m \otimes n) = \overline{(f;g)}(\otimes(m,n)) = (f;g)(m,n) = f(m) \otimes g(n).$$

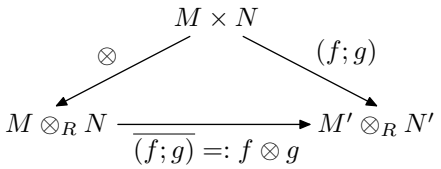



Figure 6.1:

The homomorphism $\overline{(f;g)}$ is called the **tensor product of the homomorphisms** $f$ **and** $g$ **of modules** and it is denoted by $f \otimes g$. As we saw,

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n),$$

for every $m \in M$ and $n \in N$. Since $f \otimes g$ is a group homomorphism, for every element $\sum_{k=1}^{k^*} m_k \otimes n_k \in M \otimes_R N$, we have

$$(f \otimes g)\left(\sum_{k=1}^{k^*} m_k \otimes n_k\right) = \sum_{k=1}^{k^*} (f \otimes g)(m_k \otimes n_k) = \sum_{k=1}^{k^*} f(m_k) \otimes g(n_k).$$

In the next two propositions we prove several useful properties of tensor products of homomorphisms.

**Proposition 6.17.** *Let $R$ be a ring, $M_R$, $M'_R$, ${}_RN$ and ${}_RN'$ be $R$-modules, $f, f' \in \mathrm{Hom}_R(M, M')$ and $g, g' \in {}_R\mathrm{Hom}(N, N')$. Then*

1. $(f + f') \otimes g = f \otimes g + f' \otimes g$,
2. $f \otimes (g + g') = f \otimes g + f \otimes g'$,
3. $f \otimes \mathbf{0} = \mathbf{0} \otimes g = \mathbf{0}$,
4. $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_R N}$.

*Proof.* We show that the listed properties hold on the generators $m \otimes n$ of the tensor product $M \otimes_R N$. From this it follows that these properties hold on all elements of $M \otimes_R N$. Let $m \otimes n \in M \otimes_R N$.

1. We have

$$\begin{aligned}((f + f') \otimes g)(m \otimes n) &= (f + f')(m) \otimes g(n) \\ &= (f(m) + f'(m)) \otimes g(n) \\ &= f(m) \otimes g(n) + f'(m) \otimes g(n) \\ &= (f \otimes g)(m \otimes n) + (f' \otimes g)(m \otimes n) \\ &= (f \otimes g + f' \otimes g)(m \otimes n).\end{aligned}$$

2. Analogous to the previous case.
3. We have

$$(f \otimes \mathbf{0})(m \otimes n) = f(m) \otimes 0_{N'} = f(m) \otimes 0_R 0_{N'} = f(m)0_R \otimes 0_{N'} = 0_{M'} \otimes 0_{N'},$$

that is, the mapping $f \otimes \mathbf{0}$ takes an element $m \otimes n$ to the zero element of the abelian group $M' \otimes_R N'$. Therefore it takes all elements of $M \otimes_R N$ to zero. Hence $f \otimes \mathbf{0}$ is the zero mapping. Analogously $\mathbf{0} \otimes g = \mathbf{0}$.

4. We have

$$(\mathrm{id}_M \otimes \mathrm{id}_N)(m \otimes n) = \mathrm{id}_M(m) \otimes \mathrm{id}_N(n) = m \otimes n = \mathrm{id}_{M \otimes_R N}(m \otimes n).$$

□

**Proposition 6.18.** *Let $R$ be a ring and let $f\colon M_R \longrightarrow M'_R$, $f'\colon M'_R \longrightarrow M''_R$, $g\colon {}_RN \longrightarrow {}_RN'$, $g'\colon {}_RN' \longrightarrow {}_RN''$ be homomorphisms of $R$-modules. Then*

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g).$$

*Proof.* If $m \otimes n \in M \otimes_R N$, then

$$\begin{aligned}((f' \otimes g') \circ (f \otimes g))(m \otimes n) &= (f' \otimes g')(f(m) \otimes g(n)) \\ &= f'(f(m)) \otimes g'(g(n)) \\ &= (f' \circ f)(m) \otimes (g' \circ g)(n) \\ &= ((f' \circ f) \otimes (g' \circ g))(m, n).\end{aligned}$$

□

**Corollary 6.19.** *Let $R$ be a ring and let $M_R$, $M'_R$, ${}_RN$, ${}_RN'$ be $R$-modules. If $f\colon M_R \longrightarrow M'_R$ and $g\colon {}_RN \longrightarrow {}_RN'$ are split monomorphisms, split epimorphisms or isomorphisms, then $f \otimes g$ has the same property. For isomorphisms,*

$$(f \otimes g)^{-1} = f^{-1} \otimes g^{-1}.$$

It turns out that tensoring preserves surjectivity of homomorphisms.

**Proposition 6.20.** *Let $R$ be a ring. If $f\colon M_R \longrightarrow M'_R$ and $g\colon N_R \longrightarrow N'_R$ are surjective homomorphisms, then $f \otimes g$ is also surjective.*

*Proof.* Let $f\colon M_R \longrightarrow M'_R$ and $g\colon N_R \longrightarrow N'_R$ be surjective homomorphisms and consider an element $\sum_{k=1}^{k^*} m'_k \otimes n'_k \in M' \otimes_R N'$. For every $k \in \{1, \ldots, k^*\}$ there exist $m_k \in M$ and $n_k \in N$ such that $m'_k = f(m_k)$ and $n'_k = g(n_k)$. Now

$$\sum_{k=1}^{k^*} m'_k \otimes n'_k = \sum_{k=1}^{k^*} f(m_k) \otimes g(n_k) = (f \otimes g)\left(\sum_{k=1}^{k^*} m_k \otimes n_k\right).$$

Hence $f \otimes g\colon M \otimes_R N \longrightarrow M' \otimes_R N'$ is a surjective mapping. □

## 6.4 Tensor functors

We will show that tensoring by a bimodule induces a functor between certain module categories.

**Proposition 6.21.** *Let $R$, $S$ be rings and ${}_RN_S$ an $(R,S)$-bimodule. The assignment*

$$\begin{array}{ccc} M_R & \longmapsto & M \otimes_R N \\ f \downarrow & & \downarrow f \otimes \mathrm{id}_N \\ M'_R & \longmapsto & M' \otimes_R N \end{array}$$

*defines a functor $\_ \otimes_R N \colon \mathsf{Mod}_R \longrightarrow \mathsf{Mod}_S$.*

*Proof.* Let $F$ be the assignment given in the above figure. For every $M_R \in \mathrm{Ob}(\mathsf{Mod}_R)$, there exists the tensor product $M \otimes_R N$, which is a right $S$-module by Proposition 6.10. Hence the assignment $F \colon \mathrm{Ob}(\mathsf{Mod}_R) \longrightarrow \mathrm{Ob}(\mathsf{Mod}_S)$ is a mapping. We show that $F$ satisfies the conditions of Definition 5.15.

1. For every morphism $f \in \mathrm{Mor}_{\mathsf{Mod}_R}(M, M') = \mathrm{Hom}_R(M, M')$, there exists the tensor product $F(f) = f \otimes \mathrm{id}_N \colon M \otimes_R N \longrightarrow M' \otimes_R N$, which is a morphism in the category $\mathsf{Mod}_S$.
2. If $f \in \mathrm{Mor}_{\mathsf{Mod}_R}(M, M')$ and $g \in \mathrm{Mor}_{\mathsf{Mod}_R}(M', M'')$, then, by Proposition 6.18,
$$\begin{aligned} F(g \circ f) &= (g \circ f) \otimes \mathrm{id}_N = (g \circ f) \otimes (\mathrm{id}_N \circ \mathrm{id}_N) = (g \otimes \mathrm{id}_N) \circ (f \otimes \mathrm{id}_N) \\ &= F(g) \circ F(f). \end{aligned}$$
3. Let $M_R \in \mathsf{Mod}_R$. By Proposition 6.17(4),
$$F(\mathrm{id}_M) = \mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes N}.$$

Thus $F$ is a functor, which we will denote by $\_ \otimes_R N$. □

Analogously, by Corollary 6.12 we obtain a tensor functor between categories of bimodules.

**Corollary 6.22.** *Let $R$, $S$, $T$ be rings and ${}_RN_S$ an $(R,S)$-bimodule. Then there exists a functor*

$$\_ \otimes_R N \colon {}_T\mathsf{Mod}_R \longrightarrow {}_T\mathsf{Mod}_S.$$

Of course, one can also consider functors of tensoring from the left.

**Corollary 6.23.** *Let $R$, $S$, $T$ be rings and ${}_TM_R$ a $(T,R)$-bimodule. Then there exist functors*

$$\begin{aligned} M \otimes_R \_ &\colon {}_R\mathsf{Mod} \longrightarrow {}_T\mathsf{Mod}, \\ M \otimes_R \_ &\colon {}_R\mathsf{Mod}_S \longrightarrow {}_T\mathsf{Mod}_S. \end{aligned}$$

It is also clear that tensoring by a one-sided module produces an abelian group.

**Corollary 6.24.** *Let $R$ be a ring, $M_R \in \mathrm{Ob}(\mathsf{Mod}_R)$ and ${}_RN \in \mathrm{Ob}({}_R\mathsf{Mod})$. There exist functors*

$$M \otimes_R \_ \colon {}_R\mathsf{Mod} \longrightarrow \mathsf{Ab}, \tag{6.6}$$

$$\_ \otimes_R N \colon \mathsf{Mod}_R \longrightarrow \mathsf{Ab}. \tag{6.7}$$

## 6.5 Firm modules

Recall that each ring $R$ can be considered as a bimodule ${}_RR_R$. Let $M_R$ be a right $R$-module. By Proposition 6.10 we know that $M \otimes_R R$ is also a right $R$-module. We show that there exists a canonical homomorphism $M \otimes_R R \longrightarrow M$.

