Chapter 3
Commutative Monoids, Noncommutative Rings and Modules

Alberto Facchini

Abstract These are the notes of a non-standard course of Algebra. It deals with elementary theory of commutative monoids and non-commutative rings. Most of what is taught in a master course of Commutative Algebra holds not only for commutative rings, but more generally for any commutative monoid, which shows that the additive group structure on a commutative ring has little importance.

In the rest of the notes of the course presented here, we introduce the basic notions of non-commutative rings and their modules, stressing the difference with what happens in the case of commutative rings.

Keywords Commutative monoid · Preordered abelian group · Associative ring · Module over a ring

Math. Subj. Classification: 06F05 · 16-01 · 16Dxx · 20Mxx

Introduction

These are the notes of a course I gave in Louvain-la-Neuve in September 2018. It is a non-standard course of Algebra. It contains some topics that are not usually taught in master courses in Mathematics. The first topic is the elementary theory of commutative monoids. It is very standard to teach a course of Commutative Algebra, teaching commutative rings and modules over them (localization at prime ideals, and so on). But most things taught in those courses hold not only for commutative rings, but more generally for any commutative monoid. This occurs from the most elementary things (prime ideals, localizations, spectrum of the ring), to more "advanced" topics (valuations, Krull domains/monoids, divisorial ideals, class group). In other words, the additive group structure on a commutative ring is of little consequence.

A. Facchini (✉)
Dipartimento di Matematica "Tullio Levi-Civita", Università di Padova, Via Trieste 63,
35121 Padova, Italy
e-mail: facchini@math.unipd.it

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

M. M. Clementino et al. (eds.), *New Perspectives in Algebra, Topology and Categories*, Coimbra Mathematical Texts 1,
https://doi.org/10.1007/978-3-030-84319-9_3

The promoter of this idea was Chouinard [5]. In this topic, what I present is very easy, but not so much known among mathematicians.

Then I pass to a quick introduction to the theory of non-commutative rings, their modules, and Grothendieck group. My main aim, as far as non-commutative rings and their modules are concerned, is to stress the points where their properties differ from those of modules over commutative rings. The path I follow explaining the various topics is also partially non-standard, and relies on my personal taste.

I don't give most proofs. The interested reader can find them in several text books. For examples, for further notions about commutative monoids, one can see the books [6] and [13]. For non-commutative rings the best text books are [2] and [14]. My books [7] and [8] are also a possible reference.

1 Commutative Monoids

One of the structures in which we can come across most frequently in Algebra is the structure of monoid.

1.1 Commutative Monoids and Their Morphisms

An *(additive) monoid* M is a set with an operation (addition)

$$+\colon M \times M \to M, \qquad (x, y) \mapsto x + y,$$

which is associative (that is, $x + (y + z) = (x + y) + z$ for every $x, y, z \in M$) and has a *zero element*, usually denoted by 0, that is, an element $0 \in M$ such that $x + 0 = 0 + x = x$ for every $x \in M$. In these notes, all the monoids we will consider will be commutative, that is, $x + y = y + x$ for every $x, y \in M$. In other words, "monoid" and "commutative monoid" will have the same meaning for us.

A *monoid morphism* is a mapping f of a monoid M into a monoid N such that $f(0) = 0$ and $f(x + y) = f(x) + f(y)$ for every $x, y \in M$. The composite mapping of two monoid morphisms is a monoid morphism. Thus we have a category of commutative monoids, which we will denote by CMon.

Monomorphisms in the category CMon (that is, the morphisms $f\colon M \to N$ such that, for every pair $g, h\colon P \to M$ of monoid morphisms, $fg = fh$ implies $g = h$) are exactly the monoid morphisms that are injective mappings. This is not the case for epimorphisms: not all epimorphisms in CMon (that is, the morphisms $f\colon M \to N$ such that, for every pair $g, h\colon N \to P$ of monoid morphisms, $gf = hf$ implies $g = h$) are necessarily onto mappings. It is sufficient to consider the inclusion of the monoid $\mathbb{N}_0$ of non-negative integers into the additive monoid $\mathbb{Z}$ of integers, which is a non-surjective epimorphism.

A subset N of a commutative additive monoid M is a *submonoid* of M if it is closed under the addition of M and contains the zero element of M. For a monoid M, the set of all elements $a \in M$ with an opposite in M will be denoted by $U(M)$, that is, $U(M) := \{\, x \in M \mid \text{there exists } y \in M \text{ with } x + y = 0 \,\}$. If such an element $y \in M$ exists, it is unique, is denoted by $-x$, and is called the *opposite* of x. The subset $U(M)$ turns out to be a submonoid of M, and is an abelian group, often (improperly) called the *group of units* of M. The monoid M is *reduced* if $U(M) = \{0\}$, that is, if $x + y = 0$ implies $x = y = 0$ for every $x, y \in M$.

1.2 Preorders

A *preorder* on a set A is a relation on A that is reflexive and transitive. We will denote by Preord the category of all preordered sets. Its objects are the pairs (A, ρ), where A is a set and ρ is a preorder on A. The morphisms $f : (A, \rho) \to (A', \rho')$ in Preord are the mappings f of A into A' such that $a\rho b$ implies $f(a)\rho' f(b)$ for all $a, b \in A$. As usual, when there is no danger of confusion, that is, when the preorder is clear from the context, we will denote the preordered set (A, ρ) simply by A.

The main examples of preordered sets (A, ρ) are those in which the preorder ρ is a partial order (i.e., ρ is antisymmetric) or an equivalence relation (i.e., ρ is symmetric). The full subcategories of Preord whose objects are all preordered sets (A, ρ) with ρ a partial order (an equivalence relation) will be denoted by ParOrd (Equiv, respectively).

Proposition 1.1 *Let A be a set. There is a one-to-one correspondence between the set of all preorders ρ on A and the set of all pairs $(\sim, \leq)$, where $\sim$ is an equivalence relation on A and $\leq$ is a partial order on the quotient set $A/\!\sim$. The correspondence associates with every preorder ρ on A the pair $(\simeq_\rho, \leq_\rho)$, where $\simeq_\rho$ is the equivalence relation defined, for every $a, b \in A$, by $a \simeq_\rho b$ if $a\rho b$ and $b\rho a$, and $\leq_\rho$ is the partial order on $A/\!\simeq_\rho$ defined, for every $a, b \in A$, by $[a]_{\simeq_\rho} \leq_\rho [b]_{\simeq_\rho}$ if $a\rho b$. Conversely, for any pair $(\sim, \leq)$ with $\sim$ an equivalence relation on A and $\leq$ a partial order on $A/\!\sim$, the corresponding preorder $\rho_{(\sim,\leq)}$ on A is defined, for every $a, b \in A$, by $a\rho_{(\sim,\leq)}b$ if $[a]_\sim \leq [b]_\sim$.*

The objects of Preord that are objects in both the full subcategories ParOrd and Equiv are the objects of the form $(A, =)$, where $=$ denotes the equality relation on A. The pair (Equiv,ParOrd) is a pretorsion theory in Preord in the sense of [9].

The category of finite preordered sets is isomorphic to the category of finite topological spaces, the full subcategory of Top whose objects are the topological spaces with only finitely many points. (If X is a finite topological space, the corresponding preorder $\leq$ on X is defined by $x \leq y$ if and only if x belongs to the closure of the subset $\{y\}$ of X. Every closed set in a finite topological space X is a union of closures of points.)

More generally, the category of preordered sets is isomorphic to the category of Alexandrov topological spaces, the full subcategory of Top whose objects are the topological spaces whose topology is an Alexandrov topology. A topology is *Alexandrov* if the intersection of any family of open subsets is an open set (equivalently, if the union of any family of closed subsets is a closed subset).

If M is a commutative additive monoid, a preorder $\leq$ on M is *translation-invariant* if, for every $x, y, z \in M$, $x \leq y$ implies $x + z \leq y + z$. There is a natural translation-invariant preorder on any commutative additive monoid M, called the *algebraic preorder* on M, defined, for all $x, y \in M$, by $x \leq y$ if there exists $z \in M$ such that $x + z = y$. If x is an element of a monoid M and $n \geq 0$, we can inductively define the *n-th multiple nx* of x setting $0x := 0$ and $nx := (n-1)x + x$. An element u of a commutative monoid M is an *order-unit* if for every $x \in M$ there exists an integer $n \geq 0$ such that $x \leq nu$. For example, let M be the monoid $\mathbb{N}_0^n$ of all n-tuples of non-negative integers. The algebraic preorder on M is the component-wise order, that is, $(x_1, \dots, x_n) \leq (y_1, \dots, y_n)$ if and only if $x_i \leq y_i$ for every $i = 1, \dots, n$, and an element $(u_1, \dots, u_n)$ of $\mathbb{N}_0^n$ is an order-unit if and only if $u_i > 0$ for every $i = 1, \dots, n$.

A submonoid N of a monoid M is said to be *divisor-closed* if $x \in M$, $y \in N$, and $x \leq y$ in the algebraic preorder $\leq$ of M, implies $x \in N$. The term "divisor-closed" becomes clear if we move on to the multiplicative notation. More precisely, if the operation in the commutative monoid M is denoted as multiplication instead of addition, then the algebraic preorder on M is the relation | (divides), and a submonoid N of M is divisor-closed if, for every element $y \in N$, it contains all divisors of y in M. The group of units $U(M)$ of an arbitrary commutative monoid M is a divisor-closed submonoid of M contained in all divisor-closed submonoids of M.

Let X be a subset of a monoid M. Let $\mathcal{F}$ be the family of all submonoids of M that contain X. The family $\mathcal{F}$ is always non-empty, because $M \in \mathcal{F}$. The intersection of all the submonoids in $\mathcal{F}$ is the smallest submonoid of M that contains X. It is called the submonoid of M *generated* by X and is denoted by $[X]$. It is easily seen that if $X = \emptyset$, then $[X] = \{0\}$, the zero submonoid of M. If $X \neq \emptyset$, then $[X] = \{\, x_1 + \dots + x_n \mid n \geq 0 \text{ and } x_i \in X \text{ for } i = 1, \dots, n \,\}$ (sums of finitely many elements of X, possibly with repetitions). Conventionally, the sum of zero elements of M, that is, the sum of no element of M, is the zero element of M.

A subset X of a monoid M is a *set of generators* of M if $[X] = M$. A monoid M is *finitely generated* if it has a finite set of generators, and *cyclic* if it has a set of generators with one element.

1.3 Congruences

If $f : M \to N$ is a monoid morphism, the *kernel pair* of f is the equivalence relation $\sim_f$ on the set M defined, for every $x, y \in M$, by $x \sim_f y$ if $f(x) = f(y)$.

A *congruence* on a monoid M is an equivalence relation $\sim$ on the set M such that $x \sim y$ and $z \sim w$ implies $x + z \sim y + w$ for every $x, y, z, w \in M$. Equivalently, an equivalence relation $\sim$ on a monoid M is a congruence if $x \sim y$ implies $x + z \sim$

$y + z$ for every $x, y, z \in M$. It is easily verified that the kernel pair $\sim_f$ of any monoid morphism $f: M \to N$ is a congruence on the monoid M.

If M is a monoid and $\sim$ is a congruence on M, the *factor monoid* $M/\sim$ is the set of all *congruence classes* $[x]_\sim := \{\, y \in M \mid y \sim x \,\}$, where x ranges in M, with the addition inherited from that of M:

$$[x]_\sim + [y]_\sim := [x + y]_\sim \quad \text{for every } x, y \in M.$$

This operation on $M/\sim$ is well defined, as is easily verified. It is the unique operation on the quotient set $M/\sim$ which makes the *canonical projection* $\pi: M \to M/\sim$, defined by $\pi(x) = [x]_\sim$ for every $x \in M$, a monoid morphism. Every congruence on a monoid is the kernel pair of a monoid morphism.

A subset P of $M \times M$ is a *set of generators* for a congruence $\sim$ of the monoid M if the intersection of all congruences of M that contain P is $\sim$. A congruence $\sim$ on a monoid M is *finitely generated* if it has a finite set of generators.

An element x of a monoid M is said to be *idempotent* if $x + x = x$. A monoid M is *archimedean* if for every pair (x, y) of elements of M with $y \not\leq 0$ there exists a positive integer n such that $x \leq ny$. Equivalently, this means that M is either $\{0\}$ or has exactly two divisor closed submonoids. More generally, for any x, y in a commutative monoid M, define $x \asymp y$ if there exist positive integers n and m such that $x \leq ny$ and $y \leq mx$. It is easy to prove that $\asymp$ is the smallest congruence on M such that every element in the quotient monoid $M/\asymp$ is idempotent. The equivalence classes of M modulo $\asymp$ are additively closed subsets of M, called the *archimedean components* of M.

Here is another important example of congruence. Recall that, for any monoid M, $U(M)$ denotes the abelian additive group of all the elements of M with an opposite in M. The relation $\sim$ on M, defined, for every $x, y \in M$, by $x \sim y$ if there exists $z \in U(M)$ with $x = y + z$, turns out to be a congruence on M. The congruence class $[x]_\sim$ is the *coset* $x + U(M) := \{\, x + z \mid z \in U(M) \,\}$. We will denote by M_{red} the factor monoid $M/\sim$. The monoid M_{red} is always a reduced monoid, i.e., does not have non-zero elements with an opposite element. Thus every commutative monoid M is an extension of the reduced monoid M_{red} by the abelian group $U(M)$. Again, we have a pretorsion theory in the category CMon. The torsion class is the class of abelian groups. The torsionfree class is the class of all reduced commutative monoids.

As a further example of congruence, define an equivalence $\sim$ on any commutative monoid M, setting, for every $x, y \in M$, $x \equiv y$ if there exists $z \in M$ with $x + z = y + z$. It is easily seen that $\equiv$ is a congruence on M, called the *stable congruence*, and that the factor monoid $M/\equiv$ is a cancellative monoid. Recall that a monoid N is *cancellative* if $x + z = y + z$ implies $x = y$ for every $x, y, z \in N$. Hence $\equiv$ is the smallest congruence on M with $M/\equiv$ cancellative.

1.4 The Additive Monoid $\mathbb{N}_0$ of Natural Numbers

Consider the additive monoid $\mathbb{N}_0$ whose elements are the natural numbers $0, 1, 2, \dots$ Fix k and n in $\mathbb{N}_0$ with $n \geq 1$, and define the relation $\sim_{k,n}$ on $\mathbb{N}_0$ setting, for every $x, y \in \mathbb{N}_0$,

$$x \sim_{k,n} y \text{ if } \begin{cases} x = y \\ \text{or} \\ x \geq k, \ \ y \geq k \text{ and } x \equiv y \pmod{n}. \end{cases}$$

Here $x \equiv y \pmod{n}$ means that x and y are integers congruent modulo n, that is, n divides $x - y$ in $\mathbb{Z}$. It is easily verified that $\sim_{k,n}$ is a congruence on $\mathbb{N}_0$. In the factor monoid

$$\mathbb{N}_0/{\sim_{k,n}} = \{[x]_{\sim_{k,n}} \mid x \in \mathbb{N}_0\},$$

the elements are $[0]_{\sim_{k,n}}, [1]_{\sim_{k,n}}, \dots, [k+n-1]_{\sim_{k,n}}$. They are pairwise distinct elements. Therefore $\mathbb{N}_0/{\sim_{k,n}}$ is a monoid with exactly $k + n$ elements. Notice that

$$\begin{aligned}
&[0]_{\sim_{k,n}} = \{0\},\\
&[1]_{\sim_{k,n}} = \{1\},\\
&[2]_{\sim_{k,n}} = \{2\},\\
&\vdots\\
&[k-2]_{\sim_{k,n}} = \{k-2\},\\
&[k-1]_{\sim_{k,n}} = \{k-1\},\\
&[k]_{\sim_{k,n}} = \{k, k+n, k+2n, k+3n, \dots\},\\
&[k+1]_{\sim_{k,n}} = \{k+1, k+1+n, k+1+2n, k+1+3n, \dots\},\\
&\vdots\\
&[k+n-2]_{\sim_{k,n}} = \{k+n-2, k+n-2+n, k+n-2+2n, \dots\},\\
&[k+n-1]_{\sim_{k,n}} = \{k+n-1, k+n-1+n, k+n-1+2n, \dots\}.
\end{aligned}$$

1.5 Congruences in the Monoid $\mathbb{N}_0$

In the additive monoid $\mathbb{N}_0$, the congruences are exactly the equality $=$ and the congruences $\sim_{k,n}$, where $k \geq 0$ and $n \geq 1$. To see it, notice that if $\equiv$ is a congruence on $\mathbb{N}_0$ different from the equality, then there are natural numbers $a < b$ with $a \equiv b$. Let k be the smallest $a \in \mathbb{N}_0$ such that $a \equiv b$ for some $b \neq a$, let b_0 be the smallest natural number $b > k$ with $k \equiv b$, and set $n := b_0 - k$. The congruence $\sim_{k,n}$ is the principal congruence generated by the relation $(k, k+n)$.

