

Module theory

By a *ring* we always mean a ring with 1, and by a module we always mean an unitary left-module.

1.1. Homomorphisms; Projective and injective modules

Let R and S be rings.

For additive abelian groups A, B , we denote by $\text{Hom}(A, B)$ the group of all homomorphisms $A \rightarrow B$, equipped with pointwise addition and zero homomorphism $0: A \rightarrow B$, and by $\text{End}(A) = \text{Hom}(A, A)$ the endomorphism ring of A , with multiplication $(f, g) \mapsto f \circ g$. $\mathbf{0} = \{0\}$ denotes the trivial additive abelian group and also the zero ring.

Let M be an abelian group.

Let $\sigma: R \times M \rightarrow M$, $(r, m) \mapsto rm$, be a (left) R -module structure on M . For $r \in R$, define $\sigma^*(r): M \rightarrow M$ by $\sigma^*(r)(m) = rm$. Then $\sigma^*(r) \in \text{End}(M)$, and the map $\sigma^*: R \rightarrow \text{End}(M)$ is a ring homomorphism. Conversely, if $\theta: R \rightarrow \text{End}(M)$ is a ring homomorphism, then $\theta_*: R \times M \rightarrow M$, defined by $\theta_*(r, m) = \theta(r)(m)$, is a (left) R -module structure on M , and $(\theta_*)^* = \theta$. If $\sigma: R \times M \rightarrow M$ is any (left) R -module structure on M , then $(\sigma^*)_* = \sigma$.

Next, let $\sigma: M \times R \rightarrow M$, $(m, r) \mapsto mr$, be a right R -module structure on M . Let R^{op} be the opposite ring of R , having the same addition law as R and the multiplication law $x \cdot_{\text{op}} y = yx$. For $r \in R$, the map $\sigma^*(r): M \rightarrow M$, defined by $\sigma^*(r)(m) = mr$, is again an endomorphism of M , but for $r, s \in R$, we have $\sigma^*(rs) = \sigma^*(s) \circ \sigma^*(r)$, and therefore $\sigma^*: R^{\text{op}} \rightarrow \text{End}(M)$ is a ring homomorphism. Conversely, if $\theta: R^{\text{op}} \rightarrow \text{End}(M)$ is a ring homomorphism, then $\theta_*: M \times R \rightarrow M$, defined by $\theta_*(m, r) = \theta(r)(m)$, is a right R -module structure on M , and $(\theta_*)^* = \theta$. If $\sigma: M \times R \rightarrow M$ is any right R -module structure on M , then $(\sigma^*)_* = \sigma$.

A (left) R -module is an abelian group M , together with an R -module structure, defined either by a scalar product $R \times M \rightarrow M$ or by a homomorphism $R \rightarrow \text{End}(M)$. We write ${}_R M$ to indicate that M is an R -module. For R -modules M, N , we denote by $\text{Hom}_R(M, N)$ the set of all R -homomorphisms $M \rightarrow N$, and we denote by $R\text{-Mod}$ the category of all R -modules.

A right R -module is an abelian group M , together with a right R -module structure, defined either by a scalar product $M \times R \rightarrow M$ or by a homomorphism $R^{\text{op}} \rightarrow \text{End}(M)$. Consequently, a right R -module is the same as an R^{op} -module. However, we shall usually avoid the notion R^{op} and write $M = M_R$ to indicate that M is right R -module. For right R -modules M, N , we denote again by $\text{Hom}_R(M, N)$ the set of all R -homomorphisms $M \rightarrow N$, and we denote by $\mathbf{Mod}\text{-}R = R^{\text{op}}\text{-Mod}$ the category of all right R -modules.

In any case, $\text{Hom}_R(M, N)$, equipped with pointwise addition, is a subgroup of $\text{Hom}(M, N)$. Note that in general $\text{Hom}_R(M, N)$ does not have the structure of an R -module.

If R is commutative, then $R = R^{\text{op}}$, and $R\text{-Mod} = \mathbf{Mod}\text{-}R$. In particular, $\mathbb{Z}\text{-Mod} = \mathbf{Ab}$ is the category of abelian groups. For $A, B \in \mathbf{Ab}$, we have $\text{Hom}_{\mathbb{Z}}(A, B) = \text{Hom}(A, B)$. We denote by $\mathbf{0}$ the zero group. It has a unique R -module structure.

Let M be an abelian group, let R_1, R_2 be rings, and for $i \in \{1, 2\}$, let $\theta_i: R_i \rightarrow \text{End}(M)$ be an R_i -module structure on M . Then M is called an (R_1, R_2) -bimodule if $\theta(r_1) \circ \theta(r_2) = \theta(r_2) \circ \theta(r_1)$ for all $r_1 \in R_1$ and $r_2 \in R_2$. More generally, if $k \in \mathbb{N}$, R_1, \dots, R_k are rings and M is an abelian group carrying an R_i -module structure for each $i \in [1, k]$, then M is called an (R_1, \dots, R_k) -multimodule if M is an (R_i, R_j) -bimodule for all $i, j \in [1, k]$ such that $i \neq j$. If M, N are (R_1, \dots, R_k) -multimodules, then a

map $M \rightarrow N$ is called an (R_1, \dots, R_k) -homomorphism if it is an R_i -homomorphism for each $i \in [1, k]$, and we denote by $\text{Hom}_{R_1, \dots, R_k}(M, N)$ the abelian group of all (R_1, \dots, R_k) -homomorphisms $M \rightarrow N$.

If $k, l \in \mathbb{N}$, $R_1, \dots, R_k, S_1, \dots, S_l$ are rings, then an (R_1, \dots, R_k) -left and (S_1, \dots, S_l) -right multimodule M is an $(R_1, \dots, R_k, S_1^{\text{op}}, \dots, S_l^{\text{op}})$ -multimodule, and we write $M = {}_{R_1, \dots, R_k}M_{S_1, \dots, S_l}$ to indicate that M carries this multimodule structure. We denote by $(R_1, \dots, R_k)\text{-Mod-}(S_1, \dots, S_l)$ the category of (R_1, \dots, R_k) -left and (S_1, \dots, S_l) -right multimodules.

Three types of bimodules will be of interest in the sequel: ${}_{R,S}M$ (called one-sided left (R, S) -bimodules), ${}_R M_S$ (called two-sided (R, S) -bimodules), $M_{R,S}$ (called one-sided right (R, S) -bimodules).

Examples.

1. Every R -module is a one-sided and a two-sided (R, \mathbb{Z}) -bimodule: ${}_R M = {}_{R, \mathbb{Z}} M = {}_R M_{\mathbb{Z}}$ and $M_R = {}_{\mathbb{Z}} M_R = M_{\mathbb{Z}, R}$.
2. If R is commutative, then every R -module is a one-sided and a two-sided (R, R) -bimodule: ${}_R M = {}_{R, R} M = {}_R M_R$.
3. Let M be an R -module. Then $\text{End}_R(M) = \text{Hom}_R(M, M) \subset \text{End}(M) = \text{End}_{\mathbb{Z}}(M)$ is a subring, and M is an $\text{End}_R(M)$ -module by means of $\varphi m = \varphi(m)$. Moreover, $M = {}_{\text{End}_R(M), R} M$ is a one-sided $\text{End}_R(M), R$ -bimodule (indeed, $\varphi r m = r \varphi m$ for all $\varphi \in \text{End}_R(M)$, $r \in R$ and $m \in M$).
4. R is a two-sided (R, R) -bimodule, $R = {}_R R_R$. For any set I , component-wise scalar multiplication makes both R^I and on $R^{(I)} = \{(x_i)_{i \in I} \in R^I \mid x_i = 0 \text{ for almost all } i \in I\}$ into two-sided (R, R) -bimodules.
5. Let $f: R \rightarrow S$ be a ring homomorphism. Then every S -module $N = {}_S N$ is an R -module by means of $r n = f(r) n$ for all $r \in R$ and $n \in N$, and (similarly) every right S -module $N = N_S$ is a right R -module. In particular, ${}_S R$ is a two-sided (S, R) -bimodule (and also a two-sided (R, S) -bimodule). If N, N' are S -modules, then it follows that $\text{Hom}_S(N, N') \subset \text{Hom}_R(N, N')$, and equality holds if f is surjective.
6. Let R be commutative. By an R -algebra we mean a ring S , together with an R -module structure $R \times S \rightarrow S$, $(r, s) \mapsto r s$ such that $r(ss') = (rs)s' = s(rs')$ for all $r \in R$ and $s, s' \in S$. Then the map $f: R \rightarrow S$, defined by $f(r) = r 1_S$, is a ring homomorphism satisfying $f(R) \subset \text{center}(S)$ [indeed, if $r, r' \in R$, then $f(rr') = (rr') 1_S = r(r' 1_S) = r[1_S(r' 1_S)] = (r 1_S)(r' 1_S) = f(r)f(r')$, and if $s \in S$, then $f(r)s = (r 1_S)s = r(1_S s) = r(s 1_S) = s(r 1_S) = s f(r)$]. The homomorphism f is called the *structural homomorphism* of the R -algebra S . Conversely, if $f: R \rightarrow S$ is a ring homomorphism such that $f(R) \subset \text{center}(S)$, then S is an R -module by means of $r s = f(r)s$ for all $r \in R$ and $s \in S$, and with this R -module structure the ring S is an R -algebra with structural homomorphism f . Therefore also the homomorphism $f: R \rightarrow S$ itself is called an R -algebra. Every ring R is a \mathbb{Z} -algebra in a unique way [indeed, there is a unique homomorphism $\varepsilon: \mathbb{Z} \rightarrow R$, given by $\varepsilon(g) = g 1_R$ for all $g \in \mathbb{Z}$].

If $f: R \rightarrow S$ is an R -algebra, then every S -module N is an (R, S) -bimodule, ${}_S N = {}_{R, S} N$.

Examples of algebras:

Every homomorphism $f: R \rightarrow S$ of commutative rings is an R -algebra. Let S be a ring and $R \subset \text{center}(S)$ a subring. then S is an R -algebra. If R is commutative and $n \in \mathbb{N}$, then the matrix ring $M_n(R)$ is an R -algebra. If R is commutative and M is an R -module, then $\text{End}_R(M)$ is an R -algebra.

Theorem and Definition 1.1.1. *Let M, N be R -modules.*

1. *Assume that $M = {}_R M_S$. For $s \in S$ and $f \in \text{Hom}_R(M, N)$ let $sf: M \rightarrow N$ be defined by $(sf)(m) = f(ms)$ for all $s \in S$ and $m \in M$. Then sf is an R -homomorphism, and $(s, f) \mapsto sf$ is an S -module structure on $\text{Hom}_R(M, N)$:*

$${}_S \text{Hom}_R({}_R M_S, {}_R N); \quad \text{in the same way: } \text{Hom}_R({}_R M_S, {}_R N)_S.$$

2. Assume that $N = {}_{R,S}N$. For $s \in S$ and $f \in \text{Hom}_R(M, N)$ let $sf: M \rightarrow N$ be defined by $(sf)(m) = sf(m)$. Then sf is an R -homomorphism, and $(s, f) \mapsto sf$ is an S -module structure on $\text{Hom}_R(M, N)$:

$${}_S\text{Hom}_R({}_R M, {}_{R,S}N); \quad \text{in the same way: } \text{Hom}_R({}_R M, {}_R N_S)_S.$$

3. Let R be commutative. Then $\text{Hom}_R(M, N)$ is an R -module by means of $(rf)(m) = f(rm)$ for all $f \in \text{Hom}_R(M, N)$, $r \in R$ and $m \in M$.

PROOF. 1. We must prove :

- For all $f \in \text{Hom}_R(M, N)$ and $s \in S$, the map $sf: M \rightarrow N$ is an R -homomorphism, that is
 - $(sf)(m + m') = (sf)(m) + (sf)(m')$ for all $m, m' \in M$;
 - $(sf)(rm) = r[(sf)(m)]$ for all $m \in M$ and $r \in R$ [here we use the bimodule structure].
- $(s, f) \mapsto sf$ is an S -module structure on $\text{Hom}_R(M, N)$, that is, for all $f, f' \in \text{Hom}_R(M, N)$ and all $s, s' \in S$, the following equalities hold pointwise for all $m \in M$:
 - $(s(f + f')) = sf + sf'$;
 - $(s + s')f = sf + s'f$;
 - $(ss')f = s(s'f)$;
 - $1_S f = f$.

All this is easy.

2. The same things as in 1. must be checked.
 3. By 2., since $N = {}_{R,R}N$. □

For R -modules M, N, P , the composition map

$$\text{Hom}_R(N, P) \times \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M, P), \quad (g, f) \mapsto g \circ f,$$

is \mathbb{Z} -bilinear [that is, $g \circ (f + f') = g \circ f + g \circ f'$ and $(g + g') \circ f = g \circ f + g' \circ f$ for all $g, g' \in \text{Hom}_R(N, P)$ and $f, f' \in \text{Hom}_R(M, N)$].

Let $f: M \rightarrow M'$ be an R -homomorphism and N an R -module. We define

$$f_* = \text{Hom}_R(N, f): \text{Hom}_R(N, M) \rightarrow \text{Hom}_R(N, M') \quad \text{by} \quad f_*(\varphi) = \text{Hom}(N, f)(\varphi) = f \circ \varphi$$

and

$$f^* = \text{Hom}_R(f, N): \text{Hom}_R(M', N) \rightarrow \text{Hom}_R(M, N) \quad \text{by} \quad f^*(\varphi) = \text{Hom}(f, N)(\varphi) = \varphi \circ f.$$

Then f_* and f^* are group homomorphisms satisfying $(f + g)_* = f_* + g_*$ and $(f + g)^* = f^* + g^*$ for all $f, g \in \text{Hom}_R(M, M')$. If $M \xrightarrow{f} M' \xrightarrow{f'} M''$ are R -homomorphisms, then $(f' \circ f)_* = f'_* \circ f_*$ and $(f' \circ f)^* = f'^* \circ f^*$.

A (covariant or contravariant) functor $T: R\text{-Mod} \rightarrow \mathbf{Ab}$ is called *additive* if, for all $M, N \in R\text{-Mod}$, the map $T: \text{Hom}_R(M, N) \rightarrow \text{Hom}(TM, TN)$ is a group homomorphism [explicitly, $T(f + g) = Tf + Tg$ for all R -homomorphisms $f, g: M \rightarrow N$ of R -modules.] If T is an additive functor, then $T\mathbf{0} = \mathbf{0}$ [indeed, if M is an R -module, then $M = \mathbf{0}$ if and only if $\text{id}_M = 0$, and then $\text{id}_{TM} = T\text{id}_M = T0 = 0$].

For $N \in R\text{-Mod}$, the map $\text{Hom}_R(N, -): R\text{-Mod} \rightarrow \mathbf{Ab}$ is a (covariant) additive functor, and the map $\text{Hom}_R(-, N): R\text{-Mod} \rightarrow \mathbf{Ab}$ is a contravariant additive functor.

Theorem 1.1.2. *Let M be an R -module. Then the map*

$$\Phi = \Phi_M: M \rightarrow \text{Hom}_R(R, M), \quad \text{defined by } m \mapsto (r \mapsto rm),$$

is an R -isomorphism which is functorial in M , and $\Phi^{-1}(f) = f(1)$ for all $f \in \text{Hom}_R(R, M)$.

PROOF. The R -module structure on $\text{Hom}_R(R, M) = \text{Hom}_R({}_R R, {}_R M)$ is given by $(\lambda f)(r) = f(r\lambda)$ for all $f \in \text{Hom}_R(R, M)$ and $\lambda, r \in R$. We must prove :

- 1) For every $m \in M$, the map $\Phi(m) = (r \mapsto rm)$ is an R -homomorphism.
- 2) $\Phi: M \rightarrow \text{Hom}_R(R, M)$ is an R -homomorphism.
- 3) If $\Psi: \text{Hom}_R(R, M) \rightarrow M$ is defined by $\Psi(f) = f(1)$, then $\Psi \circ \Phi = \text{id}_M$ and $\Phi \circ \Psi = \text{id}_{\text{Hom}_R(R, M)}$.