**Lemma 6.25.** *Let $R$ be a ring and $M_R$ a right $R$-module. There exists a homomorphism*

$$\mu_M \colon \ M \otimes_R R \longrightarrow M, \qquad \sum_{k=1}^{k^*} m_k \otimes r_k \mapsto \sum_{k=1}^{k^*} m_k r_k.$$

*of right $R$-modules. Moreover, $\mu = (\mu_M)_{M \in \mathrm{Ob}(\mathsf{Mod}_R)} \colon (\_ \otimes_R R) \Rightarrow \mathrm{id}_{\mathsf{Mod}_R}$ is a natural transformation.*

*Proof.* Let $R$ be a ring and $M_R \in \mathrm{Ob}(\mathsf{Mod}_R)$. Consider the mapping

$$\hat{\mu} : M \times R \longrightarrow M, \ \ (m, r) \mapsto mr.$$

For every $m, m' \in M$, $r, r' \in R$,

$$\begin{aligned} \hat{\mu}(m + m', r) &= (m + m')r = mr + m'r = \hat{\mu}(m, r) + \hat{\mu}(m', r), \\ \hat{\mu}(m, r + r') &= m(r + r') = mr + mr' = \hat{\mu}(m, r) + \hat{\mu}(m, r'), \\ \hat{\mu}(mr, r') &= (mr)r' = m(rr') = \hat{\mu}(m, rr'). \end{aligned}$$

Thus $\hat{\mu}$ is $R$-balanced and, by the universal property (and Lemma 6.6), we obtain a group homomorphism $\mu_M = \overline{\hat{\mu}}$. For every $\sum_{k=1}^{k^*} m_k \otimes r_k \in M \otimes_R R$ and $r \in R$,

$$\begin{aligned} \mu_M \left( \left( \sum_{k=1}^{k^*} m_k \otimes r_k \right) r \right) &= \mu_M \left( \sum_{k=1}^{k^*} m_k \otimes r_k r \right) = \sum_{k=1}^{k^*} m_k r_k r \\ &= \left( \sum_{k=1}^{k^*} m_k r_k \right) r = \mu_M \left( \sum_{k=1}^{k^*} m_k \otimes r_k \right) r. \end{aligned}$$

So $\mu_M$ is a homomorphism of right $R$-modules.

Let $M_R, N_R \in \mathrm{Ob}(\mathsf{Mod}_R)$ and $f \in \mathrm{Hom}_R(M, N)$. Consider the diagram

$$\begin{array}{ccc} M \otimes_R R & \xrightarrow{\ \mu_M\ } & M \\ {\scriptstyle f \otimes \mathrm{id}_R}\downarrow & & \downarrow{\scriptstyle f} \\ N \otimes_R R & \xrightarrow[\ \mu_N\ ]{} & N \end{array}.$$

For every generator $m \otimes r \in M \otimes_R R$,

$$\begin{aligned} (f \circ \mu_M)(m \otimes r) &= f(mr) = f(m)r = \mu_N(f(m) \otimes r) \\ &= \mu_N((f \otimes \mathrm{id}_R)(m \otimes r)) = (\mu_N \circ (f \otimes \mathrm{id}_R))(m \otimes r). \end{aligned}$$

Consequently, $f \circ \mu_M = \mu_N \circ (f \otimes \mathrm{id}_R)$. We have shown that $\mu = (\mu_M)_{M \in \mathrm{Ob}(\mathsf{Mod}_R)}$ is a natural transformation. □

**Definition 6.26.** Let $R$ be a ring. A right $R$-module $M_R$ is called **firm**[1] if the canonical homomorphism $\mu_M$ is an isomorphism.

By $\mathsf{FMod}_R$ we denote the full subcategory of $\mathsf{Mod}_R$ generated by firm modules. Dually, a left $R$-module ${}_RM \in \mathrm{Ob}({}_R\mathsf{Mod})$ is called **firm** if the homomorphism

$$\nu_M \colon R \otimes_R M \longrightarrow M, \quad r \otimes m \mapsto rm$$

is an isomorphism. The category of firm left $R$-modules is denoted by ${}_R\mathsf{FMod}$.

**Proposition 6.27.** *Let $S$ be a ring with identity. A module $M_S$ is firm if and only if it is unitary.*

*Proof.* NECESSITY. A module $M_S$ is unitary if and only if the homomorphism $\mu_M$ is surjective. Hence every firm module is unitary.
SUFFICIENCY. Since $M_S$ is unitary, the mapping $\mu_M$ is surjective. On the other hand, let $\sum_{k=1}^{k^*} m_k \otimes s_k \in M \otimes_S S$ be such that $\sum_{k=1}^{k^*} m_k s_k = 0$. Then

$$\sum_{k=1}^{k^*} m_k \otimes s_k = \sum_{k=1}^{k^*} m_k \otimes s_k 1 = \left( \sum_{k=1}^{k^*} m_k s_k \right) \otimes 1 = 0 \otimes 1 = 0.$$

Hence $\operatorname{Ker} \mu_M = \{0\}$. Therefore $\mu_M$ is also injective and thus an isomorphism of $S$-modules. □

**Corollary 6.28.** *If $S$ is a ring with identity, then $\mathsf{FMod}_S = \mathsf{UMod}_S$.*

## 6.6 Firm and idempotent rings

**Definition 6.29.** A ring $R$ is called **firm** if the module $R_R$ is firm, that is, the mapping

$$\mu_R \colon \ R \otimes_R R \mapsto R, \qquad \sum_{k=1}^{k^*} r_k \otimes r'_k \mapsto \sum_{k=1}^{k^*} r_k r'_k$$

is bijective.

For every ring $R$ we may consider the subset $RR \subseteq R$.

**Definition 6.30.** A ring $R$ is called **idempotent** if $RR = R$, that is, for every $r \in R$ there exist a natural number $k^* \in \mathbb{N}$, and elements $r_1, r'_1, \ldots, r_{k^*}, r'_{k^*} \in R$ such that

$$r = \sum_{k=1}^{k^*} r_k r'_k.$$

[1] There are also other terms used for firm modules in the literature: *coclosed* or *regular module*

It is easy to understand that a ring $R$ is idempotent if and only if the mapping $\mu_R$ is surjective. Hence every firm ring is idempotent. Therefore we have the implications

$$\text{ring with } 1 \implies \text{firm ring} \implies \text{idempotent ring}\,.$$

Clearly every ring with identity is an idempotent ring. Next we will give some examples of idempotent rings without identity.

**Example 6.31** (Idempotent rings)**.**

1. Let $X$ be an infinite set and let $\wp_{\text{fin}}(X)$ be the set of all finite subsets of $X$. Then $(\wp_{\text{fin}}(X); \Delta, \cap)$ is an idempotent ring, because every $A \in \wp_{\text{fin}}(X)$ can be presented as $A = A \cap A$. This ring does not have an identity element.
2. Consider residue class rings $\mathbb{Z}_k$, $k \in \mathbb{N}$, and their **external direct sum** $\bigoplus_{k=1}^{\infty} \mathbb{Z}_k$, that is, the subset of the direct product $\prod_{k=1}^{\infty} \mathbb{Z}_k$ consisting of those sequences that have finitely many nonzero components. The set $\bigoplus_{k=1}^{\infty} \mathbb{Z}_k$ is a ring with respect to componentwise operations. This ring is idempotent. To see this, take $(a_1, a_2, \ldots) \in \bigoplus_{k=1}^{\infty} \mathbb{Z}_k$. Then there exists a natural number $n$ such that $a_n = \overline{0}$ for every $n' > n$. Now

$$(a_1, a_2, \ldots) = (a_1, \ldots, a_n, \overline{0}, \ldots) = (\overline{1}, \ldots, \underset{n\text{th place}}{\overline{1}}, \overline{0}, \ldots)(a_1, \ldots, a_n, \overline{0}, \ldots).$$

   But this ring does not have an identity element, because the sequence $(\overline{1}, \overline{1}, \overline{1}, \ldots)$ does not belong to $\bigoplus_{k=1}^{\infty} \mathbb{Z}_k$.

We will show that unitarity of modules is a weaker condition than firmness. The next example was given in an article "A note on Taylor's Brauer group" (1998) by Caenepeel and Grandjean.

**Example 6.32** (Unitary non-firm module)**.** Let $R := \mathbb{Z}_2 \times \mathbb{Z}$. On the set $R$ we consider componentwise addition and we define a multiplication by

$$(\overline{z_1}, a_1)(\overline{z_2}, a_2) := (a_1\overline{z_2}, a_1a_2).$$

It can be verified that with these operations $R$ is a ring. Moreover, $R$ is an idempotent ring, because

$$(\overline{0}, 1)(\overline{z}, a) = (1\overline{z}, 1a) = (\overline{z}, a)$$

for every $(\overline{z}, a) \in R$. Hence $R_R$ is a unitary module.

Fix an element $c = (\overline{0}, 2) \in R$. Consider the principal right ideal

$$cR = \{(\overline{0}, 2b) \mid b \in \mathbb{Z}\} \cong 2\mathbb{Z}$$

as a right $R$-module. Note that, for every $(\overline{0}, 2b) \in cR$,

$$(\overline{0}, 2b) = (\overline{0}, 2)(\overline{0}, b) = c(\overline{0}, b) = c(\overline{0}, 1)(\overline{0}, b) \in (cR)R,$$

whence $cR$ is a unitary $R$-module.