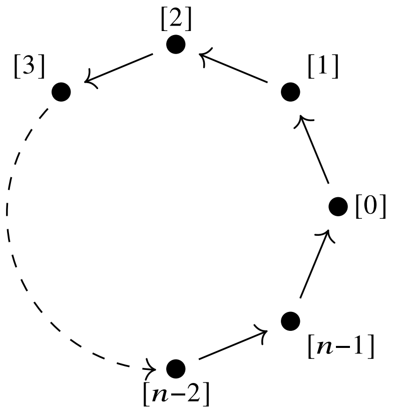

Fig. 1 The cyclic group $\mathbb{Z}/n\mathbb{Z}$

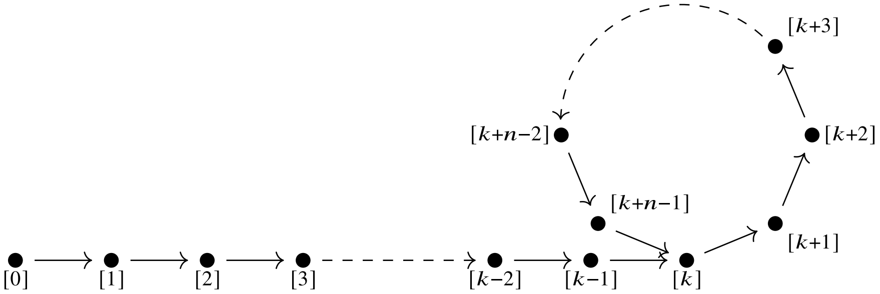

Fig. 2 The cyclic monoid $\mathbb{N}_0/{\sim_{k,n}}$

The monoid $\mathbb{N}_0$ is cyclic generated by 1. The monoids $\mathbb{N}_0/{\sim_{k,n}}$ are cyclic generated by $[1]_{\sim_{k,n}}$. Conversely, every cyclic monoid is isomorphic to either $\mathbb{N}_0$ or $\mathbb{N}_0/{\sim_{k,n}}$ for some $k, n \in \mathbb{N}_0$, $n \geq 1$.

Recall that finite cyclic groups are isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some n and that the most natural representation of $\mathbb{Z}/n\mathbb{Z}$ is that in Fig. 1. Finite cyclic *monoids* have a slightly different behavior. The representation of $\mathbb{N}_0/{\sim_{k,n}}$, analogous to that of $\mathbb{Z}/n\mathbb{Z}$ in Fig. 1, is that in Fig. 2, i.e., $\mathbb{N}_0/{\sim_{k,n}}$ consists of a cycle of length n with a tail of length k that begins in $[0]_{\sim_{k,n}}$.

1.6 Prime Ideals and Localizations

An *ideal* of a commutative monoid M is a subset I of M such that $x \in I$ and $y \in M$ imply $x + y \in I$. A *prime ideal* of a commutative monoid M is a subset P of M such that $M \setminus P$ is a divisor-closed submonoid of M. That is, P is a proper subset of M and, for any $x, y \in M$, one has $x + y \in P$ if and only if either $x \in P$ or $y \in P$.

The union of any family of prime ideals of a commutative monoid M is a prime ideal, so that the set $\mathrm{Spec}(M)$ of all prime ideals of M, partially ordered by set inclusion, is a complete lattice whose greatest element is the prime ideal $M \setminus U(M)$ and whose least element is the empty ideal $\emptyset$. In particular, a commutative monoid has one prime ideal if and only if M is an abelian group. The spectrum $\mathrm{Spec}(M)$ of a commutative monoid M is a commutative monoid. The monoid structure in $\mathrm{Spec}(M)$ is given by the union $\bigcup$ of prime ideals, and the zero is the empty ideal. The spectrum $\mathrm{Spec}(M)$ is also equipped with a topology, where a basis of open sets is given by the sets

$$D(a) := \{\, P \in \mathrm{Spec}(M) \mid a \notin P \,\}, \quad a \in M.$$

For any monoid morphism $f\colon M \to N$, there is a continuous map

$$f^*\colon \mathrm{Spec}(N) \to \mathrm{Spec}(M), \quad Q \mapsto f^{-1}(Q)$$

(notice that the inverse image of a prime ideal via a monoid morphism is a prime ideal). The operation $\bigcup$ on $\mathrm{Spec}(M)$ and the topology of $\mathrm{Spec}(M)$ are compatible, i.e., the mapping $\bigcup\colon \mathrm{Spec}(M) \times \mathrm{Spec}(M) \to \mathrm{Spec}(M)$ is continuous [16]. Thus $\mathrm{Spec}(M)$ is a topological monoid. For any commutative monoid M, there is a natural isomorphism of topological monoids

$$\mathrm{Spec}(M) \cong \mathrm{Hom}_{\mathsf{CMon}}(M, \{0, 1\})$$

[16]. Here the monoid $\{0, 1\}$ is endowed with multiplication and is a topological monoid with respect to the topology in which the open subsets are $\emptyset$, $\{1\}$ and $\{0, 1\}$. For instance, the topological monoids $\mathrm{Spec}(\mathbb{N})$ and $\{0, 1\}$ are isomorphic. Observe that the set $\mathrm{Hom}_{\mathsf{CMon}}(M, \{0, 1\})$ is contained in $\{0, 1\}^M$. The topology on $\mathrm{Hom}_{\mathsf{CMon}}(M, \{0, 1\})$ is the subspace topology induced by the product topology on $\{0, 1\}^M$.

One has that $\mathrm{Spec}(M) \cong \mathrm{Spec}(M/\asymp)$, where $\asymp$ is the smallest congruence on M for which every element in the quotient monoid $M/\asymp$ is idempotent (see 1.3). More precisely, the canonical morphism $q\colon M \to M/\asymp$ induces an isomorphism of topological monoids $q^*\colon \mathrm{Spec}(M/\asymp) \to \mathrm{Spec}(M)$. See [16].

There is a relation between monoids and semilattices. A *join-semilattice* (or *upper semilattice*) is a partially ordered set in which every nonempty finite subset has a least upper bound. Dually, a *meet-semilattice* (or *lower semilattice*) is a partially ordered set in which every nonempty finite subset has a greatest lower bound. A *semilattice with* 1 is a meet-semilattice with a greatest element 1. A morphism of semilattices with 1 is a mapping that respects the greatest lower bound of two elements and the greatest elements 1. If M is a commutative additive monoid in which $2x = x$ for all $x \in M$, that is, every element is *idempotent*, one defines $y \leq x$ if $x + y = y$. In this way, M becomes a semilattice with 1. Conversely, if L is a semilattice with 1, then L is a monoid with respect to the operation $\wedge$. The category of monoids satisfying the identity $2x = x$ turns out to be equivalent to the category of semilattices with 1.

There is a notion of tensor product of commutative monoids, and one finds the isomorphism $M/\asymp\ \cong M \otimes \{0, 1\}$. For all finitely generated semilattices L with 1, there is an isomorphism $\mathrm{ev}\colon L \to \mathrm{Hom}(\mathrm{Hom}(L, \{0, 1\}), \{0, 1\})$, defined by $\mathrm{ev}(x)(f) = f(x)$ for every $x \in L$ and $f \in \mathrm{Hom}(L, \{0, 1\})$.

The localization of a commutative monoid M at a prime ideal P is similar to that of commutative rings. If P is a prime ideal of M, consider the cartesian product $M \times (M \setminus P)$, that is, the set of all pairs (x, s) with $x, s \in M$ and $s \notin P$. Define an equivalence relation $\equiv$ on $M \times (M \setminus P)$ setting $(x, s) \equiv (x', s')$ if there exists an element $t \in M \setminus P$ such that $x + s' + t = x' + s + t$. Let $x - s$ denote the equivalence class of (x, s) modulo the equivalence relation $\equiv$ (notice here that the minus sign in $x - s$ is just suggestive notation). The *localization* M_P of M at P is the monoid whose elements are all $x - s$ with $x \in M$ and $s \in M \setminus P$, and in which the addition is defined by

$$(x - s) + (x' - s') = (x + x') - (s + s').$$

There is a canonical morphism $f\colon M \to M_P$, defined by $f(x) = x - 0$ for every $x \in M$.

For instance, we have already seen that every monoid M has a unique least prime ideal $\emptyset$ and a unique greatest prime ideal $\overline{P} := M \setminus U(M)$. The localization $M_\emptyset$ of M at its empty prime ideal $\emptyset$ is an abelian group, which is usually called the *Grothendieck group* of M, or the *group of differences*, or the *enveloping group* of M, and denoted by $G(M)$. If M is cancellative, $M_P \subseteq M_\emptyset$ for every prime ideal P of M (more precisely, there is an embedding of monoids $M_P \to M_\emptyset$ for each prime P). The localization $M_{\overline{P}}$ of M at $\overline{P} := M \setminus U(M)$ is isomorphic to M.

Proposition 1.2 *Let M be a commutative monoid and P a prime ideal. For every prime ideal Q of M contained in P, set $Q_P := \{x - y \in M_P \mid x \in Q, y \in M \setminus P\}$. Then the prime ideals of M_P are in one-to-one correspondence $(Q \leftrightarrow Q_P)$ with the prime ideals of M contained in P.*

And now we present an operation that does not have an analogue for commutative rings. For every prime ideal P of a commutative monoid M, the monoid $(M_P)_{\mathrm{red}} = M_P/U(M_P)$ is called the *reduced localization* of M at P. If $x, x' \in M$ and $s, s' \in M \setminus P$, then $x - s + U(M_P) = x' - s' + U(M_P)$ in $(M_P)_{\mathrm{red}}$ if and only if there exist elements $t, t' \in M \setminus P$ such that $x + t = x' + t'$.

For every prime ideal P, there is a canonical morphism $\varphi\colon M \to (M_P)_{\mathrm{red}}$, defined by $\varphi(x) = x - 0 + U(M_P)$, which is surjective. Its kernel pair is the congruence $\sim_P$ on M defined, for every $x, y \in M$, by $x \sim_P y$ if there exist $z, t \in M \setminus P$ such that $x + z = y + t$. Hence we could have equivalently defined the reduced localization $(M_P)_{\mathrm{red}}$ of a commutative monoid M at a prime ideal P as the factor monoid $M/\sim_P$. For instance, the largest prime ideal of a commutative monoid M is $M \setminus U(M)$, and the smallest one is $\emptyset$. We leave to the reader to show that the reduced localization of M at the prime ideal $M \setminus U(M)$ is M_{red}, and the reduced localization of M at the prime ideal $\emptyset$ is the trivial monoid with one element.

Proposition 1.3 *Let M be a commutative monoid and $\pi : M \to M_{\mathrm{red}} = M/U(M)$, $\pi : x \mapsto x + U(M)$, the canonical projection. Then $\pi^* \colon \operatorname{Spec}(M_{\mathrm{red}}) \to \operatorname{Spec}(M)$ is a homeomorphism.*

The proofs of all these results are easy. Possible references for the results presented here about commutative monoids are [10] and [13].

2 Preordered Groups, Positive Cones

A structure often useful to describe factorizations of elements in an integral domain or direct-sum decompositions in particular classes of modules is the structure of preordered abelian group.

If G is an abelian group, a translation-invariant preorder $\leq$ on G is completely determined by the set of elements $x \in G$ with $x \geq 0$, because for any $x, y \in G$, we have that $x \leq y$ if and only if $y - x \geq 0$. (To see this, notice that $x \leq y$ implies $0 = x + (-x) \leq y + (-x)$, and conversely $y - x \geq 0$, that is, $0 \leq y - x$, implies $x = 0 + x \leq (y - x) + x = y$.) More precisely:

Lemma 2.1 *There is a one-to-one correspondence between the set of all submonoids of an abelian group G and the set of all translation-invariant preorders on G. This correspondence associates with every translation-invariant preorder $\leq$ on G the* positive cone $G^+ := \{ x \in G \mid 0 \leq x \}$. *Conversely, if M is a submonoid of G, the corresponding preorder $\leq_M$ on G is defined, for every $x, y \in G$, by $x \leq_M y$ if $y - x \in M$.*

A *preordered abelian group* $(G, +, \leq)$ is an abelian group $(G, +)$ with a translation-invariant preorder $\leq$ on G. Equivalently, a preordered abelian group can be defined as a pair (G, C), where G is an abelian group and C is a submonoid of G. Preordered abelian groups form a category in which the morphisms $f \colon (G, +, \leq) \to (H, +, \leq)$ are the group morphisms $f \colon G \to H$ for which $x \leq y$ implies $f(x) \leq f(y)$ for every $x, y \in G$ (equivalently, such that $f(G^+) \subseteq H^+$). For a very nice introduction about preordered abelian groups, a very nice reference is a chapter in the book [12], where most of the proofs about preordered groups we present here are given.

A *partially ordered abelian group* is a preordered abelian group $(G, +, \leq)$ in which $\leq$ is a partial order, that is, the preorder $\leq$ is antisymmetric.

A submonoid of an abelian group G is sometimes called a *cone* in G. A reduced submonoid of an abelian group G is sometimes called a *strict cone* in G. Thus a strict cone is a submonoid C with the property that $x \in C$ and $-x \in C$ imply $x = 0$.

It is easily seen that, for a preordered abelian group $(G, +, \leq)$, $\leq$ is a partial order if and only if the positive cone G^+ of G is a reduced submonoid of G. Thus the one-to-one correspondence of the previous lemma induces a one-to-one correspondence between the set of all reduced submonoids of the abelian group G and the set of all translation-invariant partial orders on G.

In the category of preordered abelian groups there is also a pretorsion theory very similar to the pretorsion theory we met in Sect. 1.2. The torsionfree objects are now the partially ordered abelian groups. The torsion objects are the preordered abelian groups for which the preorder is an equivalence relation, as follows.

Recall that for any preorder $\leq$ on a set S, the *equivalence relation* $\simeq_\leq$ *associated with* $\leq$ is defined, for all $x, y \in S$, by $x \simeq_\leq y$ if $x \leq y$ and $y \leq x$ (Proposition 1.1). In the case of preordered abelian groups, we have the following.

Proposition 2.2 *Let G be a preordered abelian group. Set $H := \{x \in G \mid x \leq 0$ and $0 \leq x\}$. Then:*

(a) *H is a subgroup of G.*
(b) *Define a relation $\preceq$ on G/H by $x + H \preceq y + H$ if $x \leq y$, for every $x, y \in G$. This definition is independent of the choice of the representatives x and y of $x + H$ and $y + H$, that is, the relation $\preceq$ on G/H is well defined.*
(c) *The relation $\preceq$ defined in* (b) *is a partial order on G/H, and G/H, with this partial order, turns out to be a partially ordered group.*

Conversely, if G is an abelian group, H is a subgroup of G and $\preceq$ is a translation-invariant partial order on G/H, the relation $\leq$ on G, defined by $x \leq y$ if $x + H \preceq y + H$, is a translation-invariant preorder on G. There is a canonical one-to-one correspondence between the set of all translation-invariant preorders on G and the set of all pairs $(H, \preceq)$ with H a subgroup of G and $\preceq$ a translation-invariant partial order on G/H.

Proposition 2.2 is the analogue of Proposition 1.1 for abelian groups. The pretorsion theory is therefore the following. For any preordered abelian group G, the torsionfree quotient of G is G/H with the induced partial order. The torsion subobject is G endowed with the equivalence relation for which two elements $g, g' \in G$ are equivalent if and only if $g - g' \in H$.

Notice that, in Proposition 2.2, if G^+ is the positive cone of the preordered group G, then the positive cone of the corresponding partial group G/H is $G^+/H = (G^+)_{\mathrm{red}}$. Therefore the pretorsion theory on the category of preordered abelian groups corresponds to the pretorsion in the category of commutative monoids CMon, in which the torsion objects are abelian groups, and torsionfree objects are reduced commutative monoids.