4) Every homomorphism $\varphi: M \rightarrow M'$ of R -modules induces a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\Phi_M} & \text{Hom}_R(R, M) \\ \varphi \downarrow & & \downarrow \text{Hom}(R, \varphi) \\ M' & \xrightarrow{\Phi_{M'}} & \text{Hom}_R(R, M'). \end{array}$$

All this is easy. \square

A sequence $M' \xrightarrow{f} M \xrightarrow{g} M''$ of R -(module)-homomorphisms is called *exact* if $\text{Ker}(g) = \text{Im}(f)$, and an (eventually long) sequence $\dots \rightarrow M_{i+1} \rightarrow M_i \rightarrow M_{i-1} \rightarrow \dots$ of R -homomorphisms is called *exact* if every 3-term subsequence is exact. Special cases:

- $\mathbf{0} \rightarrow M' \xrightarrow{f} M$ is exact if and only if f is a monomorphism.
- $M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ is exact if and only if g is an epimorphism.
- Every R -homomorphism $f: M \rightarrow N$ induces an exact sequence

$$\mathbf{0} \rightarrow \text{Ker}(f) \hookrightarrow M \xrightarrow{f} N \rightarrow \text{Coker}(f) = M/\text{Im}(f) \rightarrow \mathbf{0}.$$

- An exact sequence $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ is called a *short exact sequence*. By definition, $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ is a short exact sequence if and only if f is a monomorphism, g is an epimorphism, $g \circ f = 0$ and $\text{Ker}(g) \subset \text{Im}(f)$. Then $f: M' \xrightarrow{\sim} \text{Ker}(g) = \text{Bi}(f)$ is an isomorphism, g induces an isomorphism $g^*: M/\text{Im}(f) = M/\text{Ker}(g) \xrightarrow{\sim} M''$, and we obtain the commutative diagram

$$\begin{array}{ccccccc} \mathbf{0} & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & \mathbf{0} \\ & & f \downarrow & & \downarrow \text{id}_M & & \uparrow g^* & & \\ \mathbf{0} & \longrightarrow & \text{Im}(f) & \longrightarrow & M & \xrightarrow{\pi} & M/\text{Im}(f) & \longrightarrow & \mathbf{0} \end{array}$$

where the vertical arrows are isomorphisms.

- Let $\mathbf{0} \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow \mathbf{0}$ be a short exact sequence of R -modules. If both M' and M'' are finitely generated, then M is finitely generated. Conversely, if M is finitely generated, then M'' is finitely generated, and if R is left noetherian, then M' is also finitely generated.
- An R -module M is called *finitely presented* if there is an exact sequence $F' \rightarrow F \rightarrow M \rightarrow \mathbf{0}$ with finitely generated free R -modules [equivalently, there is an epimorphism $\pi: F \rightarrow M$, where F is a finitely generated free R -module and $\text{Ker}(\pi)$ is finitely generated. Every finitely presented R -module is finitely generated, and if R is left noetherian, then every finitely generated R -module is finitely presented.
- Let M', M'' be R -modules and $M' \oplus M''$ the (outer) direct sum. Let $\varepsilon': M' \rightarrow M' \oplus M''$ and $\varepsilon'': M'' \rightarrow M' \oplus M''$ be the canonical injections and $p': M' \oplus M'' \rightarrow M'$, $p'': M' \oplus M'' \rightarrow M''$ the canonical projections, defined by

$$\varepsilon'(m') = (m', 0), \quad \varepsilon''(m'') = (0, m''), \quad p'(m', m'') = m' \quad \text{and} \quad p''(m', m'') = m''.$$

Then $p' \circ \varepsilon' = \text{id}_{M'}$, $p'' \circ \varepsilon'' = \text{id}_{M''}$, $p' \circ \varepsilon'' = 0$, $p'' \circ \varepsilon' = 0$, $\varepsilon' \circ p' + \varepsilon'' \circ p'' = \text{id}_{M' \oplus M''}$, and there are short exact sequences

$$\mathbf{0} \rightarrow M' \xrightarrow{\varepsilon'} M' \oplus M'' \xrightarrow{p''} M'' \rightarrow \mathbf{0} \quad \text{and} \quad \mathbf{0} \rightarrow M'' \xrightarrow{\varepsilon''} M' \oplus M'' \xrightarrow{p'} M' \rightarrow \mathbf{0}.$$

If $M', M'' \subset M$ are submodules of an R -module M , the M is called (internal) direct sum of M' and M'' if one of the following equivalent conditions is satisfied:

- $M = M' + M''$ and $M' \cap M'' = \mathbf{0}$.
- The map $M' \oplus M'' \rightarrow M$, $(m', m'') \mapsto m' + m''$, is an isomorphism.
- Every $m \in M$ has a unique representation $m = m' + m''$, where $m' \in M'$ and $m'' \in M''$.

If these conditions are fulfilled, then we write $M = M' \dot{+} M''$ and denote by $p': M \rightarrow M'$ and $p'': M \rightarrow M''$ the maps defined by $p'(m' + m'') = m'$ and $p''(m' + m'') = m''$ for all $m' \in M'$ and $m'' \in M''$. Then p' and p'' are R -homomorphisms, $p'|M' = \text{id}_{M'}$ and $p''|M'' = \text{id}_{M''}$. We call p' and p'' the *projections* of M onto M' and M'' .

An R -submodule $N \subset M$ is called a *direct summand* if $M = N \dot{+} N'$ for some R -submodule $N' \subset M$. In this case, we write $N \triangleleft M$.

Theorem and Definition 1.1.3.

1. An R -submodule $M' \subset M$ is a direct summand of M if and only if there exists an R -homomorphism $p: M \rightarrow M'$ such that $p|M' = \text{id}_{M'}$.
2. Let $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ be a short exact sequence of R -modules. Then the following assertions are equivalent:

(a) There exists an R -isomorphism $\Phi: M' \oplus M'' \rightarrow M$ such that the following diagram is commutative:

$$\begin{array}{ccccccc} \mathbf{0} & \longrightarrow & M' & \xrightarrow{\varepsilon'} & M' \oplus M'' & \xrightarrow{p''} & M'' \longrightarrow \mathbf{0} \\ & & \text{id}_{M'} \downarrow & & \downarrow \Phi & & \downarrow \text{id}_{M''} \\ \mathbf{0} & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' \longrightarrow \mathbf{0} \end{array}$$

- (b) $\text{Im}(f) = \text{Ker}(g)$ is a direct summand of M .
(c) There exists some R -homomorphism $\varphi: M \rightarrow M'$ such that $\varphi \circ f = \text{id}_{M'}$.
(d) There exists some R -homomorphism $\psi: M'' \rightarrow M$ such that $g \circ \psi = \text{id}_{M''}$.

Moreover, the following assertions hold:

- (i) If $\varphi: M \rightarrow M'$ is any R -homomorphism such that $\varphi \circ f = \text{id}_{M'}$, then $M = \text{Bi}(f) \dot{+} \text{Ker}(\varphi)$.
- (ii) If $\psi: M'' \rightarrow M$ is any R -homomorphism such that $g \circ \psi = \text{id}_{M''}$, then $M = \text{Ker}(g) \dot{+} \text{Bi}(\psi)$.
- (iii) The homomorphisms φ and ψ in (c) and (d) above can be chosen so that $f \circ \varphi + \psi \circ g = \text{id}_M$.

If these conditions are satisfied, we say that the short exact sequence $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ *splits* or is a *split exact sequence*. An R -monomorphism $f: M' \rightarrow M$ is said to *split* if there exists some R -homomorphism $\varphi: M \rightarrow M'$ such that $\varphi \circ f = \text{id}_{M'}$ [equivalently, $\text{Im}(f) \triangleleft M$]. An R -epimorphism $g: M \rightarrow M''$ is said to *split* if there exists an R -homomorphism $\psi: M'' \rightarrow M$ such that $g \circ \psi = \text{id}_{M''}$ [equivalently, $\text{Ker}(g) \triangleleft M$].

3. Suppose that $M' \xrightarrow{f} M \xrightarrow{g} M''$ and $M'' \xrightarrow{\psi} M \xrightarrow{\varphi} M'$ are homomorphisms of R -modules such that $\varphi \circ f = \text{id}_{M'}$, $g \circ \psi = \text{id}_{M''}$ and $f \circ \varphi + \psi \circ g = \text{id}_M$. Then $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ and $\mathbf{0} \rightarrow M'' \xrightarrow{\psi} M \xrightarrow{\varphi} M' \rightarrow \mathbf{0}$ are split exact sequences.
4. Let $T: R\text{-Mod} \rightarrow \mathbf{Ab}$ be an additive functor and $\mathbf{0} \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow \mathbf{0}$ a split exact sequence. Then $\mathbf{0} \rightarrow TM' \rightarrow TM \rightarrow TM'' \rightarrow \mathbf{0}$ is also a split exact sequence. In particular, $T(M' \otimes M'') \cong TM' \oplus TM''$.

PROOF. 1. If $M' \subset M$ is a direct summand and $p: M \rightarrow M'$ is the projection of M onto M' , then $p|M' = \text{id}_{M'}$.

Conversely, let $p \in \text{Hom}_R(M, M')$ be such that $p|M' = \text{id}_{M'}$. We assert that $M = M' \dot{+} \text{Ker}(p)$. If $m \in M$, then $p(m - p(m)) = p(m) - p(m) = 0$, and $m = p(m) + (m - p(m)) \in M' + \text{Ker}(p)$. If $m \in M' \cap \text{Ker}(p)$, then $0 = p(m) = m$, and thus $M = M' \dot{+} \text{Ker}(p)$.

2. (a) \Rightarrow (b) Since $M' \oplus M'' = \varepsilon'(M') \dot{+} \varepsilon''(M'')$, it follows that $\varepsilon'(M')$ is a direct summand of $M' \oplus M''$, and therefore $\text{Im}(f) = f(M') = \Phi \circ \varepsilon'(M')$ is a direct summand of $\Phi(M' \oplus M'') = M$.

(b) \Rightarrow (c) By 1., there exists some $p \in \text{Hom}_R(M, \text{Im}(f))$ such that $p|\text{Im}(f) = \text{id}_{\text{Im}(f)}$. Since $f: M' \xrightarrow{\sim} \text{Im}(f)$ is an isomorphism and $p \circ f = \text{id}_{\text{Im}(f)}$, it follows that $\varphi = f^{-1} \circ p \in \text{Hom}_R(M, M')$, and $\varphi \circ f = f^{-1} \circ p \circ f = f^{-1} \circ \text{id}_{\text{Im}(f)} = \text{id}_{M'}$.

(i) Let $\varphi \in \text{Hom}_R(M, M')$ be such that $\varphi \circ f = \text{id}_{M'}$. If $m \in M$, then

$$\varphi(m - f \circ \varphi(m)) = \varphi(m) - \varphi \circ f \circ \varphi(m) = 0,$$

and $m = f \circ \varphi(m) + [m - f \circ \varphi(m)] \in \text{Im}(f) + \text{Ker}(\varphi)$. If $m \in \text{Im}(f) \cap \text{Ker}(\varphi)$, then $m = f(m')$ for some $m' \in M'$, and $0 = \varphi(m) = \varphi \circ f(m') = m'$. Hence $m = 0$, and $M = \text{Im}(f) + \text{Ker}(\varphi)$.

(c) \Rightarrow (d) and (iii) If $m'' \in M''$, let $m \in M$ be such that $m'' = g(m)$, and define

$$\psi(m'') = m - f \circ \varphi(m) \in M.$$

This definition is independent of the choice of m . Indeed, suppose that $m, m_1 \in M$ are such that $m'' = g(m) = g(m_1)$. Then $m - m_1 \in \text{Ker}(g) = \text{Im}(f)$, say $m - m_1 = f(m')$ for some $m' \in M'$. Then

$$[m - f \circ \varphi(m)] - [m_1 - f \circ \varphi(m_1)] = (m - m_1) - (f \circ \varphi)(m - m_1) = f(m') - f \circ \varphi \circ f(m') = 0.$$

Next we prove that $\psi: M'' \rightarrow M$ is an R -homomorphism. Thus let $m'', m_1'' \in M''$ and $r \in R$. Let $m, m_1 \in M$ be such that $g(m) = m''$ and $g(m_1) = m_1''$. Then $g(m + m_1) = m'' + m_1''$ and $g(rm) = rm''$. Hence $\psi(m'' + m_1'') = (m + m_1) - (f \circ \varphi)(m + m_1) = [m - f \circ \varphi(m)] + [m_1 - f \circ \varphi(m_1)] = \psi(m'') + \psi(m_1'')$, and $\psi(rm) = rm - f \circ \varphi(rm) = r(m - f \circ \varphi(m)) = r\psi(m'')$.

If $m'' = g(m)$ for some $m \in M$, then $g \circ \psi(m'') = g(m - f \circ \varphi(m)) = g(m) - g \circ f \circ \varphi(m) = m''$, and therefore $g \circ \psi = \text{id}_{M''}$.

If $m \in M$, then $\psi \circ g(m) = m - f \circ \varphi(m)$, and therefore $f \circ \varphi + \psi \circ g = \text{id}_M$, which proves (iii).

(ii) Let $\psi \in \text{Hom}_R(M'', M)$ be such that $g \circ \psi = \text{id}_{M''}$. If $m \in M$, then

$$g(m - \psi \circ g(m)) = g(m) - g \circ \psi \circ g(m) = 0,$$

and $m = (m - \psi \circ g(m)) + \psi \circ g(m) \in \text{Ker}(g) + \text{Im}(\psi)$. If $m \in \text{Ker}(g) \cap \text{Im}(\psi)$, then $m = \psi(m'')$ for some $m'' \in M''$, and $0 = g(m) = g \circ \psi(m'') = m''$. Hence $m = 0$, and $M = \text{Ker}(g) + \text{Im}(\psi)$.

(d) \Rightarrow (d) As $g \circ \psi = \text{id}_{M''}$, it follows that ψ is a monomorphism. Now we define $\Phi: M' \oplus M'' \rightarrow M$ by $\Phi(m', m'') = f(m') + \psi(m'')$ for all $(m', m'') \in M' \times M''$. Then Φ is an R -homomorphism, and it is surjective since $M = \text{Ker}(g) + \text{Im}(\psi) = \text{Im}(f) + \text{Im}(\psi)$. If $(m', m'') \in \text{Ker}(\Phi)$, then $f(m') + \psi(m'') = 0$, hence $0 = g \circ f(m') + g \circ \psi(m'') = m''$, $f(m') = 0$ and therefore also $m' = 0$. Hence Φ is an isomorphism.

If $m' \in M'$, then $\Phi \circ \varepsilon'(m') = \Phi(m', 0) = f(m')$, and thus $\Phi \circ \varepsilon' = f$. If $(m', m'') \in M' \oplus M''$, then $g \circ \Phi(m', m'') = g \circ f(m') + g \circ \psi(m'') = m''$, and therefore $g \circ \Phi = p''$.

3. Since $\varphi \circ f = \text{id}_{M'}$ and $g \circ \psi = \text{id}_{M''}$, it follows that f and ψ are monomorphisms and g is an epimorphism. Now we obtain $f = (f \circ \varphi + \psi \circ g) \circ f = f + \psi \circ g \circ f$, hence $\psi \circ g \circ f = 0$, and therefore $g \circ f = 0$. If $m \in \text{Ker}(g)$, then $m = (f \circ \varphi + \psi \circ g)(m) = f \circ \varphi(m) \in \text{Im}(f)$. Hence the sequence $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ is exact. The same arguments show that the sequence $\mathbf{0} \rightarrow M'' \xrightarrow{\psi} M \xrightarrow{\varphi} M' \rightarrow \mathbf{0}$ is exact, and by definition both sequences split.