Consider the elementary tensor $(\overline{0}, 2) \otimes (\overline{1}, 0) \in cR \otimes_R R$. Then

$$\mu_{cR}((\overline{0}, 2) \otimes (\overline{1}, 0)) = (\overline{0}, 2)(\overline{1}, 0) = (\overline{0}, 0).$$

Define a mapping

$$f\colon\ cR \times R \longrightarrow \mathbb{Z}_2, \qquad ((\overline{0}, 2b), (\overline{z}, a)) \mapsto b\overline{z}.$$

For every $(\overline{0}, 2b), (\overline{0}, 2b') \in cR$ and $(\overline{z}, a), (\overline{z'}, a') \in R$,

$$\begin{aligned} f((\overline{0}, 2b) + (\overline{0}, 2b'), (\overline{z}, a)) &= f((\overline{0}, 2(b+b')), (\overline{z}, a)) = (b+b')\overline{z} = b\overline{z} + b'\overline{z}, \\ f((\overline{0}, 2b), (\overline{z}, a) + (\overline{z'}, a')) &= f((\overline{0}, 2b), (\overline{z} + \overline{z'}, a + a')) = b(\overline{z} + \overline{z'}) = b\overline{z} + b\overline{z'}, \\ f((\overline{0}, 2b)(\overline{z'}, a'), (\overline{z}, a)) &= f((0, 2ba'), (\overline{z}, a)) = ba'\overline{z} = f((\overline{0}, 2b), (a'\overline{z}, a'a)) \\ &= f((\overline{0}, 2b), (\overline{z'}, a')(\overline{z}, a)), \end{aligned}$$

so $f$ is $R$-balanced. By the universal property we know that

$$\overline{f}\colon\ cR \otimes_R R \longrightarrow \mathbb{Z}_2, \qquad \sum_{k=1}^{k^*} (\overline{0}, 2b_k) \otimes (\overline{z_k}, a_k) \mapsto \sum_{k=1}^{k^*} b_k \overline{z_k}$$

is a well defined group homomorphism. Now

$$\overline{f}((\overline{0}, 2) \otimes (\overline{1}, 0)) = 1 \cdot \overline{1} = \overline{1} \neq \overline{0}$$

in $\mathbb{Z}_2$. Hence $(\overline{0}, 2) \otimes (\overline{1}, 0)$ is not the zero element of the abelian group $cR \otimes_R R$, because a group homomorphism preserves zero. But this means that $\mu_{cR}$ is not injective. In conclusion we have shown that $cR$ is a unitary, but not firm $R$-module.

We will prove two more results about the homomorphism $\mu_M$.

**Lemma 6.33.** *Let $R$ be a ring. For every module $M_R$,*

$$(\operatorname{Ker} \mu_M)R = \{0\}.$$

*Proof.* If $\sum_{k=1}^{k^*} m_k \otimes r_k \in \operatorname{Ker} \mu_M$ and $r \in R$, then

$$\left( \sum_{k=1}^{k^*} m_k \otimes r_k \right) r = \sum_{k=1}^{k^*} (m_k \otimes r_k r) = \sum_{k=1}^{k^*} (m_k r_k \otimes r) = \left( \sum_{k=1}^{k^*} m_k r_k \right) \otimes r = 0 \otimes r = 0,$$

which means that $(\operatorname{Ker} \mu_M)R = \{0\}$. □

**Lemma 6.34.** *Let $R$ be a ring and $M_R \in \operatorname{Ob}(\mathsf{UMod}_R)$. The canonical homomorphism $\mu_M\colon M \otimes_R R \longrightarrow M_R$ is a monomorphism in the category $\mathsf{UMod}_R$ of unitary right $R$-modules.*

*Proof.* Let $N_R \in \operatorname{Ob}(\mathsf{UMod}_R)$ and let $f\colon N_R \longrightarrow M \otimes_R R$ be such that $\mu_M \circ f = \mathbf{0}$. Then $\operatorname{Im} f \subseteq \operatorname{Ker} \mu_M$. By Lemma 6.33, we know that $(\operatorname{Ker} \mu_M)R = \{0\}$.

Let $n \in N$. Since $N_R$ is unitary, there exist $n_1, \ldots, n_{k^*} \in N$ and $r_1, \ldots, r_{k^*} \in R$ such that $n = n_1 r_1 + \ldots + n_{k^*} r_{k^*}$. For every $k \in \{1, \ldots, k^*\}$, we have $f(n_k) \in \operatorname{Ker} \mu_M$. Hence $f(n_k) r_k = 0$. Now

$$f(n) = f\left( \sum_{k=1}^{k^*} n_k r_k \right) = \sum_{k=1}^{k^*} f(n_k) r_k = 0.$$

Thus $f = \mathbf{0}$ and by Proposition 5.13 we conclude that $\mu_M$ is a monomorphism. □

**Remark 6.35.** This lemma shows that module categories may contain non-injective monomorphisms. Namely, if $M_R$ is a unitary module, which is not firm, then $\mu_M$ is a surjective monomorphism, which is not injective (because $\mu_M$ is not bijective).

Tensor functors are right exact.

**Theorem 6.36.** *Let $R$ be a ring and ${}_RN \in \mathrm{Ob}({}_R\mathsf{Mod})$ be an $R$-module. The tensor functor $\_ \otimes_R N \colon \mathsf{Mod}_R \longrightarrow \mathsf{Ab}$ is right exact, that is, if*

$$\{0\} \xrightarrow{\mathbf{0}} M_R \xrightarrow{f} K_R \xrightarrow{g} L_R \xrightarrow{\mathbf{0}} \{0\}$$

*is a short exact sequence in the category $\mathsf{Mod}_R$, then*

$$M \otimes_R N \xrightarrow{f\otimes \mathrm{id}_N} K \otimes_R N \xrightarrow{g\otimes \mathrm{id}_N} L \otimes_R N \xrightarrow{\mathbf{0}} \{0\}. \tag{6.8}$$

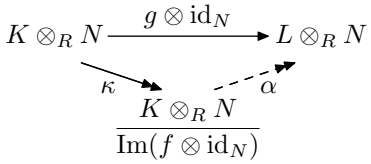
*is an exact sequence in the category $\mathsf{Ab}$.*

*Proof.* By Proposition 6.20, $g \otimes \mathrm{id}_N$ is surjective, so the sequence (6.8) is exact at $L \otimes_R N$. It remains to prove that it is exact at $K \otimes_R N$.

Using Propositions 6.17 and 6.18 we see that

$$(g \otimes \mathrm{id}_N) \circ (f \otimes \mathrm{id}_N) = (g \circ f) \otimes (\mathrm{id}_N \circ \mathrm{id}_N) = \mathbf{0} \otimes \mathrm{id}_N = \mathbf{0}.$$

Hence $\mathrm{Im}(f \otimes \mathrm{id}_N) \subseteq \mathrm{Ker}(g \otimes \mathrm{id}_N)$, and to complete the proof it suffices to prove the opposite inclusion. Applying The Homomorphism Theorem we obtain a surjective homomorphism $\alpha$, such that the diagram




commutes, where $\kappa$ is the canonical surjection and

$$\alpha([k \otimes n]) = g(k) \otimes n$$

for every $k \in K$ and $n \in N$. We will construct an inverse for $\alpha$. For this, we first define a mapping

$$\beta \colon L \times N \longrightarrow \frac{K \otimes_R N}{\mathrm{Im}(f \otimes \mathrm{id}_N)}, \qquad (l, n) \mapsto [k \otimes n],$$

where $g(k) = l$ (such an element $k$ exists due to surjectivity of $g$). We show that $\beta$ is well defined. If $k, k' \in K$ are such that $g(k) = g(k') = l$ for some $l \in L$, we have $k' - k \in \mathrm{Ker}\, g = \mathrm{Im}\, f$. Hence $(k' - k) \otimes n \in \mathrm{Im}(f \otimes \mathrm{id}_N)$. Now

$$[k \otimes n] = [k \otimes n] + [0] = [k \otimes n] + [(k' - k) \otimes n] = [(k + k' - k) \otimes n] = [k' \otimes n].$$

Consequently, $\beta$ is well defined. Let now $l, l' \in L$, $n, n' \in N$ and $r \in R$. Also, let $k, k' \in K$ be such that $g(k) = l$ and $g(k') = l'$. Then

$$\begin{aligned}\beta(l + l', n) &= [(k + k') \otimes n] = [k \otimes n] + [k' \otimes n] = \beta(l, n) + \beta(l, n'),\\ \beta(l, n + n') &= [k \otimes (n + n')] = [k \otimes n] + [k \otimes n'] = \beta(l, n) + \beta(l, n'),\\ \beta(lr, n) &= [kr \otimes n] = [k \otimes rn] = \beta(l, rn),\end{aligned}$$

where in the last line we use that $lr = g(k)r = g(kr)$. Hence $\beta$ is $R$-balanced. By the universal property, we obtain a group homomorphism

$$\overline{\beta}\colon L \otimes_R N \longrightarrow \frac{K \otimes_R N}{\operatorname{Im}(f \otimes \mathrm{id}_N)}, \qquad l \otimes n \mapsto [k \otimes n].$$

Note that, for every generator $[k \otimes n] \in (K \otimes_R N)/\operatorname{Im}(f \otimes \mathrm{id}_N)$,

$$(\overline{\beta} \circ \alpha)([k \otimes n]) = \overline{\beta}(g(k) \otimes n) = [k \otimes n].$$

and, for every $l \otimes n \in L \otimes_R N$,

$$(\alpha \circ \overline{\beta})(l \otimes n) = \alpha([k \otimes n]) = g(k) \otimes n = l \otimes n.$$

Hence $\overline{\beta} \circ \alpha = \mathrm{id}$ and $\alpha \circ \overline{\beta} = \mathrm{id}$. This means that $\alpha$ is an isomorphism. The equality $g \otimes \mathrm{id}_N = \alpha \circ \kappa$ implies

$$\overline{\beta} \circ (g \otimes \mathrm{id}_N) = \overline{\beta} \circ \alpha \circ \kappa = \mathrm{id} \circ \kappa = \kappa.$$

If $x \in \operatorname{Ker}(g \otimes \mathrm{id}_N)$, then

$$x + \operatorname{Im}(f \otimes \mathrm{id}_N) = \kappa(x) = \overline{\beta}((g \otimes \mathrm{id}_N)(x)) = \overline{\beta}(0) = \operatorname{Im}(f \otimes \mathrm{id}_N),$$

whence $x \in \operatorname{Im}(f \otimes \mathrm{id}_N)$. So $\operatorname{Ker}(g \otimes \mathrm{id}_N) \subseteq \operatorname{Im}(f \otimes \mathrm{id}_N)$, and we have shown that

$$\operatorname{Ker}(g \otimes \mathrm{id}_N) = \operatorname{Im}(f \otimes \mathrm{id}_N).$$

We have proved that the sequence (6.8) is exact. □

Now we will show that if $R$ and $S$ are idempotent rings, then the tensor product of a firm right $R$-moodule and a unitary $(R, S)$-bimodule is a firm right $S$-module. Note that a bimodule is called **unitary** if it is unitary both as a left and right module.