For any commutative monoid M, endow the Grothendieck group $G(M)$ of M with the structure of preordered group given by $G(M)^+ = \{[m] \mid m \in M\}$, where $[m]$ is the image of $m \in M$ under the canonical map $\psi_M \colon M \to G(M)$. Every monoid morphism $\varphi \colon M \to N$ induces a morphism of preordered groups $G(\varphi) \colon G(M) \to G(N)$. Hence G is a functor of CMon into the category of preordered abelian groups. For every monoid morphism $\varphi \colon M \to N$, there is a commutative diagram

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi_M"'] & N \arrow[d, "\psi_N"] \\ G(M) \arrow[r, "G(\varphi)"] & G(N) \end{tikzcd}$$

It follows that if F is the forgetful functor of the category of preordered abelian groups into the category CMon that sends a preordered abelian group $(G, +, \leq)$ to the commutative monoid $(G, +)$, then ψ is a natural transformation of the identity functor $\mathsf{CMon} \to \mathsf{CMon}$ into the composite functor $FG\colon \mathsf{CMon} \to \mathsf{CMon}$. The functor FG is the functor "localization at the empty prime ideal $\emptyset$".

For the proofs and related results we refer the reader to the paper [3].

3 Some Set Theory

Some students ask me what the difference is between sets and classes. This will be needed in the sequel. For instance, in Lemma 4.1 we will deal with a monoid $V(\mathscr{C})$ that is large in the sense that it can be a class and not a set. To this end, we need some notions of axiomatic set theory.

3.1 ZFC

The most popular and accepted form of axiomatic set theory is ZFC, the *Zermelo-Fraenkel set theory* with the axiom of choice. It has a single primitive ontological notion, the notion of set. That is, it treats only sets (and not classes): all individuals in the universe of discourse are sets. Sets are denoted with lower case letters. The only binary relations are equality and set membership, denoted by $\in$. Thus the formula $x \in y$ indicates that x and y are sets and that x *belongs to* y (or x *is an element* of y, or x *is a member* of y). We can only use the logical symbols $(\neg, \wedge, \vee, \rightarrow\ , \leftrightarrow\ , \forall, \exists)$, $=$ (equality), parentheses, lower case letters (variable symbols) and the symbol $\in$. (One must follow the rules studied in any course of mathematical logic to get well-formed formulas!) Here is a list of the axioms of ZFC. Notice that the axioms are formulas, to which we have added some comments for clarity.

1. Axiom of extensionality. Two sets are equal if they have the same elements, that is, a set is determined by its elements:

$$\forall x \forall y (\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y).$$

2. Axiom of regularity. Every non-empty set x contains an element y such that x and y are disjoint sets.

$$\forall x [\exists a (a \in x) \Rightarrow \exists y (y \in x \wedge \neg \exists z (z \in y \wedge z \in x))].$$

3. Axiom schema of specification (also called the axiom schema of separation). If z is a set, and ϕ is a property that the elements x of z can have or not have,

then there exists a subset y of z containing the elements x of z which satisfy the property ϕ.

$$\forall z \forall w_1 \ldots w_n \exists y \forall x (x \in y \Leftrightarrow (x \in z \wedge \phi)).$$

Here ϕ is a formula in the language of ZFC in the variables

$$x, y, z, w_1, \ldots, w_n$$

with free variables among $x, z, w_1, \ldots, w_n$ and y not free in ϕ.

4. Axiom of pairing. If x and y are sets, then there exists a set whose elements are exactly x and y.

$$\forall x \forall y \exists z \forall w (w \in z \Leftrightarrow w = x \vee w = y).$$

5. Union axiom. For any set x there is a set whose elements are exactly the elements of the elements of x:

$$\forall x \, \exists y \, \forall z (z \in y \Leftrightarrow \exists w (z \in w \wedge w \in x)).$$

6. Axiom schema of collection. If ϕ is a formula in the language of ZFC with free variables among $x, y, z, w_1, \ldots, w_n$ and with a non-free variable w, then

$$\forall z \, \forall w_1, \ldots, w_n ((\forall x \in z \exists ! y \phi) \Rightarrow \exists w \forall x \in z \exists y \in w \, \phi).$$

Here $\exists ! y$ means "there exists a unique y such that…". The axiom essentially says that if $f : z \to z'$ is a function, then the image of f is set. A function $f : z \to z'$ is a triple (f, z, z') of sets, where $f \subseteq z \times z'$ and for every $x \in z$ there exists a unique $y \in z'$ with $(x, y) \in f$.

7. Axiom of infinity. The axiom essentially states that there exists a set with infinitely many members.

$$\exists x \, (\emptyset \in x \wedge \forall y (y \in x \Rightarrow y \cup \{y\} \in x)) \, .$$

8. Axiom of power set. For any set x, there is a set y whose elements are exactly the subsets of x.

$$\forall x \exists y \forall z (z \in y \Leftrightarrow (\forall q (q \in z \Rightarrow q \in x))).$$

9. Axiom of choice. For any set X, every equivalence relation on X has a set of representatives.

The axiom of choice AC is independent from the other axioms of ZFC, and ZFC is independent from the continuum hypothesis $2^{\aleph_0} = \aleph_1$.

3.2 Grothendieck's Universes

The idea is: fix a set, which we call a *universe*, big enough because we put in it all what we need, but not too big because we want it to be a set and not a class. The formal definition is the following:

A *universe* is a set U satisfying the following properties:

(a) $X \in Y \in U \to X \in U$.
(b) $X, Y \in U \to \{X, Y\} \in U$.
(c) $X, Y \in U \to X \times Y \in U$.
(d) $X \in U \to \mathcal{P}(X) \in U$.
(e) $X \in U \to \bigcup_{Y \in X} Y \in U$.
(f) The set ω of natural numbers is an element of U.
(g) If $X \in U$ and $f\colon X \to U$ is a mapping, then $\{\, f(Y) \mid Y \in X \,\} \in U$.

Important: the axioms of ZFC do not guarantee the existence of a universe. Following Grothendieck, we adjoin a further axiom to the axioms of ZFC:

Axiom of Universes: Every set is a member of a universe.

Given any universe U, if the axioms of ZFC are satisfied by the class of all sets with the relation $\in$, then they are also satisfied by the set of all sets belonging to U with the relation $\in$ between them. Hence we can argue remaining in the universe U, which we suppose fixed once for all. In the universe, we find all what we need, and if we do not find it, we can always adjoin it to the universe thanks to the Axiom of universes. In other words, we decide to work in a set that we possibly expand.

But the problem remains: it is not possible to deal with the category Set of all sets in our universe, in this universe in expansion.

3.3 NBG

For the notion of class, we must introduce NBG.

The *Von Neumann-Bernays-Gödel set theory* (NBG) is a conservative extension of ZFC. The ontology of NBG includes proper classes. The members of both sets and proper classes are sets. Classes cannot be members. "Conservative extension" means that a statement in the language of ZFC is provable in NBG if and only if it is provable in ZFC, that is, any theorem in NBG which speaks only about sets is a theorem in ZFC. In NBG, quantified variables in the defining formula can range only over sets.

Let us try to be more precise. The characteristic of NBG is the distinction between proper classes and sets. NBG is a two-sorted theory, that is, two types of variables are used in NBG. Lower case letters will denote variables ranging over sets, and upper case letters will denote variables ranging over classes. The atomic sentences $a \in b$ and $a \in A$ are defined for a, b sets and A a class, but $A \in a$ or $A \in B$ are not defined for any two classes A, B. Equality can have the form $a = b$ or $A = B$. $a = A$ stands for $\forall x(x \in a \leftrightarrow x \in A)$ and is an abuse of notation.

NBG can also be presented as a one-sorted theory of classes, with sets being those classes that are members of at least one other class. That is, NBG can be presented as a system having only one type of variables (class variables) with a unary relation $\mathcal{M}(A)$ ($\mathcal{M}$ stands for the German word Menge, set), and $\mathcal{M}(A)$ indicates that A is a set. Thus $\mathcal{M}(A) \leftrightarrow \exists B(A \in B)$. Notice that NBG admits the class V of all sets, but it does not admit the class of all classes or the set of all sets.

Here is a list of the axioms of NBG. Notice that the first five ones coincide with five axioms of ZFC and deal only with sets, not classes.

1. Axiom of extensionality. Two sets are equal if they have the same elements:
$$\forall a \forall b (\forall z (z \in a \Leftrightarrow z \in b) \Rightarrow a = b).$$
2. Axiom of pairing. If x and y are sets, then there exists a set whose elements are exactly x and y.
3. Union axiom. For any set x there is a set whose elements are exactly the elements of the elements of x.
4. Axiom of power set. For any set x, there is a set y whose elements are exactly the subsets of x.
5. Axiom of infinity.
$$\exists x \left(\emptyset \in x \wedge \forall y (y \in x \Rightarrow y \cup \{y\} \in x) \right).$$

The remaining axioms are primarily concerned with classes rather than sets.

6. Axiom of extensionality for classes. Two classes are equal if they have the same elements:
$$A = B \Leftrightarrow \forall x(x \in A \leftrightarrow x \in B).$$
7. Axiom of regularity for classes. Every non-empty class A contains an element disjoint from A.
$$\exists x(x \in A) \Rightarrow \exists y(y \in A \wedge \neg \exists z(z \in y \wedge z \in A)).$$

Finally, the last two axioms are particular to NBG:

8. Axiom of limitation of size: For any class A, there exists a set a such that $a = A$ if and only if there is no bijection between A and the class V of all sets.

This is really a powerful axiom. By this axiom, every proper class is equipotent to the class V of all sets. Moreover, the axiom of choice for classes holds, because the class of ordinals is not a set, so that there is a bijection between the ordinals and any proper class, and any class can be well ordered. Equivalently, if A is any class and $\sim$ is an equivalence relation on A, a class of representatives exists.

9. Class comprehension schema: For any formula ϕ containing no quantifiers over classes (it may contain class and set parameters), there exists a class A such that $\forall x(x \in A \leftrightarrow \phi(x))$.

It can be proved that NBG can be finitely axiomatized. What is important for us, is that in NBG, which is a conservative extension of ZFC, we can deal with classes and have the axiom of choice for classes. Thus every category has a skeleton, we have a class of representatives for any equivalence relation on any class, and we can define an equivalence between two categories either as a functor with a quasi-inverse or as a fully faithful essentially surjective functor.

4 The Monoid $V(\mathscr{C})$, Discrete Valuations, Krull Monoids

4.1 The Monoid $V(\mathscr{C})$

We will denote by $\operatorname{Ob}\mathscr{C}$ the class of objects of any category $\mathscr{C}$. Recall that a *terminal object* in a category $\mathscr{C}$ is an object T of $\mathscr{C}$ with the property that, for every $A \in \operatorname{Ob}(\mathscr{C})$, there is a unique morphism $A \to T$ in $\mathscr{C}$. Similarly, I is called an *initial object* of $\mathscr{C}$ if for every $A \in \operatorname{Ob}(\mathscr{C})$ there is exactly one morphism $I \to A$. Finally, an object Z of $\mathscr{C}$ is called a *null object* (or a *zero object*) if it is both initial and terminal. Thus an object I is initial if and only if $\operatorname{Hom}_{\mathscr{C}}(I, A)$ has cardinality 1 for every object A, and T is terminal if and only if $\operatorname{Hom}_{\mathscr{C}}(A, T)$ has cardinality 1 for every A. Obviously, an object is an initial object in a category $\mathscr{C}$ if and only if it is a terminal object in the dual category $\mathscr{C}^{\mathrm{op}}$.

Let $\mathscr{C}$ be a category and let 0 be a zero object of $\mathscr{C}$. Then there exist exactly one morphism $A \to 0$ and exactly one morphism $0 \to B$ for every pair A, B of objects. Their composite morphism $A \to B$ is called the *zero morphism* of A into B. In fact, it is easily seen that, in a category $\mathscr{C}$ with a zero object, there is a unique zero morphism $A \to B$ for every pair A, B of objects of $\mathscr{C}$. (One must prove that if $0, 0'$ are two zero objects, then the composite morphism $A \to 0 \to B$ is equal to the composite morphism $A \to 0' \to B$.)

Let $\mathscr{C}$ be a category. For every object A of $\mathscr{C}$, let $\operatorname{Iso}(A)$ denote the *isomorphism class* of A, that is, the class of all objects of $\mathscr{C}$ isomorphic to A. The class $\operatorname{Iso}(A)$ is a subclass of the class $\operatorname{Ob}(\mathscr{C})$ of all objects of $\mathscr{C}$, and the isomorphism classes $\operatorname{Iso}(A)$ form a partition of $\operatorname{Ob}(\mathscr{C})$. Let $V(\mathscr{C})$ denote a *skeleton* of $\mathscr{C}$, that is, a class of representatives of the objects of $\mathscr{C}$ modulo isomorphism. Notice that $V(\mathscr{C})$ exists by the axiom of choice for classes (see Sect. 3.3, Axiom 8). For every object A in $\mathscr{C}$, there is a unique object $\langle A\rangle$ in $V(\mathscr{C})$ isomorphic to A. Thus there is a mapping $\mathscr{C} \to V(\mathscr{C})$, $A \mapsto \langle A\rangle$, that associates with every object A of $\mathscr{C}$ the unique object $\langle A\rangle$ in $V(\mathscr{C})$ isomorphic to A. Assume that a product $A \times B$ exists in $\mathscr{C}$ for every pair A, B of objects of $\mathscr{C}$. Define an addition $+$ in $V(\mathscr{C})$ by $A + B := \langle A \times B\rangle$ for every $A, B \in V(\mathscr{C})$. In this way we get a monoid that is *large*, in the sense that it is a class and not a set when the category $\mathscr{C}$ is not skeletally small:

Lemma 4.1 *Let $\mathscr{C}$ be a category with a terminal object and in which a product $A \times B$ exists for every pair A, B of objects of $\mathscr{C}$. Then $V(\mathscr{C})$ is a large reduced commutative monoid.*

Notice that if $\mathscr{C}$ is an arbitrary category, so that the product $A \times B$ does not necessarily exist for any pair A, B of objects of $\mathscr{C}$, then the skeleton $V(\mathscr{C})$ turns out to be a class in which the operation induced by product is only partially defined, that is, it is a mapping $+\colon S \to V(\mathscr{C})$ for a subclass S of $V(\mathscr{C}) \times V(\mathscr{C})$.

4.2 Discrete Valuations, Krull Monoids

Let M be a monoid. A *discrete valuation* on a monoid M is a non-zero monoid morphism $v\colon M \to \mathbb{N}_0$. Here $\mathbb{N}_0$ is the additive monoid of nonnegative integers. Every discrete valuation $M \to \mathbb{N}_0$ induces a non-zero group morphism $G(M) \to \mathbb{Z}$ that maps $\psi_M(M)$ into $\mathbb{N}_0$. Here $\psi_M\colon M \to G(M)$ is the canonical map that sends each $x \in M$ to $x - 0$. Conversely, every non-zero group morphism $f\colon G(M) \to \mathbb{Z}$ with $f(\psi_M(M)) \subseteq \mathbb{N}_0$ induces a discrete valuation $M \to \mathbb{N}_0$. Thus discrete valuations can be also seen as those non-zero group morphisms $G(M) \to \mathbb{Z}$ that map $\psi_M(M)$ into $\mathbb{N}_0$, i.e., non-zero morphisms of preordered groups, where $G(M)$ is the preordered group whose positive cone is the image $\psi_M(M)$ of M in $G(M)$, and $\mathbb{Z}$ is endowed with its usual linear order.

A monoid morphism $f\colon M \to M'$ is called a *divisor morphism* if, for every $x, y \in M$, $f(x) \leq f(y)$ implies $x \leq y$. Here $\leq$ denotes the algebraic preorder. A monoid M is a *Krull monoid* if there exists a divisor morphism of M into a free commutative monoid. Equivalently, a monoid M is a Krull monoid if and only if there exists a set $\{\, v_i \mid i \in I \,\}$ of monoid morphisms $v_i\colon M \to \mathbb{N}_0$ such that: (1) if $x, y \in M$ and $v_i(x) \leq v_i(y)$ for every $i \in I$, then $x \leq y$; (2) for every $x \in M$, the set $\{\, i \in I \mid v_i(x) \neq 0 \,\}$ is finite.

Our main application of Krull monoids will be to the *reduced* monoid $V(\mathscr{C})$. We leave to the reader the proof of the following elementary Lemma.

Lemma 4.2 *A commutative monoid M is a Krull monoid if and only if the reduced monoid M_{red} is a Krull monoid.*

Reduced Krull monoids are characterized among Krull monoids in the next elementary Lemma.