4. Let $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ be a split exact sequence. Then there exist R -homomorphisms $\varphi: M \rightarrow M'$ and $\psi: M'' \rightarrow M$ such that $\varphi \circ f = \text{id}_{M'}$, $g \circ \psi = \text{id}_{M''}$ and $f \circ \varphi + \psi \circ g = \text{id}_M$. Then it follows that $T\varphi \circ Tf = T(\varphi \circ f) = \text{id}_{TM'}$, $Tg \circ T\psi = \text{id}_{TM''}$, and $\text{id}_{TM} = T(f \circ \varphi + \psi \circ g) = Tf \circ T\varphi + T\psi \circ Tg$. By 3., $\mathbf{0} \rightarrow TM' \xrightarrow{Tf} TM \xrightarrow{Tg} TM'' \rightarrow \mathbf{0}$ is a split exact sequence. \square

Theorem 1.1.4 (Snake Lemma). *Let*

$$\begin{array}{ccccccc} A' & \xrightarrow{i} & A & \xrightarrow{f} & A'' & \longrightarrow & \mathbf{0} \\ u' \downarrow & & u \downarrow & & u'' \downarrow & & \\ \mathbf{0} & \longrightarrow & B' & \xrightarrow{j} & B & \xrightarrow{g} & B'' \end{array}$$

be a commutative diagram of R -module homomorphisms with exact rows. Then there exists an R -homomorphism $\omega: \text{Ker}(u'') \rightarrow \text{Coker}(u')$ such that there is a long exact sequenc

$$\text{Ker}(u') \xrightarrow{i_0} \text{Ker}(u) \xrightarrow{f_0} \text{Ker}(u'') \xrightarrow{\omega} \text{Coker}(u') \xrightarrow{j^*} \text{Coker}(u) \xrightarrow{g^*} \text{Coker}(u''),$$

where $i_0 = i|_{\text{Ker}(u')}$, $f_0 = f|_{\text{Ker}(u)}$, j^* is induced by j , and g^* is induced by g . If i is a monomorphism, then i_0 is a monomorphism, and if g is an epimorphism, then g^* is an epimorphism. Moreover, ω and the long exact sequence are functorial in the original commutative diagram.

PROOF. 1. Since $j \circ u' = u \circ i$, we get $i(\text{Ker}(u')) \subset \text{Ker}(u)$, and since $g \circ u = u'' \circ f$, we get $f(\text{Ker}(u)) \subset \text{Ker}(u'')$. Hence we obtain R -homomorphisms $i_0 = i|_{\text{Ker}(u')}: \text{Ker}(u') \rightarrow \text{Ker}(u)$ and $f_0 = f|_{\text{Ker}(u)}: \text{Ker}(u) \rightarrow \text{Ker}(u'')$. If i is a monomorphism, then i_0 is also a monomorphism, and $f_0 \circ i_0 = f \circ i|_{\text{Ker}(u')} = 0$. If $a \in \text{Ker}(f_0) \subset \text{Ker}(u) \subset A$, then $f(a) = f_0(a) = 0$, and thus $a = i(a')$ for some $a' \in A'$. Since $j \circ u'(a') = u \circ i(a') = u(a) = 0$ and j is a monomorphism, we get $u'(a') = 0$, hence $a' \in \text{Ker}(u')$, and therefore $a = i(a') = i_0(a') \in \text{Im}(i_0)$. Hence there is an exact sequence $\text{Ker}(u') \xrightarrow{i_0} \text{Ker}(u) \xrightarrow{f_0} \text{Ker}(u'')$.

2. Since $j \circ u' = u \circ i$ and $g \circ u = u'' \circ f$ and $g(\text{Im}(u)) \subset \text{Im}(u'')$. Thus j induces an R -homomorphism $j^*: \text{Coker}(u') = B'/\text{Im}(u') \rightarrow B/\text{Im}(u) = \text{Coker}(u)$, given by $j^*(b' + \text{Im}(u')) = j(b') + \text{Im}(u)$ for all $b' \in B'$, and g induces an R -homomorphism $g^*: \text{Coker}(u) = B/\text{Im}(u) \rightarrow B''/\text{Im}(u'') = \text{Coker}(u'')$, given by $g^*(b + \text{Im}(u)) = g(b) + \text{Im}(u'')$ for all $b \in B$. If g is an epimorphism, then g^* is also an epimorphism, and if $b' \in B'$, then $g^* \circ j^*(b' + \text{Im}(u')) = g \circ j(b') + \text{Im}(u'') = 0 \in \text{Coker}(u'')$. If $b \in B$ and $b + \text{Im}(u) \in \text{Ker}(g^*)$, then $g(b) \in \text{Im}(u'')$, and therefore there exists some $a \in A$ such that $g(b) = u'' \circ f(a) = g \circ u(a)$. Hence $g(b - u(a)) = 0$, and $b - u(a) \in \text{Ker}(g) = \text{Im}(j)$. Let $b' \in B'$ be such that $b - u(a) = j(b')$. Then $b + \text{Im}(u) = j(b') + \text{Im}(u) = j^*(b' + \text{Im}(u')) \in \text{Im}(j^*)$. Hence there is an exact sequence $\text{Coker}(u') \xrightarrow{j^*} \text{Coker}(u) \xrightarrow{g^*} \text{Coker}(u'')$.

3. Now we are going to define ω . Let $a'' \in \text{Ker}(u'') \subset A''$ and $a \in A$ such that $a'' = f(a)$. Then $0 = u'' \circ f(a) = g \circ u(a)$, hence $u(a) \in \text{Ker}(g) = \text{Im}(j)$, and thus $u(a) = j(b')$ for some $b' \in B'$. We set $\omega(a'') = b' + \text{Im}(u') \in \text{Coker}(u')$, and we show that this definition does not depend on the made choices. Indeed, let $a_1 \in A$ be another element such that $a'' = f(a_1)$, and let $b'_1 \in B'$ be such that $u(a_1) = j(b'_1)$. Then $a - a_1 \in \text{Ker}(f) = \text{Im}(i)$, say $a - a_1 = i(a')$, where $a' \in A'$, and therefore $j(b' - b'_1) = u(a - a_1) = u \circ i(a') = j \circ u'(a')$. As j is injective, we obtain $b' - b'_1 = u'(a') \in \text{Im}(u')$, and consequently $b' + \text{Im}(u') = b'_1 + \text{Im}(u')$.

To prove that ω is an R -homomorphism, let $a'', a''_1 \in \text{Ker}(u'')$ and $r \in R$. If $a, a_1 \in A$ are such that $f(a) = a''$ and $f(a_1) = a''_1$, then $f(a + a_1) = a'' + a''_1$ and $f(ra) = ra''$. Let $b', b'_1 \in B'$ be such that $u(a) = j(b')$ and $u(a_1) = j(b'_1)$. Then $u(a + a_1) = j(b' + b'_1)$ and $u(ra) = j(rb')$. Hence we obtain $\omega(a'' + a''_1) = (b' + b'_1) + \text{Im}(u') = (b' + \text{Im}(u')) + (b'_1 + \text{Im}(u')) = \omega(a'') + \omega(a''_1)$, and $\omega(ra'') = rb' + \text{Im}(u') = r(b' + \text{Im}(u'))$.

Next we show that $j^* \circ \omega = 0$. If $a'' = f(a) \in A''$, where $a \in A$ and $u(a) = j(b')$ with $b' \in B'$, then $j^* \circ \omega(a'') = j^*(b' + \text{Im}(u')) = j(b') + \text{Im}(u) = 0 \in \text{Coker}(u)$.

Finally, we prove that $\text{Ker}(\omega) \subset \text{Im}(f_0)$. Thus let $a'' \in \text{Ker}(\omega)$, $a'' = f(a)$, where $a \in A$, and $u(a) = j(b')$, where $b' \in B'$. Then $b' + \text{Im}(u') = \omega(a'') = 0$, hence $b' = u'(a')$ for some $a' \in A'$, and therefore $u(a) = j \circ u'(a') = u \circ i(a')$. Hence it follows that $a - i(a') \in \text{Ker}(u)$, and therefore $f_0(a - i(a')) = f(a) - f \circ i(a') = f(a) = a'' \in \text{Im}(f_0)$.

4. It remains to prove that the whole construction is functorial in the initial data. This is tedious but easy and is left as an exercise. \square

Corollary. Let $\mathbf{0} \rightarrow K \xrightarrow{f} F \xrightarrow{g} M \rightarrow \mathbf{0}$ an exact sequence of R -modules. If M be a finitely presented and F is finitely generated, then K is also finitely generated.

PROOF. As M is finitely presented, there exists an exact sequence $F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} M \rightarrow \mathbf{0}$, where F_1, F_2 are finitely generated free R -modules. Let (u_1, \dots, u_n) be an R -basis of F_1 . Then there exist $x_1, \dots, x_n \in F$ such that $g(x_i) = f_1(u_i)$ for all $i \in [1, n]$, and there exists a unique $\varphi \in \text{Hom}_R(F_1, F)$ such that $\varphi(u_i) = x_i$ for all $i \in [1, n]$. Hence it follows that $f_1(u_i) = g \circ \varphi(u_i)$ for all $i \in [1, n]$, and consequently $f_1 = g \circ \varphi$. Since $g \circ \varphi \circ f_2 = f_1 \circ f_2 = 0$, it follows that $\varphi \circ f_2(F_2) \subset \text{Ker}(g) = \text{Im}f$, and therefore there exists some $\psi \in \text{Hom}_R(F_2, K)$ such that $f \circ \psi = \varphi \circ f_2$. We obtain the following

commutative diagram with exact rows:

$$\begin{array}{ccccccc}
 F_2 & \xrightarrow{f_2} & F_1 & \xrightarrow{f_1} & M & \longrightarrow & \mathbf{0} \\
 \psi \downarrow & & \varphi \downarrow & & \text{id}_M \downarrow & & \\
 \mathbf{0} & \longrightarrow & K & \xrightarrow{f} & F & \xrightarrow{g} & M
 \end{array}$$

Lemma 1.1.4 yields an exact sequence $\mathbf{0} = \text{Ker}(\text{id}_M) \rightarrow \text{Coker}(\psi) \rightarrow \text{Coker}(\varphi) \rightarrow \text{Coker}(\text{id}_M) = \mathbf{0}$, and therefore $K/\text{Im}(\psi) = \text{Coker}(\psi) \cong \text{Coker}(\varphi) = F/\text{Im}(\varphi)$ is finitely generated. Since $\text{Im}(\psi) = \psi(F_2)$ is also finitely generated, it follows that K is finitely generated. \square

Theorem 1.1.5.

1. A sequence $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ of R -homomorphisms is exact if and only if, for every R -module X , the sequence $\mathbf{0} \rightarrow \text{Hom}_R(X, M') \xrightarrow{f_*} \text{Hom}_R(X, M) \xrightarrow{g_*} \text{Hom}_R(X, M'')$ is exact (where $f_* = \text{Hom}(X, f)$ and $g_* = \text{Hom}(X, g)$).
2. A sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ of R -homomorphisms is exact if and only if, for every R -module X , the sequence $\mathbf{0} \rightarrow \text{Hom}_R(M'', X) \xrightarrow{g^*} \text{Hom}_R(M, X) \xrightarrow{f^*} \text{Hom}_R(M', X)$ is exact (where $g^* = \text{Hom}(g, X)$ and $f^* = \text{Hom}(f, X)$).

PROOF. 1. Assume first that $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact, and let X be an R -module. If $(\varphi: X \rightarrow M') \in \text{Ker}(f_*)$, then $0 = f_*(\varphi) = f \circ \varphi$, and as f is a monomorphism, we obtain $\varphi = 0$. Hence f_* is a monomorphism. $g_* \circ f_* = (g \circ f)_* = 0_* = 0$, and it remains to prove that $\text{Ker}(g_*) \subset \text{Im}(f_*)$. If $(\varphi: X \rightarrow M) \in \text{Ker}(g_*)$, then $0 = g_*(\varphi) = g \circ \varphi$, hence $\text{Im}(\varphi) \subset \text{Ker}(g) = \text{Im}(f)$. Since $f: M' \rightarrow \text{Im}(f)$ is an isomorphism, it follows that $\varphi' = f^{-1} \circ \varphi \in \text{Hom}(X, M')$, and $\varphi = f \circ \varphi' = f_*(\varphi') \in \text{Im}(f_*)$.

To prove the converse, we consider the assumption with $X = R$ and obtain the commutative diagram

$$\begin{array}{ccccccc}
 \mathbf{0} & \longrightarrow & \text{Hom}_R(R, M') & \xrightarrow{f_*} & \text{Hom}_R(R, M) & \xrightarrow{g_*} & \text{Hom}_R(R, M'') \\
 & & \cong \downarrow & & \downarrow \cong & & \downarrow \cong \\
 \mathbf{0} & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M''
 \end{array}$$

where the vertical arrows are the isomorphisms of Theorem 1.1.2 and the bottom line is exact. Hence the upper line is also exact.

2. Assume first that the sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ is exact, and let X be an R -module. If $(\psi: M'' \rightarrow X) \in \text{Ker}(g^*)$, then $0 = g^*(\psi) = \psi \circ g$, and as g is an epimorphism, we obtain $\psi = 0$. Hence g^* is a monomorphism. $f^* \circ g^* = (g \circ f)^* = 0^* = 0$, and it remains to prove that $\text{Ker}(f^*) \subset \text{Im}(g^*)$. If $(\varphi: M \rightarrow X) \in \text{Ker}(f^*)$, then $0 = f^*(\varphi) = \varphi \circ f$, and therefore $\text{Ker}(g) = \text{Im}(f) \subset \text{Ker}(\varphi)$. Hence φ induces a homomorphism $\tilde{\varphi}: M/\text{Ker}(g) \rightarrow X$, and g induces an isomorphism $\tilde{g}: M/\text{Ker}(g) \xrightarrow{\sim} M''$. Then $\varphi' = \tilde{\varphi} \circ \tilde{g}^{-1} \in \text{Hom}_R(M'', X)$ and $\varphi = \varphi' \circ g = g^*(\varphi') \in \text{Im}(g^*)$.

Assume now that the sequence $\mathbf{0} \rightarrow \text{Hom}_R(M'', X) \xrightarrow{g^*} \text{Hom}_R(M, X) \xrightarrow{f^*} \text{Hom}_R(M', X)$ is exact for every R -module X . If $X = M''$, then $0 = f^* \circ g^*(\text{id}_{M''}) = (g \circ f)^*(\text{id}_{M''}) = g \circ f$.

Next we prove that $\text{Ker}(g) \subset \text{Im}(f)$. Let $X = M/\text{Im}(f)$ and denote by $\pi \in \text{Hom}_R(M, X)$ the residue class homomorphism. Since $f^*(\pi) = \pi \circ f = 0$, we obtain $\pi \in \text{Ker}(f^*) = \text{Im}(g^*)$. Let $\varphi \in \text{Hom}_R(M'', X)$ be such that $\pi = g^*(\varphi) = \varphi \circ g$. Now, if $x \in \text{Ker}(g)$, then $\pi(x) = 0$, and thus $x \in \text{Im}(f)$.

It remains to prove that g is an epimorphism. For this, we set $X = M''/\text{Im}(g)$, and we denote by $\pi \in \text{Hom}_R(M'', X)$ the residue class homomorphism. Then $g^*(\pi) = \pi \circ g = 0$, hence $\pi = 0$, since g^* is a monomorphism, and therefore $M'' = \text{Im}(g)$. Hence g is an epimorphism. \square

An additive functor $T: R\text{-Mod} \rightarrow \mathbf{Ab}$ is called

- *left-exact* if, for every exact sequence $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ in $R\text{-Mod}$, the induced sequence $\mathbf{0} \rightarrow TM' \xrightarrow{Tf} TM \xrightarrow{Tg} TM''$ in \mathbf{Ab} is exact;

- *right-exact* if, for every exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ in $R\text{-Mod}$, the induced sequence $TM' \xrightarrow{Tf} TM \xrightarrow{Tg} TM'' \rightarrow \mathbf{0}$ in \mathbf{Ab} is exact;
- *exact* if, for every exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M''$ in $R\text{-Mod}$, the induced sequence $TM' \xrightarrow{Tf} TM \xrightarrow{Tg} TM''$ in \mathbf{Ab} is exact;

An additive contravariant functor $T: R\text{-Mod} \rightarrow \mathbf{Ab}$ is called

- *left-exact* if, for every exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ in $R\text{-Mod}$, the induced sequence $\mathbf{0} \rightarrow TM'' \xrightarrow{Tg} TM \xrightarrow{Tf} TM'$ in \mathbf{Ab} is exact;
- *right-exact* if, for every exact sequence $\mathbf{0} \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ in $R\text{-Mod}$, the induced sequence $TM'' \xrightarrow{Tg} TM \xrightarrow{Tf} TM' \rightarrow \mathbf{0}$ in \mathbf{Ab} is exact;
- *exact* if, for every exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M''$ in $R\text{-Mod}$, the induced sequence $TM'' \xrightarrow{Tg} TM \xrightarrow{Tf} TM'$ in \mathbf{Ab} is exact.