**Proposition 6.37.** *Let $R$ and $S$ be idempotent rings, $M_R$ a firm $R$-module and ning ${}_RN_S$ a unitary $(R, S)$-bimodule. Then $M \otimes_R N$ is a firm right $S$-module.*

*Proof.* Let $R$ and $S$ be idempotent rings, $M_R \in \mathrm{Ob}(\mathsf{FMod}_R)$ and ${}_RN_S \in \mathrm{Ob}({}_R\mathsf{UMod}_S)$. We denote the composite

$$R \otimes_R N \otimes_S S \xrightarrow{\nu_N \otimes \mathrm{id}_S} N \otimes_S S \xrightarrow{\mu_N} N, \quad r \otimes n \otimes s \mapsto rns$$

by $\mathbf{m}_N$. Since ${}_RN_S$ is unitary, this mapping is surjective. Hence we can consider the short exact sequence

$$\{0\} \xrightarrow{\mathbf{0}} \operatorname{Ker}\mathbf{m}_N \xrightarrow{\iota_{\operatorname{Ker}\mathbf{m}_N}} R \otimes_R N \otimes_S S \xrightarrow{\mathbf{m}_N} N \xrightarrow{\mathbf{0}} \{0\},$$

where $\iota_{\operatorname{Ker}\mathbf{m}_N}$ is the inclusion mapping. By Theorem 6.36, we know that also the sequence

$$M \otimes_R \operatorname{Ker}\mathbf{m}_N \xrightarrow{\mathrm{id}_M \otimes \iota_{\operatorname{Ker}\mathbf{m}_N}} M \otimes_R R \otimes_R N \otimes_S S \xrightarrow{\mathrm{id}_M \otimes \mathbf{m}_N} M \otimes_R N \xrightarrow{\mathbf{0}} \{0\}.$$

is exact. From Lemma 6.33 we conclude that $R(\operatorname{Ker}(\mathbf{m}_N)) = \{0\}$. Consider an element $\sum_{h=1}^{h^*} m_h \otimes x_h \in M \otimes_R \operatorname{Ker}\mathbf{m}_N$. Since $M_R$ is unitary, there exists a number $j^* \in \mathbb{N}$ and for every $h \in \{1, \ldots, h^*\}$ there exist elements $m_{h1}, \ldots, m_{hj^*} \in M$ and $r_{h1}, \ldots, r_{hj^*} \in R$ such that $m_h = m_{h1}r_{h1} + \ldots + m_{hj^*}r_{hj^*}$. Now

$$\sum_{h=1}^{h^*} m_h \otimes x_h = \sum_{h=1}^{h^*}\sum_{j=1}^{j^*} m_{hj}r_{hj} \otimes x_h = \sum_{h=1}^{h^*}\sum_{j=1}^{j^*} m_{hj} \otimes r_{hj}x_h = \sum_{h=1}^{h^*}\sum_{j=1}^{j^*} m_{hj} \otimes 0 = 0.$$

Hence $M \otimes_R \operatorname{Ker}\mathbf{m}_N = \{0\}$, yielding that $\mathrm{id}_M \otimes \mathbf{m}_N$ is an isomorphism. Consider the commutative diagram

$$\begin{array}{ccc} M \otimes_R R \otimes_R N \otimes_S S & \xrightarrow{\mathrm{id}_M \otimes \mathbf{m}_N} & M \otimes_R N \\ & {\scriptstyle \mu_M \otimes \mathrm{id}_{N\otimes S}} \searrow \quad \nearrow {\scriptstyle \mu_{M\otimes N}} & \\ & M \otimes_R N \otimes_S S & \end{array}$$

Since $M_R$ is firm, $\mu_M$ is an isomorphism, hence also $\mu_M \otimes \mathrm{id}_{N\otimes S}$ is na isomorphism (by Corollary 6.19). Now we note that

$$\mu_{M\otimes N} = (\mu_M \otimes \mathrm{id}_{N\otimes S})^{-1} \circ (\mathrm{id}_M \otimes \mathbf{m}_N),$$

Whence $\mu_{M\otimes N}$ is also an isomorphism and $M \otimes_R N$ is a firm right $S$-module. □

# Chapter 7

# Morita theory

## 7.1 Definition of Morita equivalence

The starting point of Morita theory is an article "Duality for modules and its applications to the theory of rings with minimum condition" (1958) by Kiiti Morita[1] He defined a certain equivalence relation on the class of all rings with identity, which later has been termed 'Morita equivalence relation'. Morita theory has been very fruitful. By now it has been developed for a large variety of algebraic structures, including rings without identity, monoids, semigroups, semirings, small categories, quantales, C*-algebras etc.

In this chapter, if we speak about rings with identity, then we will assume that the identity is not zero.

**Definition 7.1.** Two rings with identity $R$ and $S$ are called **Morita equivalent** if a category equivalence $\mathsf{UMod}_R \approx \mathsf{UMod}_S$ holds.

If $R$ and $S$ are Morita equivalent rings, then we write $R \approx_{\mathrm{ME}} S$.

It turns out that defining Morita equivalence of rings without identity using categories of unitary modules is not a very good idea (for the reasons that we will not explain here). However, there are other natural subcategories of $\mathsf{Mod}_R$ that can be used. One such subcategory is the category $\mathsf{FMod}_R$ of firm modules.

**Definition 7.2.** Two rings $R$ and $S$ are called **Morita equivalent** if a category equivalence $\mathsf{FMod}_R \approx \mathsf{FMod}_S$ holds.

**Remark 7.3.** 1. We have defined Morita equivalence using right modules. It can be shown that, for idempotent rings $R$ and $S$, $\mathsf{FMod}_R \approx \mathsf{FMod}_S$ if and only ${}_R\mathsf{FMod} \approx {}_S\mathsf{FMod}$.

2. Since category equivalence is an equivalence relation, also Morita equivalence is an equivalence relation on the class of all rings.

3. If two rings are isomorphic, then they are Morita equivalent. The converse is not true, so Morita equivalence relation is weaker than isomorphism relation.

4. From Corollary 6.28 we see that rings $R$ and $S$ with identity are Morita equivalent in the sense of Definition 7.1 if and only if they are Morita equivalent in the sense of Definition 7.2.

[1] Kiiti Morita (1915–1995) – a Japanese mathematician.

5. If $R$ and $S$ are arbitrary Morita equivalent rings, then it is rather difficult to say anything about them. However, for idempotent rings, quite a satisfactory Morita theory has been developed by now.

Some of the typical research problems in Morita theory are the following.

1. Try to give some alternative descriptions of Morita equivalence, which do not use the notion of equivalence functors. Usually, functors are difficult to use if we want to study some properties of rings which are defined in terms of its elements (e.g. regularity). In this course we will briefly consider two such descriptions: using Morita contexts and using enlargements.

2. For some 'nice' ring (e.g. a division ring), try to describe all rings in its Morita equivalence class.

3. A property, which is shared by all rings in the same Morita equivalence class, is called a **Morita invariant**. Which properties are Morita invariants on the class of idempotent rings, firm rings or rings with identity?

As an example, we give the following result.

**Proposition 7.4.** *Semisimplicity is a Morita invariant for rings with identity.*

*Proof.* Suppose that $R$ and $S$ are Morita equivalent rings with identity and $R$ is semisimple. Then $\mathsf{UMod}_R \approx \mathsf{UMod}_S$ and

$$\begin{aligned} R \text{ is semisimple} &\implies \text{all objects in } \mathsf{UMod}_R \text{ are projective} && \text{(Proposition 4.17)} \\ &\implies \text{all objects in } \mathsf{UMod}_S \text{ are projective} && \text{(Exercise 5.26)} \\ &\implies S \text{ is semisimple.} && \text{(Proposition 4.17)} \end{aligned}$$

□

## 7.2 Morita equivalence and Morita contexts

A very convenient tool for studying Morita equivalence is a Morita context.

**Definition 7.5.** A **Morita context** connecting two rings $R$ and $S$ is a six-tuple $(R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$, where ${}_RP_S$ and ${}_SQ_P$ are bimodules and

$$\theta\colon {}_R(P \otimes_S Q)_R \longrightarrow {}_RR_R \qquad \text{and} \qquad \phi\colon {}_S(Q \otimes_R P)_S \longrightarrow {}_SS_S$$

are bimodule homomorphisms such that, for every $p, p' \in P$ and $q, q' \in Q$,

$$\theta(p \otimes q)p' = p\phi(q \otimes p'), \tag{7.1}$$
$$q'\theta(p \otimes q) = \phi(q' \otimes p)q. \tag{7.2}$$

**Definition 7.6.** A Morita context $(R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$ is called

- **unitary** (**firm**), if the bimodules ${}_RP_S$ and ${}_SQ_R$ are unitary (firm);
- **surjective** (**bijective**), if the homomorphisms $\theta$ are $\phi$ surjective (bijective).