Lemma 4.3 *Let $f\colon M \to F$ be a divisor morphism of a commutative monoid M into a free commutative monoid F. The following conditions are equivalent:*

(a) *The monoid M is reduced and cancellative.*
(b) *The monoid M is reduced.*
(c) *The morphism f is injective.*

Proposition 4.4 *Let M be an additive, cancellative, commutative monoid with Grothendieck group $G(M)$. The following conditions are equivalent:*

(a) *M is a Krull monoid.*
(b) *There exists a set $\{\, v_i \mid i \in I \,\}$ of non-zero group morphisms*

$$v_i \colon G(M) \to \mathbb{Z}$$

such that: (1) $M = \{\, x \in G(M) \mid v_i(x) \geq 0$ *for every* $i \in I \,\}$*; and* (2) *for every* $x \in G(M)$*, the set* $\{\, i \in I \mid v_i(x) \neq 0 \,\}$ *is finite.*
(c) *There exist an abelian group G, a set I and a subgroup H of the free abelian group $\mathbb{Z}^{(I)}$ such that $M \cong G \oplus (H \cap \mathbb{N}_0^{(I)})$.*

For the proofs, see [8] and [11].

5 Modules

We will always suppose in these notes that our rings R are associative rings with an identity 1_R (unless explicitly stated, like in the next paragraph). Ring morphisms are assumed to preserve identities.

5.1 Left Modules

Let R be a ring. It is possible to define left modules over the ring R in two equivalent ways. For every abelian group M, we denote by $\mathrm{End}(M)$ the endomorphism ring of M.

Definition 5.1 A *left R-module* (or *left module over the ring R*) is a triple $(M, +, \cdot)$, where $(M, +)$ is an additive abelian group and $\cdot \colon R \times M \to M$, $\cdot \colon (r, m) \mapsto rm$, is a mapping, called *left scalar multiplication*, with the following properties for every $r, r' \in R$, and every $m, m' \in M$:

(i) $r(r'm) = (rr')m$;
(ii) $(r + r')m = rm + r'm$;
(iii) $r(m + m') = rm + rm'$;
(iv) $1_R m = m$.

Definition 5.2 A *left R-module* (or *left module over the ring R*) is a triple $(M, +, \lambda)$, where $(M, +)$ is an additive abelian group and $\lambda \colon R \to \mathrm{End}(M)$ is a ring morphism of R into the ring $\mathrm{End}(M)$ of all endomorphisms of the abelian group $(M, +)$.

These two definitions are equivalent in the following sense. Assume that $(M, +, \cdot)$ is a module defined as in Definition 5.1. Let $\lambda \colon R \to \mathrm{End}(M)$ be the mapping defined by $\lambda(r)(m) = rm$ for every $r \in R$, $m \in M$. Then λ is a ring morphism of R into the ring $\mathrm{End}(M)$ of all endomorphisms of the abelian group $(M, +)$.

To see it, we must check four conditions: that $\lambda(r) \in \mathrm{End}(M)$ for every $r \in R$, $\lambda(r + r') = \lambda(r) + \lambda(r')$, $\lambda(rr') = \lambda(r)\lambda(r')$, $\lambda(1_R) = 1_{\mathrm{End}(M)}$. These four conditions follow from properties (iii), (ii), (i), (iv) of Definition 5.1 respectively. Thus $(M, +, \lambda)$ becomes a left module as defined in Definition 5.2.

Conversely, let $(M, +, \lambda)$ be a module as in Definition 5.2. Define a scalar multiplication $\cdot\colon R \times M \to M$ setting $\cdot\colon (r, m) \mapsto rm := \lambda(r)(m)$ for every $r \in R, m \in M$. Then from the fact that λ maps R into $\mathrm{End}(M)$ and respects addition, multiplication and the identity, we get the four properties (iii), (ii), (i), (iv) of Definition 5.1 respectively, that is, $(M, +, \cdot)$ is a left module in the sense of Definition 5.1.

Thus the two definitions of a left module are logically equivalent, and we will use both, depending on the convenience.

Definition 5.3 Let R be a ring and let M, N be left R-modules. A *module morphism* (or *module homomorphism*) of M into N is a mapping $f\colon M \to N$ such that, for every $x, y \in M$ and every $r \in R$, $f(x + y) = f(x) + f(y)$ and $f(rx) = rf(x)$.

We can be very precise and describe the logical equivalence of the two definitions 5.1 and 5.2 of left R-modules in categorical terms. Define a category R-Mod_1 in which: the objects are all modules $(M, +, \cdot)$ defined as in Definition 5.1; the morphisms $f\colon (M, +, \cdot) \to (M', +, \cdot)$ in R-Mod_1 are the module morphisms as defined in Definition 5.3. Composition in R-Mod_1 is the composition of mappings. Similarly, we can define another category R-Mod_2 whose objects are all modules $(M, +, \lambda)$ defined as in Definition 5.2. A morphism $f\colon (M, +, \lambda_M) \to (M', +, \lambda'_{M'})$ in R-Mod_2 is a group morphism $f\colon (M, +) \to (M', +)$ such that the diagram

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "\lambda_M(r)"'] & M' \arrow[d, "\lambda_{M'}(r)"] \\
M \arrow[r, "f"'] & M'
\end{tikzcd}$$

is commutative for every $r \in M$, that is, such that $f \circ \lambda_M(r) = \lambda_{M'}(r) \circ f$ for every $r \in R$. Composition in R-Mod_2 is the composition of mappings. Then the assignment $(M, +, \cdot) \mapsto (M, +, \lambda)$ can be extended to a functor $F\colon R$-$\mathrm{Mod}_1 \to R$-Mod_2, and the assignment $(M, +, \lambda) \mapsto (M, +, \cdot)$ can be extended to a functor $G\colon R$-$\mathrm{Mod}_2 \to R$-Mod_1. These two functors F and G are one the inverse of the other, so that the categories R-Mod_1 and R-Mod_2 turn out to be isomorphic.

When R is a division ring D, left D-modules are usually called *left vector spaces* over the division ring D.

5.2 Right Modules

Let us pass to define *right* modules. The definition is similar to that of left modules, but the scalars act on the right instead of on the left.

Definition 5.4 A *right R-module* (or *right module over the ring R*) is a triple $(M, +, \cdot)$, where $(M, +)$ is an additive abelian group and $\cdot\colon M \times R \to M$, $\cdot\colon (m, r) \mapsto mr$, is a mapping, called *right scalar multiplication*, with the following properties for every $r, r' \in R$, and every $m, m' \in M$:

(i) $(mr)r' = m(rr')$;
(ii) $m(r + r') = mr + mr'$;
(iii) $(m + m')r = mr + m'r$;
(iv) $m1_R = m$.

For a second equivalent definition, analogous to that of Definition 5.2, we need the notion of ring anti-homomorphism.

Definition 5.5 Let R and S be rings. A *ring anti-homomorphism* $f\colon R \to S$ is a mapping of the set R into the set S such that:

(i) $f(r + r') = f(r) + f(r')$ for every $r, r' \in R$;
(ii) $f(rr') = f(r')f(r)$ for every $r, r' \in R$;
(iii) $f(1_R) = 1_S$.

Example 5.6 Let k be a field, n be a positive integer, and $\mathbb{M}_n(k)$ be the ring of $n \times n$ matrices with entries in k. The *transposition* $t\colon \mathbb{M}_n(k) \to \mathbb{M}_n(k)$ defined by $A \mapsto A^t$ (where A^t is the transpose of A) is a ring *anti-isomorphism*, that is, a ring anti-homomorphism that is also a bijective mapping.

Example 5.7 If $(R, +, \cdot)$ is a ring, its *opposite ring* is the ring $(R, +, \circ)$, where $\circ\colon R \times R \to R$ is a new operation on the set R defined by $r \circ r' = r' \cdot r$. Usually, if R is a ring, its opposite ring is denoted by R^{op}. It is easily see that R^{op} is a ring for every ring R. Then the identity mapping $\iota_R\colon R \to R$, defined by $r \in R \mapsto r$, viewed as a mapping $R \to R^{\mathrm{op}}$, is an anti-isomorphism of R onto R^{op}.

Definition 5.8 Let R be a ring. A *right R-module* $(M, +, \rho)$ is an abelian group $(M, +)$ together with a ring anti-homomorphism $\rho\colon R \to \mathrm{End}(M)$.

For right modules it is also easy to see that the two Definitons 5.4 and 5.8 give the same structures, or, if we want to be more precise, that the two corresponding categories are isomorphic. Both for right modules and for left modules we will not distinguish between the two possible definitions. We will consider the category R-Mod of all left R-modules and we will use both definitions with left scalar multiplication or with the ring morphism $R \to \mathrm{End}(M)$. Similarly, on the other side, we will consider the category Mod-R of all right R-modules and we will use both definitions with right scalar multiplication or the ring anti-homomorphism $R \to \mathrm{End}(M)$, as it is more convenient.

Remark 5.9 It is clear that ring anti-homomorphisms

$$R \to \mathrm{End}(M)$$

and ring homomorphisms

$$R^{\mathrm{op}} \to \mathrm{End}(M)$$

coincide. Therefore right R-modules and left R^{op}-modules are exactly the same thing. Similarly, left R-modules coincide with right R^{op}-modules. Also, notice that if the ring R is commutative, a mapping

$$R \to \mathrm{End}(M)$$

is a ring homomorphism if and only if it is a ring anti-homomorphism. It follows that right modules and left modules coincide over a commutative ring R. If we want to be more precise, we can use the categorical language, and say that there is an isomorphism of categories between the category of all right R-modules and the category of all left R^{op}-modules. Similarly, for R commutative, the category of all right R-modules and the category of all left R-modules are isomorphic.

If M is a right R-module, we will usually denote it by M_R, and if M is a left R-module, we will denote it by ${}_RM$. That is, we will write the ring R of "scalars" on the side on which it acts.

If $f\colon M_R \to N_R$ is a module morphism, then f is a monomorphism in the category Mod-R if and only if f is injective, it is an epimorphism if and only if it is surjective, and it is an isomorphism if and only if it is bijective.

5.3 Abelian Groups = $\mathbb{Z}$-modules

For any ring R, there is a unique ring morphism $\mathbb{Z} \to R$, that is, $\mathbb{Z}$ is an initial object in the category of rings.

In particular, let $(G, +)$ be a non-zero abelian group and $\mathrm{End}(G)$ its endomorphism ring. As we have just said, there is a unique ring homomorphism $\lambda\colon \mathbb{Z} \longrightarrow \mathrm{End}(G)$. Equivalently, there is a unique left $\mathbb{Z}$-module structure on any abelian group G. The scalar multiplication $\cdot\colon \mathbb{Z} \times M \to M$ of M is given by $nx =$ "n-th multiple of x in the additive group M" for every $n \in \mathbb{Z}$, $x \in M$. That is,

$$nx = \begin{cases} \underbrace{x + \cdots + x}_{n \text{ times}} & \text{if } n > 0 \\ 0_M & \text{if } n = 0 \\ \underbrace{(-x) + (-x) + \cdots + (-x)}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$$

Thus, left $\mathbb{Z}$-modules and abelian groups coincide. If we want to be more precise, the category Ab of all abelian groups is isomorphic to the category $\mathbb{Z}$-Mod of all left $\mathbb{Z}$-modules, an isomorphism $F\colon \mathbb{Z}\text{-Mod} \to \mathsf{Ab}$ being the forgetful functor F.

5.4 *Is Left Better Than Right?*

The definition of left R-modules, which correspond to ring homomorphisms, seems more natural than that of right R-modules, corresponding to the less natural notion of ring anti-homomorphism. The reason of this lies in the fact that we are used to write mappings on the left, and not on the right. To be more precise, let A and B be sets and assume that we have a mapping $f\colon A \to B$. Then we use to denote the image of an element $a \in A$ by $f(a)$. Also, if $f\colon A \to B$ and $g\colon B \to C$ are two mappings, we denote their composite mapping by $g \circ f$, which is the mapping that sends an element $a \in A$ to $(g \circ f)(a) = g(f(a))$. The choice of this notation was arbitrary, and we could write mappings on the right. For a mapping $f\colon A \to B$, it is possible to denote the image of an element $a \in A$ by $(a)f$, with the mapping f on the right of the elements a on which f acts. In this case, if $f\colon A \to B$ and $g\colon B \to C$ are two mappings, it is more natural to denote the composite mapping by $f \circ g$, because it sends the element $a \in A$ to $((a)f)g$. Notice that, in some settings, mappings *are* denoted on the right. For instance, in group theory, it is common to denote an action g, for instance, conjugation, on an element a in the form a^g. Here g is written as an exponent, that is, on the right of the elements a on which it acts.

If, for any reason, we write mappings on the right, then right R-modules correspond to ring homomorphisms $R \to \operatorname{End}(M)$, and left R-modules correspond to ring anti-homomorphisms of R into $\operatorname{End}(M)$. If, in the ring $\operatorname{End}(M)$ of all endomorphisms of an abelian group M, we write endomorphisms on the right, then the ring of all endomorphisms of M with endomorphisms written on the right is $\operatorname{End}(M)^{\mathrm{op}}$.

From now on, we will always write, as usual, mappings on the left, and most modules we will consider will be right modules M_R.

5.5 *Two Exercises*

(1) Let M be a right R-module, $x, y \in M$, $r, s \in R$. Show that:

(i) $0_M r = 0_M$.
(ii) $x 0_R = 0_M$.
(iii) $(-x)r = -(xr)$ and $x(-r) = -(xr)$. We will denote the element $(-x)r = x(-r) = -(xr)$ by $-xr$.
(iv) $(x - y)r = xr - yr$ and $x(r - s) = xr - xs$.

[Recall that in any additive group G, one writes $a - b$ to denote the sum of a and the opposite of b. That is, $a - b := a + (-b)$. Notice that in this exercise we only use properties (i), (ii) and (iii) of Definition 5.4.]

(2) Let R be a ring with identity 1_R, $(M, +)$ an additive abelian group and $R \times M \to M$, $(r, m) \mapsto rm$, a mapping that satisfies properties (i), (ii) and (iii) of Definition 5.1. Let M_0 be the set of all $x \in M$ with $1_R x = 0_M$, and M_1 be the set of all $x \in M$ with $1_R x = x$. Show that:

(i) M_0 and M_1 are subgroups of M.
(ii) M is the direct sum of M_0 and M_1 as abelian groups.
(iii) $rx = 0_M$ for every $r \in R$ and $x \in M_0$.
(iv) M_1 is a left R-module with respect to the left scalar multiplication induced by the left scalar multiplication on M.

Sometimes "modules" are defined as the algebraic structures satisfying properties (i), (ii) and (iii) of Definition 5.1, and those satisfying property (iv) are called "unitary modules". Thus every "non-unitary module" M is the direct sum of a "module" M_0 on which R acts trivially and a "unitary module" M_1. A non-unitary left R-module M can be also described as an abelian group M with a "ring morphism" $R \to \mathrm{End}(M)$ that does not necessarily map 1_R to $1_{\mathrm{End}(M)}$.

6 Representations/Modules/Actions of Other Algebraic Structures

In this section I will present my personal point of view on the organization of algebraic structures and their representations (modules).

6.1 k-algebras

Let k be a commutative ring with identity. A (not necessarily associative) *k-algebra* is any unitary k-module M with a k-bilinear mapping $(x, y) \mapsto xy$ of $M \times M$ into M (equivalently, a k-linear mapping $M \otimes_K M \to M$). Thus all algebra axioms are satisfied except at most for associativity of multiplication. Here we are following Bourbaki's terminology [4]. The content of this part of these notes is essentially taken from [1, Section 2]. It is possible to construct the *opposite* M^{op} of any such algebra M by defining multiplication in M^{op} via $(x, y) \mapsto yx$.

If M, M' are k-algebras, a *k-algebra morphism* $\varphi\colon M \to M'$ is any k-linear mapping such that $\varphi(xy) = \varphi(x)\varphi(y)$ for every $x, y \in M$. A *derivation* of a k-algebra M is any k-linear mapping $D\colon M \to M$ such that $D(xy) = (D(x))y + x(D(y))$ for every $x, y \in M$.

If M is any k-algebra, its endomorphisms form a (not necessarily commutative) monoid, that is, a semigroup with a two-sided identity, with respect to composition of mappings $\circ$, and its derivations form a Lie k-algebra $\mathrm{Der}(M)$ with respect to the operation $[D, D'] = D \circ D' - D' \circ D$ for every $D, D' \in \mathrm{Der}(M)$. The definition of Lie k-algebra will be given at the beginning of Sect. 6.2.