For an R -module N , the functors $\text{Hom}_R(N, -): R\text{-Mod} \rightarrow \mathbf{Ab}$ and $\text{Hom}_R(-, N): R\text{-Mod}^{\text{op}} \rightarrow \mathbf{Ab}$ are left-exact.

Definition. An R -module C is called

- *projective* if, for every diagram

$$\begin{array}{ccc} & C & \\ & \varphi \downarrow & \\ M & \xrightarrow{g} & M'' \longrightarrow \mathbf{0} \end{array}$$

of R -homomorphisms with exact row, there exists an R -homomorphism $\psi: C \rightarrow M$ such that $g \circ \psi = \varphi$ [equivalently: For every R -epimorphism $g: M \rightarrow M''$, the induces homomorphism $g_*: \text{Hom}_R(C, M) \rightarrow \text{Hom}_R(C, M'')$ is surjective];

- *injective* if, for every diagram

$$\begin{array}{ccc} \mathbf{0} & \longrightarrow & M' \xrightarrow{f} M \\ & & \varphi \downarrow \\ & & C \end{array}$$

of R -homomorphisms with exact row, there exists an R -homomorphism $\psi: M \rightarrow C$ such that $\psi \circ f = \varphi$ [equivalently: For every R -monomorphism $f: M' \rightarrow M$, the induces homomorphism $f^*: \text{Hom}_R(M, C) \rightarrow \text{Hom}_R(M', C)$ is surjective].

Theorem 1.1.6.

1. For an R -module P , the following assertions are equivalent:
 - (a) P is projective.
 - (b) Every R -epimorphism $M \rightarrow P$ splits.
 - (c) There exists an R -module M such that $M \oplus P$ is free.
 - (d) $\text{Hom}_R(P, -): R\text{-Mod} \rightarrow \mathbf{Ab}$ is an exact functor.
2. Let $(P_i)_{i \in I}$ be a family of R -modules. Then $\bigoplus_{i \in I} P_i$ is projective if and only if all P_i are projective.
3. Every free R -module is projective. If R is a principal ideal domain, then every projective R -module is free.
4. Every finitely generated projective R -module is finitely presented.

PROOF. 1. (a) \Rightarrow (b) If $g: M \rightarrow P$ is an R -epimorphism, then $g_*: \text{Hom}_R(P, M) \rightarrow \text{Hom}_R(P, P)$ is surjective, and thus there exists some $\psi \in \text{Hom}_R(P, M)$ such that $\text{id}_P = g_*(\psi) = g \circ \psi$. Hence g splits.

(b) \Rightarrow (c) There exists a free R -module F and an R -epimorphism $p: F \rightarrow P$. By assumption, p splits, and by Theorem 1.1.3.2(a), there exists a commutative diagram

$$\begin{array}{ccccc} M \oplus P & \xrightarrow{p''} & P & \longrightarrow & \mathbf{0} \\ \downarrow \Phi & & \downarrow \text{id}_P & & \\ F & \xrightarrow{p} & P & \longrightarrow & \mathbf{0} \end{array}$$

where $M = \text{Ker}(p)$ and Φ is an isomorphism. Hence $M \oplus P$ is free.

(c) \Rightarrow (d) Let N be an R -module such that $F = P \oplus N$ is free with basis $(u_i)_{i \in I}$, let $\varepsilon: P \rightarrow F$ be the injection and $p: F \rightarrow P$ the projection of this direct sum. Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ be an exact sequence of R -modules. We must prove that the sequence $\text{Hom}_R(P, M') \xrightarrow{f_*} \text{Hom}_R(P, M) \xrightarrow{g_*} \text{Hom}_R(P, M'')$ is exact. Clearly, $g_* \circ f_* = (g \circ f)_* = 0_* = 0$, and it remains to prove that $\text{Ker}(g_*) \subset \text{Im}(f_*)$. Suppose that $(\varphi: P \rightarrow M) \in \text{Ker}(g_*)$. Then $0 = g_*(\varphi) = g \circ \varphi$, and therefore $\text{Im}(\varphi) = \varphi \circ p(F) \subset \text{Ker}(g) = \text{Im}(f)$. For each $i \in I$, let $m'_i \in M'$ be such that $f(m'_i) = \varphi \circ p(u_i)$, and let $\psi_1 \in \text{Hom}_R(F, M')$ be such that $\psi_1(u_i) = m'_i$ for all $i \in I$. Then $f \circ \psi_1(u_i) = \varphi \circ p(u_i)$ for all $i \in I$, hence $f \circ \psi_1 = \varphi \circ p$, and $\psi = \psi_1 \circ \varepsilon \in \text{Hom}_R(P, M')$. Then $f_*(\psi) = f \circ \psi = f \circ \psi_1 \circ \varepsilon = \varphi \circ p \circ \varepsilon = \varphi \in \text{Im}(f_*)$.

(d) \Rightarrow (a) If $g: M \rightarrow M''$ is an R -epimorphism, then the exactness of $M \xrightarrow{g} M'' \rightarrow \mathbf{0}$ implies the exactness of $\text{Hom}_R(P, M) \xrightarrow{g_*} \text{Hom}_R(P, M'') \rightarrow \mathbf{0}$, and thus g_* is surjective.

2. Assume first that $\bigoplus_{i \in I} P_i$ is projective, and let N be an R -module such that $F = N \oplus \bigoplus_{i \in I} P_i$ is free. If $i \in I$, then

$$F = \left(N \oplus \bigoplus_{j \in I \setminus \{i\}} P_j \right) \oplus P_i,$$

and thus P_i is free.

Assume now that, for every $i \in I$, P_i is projective, and let N_i be an R -module such that $F_i = N_i \oplus P_i$ is free. Then

$$\bigoplus_{i \in I} F_i = \left(\bigoplus_{i \in I} N_i \right) \oplus \left(\bigoplus_{i \in I} P_i \right) \text{ is free, and thus } \bigoplus_{i \in I} P_i \text{ is projective.}$$

3. If F is free, then $F \cong F \oplus \mathbf{0}$, and thus F is projective. Let R be a principal ideal domain and P a projective R -module. Let M be an R -module such that $F = M \oplus P$ is free, and let $\varepsilon: P \rightarrow F$ be the injection. Then $\varepsilon(P) \subset F$ is free, and $P \cong \varepsilon(P)$ is also free.

4. Let P be a finitely generated projective R -module. Then there exists an R -epimorphism $p: F \rightarrow P$ for some finitely generated free R -module, and the exact sequence $\mathbf{0} \rightarrow \text{Ker}(p) \hookrightarrow F \xrightarrow{p} P \rightarrow \mathbf{0}$ splits. Hence there exists an R -epimorphism $\varphi: F \rightarrow \text{Ker}(p)$, which implies that $\text{Ker}(p)$ is finitely generated, and thus P is finitely presented. \square

Let R be a domain and $K = \mathfrak{q}(R)$. For R -submodules $J, J' \subset K$, we define $J^{-1} = \{a \in K \mid aJ \subset R\}$ and $JJ' = {}_R\langle \{aa' \mid a \in J, a' \in J'\} \rangle$. Clearly, J^{-1} and JJ' are again R -submodules of K . An R -submodule $J \subset K$ is called a *fractional ideal* of R if $J \neq \mathbf{0}$ and $J^{-1} \neq \mathbf{0}$ [equivalently, there is some $c \in R^\bullet$ such that $cJ \subset R$ is a non-zero ideal of R]. A fractional ideal J is called *invertible* if $JJ^{-1} = R$ [equivalently, $1 \in JJ^{-1}$].

Theorem 1.1.7. *Let R be a domain, $K = \mathfrak{q}(R)$ and $J \subset K$ a fractional ideal of R . Then the map*

$$\Phi: J^{-1} \rightarrow \text{Hom}_R(J, R), \quad \text{defined by } \Phi(c)(x) = cx \text{ for all } c \in J^{-1} \text{ and } x \in J$$

is an R -isomorphism, and J is invertible if and only if it is a projective R -module.

PROOF. If $c \in J^{-1}$, then $cx \in R$ for all $x \in J$, and $\varphi = (x \mapsto cx) \in \text{Hom}_R(J, R)$. By definition, Φ is an R -module homomorphism, and as $J \neq \mathbf{0}$, it is a monomorphism. Hence we must prove that Φ is surjective. Thus suppose that $\varphi \in \text{Hom}_R(J, R)$, $0 \neq c \in J^{-1}$ and $x, y \in J^\bullet$. Then $\varphi(cxy) = cx\varphi(y) = cy\varphi(x)$, and therefore $x^{-1}\varphi(x) = y^{-1}\varphi(y)$. Hence there exists some $\lambda \in K$ such that $\varphi(x) = \lambda x$ for all $x \in J$. Hence $\lambda J \subset R$, whence $\lambda \in J^{-1}$ and $\varphi = \Phi(\lambda)$.

Assume now that J is invertible, and let $a_1, \dots, a_n \in J$ and $c_1, \dots, c_n \in J^{-1}$ be such that $a_1c_1 + \dots + a_nc_n = 1$. If $a \in J$, then $ac_i \in R$ for all $i \in [1, n]$, and $a = a_1c_1a + \dots + a_nc_na \in R\langle a_1, \dots, a_n \rangle$. Define $g: R^n \rightarrow J$ by $g(x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n$ for all $(x_1, \dots, x_n) \in R^n$, and $\psi: J \rightarrow R^n$ by $\psi(b) = (c_1b, \dots, c_nb)$ for all $b \in J$. Then g and ψ are R -module homomorphisms, and $g \circ \psi = \text{id}_J$. Hence ψ is a splitting monomorphism, and thus $\text{Im}(\psi) \trianglelefteq R^n$. Since $J \cong \text{Im}(\psi)$, it follows that J is projective.

Let now J be projective. Then there exists an R -module epimorphism $g: R^{(I)} \rightarrow J$ for some set I , and we denote by $(e_i)_{i \in I}$ the canonical basis of $R^{(I)}$, given by $e_i = (\delta_{i,j})_{j \in I}$ for all $i \in I$. Since J is projective, g splits, and there is some $\psi \in \text{Hom}_R(J, R^{(I)})$ such that $g \circ \psi = \text{id}_J$. We set $\psi = (\psi_i)_{i \in I}$, where $\psi_i \in \text{Hom}_R(J, R)$ for all $i \in I$, and if $x \in J$, then $\psi_i(x) = 0$ for almost all $i \in I$. Then there exist elements $c_i \in J^{-1}$ such that $\psi_i(x) = c_ix$ for all $x \in J$ and $i \in I$. If $x \in J^\bullet$, then

$$x = g \circ \psi(x) = g\left(\sum_{i \in I} \psi_i(x)e_i\right) = \sum_{i \in I} c_ixg(e_i) \quad \text{and therefore} \quad 1 = \sum_{i \in I} c_ig(e_i) \in J^{-1}J = JJ^{-1}.$$

Hence J is invertible. \square

An R -module M is called *(R -)divisible* if $\lambda M = M$ for every $\lambda \in R \setminus \mathbf{z}(R)$. Consequently, an abelian group A is divisible if $gA = A$ for all $g \in \mathbb{N}$. If K is a field containing \mathbb{Q} , then the additive groups K and K/\mathbb{Z} are divisible.

Theorem 1.1.8.

1. For an R -module Q , the following assertions are equivalent:
 - (a) Q is injective.
 - (b) For every left ideal $\mathfrak{a} \subset R$ and every R -homomorphism $f: \mathfrak{a} \rightarrow Q$ there exists an R -homomorphism $h: R \rightarrow Q$ such that $h|_{\mathfrak{a}} = f$.
 - (c) Every R -monomorphism $Q \rightarrow M$ splits.
 - (d) $\text{Hom}_R(-, Q): R\text{-Mod} \rightarrow \mathbf{Ab}$ is an exact contravariant functor.
2. A direct product of a family of R -modules is injective if and only if every factor is injective.
3. Every injective R -module is divisible. If R is a principal ideal domain, then every R -divisible R -module Q is injective. In particular, an abelian group is injective if and only if it is divisible.

PROOF. 1. (a) \Rightarrow (b) Let $\mathfrak{a} \subset R$ be a left ideal, $f \in \text{Hom}_R(\mathfrak{a}, Q)$ and $j = (\mathfrak{a} \hookrightarrow R)$ the injection. Then the map $j^*: \text{Hom}_R(R, Q) \rightarrow \text{Hom}_R(\mathfrak{a}, Q)$ is surjective, and thus there exists some $h \in \text{Hom}_R(R, Q)$ such that $f = j^*(h) = h \circ j = h|_{\mathfrak{a}}$.

(b) \Rightarrow (c) (Reinhold Baer) Let $f: Q \rightarrow M$ be an R -monomorphism. We must prove that f splits, and for this we may assume that $Q \subset M$ and $f = (Q \hookrightarrow M)$ is the injection. Indeed, if $f: Q \rightarrow M$ is any monomorphism, then there exists an R -overmodule $\overline{M} \supset Q$ and an R -isomorphism $\overline{f}: \overline{M} \xrightarrow{\sim} M$. If the injection $Q \hookrightarrow \overline{M}$ splits, then there is some $h \in \text{Hom}_R(\overline{M}, Q)$ such that $h|_Q = \text{id}_Q$. Then $h \circ \overline{f}^{-1} \in \text{Hom}_R(M, Q)$, and $(h \circ \overline{f}^{-1}) \circ f = \text{id}_M$. Hence f splits.

Thus assume that $Q \subset M$ is a submodule. We must prove that there is some $h \in \text{Hom}_R(M, Q)$ such that $h|_Q = \text{id}_Q$. Let Ω be the set of all pairs (C, φ) , where C is an R -module, $Q \subset C \subset M$, $\varphi \in \text{Hom}_R(C, Q)$, and $\varphi|_Q = \text{id}_Q$. Then $(Q, \text{id}_Q) \in \Omega$, and we define a partial order on Ω by setting $(C, \varphi) \leq (C', \varphi')$ if $C \subset C'$ and $\varphi'|_C = \varphi$. Then the union of every chain in Ω belongs again to Ω , and by Zorn's Lemma Ω contains a maximal element (C, h) . We prove that $C = M$. Assume the contrary, pick some element $q \in M \setminus C$, and set $\overline{C} = C + Rq \subset M$. Then $\mathfrak{a} = \{\lambda \in R \mid \lambda q \in C\} \subset R$ is a left ideal, and we define $\varphi: \mathfrak{a} \rightarrow Q$ by $\varphi(\lambda) = h(\lambda q)$. Then φ is an R -homomorphism, and there exists some $\psi \in \text{Hom}_R(R, Q)$ such that $\psi|_{\mathfrak{a}} = \varphi$. Now we define $\overline{h}: \overline{C} \rightarrow Q$ by $\overline{h}(c + \lambda q) = h(c) + \psi(\lambda)$ for all $c \in C$ and $\lambda \in R$. We assert that this definition does not depend on the representatives. Indeed, if

$c + \lambda q = c' + \lambda' q$ for some $c, c' \in C$ and $\lambda, \lambda' \in R$, then $(\lambda - \lambda')q = c' - c \in C$, hence $\lambda - \lambda' \in \mathfrak{a}$, and $h(c') + \psi(\lambda') = h(c + (\lambda - \lambda')q) + \psi(\lambda' - \lambda) = \psi(\lambda) = h(c) + h((\lambda - \lambda')q) + \varphi(\lambda' - \lambda) + \psi(\lambda) = h(c) + \psi(\lambda)$. Then $\bar{h} \in \text{Hom}_R(\bar{C}, Q)$, and $\bar{h}|_Q = (\bar{h}|_C)|_Q = h|_Q = \text{id}_Q$, contradicting the maximality of (C, h) .