**Example 7.7** (Morita context)**.** Let $R$ be a ring and $e \in R$ an idempotent. Then $eRe = \{ere \mid r \in R\}$ is a ring with identity $e = eee \in eRe$. It is called a local subring of $R$. Consider the six-tuple

$$\Gamma = (R, eRe, {}_RRe_{eRe}, {}_{eRe}eR_R, \theta, \phi),$$

where the acions on modules ${}_RRe_{eRe}$ and ${}_{eRe}eR_R$ are defined using the multiplication of the ring $R$ (e.g. $re \cdot er'e := reer'e = rer'e$) and

$$\theta\colon\ Re \otimes_{eRe} eR \longrightarrow R, \qquad \sum_{k=1}^{k^*} r_k e \otimes er'_k \mapsto \sum_{k=1}^{k^*} r_k e r'_k,$$

$$\phi\colon\ eR \otimes_R Re \longrightarrow eRe, \qquad \sum_{k=1}^{k^*} er_k \otimes r'_k e \mapsto \sum_{k=1}^{k^*} er_k r'_k e.$$

It is easy to see that $\theta$ and $\phi$ are bimodule homomorphisms. Note that, for every $re, r'e \in Re$ and $e\rho, e\rho' \in eR$,

$$\theta(re \otimes e\rho)r'e = (re\rho)r'e = ree\rho r'e = re(e\rho r'e) = re\phi(e\rho \otimes r'e),$$
$$e\rho'\theta(re \otimes e\rho) = e\rho'(re\rho) = e\rho' ree\rho = (e\rho' re)e\rho = \phi(e\rho' \otimes re)e\rho.$$

Hence $\Gamma$ is a Morita context. As we see, every idempotent of $R$ gives rise to a Morita context.

If $R$ is an idempotent ring, then $Re = RRee \subseteq R(Re)$ and $Re \subseteq (Re)(eRe)$, so $Re$ – and similarly $eR$ – is a unitary bimodule. In that case $\phi$ is surjective. If $e$ is a full idempotent ($R = ReR$), then $\theta$ is also surjective. Moreover, if $R$ has a full idempotent, then $R$ is idempotent ($R = ReR \subseteq RR$). In conclusion, if $e$ is a full idempotent, then the Morita context $\Gamma$ is unitary and surjective.

**Proposition 7.8.** *Any unitary and surjective Morita context between rings with is identity is bijective.*

*Proof.* Let $(R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$ be a surjective Morita context, where $R$ and $S$ are rings with identity. We will prove that $\theta$ is injective (for $\phi$ the proof is similar). We must show that $\mathrm{Ker}(\theta) = 0$. Take any $\sum_{k=1}^{k^*} p_k \otimes q_k \in \mathrm{Ker}(\theta)$. Then

$$\sum_{k=1}^{k^*} \theta(p_k \otimes q_k) = 0. \tag{7.3}$$

Since $\theta$ is surjective, there exists $\sum_{l=1}^{l^*} p'_l \otimes q'_l \in P \otimes_S Q$ such that $1_R = \sum_{l=1}^{l^*} \theta(p'_l \otimes q'_l)$.

Now

$$\begin{aligned}
\sum_{k=1}^{k^*} p_k \otimes q_k &= \sum_{k=1}^{k^*} p_k \otimes q_k 1_R && (Q_R \text{ is unitary}) \\
&= \sum_{k=1}^{k^*} p_k \otimes q_k \sum_{l=1}^{l^*} \theta(p'_l \otimes q'_l) \\
&= \sum_{k=1}^{k^*} \sum_{l=1}^{l^*} p_k \otimes q_k \theta(p'_l \otimes q'_l) && (\text{Proposition } 6.5(2)) \\
&= \sum_{k=1}^{k^*} \sum_{l=1}^{l^*} p_k \otimes \phi(q_k \otimes p'_l) q'_l && (\text{by } (7.2)) \\
&= \sum_{l=1}^{l^*} \sum_{k=1}^{k^*} p_k \phi(q_k \otimes p'_l) \otimes q'_l && (\text{Proposition } 6.5(3)) \\
&= \sum_{l=1}^{l^*} \left( \sum_{k=1}^{k^*} \theta(p_k \otimes q_k) \right) p'_l \otimes q'_l && (\text{by } (7.1)) \\
&= \sum_{l=1}^{l^*} 0_R p'_l \otimes q'_l && (\text{by } (7.3)) \\
&= \sum_{l=1}^{l^*} 0_P \otimes q'_l \\
&= 0. && (\text{Proposition } 6.5(4))
\end{aligned}$$

□

**Proposition 7.9.** *If $(R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$ is a unitary and surjective Morita context, then $S$ and $R$ are idempotent rings.*

*Proof.* Take an element $r \in R$. Due to surjectivity of $\theta$, there exists a tensor $\sum_{k=1}^{k^*} p_k \otimes q_k \in P \otimes_S Q$ such that $r = \theta(\sum_{k=1}^{k^*} p_k \otimes q_k)$. Since ${}_RP$ is unitary, for every $k \in \{1, \ldots, k^*\}$ there exist $p_{k1}, \ldots, p_{kh^*} \in P$ and $r_{k1}, \ldots, r_{kh^*} \in R$ such that $p_k = r_{k1}p_{k1} + \ldots + r_{kh^*}p_{kh^*}$. Now

$$\begin{aligned}
r = \theta \left( \sum_{k=1}^{k^*} p_k \otimes q_k \right) &= \sum_{k=1}^{k^*} \theta(p_k \otimes q_k) = \sum_{k=1}^{k^*} \theta \left( \sum_{h=1}^{h^*} r_{kh} p_{kh} \otimes q_k \right) \\
= \sum_{k=1}^{k^*} \sum_{h=1}^{h^*} \theta(r_{kh} p_{kh} \otimes q_k) &= \sum_{k=1}^{k^*} \sum_{h=1}^{h^*} r_{kh} \theta(p_{kh} \otimes q_k) \in RR.
\end{aligned}$$

We have shown that $R$ is idempotent. Analogously the ring $S$ is aslo idempotent. □

We show that every unitary and surjective Morita context induces equivalence functors between categories of firm modules.

**Theorem 7.10.** *Let $R$ and $S$ be rings and let $(R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$ be a unitary and surjective Morita context. Then the functors*

$$F := \_ \otimes_R P\colon\ \mathsf{FMod}_R \longrightarrow \mathsf{FMod}_S,$$
$$G := \_ \otimes_S Q\colon\ \mathsf{FMod}_S \longrightarrow \mathsf{FMod}_R$$

*are inverse equivalence functors.*

*Proof.* By Proposition 7.9, $R$ and $S$ are idempotent rings. Since the bimodules $P$ and $Q$ are unitary, we indeed have functors $\mathsf{FMod}_R \longrightarrow \mathsf{FMod}_S$ and $\mathsf{FMod}_S \longrightarrow \mathsf{FMod}_R$ by Lemma 6.37.

Consider a short exact sequence

$$\{0\} \xrightarrow{\mathbf{0}} \operatorname{Ker}\theta \xrightarrow{\iota_{\operatorname{Ker}\theta}} P \otimes_S Q \xrightarrow{\theta} R \xrightarrow{\mathbf{0}} \{0\}$$

of left $R$-modules and let $M_R \in \operatorname{Ob}(\mathsf{FMod}_R)$. By the dual of Theorem 6.36, the sequence

$$M \otimes_R \operatorname{Ker}\theta \xrightarrow{\mathrm{id}_M \otimes \iota_{\operatorname{Ker}\theta}} M \otimes_R P \otimes_S Q \xrightarrow{\mathrm{id}_M \otimes \theta} M \otimes_R R \xrightarrow{\mathbf{0}} \{0\}$$

is also exact. In particular, $\mathrm{id}_M \otimes \theta$ is surjective.

We will show that $M \otimes_R \operatorname{Ker}\theta = \{0\}$ (this will imply that $\mathrm{id}_M \otimes \theta$ is also injective). Let $\sum_{k=1}^{k^*} p_k \otimes q_k \in \operatorname{Ker}\theta$ and $r \in R$. Since $\theta$ is surjective, there exists $\sum_{h=1}^{h^*} p'_h \otimes q'_h \in P \otimes_S Q$ such that $r = \theta(\sum_{h=1}^{h^*} p'_h \otimes q'_h)$. Now

$$\begin{aligned}
\left(\sum_{k=1}^{k^*} p_k \otimes q_k\right) r &= \left(\sum_{k=1}^{k^*} p_k \otimes q_k\right)\theta\left(\sum_{h=1}^{h^*} p'_h \otimes q'_h\right) = \sum_{k=1}^{k^*}\sum_{h=1}^{h^*} p_k \otimes q_k\theta(p'_h \otimes q'_h) \\
&= \sum_{k=1}^{k^*}\sum_{h=1}^{h^*} p_k \otimes \phi(q_k \otimes p'_h)q'_h = \sum_{k=1}^{k^*}\sum_{h=1}^{h^*} p_k\phi(q_k \otimes p'_h) \otimes q'_h \\
&= \sum_{k=1}^{k^*}\sum_{h=1}^{h^*} \theta(p_k \otimes q_k)p'_h \otimes q'_h = \theta\left(\sum_{k=1}^{k^*} p_k \otimes q_k\right)\left(\sum_{h=1}^{h^*} p'_h \otimes q'_h\right) \\
&= 0\left(\sum_{h=1}^{h^*} p'_h \otimes q'_h\right) = 0.
\end{aligned}$$

Hence $(\operatorname{Ker}\theta)R = \{0\}$. Analogously, $R(\operatorname{Ker}\theta) = \{0\}$ and $S(\operatorname{Ker}\phi) = (\operatorname{Ker}\phi)S = \{0\}$.