The main example of associative k-algebra is, for any k-module A_k, the *endomorphism ring* $\mathrm{End}(A_k)$ of A_k. If M is any (not necessarily associative) k-algebra and $x \in M$, the mapping $\lambda_x\colon M_k \to M_k$, defined by $\lambda_x(y) = xy$ for every $y \in M$, is an element of the associative ring $\mathrm{End}(M_k)$.

For any (not necessarily associative) k-algebra M, there is a canonical mapping λ of M into the associative k-algebra $\mathrm{End}_k(M)$, defined by $\lambda\colon x \mapsto \lambda_x$ for every $x \in M$. This mapping λ is a k-algebra morphism if and only if M is associative.

Thus, for any k-algebra M, it is natural to define a left M-module as we did in Sect. 5, that is, as a k-module A_k with a k-algebra morphism $\lambda\colon M \to \mathrm{End}(A_k)$. In fact, consider the natural isomorphism

$$\mathrm{Hom}_k(X_k \otimes_k Y_k, Z_k) \cong \mathrm{Hom}_k(X_k, \mathrm{Hom}_k(Y_k, Z_k)) \qquad X_k, Y_k, Z_k \ k\text{-modules.}$$

For a fixed k-algebra M, any k-bilinear mapping $\mu\colon M_k \times A_k \to A_k$ (any *left scalar multiplication*) can be equivalently described by a k-algebra morphism $\lambda\colon M \to \mathrm{End}(A_k)$, where $\mathrm{End}(A_k)$ is the k-algebra of all endomorphisms of the k-module A_k.

Similarly, we can define *right M-modules* as k-modules A_k with a k-algebra anti-homomorphism $\rho\colon M \to \mathrm{End}(A_k)$. Again, a mapping $M \to M'$ is a k-algebra anti-homomorphism if and only if it is a k-algebra morphism $M^{\mathrm{op}} \to M'$. It follows that right M-modules coincide with left M^{op}-modules. Similarly, left M-modules coincide with right M^{op}-modules.

If the k-algebra M is commutative, then a mapping $M \to M'$ is a k-algebra anti-homomorphism if and only if it is a k-algebra homomorphism $M \to M'$, so right M-modules coincide with left M-modules whenever M is commutative.

6.2 Lie k-algebras

Let k be a commutative ring with identity. A *Lie k-algebra* L is a k-algebra for which, denoting the k-bilinear mapping of $L \times L$ into L by $(x, y) \mapsto [x, y]$, one has:

(1) *(Alternativity)* $[x, x] = 0$ for every $x \in L$.
(2) *(Jacobi identity)* $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for every $x \in L$.

The main example of Lie k-algebra is, for any k-algebra M, the *Lie k-algebra of derivations* $\mathrm{Der}_k(M)$ of the k-algebra M. If M is any k-algebra and D, D' are two derivations of M, then the composite mapping DD' is not a derivation of M in general, but $DD' - D'D$ is, as we have already remarked in Sect. 7.1. Thus, for any k-algebra M, we can define the Lie k-algebra $\mathrm{Der}_k(M)$ as the subset of $\mathrm{End}_k(M)$ consisting of all derivations of M with multiplication $[D, D'] := DD' - D'D$ for every $D, D' \in \mathrm{Der}_k(M)$.

A well known second example of Lie k-algebra is the following. Let L be any associative k-algebra. Define $[x, y] := xy - yx$ for every $x, y \in L$. This is a k-bilinear mapping $L \times L \to L$, and L, with this multiplication, turns out to be a Lie k-algebra.

As a third example, let A be any k-module and L the associative k-algebra $L := \mathrm{End}_k(A)$ of all k-endomorphisms of A. Then L with the operation $[-, -]$ defined as in the previous paragraph, is a Lie k-algebra, denoted by $\mathfrak{gl}(A)$.

For any Lie k-algebra M and any element $x \in M$, the mapping $\lambda_x\colon M \to M$, defined by $\lambda_x = [x, -]$, is a derivation of the Lie algebra M, that is, it is an element of the Lie k-algebra $\mathrm{Der}_k(M)$, usually called the *adjoint* of x, or the *inner derivation* defined by x, and usually denoted by $\mathrm{ad}_M x$ instead of λ_x.

For every Lie k-algebra M, there is a canonical Lie k-algebra morphism $\mathrm{ad}\colon M \to \mathrm{Der}_k(M)$, defined by $\mathrm{ad}\colon x \mapsto \mathrm{ad}_M x$ for every $x \in M$.

It is possible to define *left M-modules* for any Lie k-algebra M. Let M be any Lie k-algebra. A *left M-module* is a k-module A with a Lie k-algebra morphism $\lambda\colon M \to \mathfrak{gl}(A)$. Similarly, we can define *right M-modules* as k-modules A with a k-algebra anti-homomorphism $\rho\colon M \to \mathfrak{gl}(A)$. But any Lie k-algebra M is isomorphic to its opposite algebra M^{op} via the isomorphism $M \to M^{\mathrm{op}}$, $x \mapsto -x$. It follows that the category of all right M-modules is canonically isomorphic to the category of all left M-modules for any Lie k-algebra M. Therefore it is useless to introduce both right and left modules, it is sufficient to introduce left M-modules and call them simply "M-modules". This cannot be done for associative k-algebras, because for an associative k-algebra M the structure of right M-modules can be very different from that of its left M-modules. For instance, it is easy to construct examples of associative k-algebras that are right noetherian, but not left noetherian, e. g. the $\mathbb{Z}$-algebra of triangular 2 × 2-matrices $\begin{pmatrix} \mathbb{Q} & 0 \\ \mathbb{Q} & \mathbb{Z} \end{pmatrix}$. Over such an associative k-algebra, the structure of the category of right modules is very different from that of left modules.

6.3 Monoids

In Sect. 1 we have considered commutative additive monoids. In this Subsect. 6.3, we will consider *multiplicative* monoids, *not necessarily commutative*. Thus a *monoid* will be a semigroup with a two-sided identity, that is, an element $1_M \in M$ such that $1_M x = x 1_M = x$ for every $x \in M$. The main example of monoid is, for any set X, the monoid X^X of all mappings $X \to X$. In this monoid, multiplication is composition of mappings. If M is any monoid and $x \in M$, we have the mapping $\lambda_x\colon M \to M$, that is, a morphism in the category of sets, defined by $\lambda_x(y) = xy$ for every $y \in M$. This λ_x is an element of the monoid M^M. We have a canonical injective monoid morphism $\lambda\colon M \to M^M$, $\lambda\colon x \mapsto \lambda_x$.

Correspondingly, we can define "left M-modules", now called *left M-sets*, for any monoid M. A *left M-set* is any set X with a monoid morphism $\lambda\colon M \to X^X$. Similarly, we can define *right M-sets* as sets X with a monoid anti-homomorphism $\rho\colon M \to X^X$. Again, right M-sets coincide with left M^{op}-sets, and left M-sets coincide with right M^{op}-sets. If the monoid M is commutative, right M-sets coincide with left M-sets.

The concept of monoid is somehow pervasive in Category Theory, essentially because composition of morphisms is required to be associative and the requirement of identity morphisms. Hence given any fixed monoid M, one can consider any object A of any category $\mathscr{C}$ (for instance another monoid A or a vector space A) with a monoid morphism $M \to \mathrm{End}_{\mathscr{C}}(A)$. That is, a monoid M has representations in any category $\mathscr{C}$.

6.4 Monoids with Zero

A *monoid with zero* is a multiplicative monoid with an element $0_M \in M$ such that $0_M x = x 0_M = 0_M$ for every $x \in M$. The zero element in a monoid, when it exists, is unique. By definition, a morphism of monoids with zero must respect multiplication, send the identity to the identity and send zero to zero.

One of the main examples of monoid with zero is the endomorphism monoid of any object in the category of pointed sets. The *category* Set_* *of pointed sets* has as objects the pairs (X, x_0), where X is a non-empty set and x_0 is a selected element of X, called the *base point* of X. A morphism $(X, x_0) \to (X', x_0')$ in Set_* is any mapping $f\colon X \to X'$ such that $f(x_0) = x_0'$. For any pointed set (X, x_0), the endomorphism monoid $\mathrm{End}_{\mathsf{Set}_*}(X, x_0)$ of (X, x_0) in the category Set_* is a monoid with zero. The zero in this monoid is the mapping $X \to X$ that sends all the elements of X to x_0.

If M is any monoid with zero 0_M and $x \in M$, we have the morphism

$$\lambda_x\colon (M, 0_M) \to (M, 0_M)$$

in the category Set_*, defined by $\lambda_x(y) = xy$ for every $y \in M$. There is a canonical injective morphism of monoids with zero $\lambda\colon (M, 0_M) \to \mathrm{End}_{\mathsf{Set}_*}(M, 0_M)$, $\lambda\colon x \mapsto \lambda_x$.

Correspondingly, define *left M-sets* for any monoid $(M, 0_M)$ with zero, as follows. A *left M-set* is any pointed set (X, x_0) with a morphism of monoids with zero

$$\lambda\colon (M, 0_M) \to \mathrm{End}_{\mathsf{Set}_*}(X, x_0).$$

Similarly, define *right M-sets* as pointed sets (X, x_0) with an anti-homomorphism of monoids with zero $\rho\colon (M, 0_M) \to \mathrm{End}_{\mathsf{Set}_*}(X, x_0)$. Clearly, right M-sets coincide with left M^{op}-sets, left M-sets coincide with right M^{op}-sets, and, for M commutative, right M-sets coincide with left M-sets.

6.5 Near-Rings

A similar situation occurs for near-rings, where a *near-ring* is a ring $(R, +, \cdot)$ for which the group $(R, +)$ is not necessarily abelian and for which multiplication on the right distributes over addition, i.e., $(x + y)z = xz + yz$, but multiplication on the left does not necessarily distribute over addition. The main example is the near-ring G^G of all mappings $G \to G$ for a group G. Hence a left module over a near-ring R must be defined as a group H with a near-ring morphism $R \to H^H$.

6.6 Groups and the Cayley Representation

A group is a special type of monoid, so that everything that we've said about monoids applies to groups. One of the main examples of group is, for any set X, the group $\mathrm{Sym}(X)$ of all bijections $X \to X$. If G is any group and $x \in G$, the mapping $\lambda_x : G \to G$ considered in Sect. 6.3 is a bijection. We have a canonical Cayley representation $\lambda \colon G \to \mathrm{Sym}(G)$, $\lambda \colon x \mapsto \lambda_x$. The mapping λ is an injective group morphism.

Correspondingly, we have "left G-sets". A *left G-set* is any set X with a group morphism $\lambda \colon G \to \mathrm{Sym}(X)$. Similarly, *right G-sets* are sets X with a group antihomomorphism $\rho \colon G \to \mathrm{Sym}(X)$. But any group G is isomorphic to its opposite group G^{op} via the isomorphism $G \to G^{\mathrm{op}}$, $x \mapsto x^{-1}$. This is the mother of all symmetries in groups. Hence the category of all right G-sets is canonically isomorphic to the category of all left G-sets for all groups G, and it is useless to introduce both right and left G-sets.

Since groups are monoids, the categorical interpretation of left M-sets in Sect. 6.3 applies directly to left G-sets. Given any group G, we can construct the category $\mathscr{C}$ with a unique object $*$ and with endomorphism monoid $\mathrm{End}_{\mathscr{C}}(*) := G$. The functors of this category $\mathscr{C}$ into the category Set of sets correspond to G-sets and the natural transformations between two functors $\mathscr{C} \to \mathsf{Set}$ correspond to G-set morphisms.

6.7 Groups G and Action of G on G via Inner Automorphisms

There is another very natural action of a group G onto itself, different from that in the previous subsection. For any group G, we can construct its *automorphism group* $\mathrm{Aut}(G)$. If G is any group and $x \in G$, the mapping $\alpha_x : G \to G$, defined by $\alpha_x(y) = xyx^{-1}$ for every $y \in G$, is the *inner automorphism* of G given by conjugation by x. There is a canonical group morphism $\alpha \colon G \to \mathrm{Aut}(G)$, defined by $\alpha \colon x \mapsto \alpha_x$ for every $x \in G$.

Correspondingly, we have "left G-groups". For a fixed group G, a *left G-group* is any group H with a group morphism $\alpha \colon G \to \mathrm{Aut}(H)$. Similarly, we can define *right G-groups* as groups H with a group anti-homomorphism $\beta \colon G \to \mathrm{Aut}(H)$. As we have said above, any group G is isomorphic to its opposite group G^{op}. Hence the category of all right G-groups is canonically isomorphic to the category of all left G-groups for all groups G, and it is therefore useless to introduce both right G-groups and left G-groups.

As in Sect. 6.6 for G-sets, given any group G, we can construct the category $\mathscr{C}$ with a unique object $*$ and with endomorphism monoid $\mathrm{End}_{\mathscr{C}}(*) := G$. The functors of this category $\mathscr{C}$ into the category Grp of groups correspond to G-groups and the natural transformations between two functors $\mathscr{C} \to \mathsf{Grp}$ correspond to G-group morphisms.

The notion of G-group H is classical. Sometimes G is called an *operator group* on H [17, Definition 8.1].

A *G-group morphism* $f\colon (H, \varphi) \to (H', \varphi')$ is any group morphism $f\colon H \to H'$ such that $f(gh) = gf(h)$ for every $g \in G, h \in H$. We will denote by $\mathrm{Hom}_G(H, H')$ the set of all G-group morphisms of H into H'. G-groups form a category G-Grp. The category Grp of groups and the category 1-Grp, where 1 is the trivial group (that is, the group with one element), are isomorphic categories. This is the analogue of the fact that the category Ab of abelian groups and the category $\mathbb{Z}$-Mod of modules over the ring $\mathbb{Z}$ of integers are isomorphic categories, because 1 and $\mathbb{Z}$ are the initial objects in the category of groups and the category of rings, respectively.

Similarly we can present representations $G \to \mathrm{GL}_n(k)$ of a group G. Here k is a field. In general we can represent a group G fixing any category $\mathscr{C}$, an object C of $\mathscr{C}$ and a group morphism $G \to \mathrm{Aut}_{\mathscr{C}}(C)$.

7 Free Modules

7.1 Definition and First Properties of Free Modules

Let M_R be a right module over an (associative) ring R with identity. A *set X of generators* of M_R is a subset X of M_R such that if N is a submodule of M_R that contains X, then $N = M_R$. For instance, the empty set $X = \emptyset$ generates the zero module. If $X \neq \emptyset$ and $X \subseteq M_R$, then X is a set of generators of M_R if and only if, for every element $x \in M_R$, there exist $n \geq 1, x_1, \dots, x_n \in X$ and $r_1, \dots, r_n \in R$ such that $x = x_1 \cdot r_1 + \ldots + x_n \cdot r_n$.

Let us see now what a *free* set of generators is.

Definition 7.1 Let X be a set of generators of a right R-module M_R. The set X is called a *free* set of generators if, for every $n \geq 1, x_1, \dots, x_n$ distinct elements of X and $r_1, \dots, r_n$ in R, one has that $x_1 \cdot r_1 + \ldots + x_n \cdot r_n = 0$ implies $r_1 = \ldots = r_n = 0_R$.

Notice that every module M_R has sets X of generators, for instance $X = M_R$. Not every module has free sets of generators. For instance, the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ does not have a free set of generators for $n \geq 2$.

Definition 7.2 A right R-module M_R is said to be *free* if it has a free set of generators.

Let M_R be a right R-module and X a subset of M_R. We know that X is a set of generators of M_R if and only if every element of M_R can be written as a linear combination of elements of X. It is easily seen that X is a free set of generators of M_R if and only if every element of M_R can be written as a linear combination of distinct elements of X in a unique way; that is, $x_1 \cdot r_1 + \ldots + x_n \cdot r_n = x_1 \cdot r_1' + \ldots + x_n \cdot r_n'$ with $x_1, \dots, x_n$ n distinct elements of X implies $r_1 = r_1', \dots, r_n = r_n'$.