(c) \Rightarrow (d) Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ be an exact sequence in $R\text{-Mod}$. We must prove that the sequence $\text{Hom}_R(M'', Q) \xrightarrow{g^*} \text{Hom}_R(M, Q) \xrightarrow{f^*} \text{Hom}_R(M', Q)$ is exact. Clearly, $f^* \circ g^* = (g \circ f)^* = 0^* = 0$, and thus we must prove that $\text{Ker}(f^*) \subset \text{Im}(g^*)$. Suppose that $(\varphi: M \rightarrow Q) \in \text{Ker}(f^*)$. Then $0 = f^*(\varphi) = \varphi \circ f$, hence $\text{Ker}(g) = \text{Im}(f) \subset \text{Ker}(\varphi)$, and we must prove that there is some $\varphi' \in \text{Hom}_R(M'', Q)$ such that $\varphi = g^*(\varphi') = \varphi' \circ g$.

We consider the submodule $N = \{(\varphi(m), -g(m)) \mid m \in M\} \subset Q \oplus M''$ and the R -homomorphism $\psi: Q \rightarrow Q \oplus M''/N$, defined by $\psi(q) = (q, 0) + N$. If $q \in \text{Ker}(\psi)$, then $(q, 0) = (\varphi(m), -g(m))$ for some $m \in M$, hence $m \in \text{Ker}(g) \subset \text{Ker}(\varphi)$, and thus $q = \varphi(m) = 0$. Therefore ψ is a monomorphism and splits by assumption. Let $\pi: Q \oplus M''/N \rightarrow Q$ be an R -homomorphism such that $\pi \circ \psi = \text{id}_Q$, and define $\varphi': M'' \rightarrow Q$ by $\varphi'(m'') = \pi((0, m'') + N)$. Then we obtain, for all $m \in M$,

$$\varphi' \circ g(m) = \pi((0, g(m)) + N) = \pi((\varphi(m), 0) - (\varphi(m), -g(m)) + N) = \pi((\varphi(m), 0) + N) = \pi \circ \psi \circ \varphi(m) = \varphi(m),$$

and therefore $\varphi = \varphi' \circ g$.

(d) \Rightarrow (a) Let $f: M' \rightarrow M$ be an R -monomorphism. Then the exact sequence $\mathbf{0} \rightarrow M' \xrightarrow{f} M$ entails an exact sequence $\text{Hom}_R(M, Q) \xrightarrow{f^*} \text{Hom}_R(M', Q) \rightarrow \mathbf{0}$. Hence f^* is surjective, and thus Q is an injective module.

2. Exercise!

3. Let Q be an injective R -module, $\lambda \in R \setminus \mathfrak{z}(R)$. We must prove that $Q \subset \lambda Q$. Thus suppose that $m \in Q$, and define $\varphi: R\lambda \rightarrow Q$ by $\varphi(r\lambda) = rm$. As $\lambda \notin \mathfrak{z}(R)$, it follows that $r\lambda = r'\lambda$ implies $r = r'$ for all $r, r' \in R$, and therefore $\varphi \in \text{Hom}_R(R\lambda, Q)$. Since Q is injective, there exists some $\psi \in \text{Hom}_R(R, Q)$ such that $\psi|_{R\lambda} = \varphi$. Then $\lambda\psi(1) = \psi(\lambda) = \varphi(\lambda) = m \in \lambda Q$.

Let now R be a principal ideal domain and Q an R -divisible R -module. We verify condition 1.(b). Let $\mathfrak{a} \triangleleft R$ be an ideal. If $\mathfrak{a} = \mathbf{0}$, there is nothing to do. Thus suppose that $\mathfrak{a} = R\lambda$, where $\lambda \in R^\bullet$, and let $\varphi \in \text{Hom}_R(\mathfrak{a}, Q)$. Since Q is R -divisible, there exists some $x \in Q$ such that $\varphi(\lambda) = \lambda x$. We define $\psi \in \text{Hom}_R(R, Q)$ by $\psi(r) = rx$ for all $r \in R$. If $s \in \mathfrak{a} = R\lambda$, say $s = r\lambda$, where $r \in R$, then $\psi(s) = r\lambda x = r\varphi(\lambda) = \varphi(r\lambda) = \varphi(s)$, and thus $\psi|_{\mathfrak{a}} = \varphi$. \square

Theorem 1.1.9. For an abelian group A , we call $A^\vee = \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$ the dual group of A .

1. Let F be a free abelian group. Then F^\vee is divisible [hence an injective \mathbb{Z} -module].
2. Let A be an abelian group.
 - (a) The map $\beta: A \rightarrow A^{\vee\vee}$, defined by $\beta(a)(\varphi) = \varphi(a)$ for all $a \in A$ and $\varphi \in A^\vee$, is a monomorphism.
 - (b) There exists a monomorphism $A \rightarrow D$ into a divisible abelian group D .
3. Let M be an R -module. Then there exists an R -monomorphism $j: M \rightarrow Q$ into an injective R -module Q .

PROOF. 1. We may assume that $F = \mathbb{Z}^{(I)}$ for some set I . Then

$$F^\vee = \text{Hom}(\mathbb{Z}^{(I)}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \text{Hom}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z})^I \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z})^I,$$

and thus F^\vee is divisible.

2. (a) Obviously, β is a homomorphism, and therefore it suffices to prove: For every $a \in A$ such that $a \neq 0$, there exists some $\varphi \in A^\vee$ such that $\varphi(a) \neq 0$. Thus let $0 \neq a \in A$ and $m \in \mathbb{N}_0$ such that $m\mathbb{Z} = \{g \in \mathbb{Z} \mid ga = 0\}$. Then the exact sequence $\mathbf{0} \rightarrow m\mathbb{Z} \xrightarrow{j} \mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}a \rightarrow \mathbf{0}$ (where j is the injection, and $\alpha g = ga$ for all $g \in \mathbb{Z}$) induces an exact sequence

$$\mathbf{0} \rightarrow \text{Hom}(\mathbb{Z}a, \mathbb{Q}/\mathbb{Z}) \rightarrow \text{Hom}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{j^*} \text{Hom}(m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}), \quad \text{and } j^*\varphi = \varphi|_{m\mathbb{Z}} \text{ for } \varphi \in \text{Hom}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}).$$

We assert that j^* is not injective. This is obvious if $m = 0$. If $m \neq 0$, let $\varphi \in \text{Hom}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ be defined by $\varphi(g) = \frac{g}{m} + \mathbb{Z}$. Then $\varphi \neq 0$ and $j^*(\varphi) = \varphi|_{m\mathbb{Z}} = 0$. Since $\text{Ker}(j^*) \neq \mathbf{0}$, it follows that $\text{Hom}(\mathbb{Z}a, \mathbb{Q}/\mathbb{Z}) \neq \mathbf{0}$, and since \mathbb{Q}/\mathbb{Z} is divisible, the map $\text{Hom}(A, \mathbb{Q}/\mathbb{Z}) \rightarrow \text{Hom}(\mathbb{Z}a, \mathbb{Q}/\mathbb{Z})$, induced by the injection $\mathbb{Z}a \hookrightarrow A$ and given by $\varphi \mapsto \varphi|_{\mathbb{Z}a}$, is surjective. If $\varphi \in \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$ is such that $\varphi|_{\mathbb{Z}a} \neq 0$, then $\varphi(a) \neq 0$.

(b) Let F be a free abelian group such that there is an epimorphism $F \xrightarrow{p} A^\vee \rightarrow \mathbf{0}$. The induced sequence $\mathbf{0} \rightarrow A^{\vee\vee} = \text{Hom}(A^\vee, \mathbb{Q}/\mathbb{Z}) \xrightarrow{p^*} \text{Hom}(F, \mathbb{Q}/\mathbb{Z}) = F^\vee$ is exact, and if $\beta: A \rightarrow A^{\vee\vee}$ is the monomorphism defined in (a), then $p^* \circ \beta: A \rightarrow F^\vee$ is a monomorphism into a divisible abelian group.

3. By 2., there exists a group monomorphism $\iota: M \rightarrow D$ into a divisible abelian group D , and we consider the homomorphism $j: M \rightarrow \text{Hom}(R, D)$, defined by $j(m)(r) = \iota(rm)$. Then j is a group homomorphism, and if $m \in \text{Ker}(j)$, then $0 = j(m)(1) = \iota(m)$ and thus $m = 0$. Hence j is a monomorphism. The group $\text{Hom}(R, D) = \text{Hom}_{\mathbb{Z}}({}_{\mathbb{Z}}R, {}_{\mathbb{Z}}D)$ is a R -module by means of $(\lambda\varphi)(r) = \varphi(r\lambda)$ for all $\varphi \in \text{Hom}(R, D)$ and $\lambda, r \in R$, and it is easily checked that j is an R -homomorphism. Hence we are done if we can prove that $\text{Hom}(R, D)$ is an injective R -module.

Thus let $\mathbf{0} \rightarrow N' \xrightarrow{f} N$ be an exact sequence of R -modules and $\varphi: N' \rightarrow \text{Hom}(R, D)$ an R -module homomorphism. We must show that there exists an R -homomorphism $\psi: N \rightarrow \text{Hom}(R, D)$ such that $\psi \circ f = \varphi$. Let $\mu: \text{Hom}(R, D) \rightarrow D$ be defined by $\mu(h) = h(1)$. Then μ is a group homomorphism, hence $\mu \circ \varphi: N' \rightarrow D$ is a group homomorphism, and as D is divisible, there exists a group homomorphism $\psi_0: N \rightarrow D$ such that $\psi_0 \circ f = \mu \circ \varphi$. Now we define $\psi: N \rightarrow \text{Hom}(R, D)$ by $\psi(n)(c) = \psi_0(cn)$ for all $n \in N$ and $c \in R$, and we assert that ψ fulfills our requirements. We must prove: 1) If $n \in N$, then $\psi(n) \in \text{Hom}(R, D)$; 2) ψ is an R -homomorphism; 3) $\psi \circ f = \varphi$.

1) Let $n \in N$. If $c, c' \in R$, then

$$\psi(n)(c + c') = \psi_0((c + c')n) = \psi_0(cn + c'n) = \psi_0(cn) + \psi_0(c'n) = \psi(n)(c) + \psi(n)(c').$$

2) Let $n, n' \in N$ and $\lambda \in R$. Then we obtain, for all $c \in R$,

$$\psi(n + n')(c) = \psi_0(c(n + n')) = \psi_0(cn + cn') = \psi_0(cn) + \psi_0(c'n) = \psi(n)(c) + \psi(n')(c),$$

hence $\psi(n + n') = \psi(n) + \psi(n')$, and $\psi(\lambda n)(c) = \psi_0(c\lambda n) = \psi(n)(c\lambda) = [\lambda\psi(n)](c)$, and therefore $\psi(\lambda n) = \lambda\psi(n)$.

3) If $n' \in N'$ and $c \in R$, then

$$\psi \circ f(n')(c) = \psi_0(cf(n')) = \psi_0 \circ f(cn') = \mu \circ \varphi(cn') = \varphi(cn')(1) = [c\varphi(n')](1) = \varphi(n')(c). \quad \square$$

1.2. Tensor products

Let R and S be rings.

Definition. Let $M = M_R$ be a right and $N = {}_R N$ a left R -module.

1. Let F be the free \mathbb{Z} -module with basis $M \times N$. The elements of $\xi \in F$ have a unique representation

$$\xi = \sum_{(m,n) \in M \times N} \lambda_{m,n}(m,n), \quad \text{where } \lambda_{m,n} \in \mathbb{Z}, \quad \lambda_{m,n} = 0 \text{ for almost all } (m,n) \in M \times N.$$

Let $Q \subset F$ be the subgroup generated by all elements of the following types:

$$(m + m', n) - (m, n) - (m', n), \quad (m, n + n') - (m, n) - (m, n'), \quad (m\lambda, n) - (m, \lambda n)$$

for any $m, m' \in M$, $n, n' \in N$ and $\lambda \in R$. The quotient group $M \otimes_R N = F/Q$ is called the *tensor product* of M and N over R . For $(m, n) \in M \times N$, we call $m \otimes n = (m, n) + Q \in M \otimes_R N$ the *elementary tensor* of m and n . Clearly, $M \otimes N = \mathbb{Z}\langle\{m \otimes n \mid (m, n) \in M \times N\}\rangle$, and for all $m, m' \in M$, $n, n' \in N$ and $\lambda \in R$, we have

$$(m + m') \otimes n = m \otimes n + m' \otimes n, \quad m \otimes (n + n') = m \otimes n + m \otimes n' \quad \text{and} \quad m\lambda \otimes n = m \otimes \lambda n.$$

In particular, $gm \otimes n = m \otimes gn = g(m \otimes n)$ for all $g \in \mathbb{Z}$ [indeed, for $g \in \mathbb{N}$ this follows by induction, $0 \otimes n + 0 \otimes n = 0 \otimes n$ and $m \otimes 0 + m \otimes 0 = m \otimes 0$ implies $m \otimes 0 = 0 \otimes n = 0$, and if $g \in \mathbb{N}$, then $(-gm) \otimes n + gm \otimes n = 0 \otimes n = 0$ implies $(-gm) \otimes n = -(gm \otimes n) = -g(m \otimes n)$, and similarly $m \otimes (-gn) = -m \otimes gn = -g(m \otimes n)$].

Every $\xi \in M \otimes_R N$ has a (in general not unique) representation

$$\xi = \sum_{i=1}^k m_i \otimes n_i, \quad \text{where } k \in \mathbb{N}, \quad m_1, \dots, m_k \in M \quad \text{and} \quad n_1, \dots, n_k \in N.$$

Indeed, by definition

$$\xi = \sum_{i=1}^k \lambda_i(x_i, y_i) + Q = \sum_{i=1}^k (\lambda_i x_i, y_i) + Q = \sum_{i=1}^k \lambda_i x_i \otimes y_i,$$

where $\lambda_i \in \mathbb{Z}$, $x_i \in M$ and $y_i \in N$.

2. Let L be an abelian group. A map $\beta: M \times N \rightarrow L$ is called *R-balanced* if, for all $m, m' \in M$, $n, n' \in N$ and $\lambda \in R$ we have

$$\beta(m + m', n) = \beta(m, n) + \beta(m', n), \quad \beta(m, n + n') = \beta(m, n) + \beta(m, n')$$

and

$$\beta(m\lambda, n) = \beta(m, \lambda n).$$

By definition, the map $M \times N \rightarrow M \otimes_R N$ is *R-balanced*, and if $\beta: M \times N \rightarrow L$ is any *R-balanced* map, then there exists a unique group homomorphism $f: M \otimes_R N \rightarrow L$ such that $f(m \otimes n) = \beta(m, n)$ for all $(m, n) \in M \times N$ [indeed, there exists a unique \mathbb{Z} -homomorphism $\beta^*: F \rightarrow L$ such that $\beta^* \mid M \times N = \beta$, and, by definition, $Q \subset \text{Ker}(\beta^*)$. Hence β^* induces f as asserted].