Now let $\sum_{k=1}^{k^*} m_k \otimes t_k \in M \otimes_R \operatorname{Ker}\theta$. Since $M_R$ is firm and therefore also unitary, for every $k \in \{1, \ldots, k^*\}$ there exist $m_{k1}, \ldots, m_{kh^*} \in M$ and $r_{k1}, \ldots, r_{kh^*} \in R$ such that $m_k = m_{k1}r_{k1} + \ldots + m_{kh^*}r_{kh^*}$. Then

$$\begin{aligned}
\sum_{k=1}^{k^*} m_k \otimes t_k &= \sum_{k=1}^{k^*}\left(\sum_{h=1}^{h^*} m_{kh}r_{kh}\right) \otimes t_k \\
&= \sum_{k=1}^{k^*}\sum_{h=1}^{h^*} m_{kh} \otimes r_{kh}t_k && \text{(Proposition 6.5)} \\
&= \sum_{k=1}^{k^*}\sum_{h=1}^{h^*} m_{kh} \otimes 0 && \text{(since } R(\operatorname{Ker}\theta) = \{0\}\text{)} \\
&= 0. && \text{(Proposition 6.5)}
\end{aligned}$$

Hence $M \otimes_R \operatorname{Ker}\theta = \{0\}$. Lemma 2.3 implies that $\mathrm{id}_M \otimes\theta$ is an isomorphism.

For any $M'_R \in \mathrm{Ob}(\mathsf{FMod}_R)$ and $f \in \mathrm{Hom}_R(M, M')$ we consider the diagram

$$\begin{array}{ccc} M \otimes_R P \otimes_S Q & \xrightarrow{\mathrm{id}_M \otimes\theta} & M \otimes_R R \\ {\scriptstyle f \otimes \mathrm{id}_P \otimes \mathrm{id}_Q}\downarrow & & \downarrow{\scriptstyle f \otimes \mathrm{id}_R} \\ M' \otimes_R P \otimes_S Q & \xrightarrow[\mathrm{id}_{M'} \otimes\theta]{} & M' \otimes_R R \end{array} .$$

For every $\sum_{k=1}^{k^*} m_k \otimes p_k \otimes q_k \in M \otimes_R P \otimes_S Q$,

$$\begin{aligned} ((f \otimes \mathrm{id}_R) \circ (\mathrm{id}_M \otimes\theta)) \left( \sum_{k=1}^{k^*} m_k \otimes p_k \otimes q_k \right) &= \sum_{k=1}^{k^*} f(m_k) \otimes \theta(p_k \otimes q_k) \\ &= ((\mathrm{id}_{M'} \otimes\theta) \circ (f \otimes \mathrm{id}_P \otimes \mathrm{id}_Q)) \left( \sum_{k=1}^{k^*} m_k \otimes p_k \otimes q_k \right) . \end{aligned}$$

Thus we obtain a natural isomorphism $\mathrm{id} \otimes\theta \colon G \circ F \Rightarrow \_ \otimes_R R$. In the same manner we see that $\mathrm{id} \otimes\phi \colon F \circ G \Rightarrow \_ \otimes_S S$ is a natural isomorphism.

Definition of firmness and Lemma 6.25 imply that $\mu \colon \_ \otimes_R R \Rightarrow \mathrm{id}_{\mathsf{FMod}_R}$ is a natural isomorphism. Therefore also the vertical composite

$$\mu \circ (\mathrm{id} \otimes\theta) \colon G \circ F \Rightarrow \_ \otimes_R R \Rightarrow \mathrm{id}_{\mathsf{FMod}_R}$$

is a natural isomorphism. Similary we have a natural isomorphism $F \circ G \Rightarrow \mathrm{id}_{\mathsf{FMod}_S}$. Thus $G \circ F \cong \mathrm{id}_{\mathsf{FMod}_R}$ and $F \circ G \cong \mathrm{id}_{\mathsf{FMod}_S}$, as needed. □

Using Proposition 7.10 and Proposition 7.9 we obtain the following result.

**Corollary 7.11.** *If $R$ and $S$ are rings that are connected by a unitary and surjective Morita context, then these rings are idempotent and Morita equivalent.*

It can be shown (although this proof is much more complicated and we will not prove that in this course) that two idempotent Morita equivalent rings are connected by a unitary and surjective Morita contexts. Thus the following theorem holds.

**Theorem 7.12** (García and Simón 1991; Marín 1998)**.** *Two idempotent rings are Morita equivalent if and only if they are connected by a unitary and surjective Morita context.*

## 7.3 Enlargements of rings

Enlargements of rings are defined similarly to enlargements of semigroups, which were introduced by Mark Lawson in the article "Enlargements of regular semigroups" from 1996.

**Definition 7.13** (Laan and Väljako, 2021)**.** A ring $R$ is an **enlargement** of its subring $S$ if $R = RSR$ and $S = SRS$. Also, we say that $R$ is an enlargement of all the rings that are isomorphic to $S$.

If $R$ is an enlargement of $S$, then we write $S \sqsubseteq R$. Some of the basic properties of enlargments are the following.

**Proposition 7.14.** *If $R$ and $S$ are rings and $S \sqsubseteq R$, then the following assertions are true.*

1. *The ring $R$ is idempotent.*
2. *If $R$ is commutative, then $R \simeq S$.*
3. *If $S$ is an ideal of $R$, then $R = S$.*
4. *If $S = \{0\}$, then $R = \{0\}$.*

*Proof.* 1. Note that

$$R = RSR = R(SR) \subseteq RR \subseteq R.$$

Hence $RR = R$, which means that $R$ is an idempotent ring.

2. If $R$ is a commutative ring, then

$$R = RSR = RRS = RS = R(SRS) = SRRS = SRS = S.$$

(If $S' \cong S$, then we obtain $S' \cong R$.)

3. If $S \trianglelefteq R$, then

$$R = RSR \subseteq S \subseteq R.$$

Hence $R = S$.

4. This follows immediately from condition 3.

□

Next we consider enlargements of idempotent rings. Immediately from the definition of an enlargement we see that instead of proving four inclusions, verifying only two inclusions suffices.

**Lemma 7.15.** *Let $R$ and $S$ be idempotent rings such that $S$ is a subring of $R$. The ring $R$ is an enlargement of the ring $S$ if and only if $R \subseteq RSR$ and $SRS \subseteq S$.*

**Example 7.16** (Enlargement)**.** Let $S$ be an idempotent ring and $n \in \mathbb{N}$. The matrix ring $R := \mathrm{Mat}_n(S)$ is an enlargement of $S$.

Let $A_{hk}(s)$ denote the $(n \times n)$-matrix, which has $s$ at position $(h, k)$ and zero elsewhere. Then

$$S' := \{A_{11}(s) \mid s \in S\}$$

is an idempotent subring of $\mathrm{Mat}_n(S)$, which is isomorphic to $S$.

Let $s \in S$. Since $S$ is idempotent, we can write $s = \sum_{j=1}^{j^*} u_j s_j v_j$, where $u_j, s_j, v_j \in S$ for every $j$. Now

$$A_{hk}(s) = \sum_{j=1}^{j^*} A_{hk}(u_j s_j v_j) = \sum_{j=1}^{j^*} A_{h1}(u_j) \cdot A_{11}(s_j) \cdot A_{1k}(v_j) \in RS'R.$$

Since every matrix $A \in R$ can be presented as a sum of $n^2$ matrices of the form $A_{hk}(s)$, where $h, k \in \{1, \ldots, n\}$, we conclude that $R \subseteq RS'R$.

On the other hand, the inclusion $S'RS' \subseteq S'$ holds, because

$$A_{11}(s) \cdot A \cdot A_{11}(s') = A_{11}(sa_{11}s') \in S',$$

where $s, s' \in S$ and $A = [a_{hk}]_{h,k=1}^{n} \in \mathrm{Mat}_n(S)$.

Using Lemma 7.15, we see that $S \sqsubseteq \mathrm{Mat}_n(S)$.

## 7.4 Morita ring

It turns out that every Morita context induces a new ring in a natural way.

**Definition 7.17.** Let $\Gamma = (R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$ be a Morita context. The **Morita ring** $\overline{\Gamma}$ of the context $\Gamma$ is the matrix set

$$\overline{\Gamma} := \left\{ \begin{bmatrix} r & p \\ q & s \end{bmatrix} \middle| \, r \in R, s \in S, p \in P, q \in Q \right\},$$

together with componentwise addition and with multiplication

$$\begin{bmatrix} r & p \\ q & s \end{bmatrix} \begin{bmatrix} r' & p' \\ q' & s' \end{bmatrix} := \begin{bmatrix} rr' + \theta(p \otimes q') & rp' + ps' \\ qr' + sq' & \phi(q \otimes p') + ss' \end{bmatrix}. \tag{7.4}$$

Obviously, $\overline{\Gamma}$ is an abelian group. Straightforward verification shows that multiplication of $\overline{\Gamma}$ is associative and the distributivity laws hold. We show that the Morita ring $\overline{\Gamma}$ of a Morita context $\Gamma = (R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$ contains isomorphic copies of the structures $R$, $S$, ${}_RP_S$ and ${}_SQ_R$. Namely, the subsets

$$\overline{R} := \left\{ \begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix} \middle| \, r \in R \right\} \subseteq \overline{\Gamma},$$
$$\overline{S} := \left\{ \begin{bmatrix} 0 & 0 \\ 0 & s \end{bmatrix} \middle| \, s \in S \right\} \subseteq \overline{\Gamma}$$

are subrings of $\overline{\Gamma}$, which are isomorphic to rings $R$ and $S$, respectively. This enables us to consider the abelian group $\overline{\Gamma}$ as an $(R, S)$-bimodule and as an $(S, R)$-bimodule, if we define left $R$- and $S$-actions by

$$r' \begin{bmatrix} r & p \\ q & s \end{bmatrix} := \begin{bmatrix} r' & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} r & p \\ q & s \end{bmatrix} = \begin{bmatrix} r'r & r'p \\ 0 & 0 \end{bmatrix}, \tag{7.5}$$
$$s' \begin{bmatrix} r & p \\ q & s \end{bmatrix} := \begin{bmatrix} 0 & 0 \\ 0 & s' \end{bmatrix} \begin{bmatrix} r & p \\ q & s \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ s'q & s's \end{bmatrix}; \tag{7.6}$$

for every $r' \in R$, $s' \in S$ and $\left[\begin{smallmatrix} r & p \\ q & s \end{smallmatrix}\right] \in \overline{\Gamma}$; and right $R$- and $S$-actions analogously. It is easy to see that the mappings

$$\beta \colon P \longrightarrow \overline{\Gamma}, \quad p \mapsto \begin{bmatrix} 0 & p \\ 0 & 0 \end{bmatrix} \qquad \text{and} \qquad \gamma \colon Q \longrightarrow \overline{\Gamma}, \quad q \mapsto \begin{bmatrix} 0 & 0 \\ q & 0 \end{bmatrix}$$

are injective bimodule homomorphisms. Hence ${}_RP_S \cong \operatorname{Im}\beta =: {}_R\overline{P}_S$ and ${}_SQ_R \cong \operatorname{Im}\gamma =: {}_S\overline{Q}_R$. We see that all the information contained in the Morita context $\Gamma$ can also be found from the Morita ring $\overline{\Gamma}$.