Example 7.3 Let R be a ring and X be an arbitrary set. Let $R^{(X)}$ be the set of all mappings $f\colon X \to R$ such that $f(x) = 0$ for almost all $x \in X$; that is, a mapping $f\colon X \to R$ is in $R^{(X)}$ if and only if there exists a finite subset F of X with $f(x) = 0$ for every $x \in X \setminus F$. Then $R^{(X)}$ is an abelian group with respect to the operation $+$ defined by

$$(f + g)(x) = f(x) + g(x)$$

for every $f, g \in R_R^{(X)}$ and every $x \in X$. The abelian group $R^{(X)}$ becomes a free right R-module $R_R^{(X)}$ with respect to the right scalar multiplication defined by

$$(fr)(x) = f(x)r$$

for every $f \in R_R^{(X)}$, $x \in X$ and $r \in R$.

For every fixed $x_0 \in X$, let $\delta_{x_0}\colon X \to R$ be the mapping defined by

$$x \mapsto \begin{cases} 1_R \ if x = x_0, \\ 0_R \ if x \neq x_0. \end{cases}$$

It is easy to see that $\Delta := \{\, \delta_{x_0} \mid x_0 \in X \,\}$ is a free set of generators for $R_R^{(X)}$. The module $R_R^{(X)}$ is isomorphic to the direct sum of $|X|$ copies of the module R_R.

We also have the same on the left. The abelian group $R^{(X)}$ is a free left R-module ${}_RR^{(X)}$ with respect to the left scalar multiplication defined by

$$(rf)(x) = r(f(x))$$

for every $f \in {}_RR^{(X)}$, $x \in X$ and $r \in R$. In this case also, the set Δ is a free set of generators.

Proposition 7.4 (Universal Property of Free Modules). *Let M_R be a free right R-module, X a free set of generators for M_R and $\varepsilon\colon X \to M_R$ the embedding of X into M_R. Then, for every right R-module M'_R and every mapping $f\colon X \to M'_R$, there exists a unique right R-module morphism $\widetilde{f}\colon M_R \to M'_R$ making the diagram*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varepsilon"'] & M'_R \\ M_R \arrow[ur, "\widetilde{f}"'] & \end{tikzcd}$$

commute, that is, such that $\widetilde{f} \circ \varepsilon = f$.

We have the functors $F\colon \mathsf{Set} \to \text{Mod-}R$, where, for every set X, $F(X)$ is the free module $R_R^{(X)}$, and the forgetful functor $U\colon \text{Mod-}R \to \mathsf{Set}$. Proposition 7.4 says that F is a left adjoint of U, that is, $\mathrm{Hom}_R(R_R^{(X)}, M'_R) \cong M'^X$ for every set X and module M'_R.

Corollary 7.5 *If M_R is a free right module with free set X of generators, then $M_R \cong R_R^{(X)}$.*

When R is a division ring, every right R-module, that is, every right vector space over the division ring R, is free. For this, we need a:

7.2 Crash Course of Linear Algebra over Non-commutative Division Rings

Let us briefly recall some elementary notions of linear algebra. The reader is definitely an expert on the elementary theory of vector spaces over a field k: vector spaces over k (they are exactly what we have called k-modules), linear transformations (they are exactly what we have called k-module morphisms), the concept of set of generators, linear combinations, linear independence and bases. The reader knows that any two bases of a vector space over k have the same cardinality, and that this cardinality is called the dimension of the vector space. He knows that if we have a linear transformation f between two vector spaces V and W over k of finite dimensions n and m respectively, and we fix an ordered basis for V and an ordered basis for W, we can associate with f a $m \times n$ matrix with entries in k. He knows the rank of a linear transformation f (it is the dimension of the image of f), bilinear mappings, the determinant of a square matrix, its minimal polynomial, the characteristic polynomial, eigenvectors and eigenvalues and so on. Assume now that k is not a field, but a division ring, and consider right vector spaces over k, that is, right k-modules. It is very easy to see that all the previous concepts hold for right vector spaces over a division ring, until when bilinear mappings enter the picture. Bilinearity is a notion concerning modules over commutative rings, because, for a bilinear mapping $\beta\colon {}_kV \times {}_kW \to {}_kU$, we have that $\beta(\lambda v, \mu w)$ must be equal to both $\lambda\beta(v, \mu w) = \lambda\mu\beta(v, w)$ and $\mu\beta(\lambda v, w) = \mu\lambda\beta(v, w)$.

Thus, over an arbitrary division ring k we still have linear transformations (they are right k-module morphisms), sets of generators (again, we have already defined them for modules over arbitrary rings), linear combinations (that is, expressions of the form $\sum_{i=1}^n v_i\lambda_i$, where the elements v_i belong to a right vector space V_k and the scalars λ_i are in the division ring k), linear independence (a subset X of V_k is linearly independent if and only if it is a free set of generators for the subspace of V_k it generates), bases (i.e., free sets of generators). Any two bases of a right vector space over a division ring k have the same cardinality (same proof as in the case of a commutative k), and this cardinality is called the *dimension* of the right vector space. If we have a linear transformation f between two right vector spaces V_k and W_k, $\{v_1, \dots, v_n\}$ is an ordered basis of V_k and $\{w_1, \dots, w_m\}$ is an ordered basis of W_k, we can associate with f the $m \times n$ matrix $A_f = (\lambda_{i,j})_{i,j}$, where $f(v_j) = \sum_{i=1}^n w_i\lambda_{i,j}$. In this case also, if $v = \sum_{j=1}^n v_j a_j$ is an arbitrary element of

V_k and $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ is the $n \times 1$ matrix whose entries are the coefficients of v as a linear combination of $v_1, \dots, v_n$, then the $m \times 1$ matrix $A_f \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ is the matrix whose entries are the coefficients of $f(v)$ as a linear combination of $w_1, \dots, w_m$. Notice that if $f \colon V_k \to W_k$ and $g \colon W_k \to Y_k$, then $A_{g\circ f} = A_g A_f$.

The rank of a linear transformation f is the dimension of the image of f when the division ring k is non-commutative also. The difficulties in the non-commutative case appear when bilinear mappings and determinant, which are multilinear mappings, are introduced. There are notions of right determinant and left determinant, due to Dieudonné, one is linear on columns and the other on rows, but they are not easy to handle. Consequently, it becomes impossible to deal (at least easily) with the minimal polynomial, the characteristic polynomial, eigenvectors and eigenvalues. But, until the appearance of bilinear mappings and determinant, the passage from the commutative case to the non-commutative one is very smooth.

As we have already said, every module over a division ring, that is, every right vector space and every left vector space over a division ring, is free. The converse is also true: if R is a ring over which every right R-module is free, then R is a division ring.

7.3 Rank of a Free Module

Let us go back to the study of free modules over arbitrary rings. Recall that $|X|$ denotes the cardinality of a set X.

Corollary 7.6 *If M_R and N_R are free right R-modules with free sets of generators X and Y respectively, and $|X| = |Y|$, then $M_R \cong N_R$.*

If M_R is a free module, the cardinality of any free set of generators of M_R is called a *rank* of the free module M_R.

Proposition 7.7 *Let M_R be a free right R-module. If M_R is finitely generated, then every free set of generators of M_R is finite.*

Corollary 7.8 *Let R be a ring and let M_R be a free right R-module. If X is an infinite free set of generators of M_R, then every free set of generators of M_R has cardinality $|X|$.*

Hence, the rank of a free module with an infinite free set of generators is uniquely defined (Corollary 7.8), while the only thing we can say about a finitely generated free module is that every free set of generators is finite (Proposition 7.7).

8 IBN Rings

Let R be a ring (with identity). Let $\mathcal{F}_{\rm fg}$ be the full subcategory of Mod-R whose objects are all finitely generated free right R-modules. This subcategory has a zero object: the zero module, free of rank zero. We can proceed like in Sect. 4.1, constructing the monoid $V(\mathscr{C})$ for $\mathscr{C} = \mathcal{F}_{\rm fg}$. The set $\{\, R^n_R \mid n \geq 0 \text{ an integer}\,\}$ contains a skeleton $V(\mathcal{F}_{\rm fg})$: every finitely generated free right R-module is isomorphic to R^n_R for some n, possibly a finite number of natural numbers n (see Example 8.2). Hence we have a reduced commutative monoid $V(\mathcal{F}_{\rm fg})$ with the operation induced by the direct sum $\oplus$. Equivalently, we can define $V(\mathcal{F}_{\rm fg})$ as the quotient monoid $\mathbb{N}_0/\!\sim$, where $\sim$ is the congruence on the additive monoid $\mathbb{N}_0$ defined, for every $n, m \in \mathbb{N}_0$, by $n \sim m$ if $R^n_R \cong R^m_R$. Thus $\sim$ depends on the fixed ring R.

Of course, $\sim$ is a congruence on $\mathbb{N}_0$, and therefore, as we said in Sect. 1.5, the congruence $\sim$ must be either the equality $=$ or one of the congruences $\sim_{k,n}$, where $k \geq 0$ and $n \geq 1$, for a unique pair (k, n). For arbitrarily fixed integers $k, n \geq 1$, it is possible to construct rings for which the associated congruence $\sim$ is exactly the congruence $\sim_{k,n}$.

A ring R is IBN or has IBN (invariant basis number) if the congruence $\sim$ is the equality $=$, that is, if for every $n, m \geq 0$, $R^n_R \cong R^m_R$ implies $n = m$. Equivalently, a ring R is IBN if and only if $V(\mathcal{F}_{\rm fg})$ is isomorphic to the additive monoid $\mathbb{N}_0$. For instance, division rings have IBN. Notice that R^0_R has one element, and R^n_R has at least two elements for $n \geq 1$ and $R \neq 0$. This has two consequences: (1) A ring R has IBN if and only if, for every $n, m \geq 1$, $R^n_R \cong R^m_R$ implies $n = m$. (2) If $\sim_{k,n}$ is the congruence associated with a ring $R \neq 0$ as above, then necessarily $k \geq 1$.

Exercise 8.1 (1) Show that having IBN is a left/right symmetric condition, that is, a ring R has IBN if and only if ${}_RR^n \cong {}_RR^m$ implies $n = m$ for every $n, m \geq 0$.

(2) Show that a ring R has IBN if and only if for every $n,\ m \geq 1$, $A \in \mathbb{M}_{n\times m}(R)$, $B \in \mathbb{M}_{m\times n}(R)$, $AB = 1_n$, $BA = 1_m$ imply $n = m$. Here $\mathbb{M}_{n\times m}(R)$ denotes the set of all $n \times m$ matrices with entries in R.

(3) Show that if there exists a ring morphism $\varphi\colon R \to S$ and the ring S has IBN, then R has IBN as well.

(4) Show that if R is a ring, I is a two-sided ideal in R and the quotient ring R/I has IBN, then R has IBN as well. (Here notice the special case of $I = R$. In this case R/I is the zero ring, which is not an IBN ring.)

(5) Show that every non-zero commutative ring has IBN.

[Hint for (1): The functor $\mathrm{Hom}(-, R)$ induces a duality between the category of finitely generated free right R-modules and the category of finitely generated free left R-modules. Hint for (3): Apply (2). If $A \in \mathbb{M}_{n\times m}(R)$, $B \in \mathbb{M}_{m\times n}(R)$ and we apply the morphism φ to the entries of A and B, we get two matrices in $\mathbb{M}_{n\times m}(S)$ and $\mathbb{M}_{m\times n}(S)$ such that…]

Example 8.2 Here is an example of a ring $R \neq 0$ with $R_R \cong R_R \oplus R_R$, so that in particular the ring R has not IBN. Let k be a field. Let V_k be a vector space over k of infinite dimension. Then $V_k \oplus V_k \cong V_k$. Let $R := \mathrm{End}(V_k)$ be the endomorphism ring of V_k, so that ${}_R V_k$ is a R-k-bimodule. Thus there is a covariant additive functor $\mathrm{Hom}({}_R V_k, -)\colon$ Mod-$k \to$ Mod-R. Applying this functor to the right k-module isomorphism $V_k \oplus V_k \cong V_k$, we get a right R-module isomorphism $\mathrm{Hom}({}_R V_k, V_k) \oplus \mathrm{Hom}({}_R V_k, V_k) \cong \mathrm{Hom}({}_R V_k, V_k)$, that is, an isomorphism $R_R \oplus R_R \cong R_R$. This is an isomorphism between two free right R-modules of rank 2 and 1 respectively. Therefore R is not an IBN ring. Notice that, for this ring R, we have that $R_R \cong R_R^n$ for every $n \geq 1$. Thus $R_R^n \cong R_R^m$ for every $n, m \geq 1$. Hence, for this ring R, the monoid $V(\mathcal{F}_{\mathrm{fg}})$ is a monoid with two elements. It is isomorphic to the multiplicative monoid $\{0, 1\}$ with two elements. The congruence associated with the ring R as at the beginning of this Sect. 8 is $\sim_{1,1}$.

9 Simple Modules, Semisimple Modules

A *simple* right module is a non-zero right module M_R whose submodules are only M_R and 0. Thus a simple module has exactly two submodules.

Lemma 9.1 *A right module M_R is simple if and only it is isomorphic to R_R/I for some maximal right ideal I of R.*

Lemma 9.2 (Schur's Lemma) *The endomorphism ring of a simple module is a division ring.*

A module M_R is *semisimple* if every submodule of M_R is a direct summand of M_R.

Remark 9.3 (1) Every simple module is semisimple.
(2) If R is a division ring, every R-module is semisimple.
(3) A module M_R is semisimple if and only if every short exact sequence with M_R in the middle, that is, every short exact sequence of the form $0 \to A_R \to M_R \to C_R \to 0$, splits.
(4) Submodules and homomorphic images of semisimple modules are semisimple modules.

Definition 9.4 Let M_R be a right R-module. The *socle* $\mathrm{soc}(M_R)$ of M_R is the sum of all simple submodules of M_R.

Thus $\mathrm{soc}(M) = 0$ if and only if M has no simple submodules.

Theorem 9.5 *The following conditions are equivalent for a right R-module M:*

(i) *M is a sum of simple submodules, that is, M is equal to its socle.*
(ii) *M is a direct sum of simple submodules.*
(iii) *M is semisimple.*

10 Projective Modules

Definition 10.1 Let R be a ring. A right R-module P_R is *projective* if for every epimorphism $f\colon M_R \to N_R$ and every morphism $g\colon P_R \to N_R$, there exists a morphism $h\colon P_R \to M_R$ with $f \circ h = g$.

The situation in the previous definition is described by the following commutative diagram, in which the row is exact:

$$\begin{tikzcd}
P_R \arrow[d, "h"'] \arrow[dr, "g"] & & \\
M_R \arrow[r, "f"'] & N_R \arrow[r] & 0
\end{tikzcd}$$

Lemma 10.2 (i) *Every free module is projective.*
(ii) *Every direct summand of a projective module is projective.*
(iii) *Every direct sum of projective modules is projective.*

Proposition 10.3 *The following conditions are equivalent for a right R-module P_R:*

(i) *The module P_R is projective.*
(ii) *Every short exact sequence of the form* $0 \to M_R \to N_R \to P_R \to 0$ *splits.*
(iii) *The module P_R is isomorphic to a direct summand of a free module.*

Corollary 10.4 *A module P_R is a finitely generated projective module if and only if it is isomorphic to a direct summand of R_R^n for some $n \geq 0$.*

A ring R is *semisimple artinian* if it is right artinian and has no non-zero nilpotent right ideal. To be more precise, we should call such a ring a *right semisimple artinian* ring, because it is defined relatively to the structure of the right module R_R and to right ideals. Also, we should define *left semisimple artinian* rings symmetrically. But as a consequence of the Artin-Wedderburn Theorem 10.6, it will follow that a ring is right semisimple artinian if and only if it is left semisimple artinian, so that a reference to the side is useless. In order not to have a too heavy terminology, we call the rings just defined semisimple artinian, without any reference to the side.

Theorem 10.5 *The following conditions are equivalent for a ring R.*

(i) *Every right R-module is projective.*
(ii) *Every short exact sequence of right R-modules splits.*
(iii) *Every right R-module is semisimple.*
(iv) *The module R_R is semisimple.*
(v) *The ring R is semisimple artinian.*

10.1 The Ring of n × n Matrices over a Division Ring

Let us describe the structure of the ring of all $n \times n$ matrices with entries in a division ring.