Example. Let $M = {}_R M$ be an R -module and $\mathfrak{a} \subset R$ a subset. Then

$$\mathfrak{a}M = \left\{ \sum_{i=1}^n a_i m_i \mid n \in \mathbb{N}, \quad a_1, \dots, a_n \in \mathfrak{a}, \quad m_1, \dots, m_n \in M \right\} \subset M$$

is a subgroup (even an R -submodule if $\mathfrak{a} \subset R$ is a left ideal). Assume now that $\mathfrak{a} \subset R$ is a right ideal. Then the map $\mathfrak{a} \times M \rightarrow M$, defined by $(a, m) \mapsto am$, is *R-balanced* and induces a homomorphism $\mu_{\mathfrak{a}}^M: \mathfrak{a} \otimes_R M \rightarrow M$ such that $\mu_{\mathfrak{a}}^M(a \otimes m) = am$ for all $a \in \mathfrak{a}$ and $m \in M$. It is called the *multiplication homomorphism* of \mathfrak{a} on M . By definition, $\text{Im}(\mu_{\mathfrak{a}}^M) = \mathfrak{a}M$, and if $\mu_{\mathfrak{a}}^M$ is a monomorphism, then it induces an isomorphism $\mu_{\mathfrak{a}}^M: \mathfrak{a} \otimes_R M \xrightarrow{\sim} \mathfrak{a}M$.

Theorem 1.2.1. *Let $M = M_R$ be a right and $N = {}_R N$ a left R -module.*

1. *If ${}_S M_R$ is an (S, R) -bimodule, then there is a unique S -module structure on $M \otimes_R N$ such that $s(m \otimes n) = sm \otimes n$ for all $s \in S$, $m \in M$ and $n \in N$. In the same way, if ${}_R N_S$ is an (R, S) -bimodule, then there is a unique right S -module structure on $M \otimes_R N$ such that $(m \otimes n)s = m \otimes ns$ for all $s \in S$, $m \in M$ and $n \in N$:*

$${}_S({}_S M_R \otimes_R {}_R N) \quad \text{and} \quad (M_R \otimes_R {}_R N)_S.$$

2. *Let R be commutative.*

- (a) *There is a unique R -module structure on $M \otimes_R N$ such that $r(m \otimes n) = rm \otimes n = m \otimes rn$ for all $m \in M$, $n \in N$ and $r \in R$.*
- (b) *Let L be an R -module and $\beta: M \times N \rightarrow L$ an R -bilinear map. Then there exists a unique R -homomorphism $g: M \otimes_R N \rightarrow L$ such that $g(m \otimes n) = \beta(m, n)$ for all $(m, n) \in M \times N$.*

PROOF. 1. *Uniqueness.* An S -module structure on $M \otimes_R N$ is given by a ring homomorphism $\theta: S \rightarrow \text{End}(M \otimes_R N)$. If $s \in S$, then the group homomorphism $\theta(s): M \otimes_R N \rightarrow M \otimes_R N$ is uniquely determined by the values $\theta(s)(m \otimes n) \in M \otimes_R N$ for $(m, n) \in M \times N$, since $M \otimes_R N$ is the abelian group generated by the elementary tensors.

Existence. For $s \in S$, we define $\tau_s: M \times N \rightarrow M \otimes_R N$ by $\tau_s(m, n) = sm \otimes n$. Then τ_s is R -balanced. Indeed, if $m, m' \in M$, $n, n' \in N$ and $\lambda \in R$, then

$$\tau_s(m + m', n) = s(m + m') \otimes n = (sm + sm') \otimes n = sm \otimes n + sm' \otimes n = \tau_s(m, n) + \tau_s(m', n),$$

$$\tau_s(m, n + n') = sm \otimes (n + n') = sm \otimes n + sm \otimes n' = \tau_s(m, n) + \tau_s(m, n'),$$

and (now using the bimodule structure)

$$\tau_s(m\lambda, n) = s(m\lambda) \otimes n = (sm)\lambda \otimes n = sm \otimes \lambda n = \tau_s(m, \lambda n).$$

Hence τ_s induces a unique endomorphism $\theta(s) \in \text{End}(M \otimes_R N)$ such that $\theta(s)(m \otimes n) = sm \otimes n$ for all $(m, n) \in M \times N$. We must prove that $\theta: S \rightarrow \text{End}(M \otimes_R N)$ is a ring homomorphism. We must prove that $\theta(1) = \text{id}_{M \otimes_R N}$, $\theta(s + s') = \theta(s) + \theta(s')$ and $\theta(ss') = \theta(s) \circ \theta(s')$ holds in $\text{End}(M \otimes_R N)$ for all $s, s' \in S$, and it suffices to prove these relations point-wise on the elementary tensors. But this is easy. The right module structure is proved in the same way.

2. (a) Observe that $M = {}_R M_R$.

(b) If $\beta: M \times N \rightarrow L$ is R -bilinear, then $\beta(m, \lambda n) = \lambda\beta(m, n) = \beta(\lambda m, n) = \beta(m\lambda, n)$. In particular, β is R -balanced. Let $g: M \otimes_R N \rightarrow L$ be the unique group homomorphism satisfying $g(m \otimes n) = \beta(m, n)$ for all $(m, n) \in M \times N$. If $\lambda \in R$, then $g(\lambda(m \otimes n)) = g(\lambda m \otimes n) = \beta(\lambda m, n) = \lambda\beta(m, n) = \lambda g(m \otimes n)$ for all $(m, n) \in M \times N$. If $\xi \in M \otimes_R N$ is arbitrary, then

$$\xi = \sum_{i=1}^n m_i \otimes n_i \quad \text{and} \quad g(\lambda\xi) = g\left(\sum_{i=1}^n \lambda m_i \otimes n_i\right) = \sum_{i=1}^n g(\lambda m_i \otimes n_i) = \sum_{i=1}^n \lambda g(m_i \otimes n_i) = \lambda g(\xi).$$

Hence g is an R -homomorphism. □

Definition. Let $f: R \rightarrow S$ be a ring homomorphism and M an R -module. As $S = {}_S S_R$ is a two-sided (S, R) -bimodule, $S \otimes_R M$ is an S -module, and $s'(s \otimes m) = ss' \otimes m$ for all $s, s' \in S$ and $m \in M$. The S -module $S \otimes_R M$ is called the *base extension* of M with S .

Theorem and Definition 1.2.2. *Let $f: M \rightarrow M'$ be a homomorphism of right R -modules and $g: N \rightarrow N'$ a homomorphism of (left) R -modules. Then there exists a unique group homomorphism*

$$f \otimes g: M \otimes_R N \rightarrow M' \otimes_R N' \quad \text{such that} \quad (f \otimes g)(m \otimes n) = f(m) \otimes g(n) \quad \text{for all } m \in M \text{ and } n \in N.$$

It has the following properties:

1. If $f, f_1: M \rightarrow M'$ and $g, g_1: N \rightarrow N'$ are R -homomorphisms, then

$$(f + f_1) \otimes g = f \otimes g + f_1 \otimes g \quad \text{and} \quad f \otimes (g + g_1) = f \otimes g + f \otimes g_1.$$

2. If $M \xrightarrow{f} M' \xrightarrow{f'} M''$ and $N \xrightarrow{g} N' \xrightarrow{g'} N''$ are R -homomorphisms, then

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g).$$

3. If R is commutative, then $f \otimes g$ is an R -homomorphism, and if $\lambda \in R$, then $\lambda f \otimes g = f \otimes \lambda g$.

We call $f \otimes g$ the *tensor product* of the homomorphisms f and g . We write $f \otimes N = f \otimes \text{id}_N$ and $M \otimes g = \text{id}_M \otimes g$. Obviously, $\text{id}_M \otimes \text{id}_N = \text{id}_{M \otimes_R N}$. Consequently $M \otimes -: R\text{-Mod} \rightarrow \mathbf{Ab}$ and $- \otimes N: \mathbf{Mod}\text{-}R \rightarrow \mathbf{Ab}$ are additive (covariant) functors.

Caution! The tensor product $f \otimes g: M \otimes_R N \rightarrow M' \otimes_R N'$ is different from the elementary tensor $f \otimes g \in \text{Hom}_R(M, M') \otimes_{\mathbb{Z}} \text{Hom}_R(N, N')$.

PROOF. It is easily checked that the map $F: M \times N \rightarrow M' \otimes_R N'$, defined by $F(m, n) = f(m) \otimes g(n)$ is R -balanced, and thus it induces a group homomorphism $f \otimes g: M \otimes_R N \rightarrow M' \otimes_R N'$ such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ for all $(m, n) \in M \times N$. The remaining assertions are easily checked point-wise for elementary tensors, and by linearity they hold in general. \square

Theorem 1.2.3. *Let $M = M_R$ be a right and $N = {}_R N$ a left R -module.*

1. *The map $\Phi = \Phi_N: N \rightarrow R \otimes_R N$, defined by $\Phi(n) = 1 \otimes n$ for all $n \in N$, is an R -isomorphism. It is functorial in N , and $\Phi^{-1} = \mu_R^N: R \otimes_R N \rightarrow N$ is the multiplication homomorphism of R on N , given by $\mu_R^N(r \otimes n) = rn$ for all $r \in R$ and $n \in N$ (see Example 1.2).*
2. *There is a unique isomorphism $\Phi: M \otimes_R N \rightarrow N \otimes_{R^{\text{op}}} M$ such that $\Phi(m \otimes n) = n \otimes m$ for all $(m, n) \in M \times N$. It is functorial in M and N . In particular, if R is commutative, then $\Phi: M \otimes_R N \rightarrow N \otimes_R M$ is an R -module isomorphism, and we identify $M \otimes_R N = N \otimes_R M$ by means of Φ .*
3. *Let $P = {}_S P$ an S -module.*

- (a) *If $N = {}_R N_S$ is an (R, S) -bimodule, then there is a unique isomorphism*

$$\Phi: (M \otimes_R N) \otimes_S P \rightarrow M \otimes_R (N \otimes_S P)$$

such that $\Phi((m \otimes n) \otimes p) = m \otimes (n \otimes p)$ for all $m \in M$, $n \in N$ and $p \in P$. It is functorial in M , N and P , and we identify by means of $\Phi: (M \otimes_R N) \otimes_S P = M \otimes_R (N \otimes_S P)$.

- (b) *If $M = {}_S M_R$ is an (S, R) -bimodule, then the map*

$$\Phi: \text{Hom}_S(M \otimes_R N, P) \rightarrow \text{Hom}_R(N, \text{Hom}_S(M, P)),$$

defined by $\Phi(f)(m)(n) = f(m \otimes n)$ for all $f \in \text{Hom}_S(M \otimes_R N, P)$, $n \in N$ and $m \in M$, is a group isomorphism. It is functorial in M , N and P .

PROOF. 1. $R \otimes_R N = {}_R R_R \otimes_R {}_R N$ is an R -module, and $\lambda(r \otimes n) = \lambda r \otimes n$ for all $\lambda, r \in R$ and $n \in N$.

If $n, n' \in N$ and $\lambda \in R$, then $\Phi(n + n') = 1 \otimes (n + n') = 1 \otimes n + 1 \otimes n' = \Phi(n) + \Phi(n')$, and $\Phi(\lambda n) = 1 \otimes \lambda n = \lambda \otimes n = \lambda(1 \otimes n) = \lambda \Phi(n)$. Hence Φ is an R -homomorphism. If $\mu = \mu_R^N$, then $\mu \circ \Phi(n) = \mu(1 \otimes n) = n$, and $\Phi \circ \mu(r \otimes n) = \Phi(rn) = 1 \otimes rn = r \otimes n$. Hence $\mu \circ \Phi = \text{id}_N$, and since $\Phi \circ \mu: R \otimes_R N \rightarrow N$ is a homomorphism, it follows that $\Phi \circ \mu = \text{id}_{R \otimes_R N}$. Thus Φ is an isomorphism.

To prove that Φ is functorial, let $f: N \rightarrow N'$ be an R -homomorphism. Then the diagram

$$\begin{array}{ccc} N & \xrightarrow{\Phi_N} & R \otimes_R N \\ f \downarrow & & \downarrow R \otimes f \\ N' & \xrightarrow{\Phi_{N'}} & R \otimes_R N' \end{array}$$

commutes. Indeed, if $n \in N$, then $(R \otimes f) \circ \Phi_N(n) = (R \otimes f)(1 \otimes n) = 1 \otimes f(n) = \Phi_{N'} \circ f(n)$.

2. Obvious.

3. (a) Exercise!

(b) We shall proceed in 4 steps: 1) For all $n \in N$ and $f \in \text{Hom}_S(M \otimes_R N, P)$, the map $g: M \rightarrow P$, defined by $g(m) = f(m \otimes n)$, is an S -homomorphism; 2) For all $f \in \text{Hom}_S(M \otimes_R N, P)$, the map $\Phi(f): N \rightarrow \text{Hom}_S(M, P)$, defined by $\Phi(f)(n)(m) = f(m \otimes n)$, is an R -homomorphism; 3) Φ is a group homomorphism, which is functorial in M, N and P ; 4) Φ is bijective.

1) Let $n \in N$, $f \in \text{Hom}_S(M \otimes_R N, P)$, $m, m' \in M$ and $s \in S$. Then

$$g(m + m') = f((m + m') \otimes n) = f(m \otimes n + m' \otimes n) = f(m \otimes n) + f(m' \otimes n) = g(m) + g(m'),$$

and $g(sm) = f(sm \otimes n) = f(s(m \otimes n)) = sf(m \otimes n) = sg(m)$.

2) Let $f \in \text{Hom}_S(M \otimes_R N, P)$, $n, n' \in N$ and $r \in R$. For all $m \in M$ we obtain

$$\begin{aligned} \Phi(f)(n + n')(m) &= f(m \otimes (n + n')) = f(m \otimes n + m \otimes n') = f(m \otimes n) + f(m \otimes n') \\ &= \Phi(f)(n)(m) + \Phi(f)(n')(m) = [\Phi(f)(n) + \Phi(f)(n)](m), \end{aligned}$$

and $\Phi(f)(rn)(m) = f(m \otimes rn) = f(mr \otimes n) = \Phi(f)(n)(mr) = [r\Phi(f)(n)](m)$. Hence it follows that $\Phi(f)(n + n') = \Phi(f)(n) + \Phi(f)(n')$ and $\Phi(f)(rn) = r\Phi(f)(n)$.