**Exercise 7.18.** Prove that a distributivity law holds in for the ring $\overline{\Gamma}$.

## 7.5 Enlargements and Morita equivalence

In this section we see that enlargements of idempotent rings are closely related to Morita equivalence. First we show that if a ring $R$ is an enlargement of an idempotent ring $S$, then $R \approx_{\mathrm{ME}} S$.

**Proposition 7.19.** *If $R$ is an enlargement of an idempotent ring $S$, then the rings $R$ and $S$ are Morita equivalent.*

*Proof.* Let $S$ be an idempotent ring and assume that $S \sqsubseteq R$. Since isomorphic rings are Morita equivalent, we only consider the case $S \subseteq R$. Consider the subring

$$SR = \left\{ \sum_{k=1}^{k^*} s_k r_k \,\middle|\, k^* \in \mathbb{N}, s_k \in S, r_k \in R \right\} \subseteq R$$

as an $(S, R)$-bimodule and the subring $RS \subseteq R$ as an $(R, S)$-bimodule, where the actions are defined using the multiplication of $R$. Proposition 7.14(1) implies that the ring $R$ is idempotent. Hence the bimodules $SR$ and $RS$ are unitary.

It is easy to see that the mapping

$$\hat{\theta}\colon RS \times SR \longrightarrow R, \quad (\rho, \sigma) \mapsto \rho\sigma$$

is $S$-balanced. Since $SRS = S$, we also have an $R$-balanced mapping

$$\hat{\phi}\colon SR \times RS \longrightarrow S, \quad (\sigma, \rho) \mapsto \sigma\rho.$$

By the universal property of tensor products there exist group homomorphisms

$$\theta\colon \ RS \otimes_S SR \longrightarrow R, \qquad \rho \otimes \sigma \mapsto \rho\sigma, \tag{7.7}$$

$$\phi\colon \ SR \otimes_R RS \longrightarrow S, \qquad \sigma \otimes \rho \mapsto \sigma\rho. \tag{7.8}$$

For every $r \in R$, $\rho \in RS$ and $\sigma \in SR$,

$$\theta(r(\rho \otimes \sigma)) = \theta(r\rho \otimes \sigma) = (r\rho)\sigma = r(\rho\sigma) = r\theta(\rho \otimes \sigma)$$

and, analogously, $\theta((\rho \otimes \sigma)r) = \theta(\rho \otimes \sigma)r$. It follows that $\theta$ is a homomorphism of $(R, R)$-bimodules.

Take any $r \in R$. Since $S \sqsubseteq R$ and $S$ is idempotent, we have

$$R = RSR = R(SS)R = (RS)(RS).$$

Hence there exist $\rho_1, \ldots, \rho_{k^*} \in RS$ and $\sigma_1, \ldots, \sigma_{k^*} \in SR$ such that

$$r = \sum_{k=1}^{k^*} \rho_k \sigma_k = \theta\left( \sum_{k=1}^{k^*} \rho_k \otimes \sigma_k \right).$$

Therefore $\theta$ is surjective. Analogously, $\phi$ is a well-defined and surjective homomorphism of $(S, S)$-bimodules.

Finally, for every $\rho, \rho' \in RS$ and $\sigma, \sigma' \in SR$,

$$\theta(\rho \otimes \sigma)\rho' = (\rho\sigma)\rho' = \rho(\sigma\rho') = \rho\phi(\sigma \otimes \rho'),$$
$$\sigma'\theta(\rho \otimes \sigma) = \sigma'(\rho\sigma) = (\sigma'\rho)\sigma = \phi(\sigma' \otimes \rho)\sigma.$$

In conclusion, we have shown that $(R, S, RS, SR, \theta, \phi)$ is a unitary and surjective Morita context. By Theorem 7.12, $R \approx_{\mathrm{ME}} S$. □

**Corollary 7.20.** *Let $R$ be an idempotent ring and let $n \in \mathbb{N}$. The matrix ring $\mathrm{Mat}_n(R)$ is Morita equivalent to the ring $R$.*

**Definition 7.21.** A ring $T$ is called a **joint enlargement** of rings $R$ and $S$ if $T$ is an enlargement of both $S$ and $R$.

It turns out that Morita equivalent idempotent rings have a joint enlargement.

**Proposition 7.22.** *If idempotent rings $R$ and $S$ are connected by a unitary and surjective Morita context $\Gamma = (R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$, then the Morita ring $\overline{\Gamma}$ is a joint enlargement of $R$ and $S$. In particular, $\overline{\Gamma}$ is an idempotent ring.*

*Proof.* As we have mentioned above, the set

$$\overline{R} = \left\{ \begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix} \middle| r \in R \right\} \subseteq \overline{\Gamma}$$

is an idempotent subring of $\overline{\Gamma}$, which is isomorphic to the ring $R$. Hence $\overline{R} = \overline{R}\,\overline{R}, \overline{R} \subseteq \overline{R}\,\overline{\Gamma}\,\overline{R}$, and the inclusion $\overline{\Gamma}\,\overline{R}\,\overline{\Gamma} \subseteq \overline{\Gamma}$ is obvious. We will prove the inclusions

$$\overline{\Gamma} \subseteq \overline{\Gamma}\,\overline{R}\,\overline{\Gamma} \quad \text{and} \quad \overline{R}\,\overline{\Gamma}\,\overline{R} \subseteq \overline{R}.$$

Every matrix $\left[\begin{smallmatrix} r & p \\ q & s \end{smallmatrix}\right] \in \overline{\Gamma}$ can be presented as a sum

$$\begin{bmatrix} r & p \\ q & s \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & p \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ q & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & s \end{bmatrix}.$$

To prove the inclusion $\overline{\Gamma} \subseteq \overline{\Gamma}\,\overline{R}\,\overline{\Gamma}$ it suffices to show that the last four matrices belong to the set $\overline{\Gamma}\,\overline{R}\,\overline{\Gamma}$. For the matrix $\left[\begin{smallmatrix} r & 0 \\ 0 & 0 \end{smallmatrix}\right]$ this comes from the fact that $\overline{R} = \overline{RRR} \subseteq \overline{\Gamma R \Gamma}$. Consider an element $p \in P$. Since ${}_RP$ is unitary, we can find $p_1, \ldots, p_{k^*} \in P$ and $r_1, \ldots, r_{k^*} \in R$ such that $p = r_1p_1 + \ldots + r_{k^*}p_{k^*}$. Hence we have

$$\begin{bmatrix} 0 & p \\ 0 & 0 \end{bmatrix} = \sum_{k=1}^{k^*} \begin{bmatrix} r_k & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & p_k \\ 0 & 0 \end{bmatrix} \in \overline{R}\,\overline{\Gamma} = \overline{R}\,\overline{R}\,\overline{\Gamma} \subseteq \overline{\Gamma}\,\overline{R}\,\overline{\Gamma}.$$

Analogously we see that, for every $q \in Q$, $\left[\begin{smallmatrix} 0 & 0 \\ q & 0 \end{smallmatrix}\right] \in \overline{\Gamma}\,\overline{R}\,\overline{\Gamma}$. For the element $s \in S$, there exists $\sum_{k=1}^{k^*} q_k \otimes p_k \in Q \otimes_R P$, such that $s = \phi(\sum_{k=1}^{k^*} q_k \otimes p_k)$, because $\phi$ is surjective. Hence

$$\begin{bmatrix} 0 & 0 \\ 0 & s \end{bmatrix} = \sum_{k=1}^{k^*} \begin{bmatrix} 0 & 0 \\ 0 & \phi(q_k \otimes p_k) \end{bmatrix} = \sum_{k=1}^{k^*} \begin{bmatrix} 0 & 0 \\ q_k & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & p_k \\ 0 & 0 \end{bmatrix} \in \overline{\Gamma}(\overline{\Gamma}\,\overline{R}\,\overline{\Gamma}) \subseteq \overline{\Gamma}\,\overline{R}\,\overline{\Gamma}.$$

We have proved the inclusion $\overline{\Gamma} \subseteq \overline{\Gamma}\,\overline{R}\,\overline{\Gamma}$.

Note that, for every $r, r', r'' \in R$, $s \in S$, $q \in Q$ and $p \in P$,

$$\begin{bmatrix} r' & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} r & p \\ q & s \end{bmatrix} \cdot \begin{bmatrix} r'' & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} r'r & r'p \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} r'' & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} r'rr'' & 0 \\ 0 & 0 \end{bmatrix} \in \overline{R},$$

which implies $\overline{R}\,\overline{\Gamma}\,\overline{R} \subseteq \overline{R}$. Using Lemma 7.15, we see that $R \cong \overline{R} \sqsubseteq \overline{\Gamma}$. Using that $S \cong \{\left[\begin{smallmatrix} 0 & 0 \\ 0 & s \end{smallmatrix}\right] \mid s \in S\} \subseteq \overline{\Gamma}$, one can similarly prove that $S \sqsubseteq \overline{\Gamma}$. □

Now we are ready to prove the main theorem of this section.