Let D be a division ring, $n \geq 1$ an integer, and $R := \mathbb{M}_n(D)$ be the ring of all $n \times n$ matrices with entries in D. It is possible to prove that R is a *simple* ring, that is, its two-sided ideals are only the trivial ones. For every $i, j = 1, 2, \dots, n$, let $E_{i,j}$ be the matrix with the (i, j) entry equal to 1, and 0 in all the other entries. Notice that the elements $E_{i,i}$ *are idempotents of* R*,* $E_{1,1} + \cdots + E_{n,n} = 1$ and $E_{i,i}E_{j,j} = 0$ for $i \neq j$. Also, $E_{i,i}R$ is the set of all $n \times n$ matrices with entries in D, that are 0 on all rows except for the i-th row, and with arbitrary entries in D on the i-th row, and

$$R_R = E_{1,1}R \oplus E_{2,2}R \oplus \cdots \oplus E_{n,n}R$$

The modules $E_{i,i}R$ *are all pairwise isomorphic.* For instance, an isomorphism $E_{1,1}R \to E_{i,i}R$ is given by left multiplication by the matrix $E_{i,1}$. Moreover, *the module* $E_{1,1}R$ *is simple.* Thus $R_R = E_{1,1}R \oplus \cdots \oplus E_{n,n}R$ *is a direct sum of* n *simple isomorphic modules,* in particular R *is a semisimple artinian ring.*

Matrix transposition $t \colon A \mapsto A^t$ is a ring isomorphism

$$t \colon \mathbb{M}_n(D) \to (\mathbb{M}_n(D^{\mathrm{op}}))^{\mathrm{op}}.$$

Therefore R is isomorphic to the opposite ring of $\mathbb{M}_n(D^{\mathrm{op}})$, where D^{op} is also a division ring. Thus all properties we have seen on the right also hold on the left. Also, the category R-Mod, which is equivalent to the category Mod-R^{op}, is equivalent to the category $\mathbb{M}_n(D^{\mathrm{op}})$-Mod.

We have that the left ideal $RE_{i,i}$ *is the set of all* $n \times n$ *matrices with entries in* D*, that are* 0 *on all columns except for the* i*-th column, and with arbitrary entries in* D *on the* i*-th column.* Therefore

$${}_RR = RE_{1,1} \oplus RE_{2,2} \oplus \cdots \oplus RE_{n,n},$$

and *the left ideals* $RE_{1,1}, \dots, RE_{n,n}$ *are isomorphic simple modules.*

It is also possible to prove that *every simple right* R*-module is isomorphic to* $E_{1,1}R$*, and the endomorphism ring* $\mathrm{End}(E_{1,1}R)$ *of the simple module* $E_{1,1}R$ *is isomorphic to the division ring* D*.*

Now if M_R is any right R-module, then M_R is semisimple by Theorem 10.5. Hence M_R is a direct sum of simple submodules. But all simple right R-modules are isomorphic to $E_{1,1}R$. Thus we have seen that *every right* R*-module is isomorphic to a direct sum* $E_{1,1}R^{(X)}$ *for some set* X*. It is possible to prove that the cardinality of such a set* X *is uniquely determined.*

Notice that $\mathrm{Hom}(E_{1,1}R, E_{1,1}R)$ is an abelian group that cannot be endowed with a right R-module structure or a left R-module structure. For instance, assume that the division ring D is a finite field with q elements and $n = 2$. It is easy to show that $\mathrm{Hom}(E_{1,1}R, E_{1,1}R) \cong E_{1,1}RE_{1,1} \cong D$, hence has q elements in this case. But every right R-module is isomorphic to a direct sum of copies of $E_{1,1}R$, which has q^2 elements. Hence every finite right R-module has q^{2t} elements for some non-negative integer t. Thus no right R-module can have q elements. This proves that $\mathrm{Hom}(E_{1,1}R, E_{1,1}R)$ cannot be endowed with a right R-module structure. Similarly, it cannot be endowed with a left R-module structure.

As we have just said above, a matrix ring with entries in a division ring is a semisimple artinian ring. This is true for any finite direct product of such matrix rings:

Let $t, n_1, \dots, n_t \geq 1$ be integers and $D_1, \dots, D_t$ division rings. Then the ring $R := M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t)$ is a semisimple artinian ring.

It is interesting that the converse of this result also holds:

Theorem 10.6 (Artin-Wedderburn) *A ring R is semisimple artinian if and only if there exist integers $t \geq 0,\ n_1, \dots, n_t \geq 1$ and division rings $D_1, \dots, D_t$ such that*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t). \tag{11.i}$$

Moreover, if R is semisimple artinian, the integers $t, n_1, \dots, n_t$ in the decomposition (11.i) are uniquely determined by R and $D_1, \dots, D_t$ are determined by R up to ring isomorphism.

11 Superfluous Submodules and Radical of a Module

A submodule N of a module M_R is *superfluous* (or *small*, or *inessential*) in M_R if, for every submodule L of M_R, $N + L = M_R$ implies $L = M_R$. To denote that N is superfluous in M_R, we will write $N \leq_s M_R$.

Here are the main elementary properties of superfluous submodules:

(i) If $K \leq N \leq M_R$, then $N \leq_s M$ if and only if $K \leq_s M$ and $N/K \leq_s M/K$.
(ii) $K \leq_s M_R$ and $M_R \leq N_R$ imply $K \leq_s N_R$.
(iii) If $N, N' \leq M_R$, then $N + N' \leq_s M$ if and only if $N \leq_s M$ and $N' \leq_s M$.
(iv) The zero submodule is always a superfluous submodule of any module M_R, when $M_R = 0$ also.
(v) If $f\colon M \to M'$ is an R-module morphism and $N \leq_s M$, then $f(N) \leq_s M'$.
(vi) Assume $K_1 \leq M_1 \leq M, K_2 \leq M_2 \leq M$ and $M = M_1 \oplus M_2$. Then $K_1 \oplus K_2 \leq_s M_1 \oplus M_2$ if and only if $K_1 \leq_s M_1$ and $K_2 \leq_s M_2$.

We will say that an epimorphism $g\colon M_R \to N_R$ is *superfluous* if $\ker g$ is a superfluous submodule of M_R.

The *radical* $\mathrm{rad}(M_R)$ of a module M_R is the intersection of all maximal submodules of M_R. Note the duality with the definition of socle, which is the sum of all simple (=minimal) submodules of M_R.

Here are some elementary properties of the radical $\mathrm{rad}(M_R)$ of a module M_R:

(1) The submodule $\mathrm{rad}(M_R)$ is the sum of all superfluous submodules of M_R.
(2) $\mathrm{rad}(M_R/\mathrm{rad}(M_R)) = 0$.
(3) If $f\colon M_R \to M'_R$ is a morphism of R-modules, then

$$f(\mathrm{rad}(M_R)) \leq \mathrm{rad}(M'_R).$$

12 The Jacobson Radical of a Ring

The radical of the right R-module R_R is called the *Jacobson radical* of the ring R. It is denoted by $J(R)$. Thus $J(R) := \mathrm{rad}(R_R)$ is the intersection of all maximal right ideals of R, but it is possible to show that $\mathrm{rad}(R_R) = \mathrm{rad}({}_RR)$ for any ring R, so that $J(R)$ is also the intersection of all maximal left ideals of R. Therefore $J(R)$ is a two-sided ideal of R.

For every right R-module M_R, the *right annihilator* $\mathrm{r.ann}_R(M_R)$ of M_R is the set of all $r \in R$ such that $Mr = 0$. The right annihilator of any right R-module is a two-sided ideal of R. If $x \in M_R$, the *right annihilator* $\mathrm{r.ann}_R(x)$ of x is the set of all $r \in R$ such that $xr = 0$. The right annihilator of an element x of M_R is a right ideal of R.

Proposition 12.1 *The Jacobson radical $J(R)$ of any ring R is the intersection of the right annihilators* $\mathrm{r.ann}_R(S_R)$ *of all simple right R-modules S_R.*

13 Injective Modules

Fix two modules M_R and N_R. There are a covariant functor

$$\mathrm{Hom}(M_R, -)\colon \text{Mod-}R \to \mathsf{Ab}$$

and a contravariant functor

$$\mathrm{Hom}(-, N_R)\colon \text{Mod-}R \to \mathsf{Ab}.$$

These functors Hom are “left exact”, in the sense that, for every fixed module M_R, if $0 \to N'_R \to N_R \to N''_R$ is exact, then so is $0 \to \mathrm{Hom}(M_R, N'_R) \to \mathrm{Hom}(M_R, N_R) \to \mathrm{Hom}(M_R, N''_R)$, and, for every fixed module N_R, if $M'_R \to M_R \to M''_R \to 0$ is exact, then so is $0 \to \mathrm{Hom}(M''_R, N_R) \to \mathrm{Hom}(M_R, N_R) \to \mathrm{Hom}(M'_R, N_R)$.

In general, the functors $\mathrm{Hom}(M_R, -)$ and $\mathrm{Hom}(-, N_R)$ are not “exact”, that is, it is not always true that, for every fixed module M_R, if $0 \to N'_R \to N_R \to N''_R \to 0$ is a short exact sequence, then $0 \to \mathrm{Hom}(M_R, N'_R) \to \mathrm{Hom}(M_R, N_R) \to \mathrm{Hom}(M_R, N''_R) \to 0$ is necessarily exact, and, for every fixed module N_R, if $0 \to M'_R \to M_R \to M''_R \to 0$ is exact, then $0 \to \mathrm{Hom}(M''_R, N_R) \to \mathrm{Hom}(M_R, N_R) \to$

$\mathrm{Hom}(M'_R, N_R) \to 0$ is necessarily exact. It is easily seen that a module M_R is projective if and only if the functor $\mathrm{Hom}(M_R, -)$ is exact, that is, for every exact sequence $0 \to N'_R \to N_R \to N''_R \to 0$, the sequence of abelian groups $0 \to \mathrm{Hom}(M_R, N'_R) \to \mathrm{Hom}(M_R, N_R) \to \mathrm{Hom}(M_R, N''_R) \to 0$ is exact.

The proof of the following result is easy.

Proposition 13.1 *The following conditions are equivalent for an R-module E_R:*

(i) *The functor* $\mathrm{Hom}(-, E_R)\colon \text{Mod-}R \to \mathsf{Ab}$ *is exact, that is, for every exact sequence* $0 \to M'_R \to M_R \to M''_R \to 0$ *of right R-modules, the sequence of abelian groups* $0 \to \mathrm{Hom}(M''_R, E_R) \to \mathrm{Hom}(M_R, E_R) \to \mathrm{Hom}(M'_R, E_R) \to 0$ *is exact.*

(ii) *For every monomorphism $M'_R \to M_R$ of right R-modules,*

$$\mathrm{Hom}(M_R, E_R) \to \mathrm{Hom}(M'_R, E_R)$$

is an epimorphism of abelian groups.

(iii) *For every submodule M'_R of a right R-module M_R, every morphism*

$$M'_R \to E_R$$

can be extended to a morphism $M_R \to E_R$.

(iv) *For every monomorphism $f\colon M'_R \to M_R$ and every morphism*

$$g\colon M'_R \to E_R,$$

there exists a morphism $h\colon M_R \to E_R$ with $h \circ f = g$.

A module E_R is *injective* if it satisfies the equivalent conditions of Proposition 13.1.

Condition (iv) is described by the following commutative diagram, in which the row is exact:

$$\begin{tikzcd}
0 \arrow[r] & M'_R \arrow[r, "f"] \arrow[dr, "g"'] & M_R \arrow[d, "h"] \\
 & & E_R
\end{tikzcd}$$

Thus we have that:

(1) A module M_R is projective if and only if every short exact sequence of the form $0 \to A_R \to B_R \to M_R \to 0$ splits.

(2) A module M_R is injective if and only if every short exact sequence of the form $0 \to M_R \to B_R \to C_R \to 0$ splits.

(3) A module M_R is semisimple if and only if every short exact sequence of the form $0 \to A_R \to M_R \to C_R \to 0$ splits.

Proposition 13.2 (Baer's criterion). *A right module E over a ring R is injective if and only if for every right ideal I of R, every morphism $\sigma \colon I \to E$ can be extended to a morphism $\sigma^* \colon R \to E$.*

Definition 13.3 An additive abelian group G is *divisible* if $nG = G$ for every nonzero integer n (equivalently, for every positive integer n). Thus G is divisible if and only if, for every $g \in G$ and every $n > 0$, there exists $h \in G$ such that $nh = g$.

For instance, the abelian group $\mathbb{Z}$ is not divisible, and the abelian group $\mathbb{Q}$ is divisible. Homomorphic images of divisible abelian groups are divisible. It is possible to prove that every divisible abelian group is a direct sum of copies of $\mathbb{Q}$ and Prüfer groups $\mathbb{Z}(p^\infty)$.

Proposition 13.4 *A $\mathbb{Z}$-module G is injective if and only if it is a divisible abelian group.*

Exercise 13.5 Show that an abelian group is divisible if and only if it is a homomorphic image of $\mathbb{Q}^{(X)}$ for some set X.

Proposition 13.6 *Direct summands of injective modules are injective.*

Theorem 13.7 *Every right R-module can be embedded in an injective right R-module.*

Corollary 13.8 *The following conditions are equivalent for a right R-module E_R:*

(i) *The module E_R is injective.*
(ii) *Every short exact sequence that begins with E_R splits, that is, every short exact sequence of right R-modules of the form $0 \to E_R \to B_R \to C_R \to 0$ splits.*
(iii) *The module E_R is a direct summand of every module of which it is a submodule.*

14 Projective Covers

Every module is a homomorphic image of a projective module, because every module M_R is a homomorphic image of the free module $R^{(M_R)}$. Now we look for the smallest possible representation of M_R as a homomorphic image of a projective module.

Definition 14.1 (Projective cover). A projective cover of a module M_R is a pair (P_R, p) where P_R is a projective right R-module and $p \colon P \to M$ is a superfluous epimorphism (that is, an epimorphism $p \colon P \to M$ with $\ker p$ a superfluous submodule of P).

Theorem 14.2 (1) (Fundamental lemma of projective covers) *Let (P, p) be a projective cover of a right R-module M. If Q is a projective module and $q \colon Q \to M$ is an epimorphism, then Q has a direct-sum decomposition $Q = P' \oplus P''$ where $P' \cong P$, $P'' \subseteq \ker(q)$ and $(P', q|_{P'} \colon P' \to M)$ is a projective cover.*

(2) (Uniqueness of projective covers up to isomorphism) *Projective covers, when they exist, are unique up to isomorphism in the following sense. If* (P, p), (Q, q) *are any two projective covers of a right* R*-module* M*, there is an isomorphism* $h \colon Q \to P$ *such that* $p \circ h = q$.

15 Injective Envelopes

A submodule N of a module M_R is *essential* (or *large*) in M_R if, for every submodule L of M_R, $N \cap L = 0$ implies $L = 0$. In this case, we will write $N \leq_e M_R$.

Exercise 15.1 Show that

(a) If $K \leq N \leq M_R$, then $K \leq_e M$ if and only if $K \leq_e N$ and $N \leq_e M$.
(b) If $N, N' \leq M_R$, then $N \cap N' \leq_e M$ if and only if $N \leq_e M$ and $N' \leq_e M$.
(c) The submodule M is always essential in M_R, when $M_R = 0$ also.
(d) If $f \colon M \to M'$ is a morphism of R-modules and $N' \leq_e M'$, then $f^{-1}(N') \leq_e M$.
(e) A submodule N of an R-module M is essential in M if and only if for every $x \in M$, $x \neq 0$, there exists $r \in R$ with $xr \in N$ and $xr \neq 0$.
(f) Assume $N_1 \leq M_1 \leq M$, $N_2 \leq M_2 \leq M$ and $M = M_1 \oplus M_2$. Show that $N_1 \oplus N_2 \leq_e M_1 \oplus M_2$ if and only if $N_1 \leq_e M_1$ and $N_2 \leq_e M_2$.

A monomorphism $f \colon N_R \to M_R$ is said to be *essential* if its image $f(N_R)$ is an essential submodule of M_R.

Exercise 15.2 (a) Show that a monomorphism $f \colon N \to M$ is essential if and only if for every module L and every morphism $g \colon M \to L$, if gf is injective, then g is injective.
(b) Let $f \colon N \to M$ and $g \colon M \to P$ be two monomorphisms. Show that the composite mapping gf is an essential monomorphism if and only if both f and g are essential monomorphisms.

Let M_R be a right R-module. An *extension* of M_R is a pair (N_R, f), where N_R is a right R-module and $f \colon M_R \to N_R$ is a monomorphism. An *essential extension* of M_R is an extension (N_R, f) where $f \colon M_R \to N_R$ is an essential monomorphism. An extension (N_R, f) of M_R is *proper* if f is not an isomorphism.