3) If $f, f' \in \text{Hom}_S(M \otimes_R N, P)$, then we obtain, for all $n \in N$ and $m \in M$,

$$\begin{aligned} \Phi(f + f')(n)(m) &= (f + f')(m \otimes n) = f(m \otimes n) + f'(m \otimes n) = \Phi(f)(n)(m) + \Phi(f')(n)(m) \\ &= [\Phi(f)(n) + \Phi(f')(n)](m) = [\Phi(f) + \Phi(f)](n)(m). \end{aligned}$$

Hence $\Phi(f + f') = \Phi(f) + \Phi(f')$. To prove that Φ is factorial, let $M' = {}_S M'_R$, $N' = {}_R N'_S$, $P' = {}_S P'_S$, and $\mu \in \text{Hom}_R(M', M)$, $\nu \in \text{Hom}_R(N', N)$ and $\pi \in \text{Hom}_S(P, P')$. Then we must prove that the following diagram commutes:

$$\begin{array}{ccc} \text{Hom}_S(M \otimes_R N, P) & \xrightarrow{\Phi} & \text{Hom}_R(N, \text{Hom}_S(M, P)) \\ (\mu \otimes \nu)^* \downarrow & & \downarrow \nu^* \\ \text{Hom}_S(M' \otimes_R N', P) & & \text{Hom}_R(N', \text{Hom}_S(M, P)) \\ \pi_* \downarrow & & \downarrow \psi_* \\ \text{Hom}_S(M' \otimes_R N', P') & \xrightarrow{\Phi'} & \text{Hom}_R(N', \text{Hom}_S(M', P')) \end{array}$$

where $\psi = \mu^* \circ \pi_*: \text{Hom}_S(M, P) \xrightarrow{\pi_*} \text{Hom}_S(M, P') \xrightarrow{\mu^*} \text{Hom}_S(M', P')$. If $f \in \text{Hom}_S(M \otimes_R N, P)$, then we obtain, for all $n' \in N'$ and $m' \in M'$,

$$[\Phi' \circ \pi_* \circ (\mu \otimes \nu)^*(f)](n')(m') = \pi_* \circ (\mu \otimes \nu)^*(f)(m' \otimes n') = \pi \circ f(\mu(m') \otimes \nu(n'))$$

and

$$\begin{aligned} [\psi_* \circ \nu^* \circ \Phi(f)](n')(m') &= [\mu^* \circ \pi_* \circ \nu^* \circ \Phi(f)](n')(m') = [\pi_* \circ \nu^* \circ \Phi(f)](n')(m') \\ &= \pi \circ \Phi(f)(\nu(n'))(\mu(m')) = \pi \circ f(\mu(m') \otimes \nu(n')). \end{aligned}$$

4) For $g \in \text{Hom}_R(N, \text{Hom}_S(M, P))$, we define $F_g: M \times N \rightarrow P$ by $F_g(m, n) = g(n)(m)$, and we assert that F_g is R -balanced. It is obviously bilinear, and if $m \in M$, $n \in N$ and $r \in R$, then $F_g(mr, n) = g(n)(mr) = [rg(n)](m) = g(rn)(m) = F_g(m, rn)$. Hence there exists a unique group homomorphism $\varphi_g: M \otimes_R N \rightarrow P$ such that $\varphi_g(m \otimes n) = g(n)(m)$ for all $(m, n) \in M \times N$, and we assert that φ_g is even an S -homomorphism. Indeed, if $s \in S$ and $(m, n) \in M \times N$, then we obtain $\varphi_g(s(m \otimes n)) = \varphi_g(sm \otimes n) = g(n)(sm) = sg(n)(m) = s\varphi_g(m \otimes n)$, and by linearity it follows that $\varphi_g(s\xi) = s\varphi_g(\xi)$ for all $\xi \in M \otimes_R N$. Now we define

$$\Psi: \text{Hom}_R(N, \text{Hom}_S(M, P)) \rightarrow \text{Hom}_S(M \otimes_R N, P) \quad \text{by} \quad \Psi(g) = \varphi_g.$$

Obviously, Ψ is a group homomorphism. If $f \in \text{Hom}_S(M \otimes_R N, P)$, then $\Psi \circ \Phi(f)(m \otimes n) = \varphi_{\Phi(f)}(m \otimes n) = \Phi(f)(n)(m) = f(m \otimes n)$ for all $(m, n) \in M \times N$, and therefore $\Psi \circ \Phi(f) = f$. If $g \in \text{Hom}_R(N, \text{Hom}_S(M, P))$,

then it follows that $\Phi \circ \Psi(g)(n)(m) = \Psi(g)(m \otimes n) = \varphi_g(m \otimes n) = g(n)(m)$ for all $(m, n) \in M \times N$, and therefore $\Phi \circ \Psi(g) = g$. \square

Theorem 1.2.4. *Let $M' \xrightarrow{i} M \xrightarrow{f} M'' \rightarrow \mathbf{0}$ be an exact sequence of right R -modules, and let $N' \xrightarrow{j} N \xrightarrow{g} N'' \rightarrow \mathbf{0}$ be an exact sequence of left R -modules.*

1. *The sequences*

$$M' \otimes_R N \xrightarrow{i \otimes N} M \otimes_R N \xrightarrow{f \otimes N} M'' \otimes_R N \rightarrow \mathbf{0} \quad \text{and} \quad M \otimes_R N' \xrightarrow{M \otimes j} M \otimes_R N \xrightarrow{M \otimes g} M \otimes_R N'' \rightarrow \mathbf{0}$$

are exact.

2. *The map $f \otimes g: M \otimes_R N \rightarrow M'' \otimes_R N''$ is an epimorphism, and*

$$\text{Ker}(f \otimes g) = \text{Im}(i \otimes N) + \text{Im}(M \otimes j).$$

is exact.

PROOF. 1. We apply Theorem 1.1.5. We must prove that, for all abelian groups X , the sequence

$$\mathbf{0} \rightarrow \text{Hom}(M'' \otimes_R N, X) \xrightarrow{(f \otimes N)^*} \text{Hom}(M \otimes_R N, X) \xrightarrow{(i \otimes N)^*} \text{Hom}(M' \otimes_R N, X)$$

is exact. If X is an abelian group, then $\mathbf{0} \rightarrow \text{Hom}(M'', X) \xrightarrow{f^*} \text{Hom}(M, X) \xrightarrow{i^*} \text{Hom}(M', X)$ is an exact sequence. By Theorem 1.2.3, we obtain a commutative diagram

$$\begin{array}{ccccc} \mathbf{0} & \longrightarrow & \text{Hom}(M'' \otimes_R N, X) & \longrightarrow & \text{Hom}(M \otimes_R N, X) & \longrightarrow & \text{Hom}(M' \otimes_R N, X) \\ & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ \mathbf{0} & \longrightarrow & \text{Hom}_R(N, \text{Hom}(M'', X)) & \longrightarrow & \text{Hom}_R(N, \text{Hom}(M, X)) & \longrightarrow & \text{Hom}_R(N, \text{Hom}(M', X)) \end{array}$$

where the bottom row is exact. Hence the upper row is also exact. The second assertion follows since there is a functorial isomorphism $M \otimes_R N \xrightarrow{\sim} N \otimes_{R^{\text{op}}} M$.

2. $f \otimes g = (M'' \otimes g) \circ (f \otimes N): M \otimes_R N \rightarrow M'' \otimes_R N \rightarrow M'' \otimes_R N''$ is an epimorphism, since $f \otimes N$ and $M'' \otimes g$ are epimorphisms. As $(f \otimes g) \circ (i \otimes N) = (f \circ i) \otimes g = 0$ and $(f \otimes g) \circ (M \otimes j) = f \otimes (g \circ j) = 0$, it follows that $\text{Im}(i \otimes N) + \text{Im}(M \otimes j) \subset \text{Ker}(f \otimes g)$.

Assume that $z \in \text{Ker}(f \otimes g)$. Since $f \otimes g = (f \otimes N'') \circ (M \otimes g): M \otimes_R N \rightarrow M \otimes_R N'' \rightarrow M'' \otimes_R N''$, it follows that $(M \otimes g)(z) \in \text{Ker}(f \otimes N'')$. By 1., there are exact sequences

$$M' \otimes_R N'' \xrightarrow{i \otimes N''} M \otimes_R N'' \xrightarrow{f \otimes N''} M'' \otimes_R N'' \rightarrow \mathbf{0} \quad \text{and} \quad M' \otimes_R N' \xrightarrow{M' \otimes j} M' \otimes_R N \xrightarrow{M' \otimes g} M' \otimes_R N'' \rightarrow \mathbf{0}.$$

Hence it follows that

$$\text{Ker}(f \otimes N'') = \text{Im}(i \otimes N'') = (i \otimes N'')(M' \otimes_R N'') = (i \otimes N'') \circ (M' \otimes g)(M' \otimes_R N) = (i \otimes g)(M' \otimes_R N),$$

and there exists some $u \in M' \otimes_R N$ such that $(M \otimes g)(z) = (i \otimes g)(u)$. Then $b = z - (i \otimes N)(u) \in M \otimes_R N$, and $(M \otimes g)(b) = (M \otimes g)(z) - (M \otimes g) \circ (i \otimes N)(u) = (i \otimes g)(u) - (i \otimes g)(u) = 0$. Hence we finally obtain $z = (i \otimes N)(u) + b \in \text{Im}(i \otimes N) + \text{Im}(M \otimes j)$. \square

Theorem 1.2.5.

1. *Let $(M_i)_{i \in I}$ be a family of right R -modules and $(N_j)_{j \in J}$ a family of left R -modules. Then there exists a unique isomorphism*

$$\Phi: \left(\bigoplus_{i \in I} M_i \right) \otimes_R \left(\bigoplus_{j \in J} N_j \right) \rightarrow \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j)$$

such that $\Phi((m_i)_{i \in I} \otimes (n_j)_{j \in J}) = (m_i \otimes n_j)_{(i,j) \in I \times J}$ for all families $(m_i)_{i \in I}$ and $(n_j)_{j \in J}$; it is functorial in $(M_i)_{i \in I}$ and in $(N_j)_{j \in J}$.

2. Let N be a free left R -module with basis $(v_j)_{j \in J}$, M a right R -module and $z \in M \otimes_R N$. Then z has a unique representation

$$z = \sum_{j \in J} m_j \otimes v_j, \quad \text{where } m_j \in M \text{ for all } j \text{ and } m_j = 0 \text{ for almost all } j \in J.$$

3. Let $f: R \rightarrow S$ be a ring homomorphism and M an R -module.

(a) If M is a free R -module with basis $(u_i)_{i \in I}$, then $S \otimes_R M$ is a free S -module with basis $(1 \otimes u_i)_{i \in I}$.

(b) If M is a projective [finitely generated] R -module, then $S \otimes_R M$ is a projective [finitely generated] S -module.

4. Let R be commutative, and let M, N be R -modules.

(a) Let M be free with basis $(u_i)_{i \in I}$ and N free with basis $(v_j)_{j \in J}$. Then $M \otimes_R N$ is a free R -module with basis $(u_i \otimes v_j)_{(i,j) \in I \times J}$.

(b) Let M and N be both finitely generated [projective], then $M \otimes_R N$ is finitely generated [projective].

PROOF. 1. We define

$$F: \left(\bigoplus_{i \in I} M_i \right) \times \left(\bigoplus_{j \in J} N_j \right) \rightarrow \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j) \quad \text{by} \quad F((m_i)_{i \in I}, (n_j)_{j \in J}) = (m_i \otimes n_j)_{(i,j) \in I \times J}.$$

Then F is R -balanced and induces a homomorphism

$$\Phi: \left(\bigoplus_{i \in I} M_i \right) \otimes_R \left(\bigoplus_{j \in J} N_j \right) \rightarrow \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j)$$

such that $\Phi((m_i)_{i \in I} \otimes (n_j)_{j \in J}) = (m_i \otimes n_j)_{(i,j) \in I \times J}$ for all families $(m_i)_{i \in I}$ and $(n_j)_{j \in J}$. Obviously, Φ is functorial in $(M_i)_{i \in I}$ and in $(N_j)_{j \in J}$. For $\lambda \in I$ and $\mu \in J$, the injections

$$\varepsilon_\lambda: M_\lambda \rightarrow \bigoplus_{i \in I} M_i \quad \text{and} \quad \eta_\mu: N_\mu \rightarrow \bigoplus_{j \in J} N_j \quad \text{induce} \quad \varepsilon_\lambda \otimes \eta_\mu: M_\lambda \otimes N_\mu \rightarrow \left(\bigoplus_{i \in I} M_i \right) \otimes_R \left(\bigoplus_{j \in J} N_j \right),$$

and

$$\Psi = (\varepsilon_i \otimes \eta_j)_{(i,j) \in I \times J}: \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j) \rightarrow \left(\bigoplus_{i \in I} M_i \right) \otimes_R \left(\bigoplus_{j \in J} N_j \right)$$

is a homomorphism satisfying $\Phi \circ \Psi = \text{id}$ and $\Psi \circ \Phi = \text{id}$.

2. As $(v_j)_{j \in J}$ is an R -basis of N , the map

$$\theta: \bigoplus_{j \in J} Rv_j \rightarrow N, \quad \text{defined by} \quad \theta((\lambda_j v_j)_{j \in J}) = \sum_{j \in J} \lambda_j v_j, \quad \text{is an isomorphism.}$$

For every $j \in J$, the isomorphism $R \rightarrow Rv_j$ induces an isomorphism $\mu_j: M \xrightarrow{\sim} M \otimes R \xrightarrow{\sim} M \otimes Rv_j$, given by $\mu_j(m) = m \otimes v_j$. Now we consider the sequence of isomorphisms

$$F: M^{(J)} \xrightarrow{(\mu_j)_{j \in J}} \bigoplus_{j \in J} M \otimes_R Rv_j \xrightarrow{\Psi} M \otimes_R \bigoplus_{j \in J} Rv_j \xrightarrow{M \otimes \theta} M \otimes_R N$$

where Ψ is the inverse of the isomorphism given in 1., and thus

$$\Psi(m_j \otimes v_j)_{j \in J} = \Psi \left(\sum_{i \in I} (m_i \otimes \delta_{i,j} v_j) \right) = \sum_{i \in I} m_i \otimes (\delta_{i,j} v_j)_{j \in J}.$$

Hence

$$F((m_j)_{j \in J}) = (M \otimes \theta) \left(\sum_{i \in I} m_i \otimes (\delta_{i,j} v_j)_{j \in J} \right) = \sum_{i \in I} m_i \otimes \sum_{j \in J} \delta_{i,j} v_j = \sum_{j \in J} m_j \otimes v_j.$$

Hence every $z \in M \otimes_R N$ has a unique representation

$$z = \sum_{j \in J} m_j \otimes v_j, \quad \text{where } m_j \in M \text{ for all } j \text{ and } m_j = 0 \text{ for almost all } j \in J.$$

3.(a) Let $(u_i)_{i \in I}$ be an R -basis of M . By 2., every $z \in S \otimes_R M$ has a unique representation

$$z = \sum_{i \in I} a_i \otimes u_i = \sum_{i \in I} a_i(1 \otimes u_i), \quad \text{where } a_i \in S, a_i = 0 \text{ for almost all } i \in I.$$

Hence $(1 \otimes u_i)_{i \in I}$ is an S -basis of $S \otimes_R M$.

(b) Let M be a projective R -module and M' an R -module such that $F = M \oplus M'$ is free. Then $S \otimes_R F$ is a free S -module, and there is an S -module isomorphism $(S \otimes_R M) \oplus (S \otimes_R M') \xrightarrow{\sim} S \otimes_R F$. Hence $S \otimes_R M$ is a projective S -module.

Let M be a finitely generated R -module, $n \in \mathbb{N}$ and $\pi: R^n \rightarrow M$ an R -epimorphism. Then $S \otimes \pi: S \otimes_R R^n \rightarrow S \otimes_R M$ is an S -epimorphism, and there is an S -isomorphism $S \otimes_R R^n \xrightarrow{\sim} S^n$. Hence $S \otimes_R M$ is a finitely generated S -module.

4.(a) By 2., we obtain the following series of isomorphisms:

$$R^{(I \times J)} = (R^{(I)})^{(J)} \xrightarrow{\sim} M^{(J)} \xrightarrow{\sim} M \otimes_R N,$$

given by

$$(\lambda_{i,j})_{(i,j) \in I \times J} = (\lambda_{i,j})_{i \in I, j \in J} \mapsto \left(\sum_{i \in I} \lambda_{i,j} u_i \right)_{j \in J} \mapsto \sum_{j \in J} \left(\sum_{i \in I} \lambda_{i,j} u_i \right) \otimes v_j = \sum_{(i,j) \in I \times J} \lambda_{i,j} (u_i \otimes v_j).$$

Hence every $z \in M \otimes_R N$ has a unique representation

$$z = \sum_{(i,j) \in I \times J} \lambda_{i,j} (u_i \otimes v_j) \quad \text{where } \lambda_{i,j} \in R \text{ and } \lambda_{i,j} = 0 \text{ for almost all } (i,j) \in I \times J.$$

Hence $(u_i \otimes v_j)_{(i,j) \in I \times J}$ is a basis of $M \otimes_R N$.

(b) Let M and N be finitely generated. Then there exist $m, n \in \mathbb{N}$ and epimorphisms $\mu: R^m \rightarrow M$ and $\nu: R^n \rightarrow N$. Hence $(\mu \otimes \nu): R^m \otimes_R R^n \rightarrow M \otimes_R N$ is an epimorphism. By 2., $R^m \otimes_R R^n \cong R^{mn}$ is finitely generated, and thus $M \otimes_R N$ is finitely generated.

If M and N are projective, then there exist R -modules M' and N' such that $M \oplus M'$ and $N \oplus N'$ are free. By (a), $(M \oplus M') \otimes_R (N \oplus N')$ is free, and by 1., $(M \oplus M') \otimes_R (N \oplus N') = (M \otimes_R N) \oplus L$, where $L = (M' \otimes N) \oplus (M' \otimes N') \oplus (M \otimes N')$. Hence $M \otimes_R N$ is projective. \square

Definitions and Remarks. Let R be commutative and $f: R \rightarrow A$ an R -algebra.