**Theorem 7.23** (Laan and Väljako, 2021)**.** *Two idempotent rings are Morita equivalent if and only if they have a joint enlargement.*

*Proof.* NECESSITY. If idempotent rings $R$ and $S$ are Morita equivalent, then by Theorem 7.12 there exist a unitary and surjective Morita context $\Gamma$ connecting them. The Morita ring $\overline{\Gamma}$ is a joint enlargement of $R$ and $S$ due to Proposition 7.22.
SUFFICIENCY. If idempotent rings $R$ and $S$ have a joint enlargement $T$, then by Proposition 7.19 we have $T \approx_{\mathrm{ME}} R$ and $T \approx_{\mathrm{ME}} S$. Since Morita equivalence relation is symmetric and transitive, we have $R \approx_{\mathrm{ME}} S$. □

**Corollary 7.24.** *The only idempotent ring, which is Morita equivalent to zero ring* $\{0\}$*, is* $\{0\}$ *itself.*

*Proof.* Let $R$ be an idempotent ring and $R \approx_{\mathrm{ME}} \{0\}$. By Theorem 7.23, the rings $\{0\}$ and $R$ have a joint enlargement $T$. Proposition 7.14(2) implies $T = \{0\}$. Hence $R = \{0\}$. □

## 7.6 The case of rings with identity

Recall that an idempotent $e$ in a ring $S$ is called a **full idempotent** if $S = SeS$.

**Theorem 7.25.** *Let $S$ and $T$ be rings with identity. Then $S$ and $T$ are Morita equivalent if and only if there exists $n \in \mathbb{N}$ and a full idempotent $e \in \mathrm{Mat}_n(S)$ such that $T \cong e(\mathrm{Mat}_n(S))e$.*

Necessity part of this theorem is complicated, but sufficiency follows easily from our earlier results. We will demonstrate this.

Assume that there exists $n \in \mathbb{N}$ and a full idempotent $e \in \mathrm{Mat}_n(S)$ such that $T \cong e(\mathrm{Mat}_n(S))e$. Denote $R := \mathrm{Mat}_n(S)$. Then $R = ReR$. We claim that $R$ is an enlargement of its local subring $eRe$. Indeed,

$$R(eRe)R = (ReR)eR = ReR = R,$$
$$(eRe)R(eRe) = e(ReR)eRe = eReRe = eRe.$$

The ring $eRe$ has an identity element $e$, hence it is an idempotent ring. Now Proposition 7.19 implies that

$$R \approx_{\mathrm{ME}} eRe \simeq T,$$

so $R \approx_{\mathrm{ME}} T$.

**Corollary 7.26.** *Let $S$ be a ring with identity and $n \in \mathbb{N}$. The rings $S$ and $\mathrm{Mat}_n(S)$ are Morita equivalent.*

*Proof.* We apply Theorem 7.25 for the full idempotent $1_S \in S$. □

## 7.7 Ideals and Morita contexts

The set $\mathrm{Id}(R)$ of all ideals of a ring $R$ with identity is a poset with respect to inclusion relation $\subseteq$. Moreover, it is a lattice, where

$$I \wedge J = I \cap J,$$
$$I \vee J = I + J$$

for every $I, J \in \mathrm{Id}(R)$.

**Theorem 7.27.** *If two rings $R$ and $S$ with identity are Morita equivalent, then the lattices of their ideals are isomorphic.*

*Proof.* If $R \approx_{\mathrm{ME}} S$, then we know that there exists a unitary and surjective Morita context $(R, S, {}_RP_S, {}_SQ_R, \theta, \phi)$. If $X$ is a subset of the tensor product $P \otimes_S Q$, then by $\theta(X)$ we will denote the set $\{\theta(x) \mid x \in X\} \subseteq R$.

For any ideal $J \in \mathrm{Id}(S)$, consider the set

$$PJ \otimes_S Q := \left\{ \sum_{k=1}^{k^*} p_k j_k \otimes q_k \,\middle|\, \forall k\colon\ p_k \in P,\, j_k \in J,\, q_k \in Q \right\} \subseteq P \otimes_S Q$$

The set

$$\theta(PJ \otimes_S Q) := \left\{ \theta\left( \sum_{k=1}^{k^*} p_k j_k \otimes q_k \right) \,\middle|\, \forall k\colon\ p_k \in P,\, j_k \in J,\, q_k \in Q \right\} \subseteq R$$

is an ideal, because $\theta$ is a homomorphism of $(R, R)$-bimodules. Analogously one can show that, for every $I \in \mathrm{Id}(R)$, the set $\phi(QI \otimes_R P)$ is an ideal of the ring $S$. This allows to define the mappings

$$\Theta\colon\ \mathrm{UId}(S) \longrightarrow \mathrm{UId}(R), \qquad \Theta(J) := \theta(PJ \otimes_S Q), \tag{7.9}$$
$$\Phi\colon\ \mathrm{UId}(R) \longrightarrow \mathrm{UId}(S), \qquad \Phi(I) := \phi(QI \otimes_R P). \tag{7.10}$$

Let $J_1, J_2 \in \mathrm{Id}(S)$ be such that $J_1 \subseteq J_2$. Then $PJ_1 \subseteq PJ_2$ and

$$\Theta(J_1) = \theta(PJ_1 \otimes_S Q) \subseteq \theta(PJ_2 \otimes_S Q) = \Theta(J_2),$$

which means that $\Theta$ preserves the order relation. Analogously $\Phi$ preserves the order relation. For every $J \in \mathrm{Id}(S)$,

$$\begin{aligned}
\Phi(\Theta(J)) &= \phi(Q\theta(PJ \otimes_S Q) \otimes_R P) && \text{(def. of } \theta, \phi) \\
&= \phi(\phi(Q \otimes_R PJ)Q \otimes_R P) && \text{(property (7.2))} \\
&= \phi(Q \otimes_R P)J\phi(Q \otimes_R P) && (\phi \text{ is a homomorphism}) \\
&= SJS && (\phi \text{ is surjective}) \\
&= J. && (J \text{ is an ideal and } S \text{ has identity})
\end{aligned}$$

Analogously $\Theta(\Phi(I)) = I$ for every $I \in \mathrm{Id}(R)$. So $\Theta$ and $\Phi$ are inverses of each other. Hence $\Theta$ and $\Phi$ are isomorphisms of posets. It follows that $\Theta$ and $\Phi$ preserve all joins and meets, so they are lattice isomorphisms. □

**Corollary 7.28.** *Let $R$ be a ring with identity and $n \in \mathbb{N}$. The lattices* $\mathrm{Id}(R)$ *and* $\mathrm{Id}(\mathrm{Mat}_n(R))$ *are isomorphic.*

*Proof.* Let $R$ be a ring with identity. Then $\mathrm{Mat}_n(R)$ is also a ring with identity. By Corollary 7.26, $R \approx_{\mathrm{ME}} \mathrm{Mat}_n(R)$, and Theorem 7.27 implies that $\mathrm{Id}(R)$ and $\mathrm{Id}(\mathrm{Mat}_n(R))$ are isomorphic lattices. □

From Theorem 7.27 it follows that every property of rings with identity, which is defined in terms of the ideal lattice, is a Morita invariant. One such property, for example, is simplicity, which means that $\mathrm{Id}(R)$ is a two-element chain.

**Corollary 7.29.** *Simplicity is a Morita invariant for rings with identity.*

## Acknowledgements

A big part of these lecture notes is based on **Kristo Väljako**'s manuscript [3]. Other parts have been prepared using materials from the list of bibliography.

During this lecture course, several students helped to improve the quality of these lecture notes. My special thanks go to **Nikita Leo** for very careful reading and for numerous suggestions, including those providing shorter and more elegant proofs of some results.

# Bibliography

[1] F.W. Anderson, K.R. Fuller, Rings and categories of modules, Springer-Verlag, 1992.

[2] R. Wisbauer, Foundations of module and ring theory, Gordon and Breach Science Publishers, 1991.

[3] K. Väljako, Idempotentsete ringide Morita ekvivalentsus, 2023, manuscript.

[4] M. Kilp, Algebra II, Tartu, 1998.

[5] W.K. Nicholson, A short proof of the Wedderburn–Artin theorem, New Zealand J. Math. 22 (1993), 83–86.

# Appendix A

# Zorn's lemma

Recall some defintions.

**Definition A.1.** A **chain** in a poset $(P, \leq)$ is a subset $S \subseteq P$ such that

$$(\forall a, b \in S)(a \leq b \text{ or } b \leq a)$$

(that is, any two elements of $S$ are comparable).

**Definition A.2.** An element $a$ of a poset $(P, \leq)$ is called

- a **maximal element** if

$$(\forall b \in P)(a \leq b \implies a = b);$$

- the **greatest element** if $b \leq a$ for all $b \in P$.

Dually one can define minimal elements and the smallest element.

**Definition A.3.** An element $a$ of a poset $(P, \leq)$ is called an **upper bound** of a subset $X \subseteq P$ if $x \leq a$ for every $x \in X$. The **least upper bound** (or the **join**) of $X$ is an upper bound of $X$ which is the smallest element in the set of all upper bounds of $X$. In that case one writes $a = \vee X$. If $X = \{x, y\}$, then $a = x \vee y$ is written.

**Zorn's lemma.** *Suppose a non-empty poset $P$ has the property that every non-empty chain has an upper bound in $P$. Then the set $P$ contains at least one maximal element.*