Proposition 15.3 *A module* M_R *is injective if and only if it does not have proper essential extensions.*

Definition 15.4 An *injective envelope* of a module M_R is a pair (E_R, i), where E_R is an injective right R-module and $i \colon M_R \to E_R$ is an essential monomorphism. Equivalently, (E_R, i) is an essential extension of M_R with E_R an injective module.

For example, if i is the inclusion of $\mathbb{Z}_\mathbb{Z}$ into $\mathbb{Q}_\mathbb{Z}$, then $(\mathbb{Q}_\mathbb{Z}, i)$ is an injective envelope of $\mathbb{Z}_\mathbb{Z}$. Dualizing the proof of the Fundamental lemma of projective covers, we get the following

Theorem 15.5 (Fundamental lemma of injective envelopes). *Let (E, i) be an injective envelope of a right R-module M. If F is an injective module and $j: M \to F$ is a monomorphism, then F has a direct-sum decomposition $F = F' \oplus F''$ where $F' \cong E$, $j(M) \subseteq F'$ and if $j': M_R \to F'$ is the mapping obtained from j restricting the codomain to F', then (F', j') is an injective envelope of M.*

Theorem 15.6 *Every right R-module has an injective envelope, which is unique up to isomorphism in the following sense: if (E, i) and (E', i') are both injective envelopes of M, then there exists an isomorphism $h: E \to E'$ such that $hi = i'$.*

Theorem 15.7 *The following conditions are equivalent for an extension (E, ε) of a right R-module M:*

1. (a) *(E, ε) is an injective envelope of M, that is, an essential injective extension of M.*
2. (b) *(E, ε) is a maximal essential extension of M.*
3. (c) *(E, ε) is a minimal injective extension of M.*

16 The Monoid $V(R)$

Our main example of monoid $V(\mathscr{C})$ is when the category $\mathscr{C}$ is the full subcategory proj-R of Mod-R whose objects are all finitely generated projective right R-modules. We will denote such a monoid $V(\text{proj-}R)$ by $V(R)$. Thus $V(R)$ is a set of representatives of all finitely generated projective right R-modules up to isomorphism. Notice that $V(R)$ is a set, because every finitely generated projective R-module is isomorphic to a direct summand of the module $R_R^{(\aleph_0)}$. For any finitely generated projective right R-module P_R, the unique module in $V(R)$ isomorphic to P_R will be denoted by $\langle P_R \rangle$. Thus we have a mapping $\langle - \rangle: \text{Ob(proj-}R) \to V(R)$, with the property that, for every $P_R, Q_R \in \text{Ob(proj-}R)$, $\langle P_R \rangle = \langle Q_R \rangle$ if and only if $P_R \cong Q_R$. The set $V(R)$ becomes a reduced commutative monoid with respect to the addition defined by $\langle P_R \rangle + \langle Q_R \rangle = \langle P_R \oplus Q_R \rangle$ for every $\langle P_R \rangle, \langle Q_R \rangle \in V(R)$. The element $\langle R_R \rangle$ of the monoid $V(R)$ is an order-unit in $V(R)$.

For instance, if R is a semisimple artinian ring, finitely generated (projective) modules are direct sums of simple modules in a unique way up to isomorphism, and there are only finitely many simple modules up to isomorphism. Thus $V(R)$ is a finitely generated free monoid in this case. More precisely, for R a semisimple artinian ring, we have that $V(R) \cong \mathbb{N}_0^n$, where n is the number of simple right R-modules up to isomorphism.

We have defined $V(R)$ using the category proj-R, that is, *right* R-modules. Let us show that if we had taken as $\mathscr{C}$ the full subcategory R-proj of R-Mod whose objects are all finitely generated projective *left* R-modules, we would have got essentially the same object, that is, we would have got isomorphic monoids.

Proposition 16.1 *The functor* $\mathrm{Hom}(-, R)\colon \text{proj-}R \to R\text{-proj}$ *is a duality, that is, an equivalence between the category* proj-R *and the dual category* $(R\text{-proj})^{\mathrm{op}}$ *of the category* R-proj.

Proof The functor $\mathrm{Hom}(-, R)$ is additive, hence preserves direct summands and finite direct sums and sends R_R to $\mathrm{Hom}(R_R, R) \cong {}_RR$.

It immediately follows that the two monoids $V(\text{proj-}R)$ and $V(R\text{-proj})$ are isomorphic via the isomorphism defined by $\langle P_R\rangle \mapsto \langle {}_R\mathrm{Hom}(P_R, R_R)\rangle$ for every $\langle P_R\rangle \in V(R)$. In other words, if, instead of finitely generated projective right R-modules, we use finitely generated projective left R-modules, we essentially get the same monoid $V(R)$. Also notice that the categories proj-R and R^{op}-proj, where R^{op} denotes the opposite ring of R, are isomorphic. Thus $V(R) \cong V(R^{\mathrm{op}})$.

A *right hereditary ring* is a ring in which every right ideal is projective. Similarly for left hereditary. There exist right hereditary rings that are not left hereditary. A *hereditary ring* is a ring that is both right hereditary and left hereditary. Hereditary commutative integral domains are called *Dedekind* domains. For instance, principal ideal domains are Dedekind domains.

Theorem 16.2 *Let R be a right hereditary ring. Then every submodule of a free right R-module is isomorphic to a direct sum of right ideals of R.*

In particular, every (finitely generated) projective right module over a right hereditary ring is isomorphic to a direct sum of (finitely many) right ideals of R.

As an example, we now compute the monoid $V(R)$ for a Dedekind domain R. Let R be a Dedekind domain. By Theorem 16.2, every finitely generated projective R-module is isomorphic to a direct sum $I_1 \oplus I_2 \oplus \cdots \oplus I_m$ of $m \geq 0$ non-zero ideals $I_1, I_2, \ldots, I_m$ of R. Moreover, two direct sums $I_1 \oplus I_2 \oplus \cdots \oplus I_m$ and $I'_1 \oplus I'_2 \oplus \cdots \oplus I'_{m'}$ of non-zero ideals I_i, I'_j are isomorphic if and only if $m = m'$ and $I_1 I_2 \ldots I_m \cong I'_1 I'_2 \ldots I'_m$ [15, Lemma 7.6]. Now every Dedekind domain is noetherian, so that the divisorial fractional ideals of R are the non-zero finitely generated R-submodules of the field of fractions K of R, and the product $I * J$ in the commutative monoid $D(R)$ of all divisorial fractional ideals of R coincides with the usual product IJ for any two ideals I, J of R. As every Dedekind domain is a Krull domain, the monoid $D(R)$ is a group. Therefore the class group $\mathrm{Cl}(R)$ of R is the factor group of the multiplicative group $D(R)$ modulo the subgroup $\mathrm{Prin}(R)$ of non-zero principal fractional ideals. Equivalently, $\mathrm{Cl}(R)$ is the multiplicative group of all isomorphism classes of non-zero ideals of the Dedekind domain R. If we map a non-zero element $\langle A_R\rangle$ of $V(R)$, with $A_R \cong I_1 \oplus I_2 \oplus \cdots \oplus I_m$ and $I_1, I_2, \ldots, I_m$ non-zero ideals of R, to the pair $(m, I_1 I_2 \ldots I_m)$, we get an isomorphism of the monoid of non-zero elements of $V(R)$ onto the direct product $\mathbb{N} \times \mathrm{Cl}(R)$ of the additive monoid $\mathbb{N}$ of positive integers and the multiplicatively group $\mathrm{Cl}(R)$. Thus $V(R)$ turns out to be isomorphic to the monoid $M := (\mathbb{N} \times \mathrm{Cl}(R)) \cup \{0\}$, that is, to the direct product $\mathbb{N} \times \mathrm{Cl}(R)$ to which a zero element is adjoined.

We will now show that the monoids $V(R)$ describe the behavior, as far as direct sums are concerned, not only of projective modules, but of *any* module or *any set* of modules. If M_R is a right module over a ring R, let $\mathrm{add}(M_R)$ be the full subcategory of Mod-R whose objects are all modules isomorphic to direct summands of direct sums M^n of finitely many copies of M. For example, proj-$R = \mathrm{add}(R_R)$.

We can construct a monoid $V(\mathrm{add}(M_R))$ in a way similar to that in which we have constructed the monoid $V(R)$. The monoid $V(\mathrm{add}(M_R))$ is the monoid $V(\mathscr{C})$ constructed in Sect. 4 when $\mathscr{C}$ is the full subcategory $\mathrm{add}(M_R)$ of Mod-R. More precisely, we replace R_R with M_R in the construction of $V(R)$. That is, we fix a set $V(\mathrm{add}(M_R))$ of representatives of the modules in $\mathrm{add}(M_R)$ up to isomorphism. Notice that $V(\mathrm{add}(M_R))$ is a set, because every module in $\mathrm{add}(M_R)$ is isomorphic to a direct summand of a direct sum of countably many copies of M_R. For a module N_R in $\mathrm{add}(M_R)$, denote by $\langle N_R\rangle$ the unique module in $V(\mathrm{add}(M_R))$ isomorphic to N_R. Then $V(\mathrm{add}(M_R))$ becomes a commutative reduced monoid with respect to the addition defined by $\langle N_R\rangle + \langle N'_R\rangle = \langle N_R \oplus N'_R\rangle$ for all $\langle N_R\rangle, \langle N'_R\rangle \in V(\mathrm{add}(M_R))$. The element $\langle M_R\rangle$ is an order-unit in $V(\mathrm{add}(M_R))$. Clearly, the commutative monoid with order-unit $(V(\mathrm{add}\, M_R), \langle M_R\rangle)$ is the algebraic object that describes the behavior of all direct-sum decompositions of the module M_R.

Given a ring S, let Proj-S denote the full subcategory of Mod-S whose objects are all projective right S-modules. If M_S is a right S-module, let $\mathrm{Add}(M_S)$ denote the full subcategory of Mod-S whose objects are all modules isomorphic to direct summands of direct sums of copies of M. Let M_S be a right S-module and let $E = \mathrm{End}(M_S)$ be its endomorphism ring, so that ${}_EM_S$ is a bimodule.

Theorem 16.3 *The functors*

$$\mathrm{Hom}_S(M, -)\colon \text{Mod-}S \to \text{Mod-}E \quad \textit{and} \quad - \otimes_E M\colon \text{Mod-}E \to \text{Mod-}S$$

induce an equivalence between the full subcategory $\mathrm{add}(M_S)$ *of* Mod-S *and the full subcategory* proj-E *of* Mod-E. *In particular, the monoids with order-unit*

$$(V(\mathrm{add}(M_S)), \langle M_S\rangle) \qquad \text{and} \qquad (V(E), \langle E_E\rangle)$$

are isomorphic. Moreover, if M_S is finitely generated, they induce an equivalence between the full subcategory $\mathrm{Add}(M_S)$ *of* Mod-S *and the full subcategory* Proj-E *of* Mod-E. □

The Grothendieck group $G(V(R))$ of the monoid $V(R)$ is usually denoted by $K_0(R)$. We conclude with three examples.

Example 16.4 *(1)* Suppose that the ring R is a division ring, or more generally a local ring, that is, a ring with a unique maximal right ideal. Over such a ring every projective module is free of unique rank (local rings are IBN). Therefore proj-$R = \mathcal{F}_{\mathrm{fg}}$ and $V(R) \cong \mathbb{N}_0$, so $K_0(R) \cong \mathbb{Z}$.

(2) For an arbitrary field F and arbitrarily fixed integers $k \geq 0$ and $n \geq 1$, it is possible to construct associative F-algebras R (called Leavitt algebras) over which every finitely generated projective module is free and for which the congruence

$\sim$ of $\mathbb{N}_0$ defined, for every $n, m \in \mathbb{N}_0$, by $n \sim m$ if $R_R^n \cong R_R^m$, is exactly the congruence $\sim_{k,n}$. See Sect. 8. Therefore, for such rings R, one has proj-$R = \mathcal{F}_{\text{fg}}$ and $V(R) \cong \mathbb{N}_0/\sim_{k,n}$. The Grothendieck group $G(M)$ of the monoid $M = \mathbb{N}_0/\sim_{k,n}$ is the cyclic group $G(M) = \mathbb{Z}/n\mathbb{Z}$, and the canonical mapping $M \to G(M)$ is the mapping $\mathbb{N}_0/\sim_{k,n} \to \mathbb{Z}/n\mathbb{Z}$, $[t]_{\sim_{k,n}} \mapsto t + n\mathbb{Z}$ for every integer $t \geq 0$.

Example 16.5 A ring R is *semilocal* if $R/J(R)$ is semisimple artinian. It is possible to prove that if R is semilocal, then $V(R)$ is a finitely generated reduced Krull monoid [8, Corollary 3.30]. If M_R is an artinian right module over an arbitrary ring R, then the endomorphism ring $E := \text{End}(M_R)$ is a semilocal ring, so that $V(\text{add}(M_R)) \cong V(E)$ is a finitely generated reduced Krull monoid [8, p. 107].

Acknowledgements The author is partially supported by Ministero dell'Istruzione, dell'Università e della Ricerca (Progetto di ricerca di rilevante interesse nazionale "Categories, Algebras: Ring-Theoretical and Homological Approaches (CARTHA)"), Fondazione Cariverona (Research project "Reducing complexity in algebra, logic, combinatorics - REDCOM" within the framework of the programme "Ricerca Scientifica di Eccellenza 2018"), and Dipartimento di Matematica "Tullio Levi-Civita" of Università di Padova (Research program DOR1828909 "Anelli e categorie di moduli").

References

1. Altun-Özarslan, M., Facchini, A.: The Krull-Schmidt-Remak-Azumaya Theorem for G-groups. In: Leroy, A., Lomp, Ch., López-Permouth, S., Oggier, F. (eds.) Rings, Modules and Codes, pp. 25–38. American Mathematical Society, Providence (2019)
2. Anderson, F.W., Fuller, K.R.: Rings and Categories of Modules, 2nd edn. Springer, New York (1992). https://doi.org/10.1007/978-1-4612-4418-9
3. Ara, P., Facchini, A.: Direct sum decompositions of modules, almost trace ideals, and pullbacks of monoids. Forum Math. **18**, 365–389 (2006)
4. Bourbaki, N.: Éléments de mathématique. Fasc. XXVI, Groupes et algèbres de Lie. Chapitre I: Algèbres de Lie, Seconde édition. Hermann, Paris (1971)
5. Chouinard, L.G., II.: Krull semigroups and divisor class groups. Canad. J. Math. **33**, 1459–1468 (1981)
6. Clifford, A.H., Preston, G.B.: The Algebraic Theory of Semigroups, vol. I. American Mathematical Society, Providence (1961)
7. Facchini, A.: Module Theory. Endomorphism Rings and Direct Sum Decompositions in Some Classes of Modules. Birkhäuser Verlag, Basel (1998, reprinted in 2010). https://doi.org/10.1007/978-3-0348-0303-8
8. Facchini, A.: Semilocal Categories and Modules with Semilocal Endomorphism Rings. Birkhäuser/Springer, Cham (2019). https://doi.org/10.1007/978-3-030-23284-910.1007/978-3-030-23284-9
9. Facchini, A., Finocchiaro, C.A.: Pretorsion theories, stable category and preordered sets. Ann. Mat. Pura Appl. **199**, 1073–1089 (2020)
10. Facchini, A., Halter-Koch, F.: Projective modules and divisor homomorphisms. J. Algebra Appl. **2**, 435–449 (2003)
11. Facchini, A., Herbera, D.: Projective modules over semilocal rings. In: Huynh, D.V., Jain, S.K., López-Permouth, S.R. (eds.) Algebra and Its Applications, pp. 181–198. American Mathematical Society, Providence (2000)

12. Goodearl, K.R.: Von Neumann Regular Rings, 2nd edn. Robert E. Krieger Publishing Co. Inc., Malabar (1991)
13. Halter-Koch, F.: Ideal Systems. An Introduction to Multiplicative Ideal Theory. Marcel Dekker, New York (1998)
14. Lam, T.Y.: A First Course in Noncommutative Rings, 2nd edn. Springer, New York (2001). https://doi.org/10.1007/978-1-4419-8616-0
15. Passman, D.S.: A Course in Ring Theory. AMS Chelsea Publishing, American Mathematical Society, Providence (2004)
16. Pirashvili, I.: On the spectrum of monoids and semilattices. J. Pure Appl. Algebra **217**, 901–906 (2013)
17. Suzuki, M.: Group Theory I. Springer, Heidelberg (1982)