1. Multiplication in A is an R -bilinear map $A \times A \rightarrow A$. Thus it induces a unique R -homomorphism

$$\mu^A: A \otimes_R A \rightarrow A \quad \text{such that } \mu^A(a_1 \otimes a_2) = a_1 a_2 \quad \text{for all } a_1, a_2 \in A.$$

For an ideal $\mathfrak{a} \subset R$, we denote by $\mathfrak{a}A = {}_A \langle f(\mathfrak{a}) \rangle$ the *extension ideal* of \mathfrak{a} in A . By definition, $\mathfrak{a}A = \mu_{\mathfrak{a}}^A(\mathfrak{a} \otimes_R A) \subset A$. In particular, $\mu^A|_R = \mu_R^A: R \otimes_R A \xrightarrow{\sim} A$ is the isomorphism given in Theorem 1.2.3.1.

2. For an R -module M , its base extension $A \otimes_R M = M \otimes_R A$ is a two-sided (A, A) -bimodule. For elementary tensors, the bimodule structure is given by $b(a \otimes m)c = bac \otimes m$ for all $a, b, c \in A$ and $m \in M$.

3. Let $g: R \rightarrow B$ be another R -algebra. Then the map

$$(A \otimes_R B) \times (A \otimes_R B) \rightarrow (A \otimes_R B) \otimes_R (A \otimes_R B) \xrightarrow{\sim} (A \otimes_R A) \otimes_R (B \otimes_R B) \xrightarrow{\mu^A \otimes \mu^B} A \otimes_R B$$

defines a multiplication on $A \otimes_R B$ such that $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$ for all $a_1, a_2 \in A$ and $b_1, b_2 \in B$. With this multiplication, $A \otimes_R B$ is a ring with unit element $1_A \otimes 1_B$. The map

$$\theta: R \xrightarrow{\sim} R \otimes_R R \xrightarrow{f \otimes g} A \otimes_R B$$

makes $A \otimes_R B$ into an R -algebra such that $r(a \otimes b) = ra \otimes b = a \otimes rb$ for all $r \in R$, $a \in A$ and $b \in B$. The R -algebra $\theta: R \rightarrow A \otimes_R B$ is called the *tensor product* of the R -algebras $f: R \rightarrow A$ and $g: R \rightarrow B$. The maps $\varepsilon_A: A \rightarrow A \otimes_R B$, defined by $\varepsilon_A(a) = a \otimes 1_B$ and $\varepsilon_B: B \rightarrow A \otimes_R B$, defined by $\varepsilon_B(b) = 1_A \otimes b$, are R -algebra homomorphisms.

Category-theoretic interpretation: $(A \otimes B, \varepsilon_A, \varepsilon_B)$ is a coproduct in A and B in the category of R -algebras. Explicitly: Given R -algebra homomorphisms $\varphi: A \rightarrow C$ and $\psi: B \rightarrow C$, there exists a unique R -algebra homomorphism $\Theta: A \otimes_R B \rightarrow C$ such that $\Theta \circ \varepsilon_A = \varphi$ and $\Theta \circ \varepsilon_B = \psi$. Explicitly, $\Theta(a \otimes b) = \varphi(a)\psi(b)$ for all $a \in A$ and $b \in B$.

Theorem 1.2.6. *Let $f: R \rightarrow A$ be an R -algebra, and let M and N be R -modules. There is a unique A -module homomorphism*

$$\Phi: A \otimes_R \text{Hom}_R(M, N) \rightarrow \text{Hom}_A(A \otimes_R M, A \otimes_R N)$$

such that $\Phi(a \otimes f)(b \otimes m) = ba \otimes f(m)$ for all $f \in \text{Hom}_R(M, N)$, $a, b \in A$ and $m \in M$. Φ is functorial in A , M and N , and if either M or A is a finitely generated projective R -module, then Φ is an isomorphism.

PROOF. 2. For any $a \in A$ and $f \in \text{Hom}_R(M, N)$, the map $F_0(a, f): A \times M \rightarrow A \otimes_R M$, defined by $F_0(a, f)(b, m) = ba \otimes f(m)$ for all $b \in A$ and $m \in M$, is R -balanced. It induces a group homomorphism $F(a, f): A \otimes_R M \rightarrow A \otimes_R M$ satisfying $F(a, f)(b \otimes m) = ba \otimes f(m)$ for all $b \in A$ and $m \in M$, and if $c \in A$, then $F(a, f)(c(b \otimes m)) = F(a, f)(cb \otimes m) = cba \otimes f(m) = cF(a, f)(b \otimes m)$. Hence $F(a, f)$ is an A -homomorphism, and the map $F: A \times \text{Hom}_R(M, N) \rightarrow \text{Hom}_A(A \otimes_R M, A \otimes_R N)$, $(a, f) \mapsto F(a, f)$, is R -balanced. Hence there is a unique homomorphism $\Phi: A \otimes_R \text{Hom}_R(M, N) \rightarrow \text{Hom}_A(A \otimes_R M, A \otimes_R N)$ satisfying $\Phi(a \otimes f)(b \otimes m) = ba \otimes f(m)$ for all $f \in \text{Hom}_R(M, N)$, $a, b \in A$ and $m \in M$. If $c \in A$, then

$$\begin{aligned} (c\Phi(a \otimes f))(b \otimes m) &= \Phi(a \otimes f)((b \otimes m)c) = \Phi(a \otimes f)(bc \otimes m) = bca \otimes f(m) = \Phi(ca \otimes f)(b \otimes m) \\ &= \Phi(c(a \otimes f))(b \otimes m), \quad \text{and therefore} \quad \Phi(c(a \otimes f)) = c\Phi(a \otimes f). \end{aligned}$$

Hence Φ is an A -homomorphism, and it is easily checked that it is functorial in M and N .

We prove now that, if M is a finitely generated projective R -module, then Φ is bijective [the case, when A is a finitely generated projective R -module is left as an exercise]. For this, it suffices to prove:

A. Let M_1, M_2 be R -modules and $M = M_1 \oplus M_2$. Then

$$\Phi: A \otimes_R \text{Hom}_R(M, N) \rightarrow \text{Hom}_A(A \otimes_R M, A \otimes_R N)$$

is an isomorphism if and only if both homomorphisms

$$\Phi_i: A \otimes_R \text{Hom}_R(M_i, N) \rightarrow \text{Hom}_A(A \otimes_R M_i, A \otimes_R N) \quad \text{for } i \in \{1, 2\}$$

are isomorphisms.

Assume that **A** holds. If M is a finitely generated projective R -module, then $R^n \cong M \oplus M'$ for some $n \in \mathbb{N}$ and some R -module M' . Hence it suffices to prove that

$$\Phi_n: A \otimes_R \text{Hom}_R(R^n, N) \rightarrow \text{Hom}_A(A \otimes_R R^n, A \otimes_R N)$$

is an isomorphism, and, again using **A**, this follows by induction on n , once we have proved it for $n = 1$. But in this there is a commutative diagram

$$\begin{array}{ccc} A \otimes_R \text{Hom}_R(R, N) & \xrightarrow{\Phi_1} & \text{Hom}_A(A \otimes_R R, A \otimes_R N) \\ \alpha \downarrow & & \downarrow \gamma \\ A \otimes_R N & \xrightarrow{\beta} & \text{Hom}_A(A, A \otimes_R N) \end{array}$$

where α is the isomorphism induced $\text{Hom}_R(R, N) \xrightarrow{\sim} N$, γ is the isomorphism induced by $A \otimes_R R \xrightarrow{\sim} A$, and β is also an isomorphism. Hence Φ_1 is an isomorphism.

Proof of A. Since the additive functors $\text{Hom}_R(-, N)$, $A \otimes_R -$ and $\text{Hom}_A(-, A \otimes_R N)$ interchange with direct sums (up to isomorphisms), we obtain a commutative diagram

$$\begin{array}{ccc} A \otimes_R \text{Hom}_R(M, N) & \xrightarrow{\cong} & (A \otimes_R \text{Hom}_R(M_1, N)) \oplus (A \otimes_R \text{Hom}_R(M_2, N)) \\ \Phi \downarrow & & \downarrow (\Phi_1, \Phi_2) \\ \text{Hom}_A(A \otimes_R M, A \otimes_R N) & \xrightarrow{\cong} & \text{Hom}_A(A \otimes_R M_1, A \otimes_R N) \oplus \text{Hom}_A(A \otimes_R M_2, A \otimes_R N) \end{array}$$

Hence Φ is an isomorphism if and only if Φ_1 and Φ_2 are both isomorphisms. \square

Examples.

1. Let M be an R -module, $\mathfrak{a} \subset R$ a right ideal and $\mu_{\mathfrak{a}}^M: \mathfrak{a} \otimes_R M \rightarrow M$ the multiplication homomorphism. The exact sequence $\mathbf{0} \rightarrow \mathfrak{a} \xrightarrow{i} R \xrightarrow{\pi} R/\mathfrak{a} \rightarrow \mathbf{0}$ of right R -modules induces a commutative diagram with exact rows

$$\begin{array}{ccccccc} \mathfrak{a} \otimes_R M & \xrightarrow{i \otimes M} & R \otimes_R M & \xrightarrow{\pi \otimes M} & R/\mathfrak{a} \otimes_R M & \longrightarrow & \mathbf{0} \\ \mu_{\mathfrak{a}}^M \downarrow & & \Phi \downarrow \cong & & & & \\ \mathbf{0} & \longrightarrow & \mathfrak{a}M & \longrightarrow & M & \longrightarrow & M/\mathfrak{a}M \longrightarrow \mathbf{0} \end{array},$$

where the second row is the canonical one, $\mu_{\mathfrak{a}}^M$ is an epimorphism and Φ is an isomorphism. The map $(\pi \otimes M) \circ \Phi^{-1}: M \rightarrow R/\mathfrak{a} \otimes_R M$ is an epimorphism with kernel $\text{Im}(\Phi \circ (i \otimes M)) = \mathfrak{a}M$, and thus it induces an isomorphism $\rho: M/\mathfrak{a}M \rightarrow R/\mathfrak{a} \otimes_R M$, given by $\rho(m + \mathfrak{a}M) = (1 + \mathfrak{a}) \otimes m$ for all $m \in M$. In particular, if $\mathfrak{a} \triangleleft R$, then ρ is an isomorphism of R -modules and of R/\mathfrak{a} -modules. If M is R -free with basis $(u_i)_{i \in I}$, then $R/\mathfrak{a} \otimes_R M$ is R/\mathfrak{a} -free with basis $((1 + \mathfrak{a}) \otimes u_i)_{i \in I}$, and therefore $M/\mathfrak{a}M$ is R/\mathfrak{a} -free with basis $(u_i + \mathfrak{a}M)_{i \in I}$.

2. Let $R \rightarrow A$ be an R -algebra, $n \in \mathbb{N}$. Then there is an isomorphism $A \otimes_R \mathbf{M}_n(R) \xrightarrow{\sim} \mathbf{M}_n(A)$. In particular, if $m \in \mathbb{N}$, then there is an isomorphism $\mathbf{M}_m(R) \otimes \mathbf{M}_n(R) \xrightarrow{\sim} \mathbf{M}_{mn}(R)$.
3. Let $R \rightarrow A$ be a commutative R -algebra and H a monoid. Then there is an isomorphism $A \otimes R[H] \xrightarrow{\sim} A[H]$. Suppose that H is a free abelian multiplicative monoid with basis $\mathbf{X} = (X_i)_{i \in I}$. Then $R[H] = R[\mathbf{X}]$ is a polynomial ring, and $A \otimes_R R[\mathbf{X}] \cong A[\mathbf{X}]$. In particular, if $A = R[\mathbf{T}]$ is a polynomial ring in a family $\mathbf{T} = (T_j)_{j \in J}$ of indeterminates, the $R[\mathbf{T}] \otimes_R R[\mathbf{X}] \cong R[\mathbf{T}, \mathbf{X}]$.

Theorem and Definition 1.2.7.

1. For an R -module E , the following conditions are equivalent:
 - (a) $- \otimes_R E: \mathbf{Mod}\text{-}R \rightarrow \mathbf{Ab}$ is an exact functor.
 - (b) For every monomorphism of right R -modules $i: M' \rightarrow M$, the induced homomorphism $i \otimes E: M' \otimes_R E \rightarrow M \otimes_R E$ is again a monomorphism.
 - (c) For every finitely generated right ideal $\mathfrak{a} \subset R$, the multiplication homomorphism

$$\mu_{\mathfrak{a}}^E: \mathfrak{a} \otimes_R E \rightarrow E$$

of \mathfrak{a} on E is a monomorphism (and thus induces an isomorphism $\mu_{\mathfrak{a}}^E: \mathfrak{a} \otimes_R E \rightarrow \mathfrak{a}E$ of abelian groups).

If these conditions are fulfilled, then E is called *(R -)flat*. An R -algebra $R \rightarrow A$ is called *flat* if A is a flat R -module.

2. Let $(E_i)_{i \in I}$ be a family of R -modules. Then

$$E = \bigoplus_{i \in I} E_i \text{ is flat if and only if all } E_i \text{ are flat.}$$

3. Every projective R -module is flat.

PROOF. (a) \Rightarrow (b) \Rightarrow (c) Obvious.

(c) \Rightarrow (a) It suffices to prove that for every right R -module M the following assertion holds:

- A.** For every R -submodule $M_1 \subset M$, the injection $i: M_1 \hookrightarrow M$ induces a monomorphism

$$i \otimes E: M_1 \otimes_R E \rightarrow M \otimes_R E.$$

Suppose that **A**. holds for every right R -module M , and let $M' \xrightarrow{f} M \xrightarrow{g} M''$ be an exact sequence of right R -modules. Then g splits in the form $g: M \xrightarrow{\pi} M/\text{Ker}(g) \xrightarrow{\sim} \text{Im}(g) \xrightarrow{i} M''$, where π denotes the residue class homomorphism and i denotes the injection. Tensoring with E , we obtain

$$g \otimes E: M \otimes_R E \xrightarrow{\pi \otimes E} M/\text{Ker}(g) \otimes E \xrightarrow{\sim} \text{Im}(g) \otimes_R E \xrightarrow{i \otimes E} M'' \otimes_R E.$$

$\pi \otimes E$ is a monomorphism by **A**., and therefore $\text{Ker}(g \otimes E) = \text{Ker}(\pi \otimes E)$. From the exact sequence $M' \xrightarrow{f} M \xrightarrow{\pi} M/\text{Ker}(g) \rightarrow \mathbf{0}$ we get the exact sequence $M' \otimes_R E \xrightarrow{f \otimes E} M \otimes_R E \xrightarrow{\pi \otimes E} M/\text{Ker}(g) \otimes_R E \rightarrow \mathbf{0}$, which implies that $\text{Im}(f \otimes E) = \text{Ker}(\pi \otimes E) = \text{Ker}(g \otimes E)$. Hence $M' \otimes_R E \xrightarrow{f \otimes E} M \otimes_R E \xrightarrow{g \otimes E} M'' \otimes_R E$ is exact.

For the proof of **A**., we show first :

A₀. If M is a right R -module, and **A** holds for every finitely generated R -submodule of M , then **A** holds for every R -submodule of M .

*Proof of A*₀. Let M be a right R -module, suppose that **A** holds for every finitely generated R -submodule of M , and let $M_1 \subset M$ be any R -submodule. Let $i: M_1 \hookrightarrow M$ be the injection, and suppose that $z \in \text{Ker}(i \otimes E: M_1 \otimes_R E \rightarrow M \otimes_R E)$, say

$$z = \sum_{\nu=1}^n a_\nu \otimes e_\nu \in M_1 \otimes_R E, \quad \text{where } n \in \mathbb{N}, a_\nu \in M_1 \text{ and } e_\nu \in E.$$

Then $M' = a_1 R + \dots + a_n R \subset M_1$, and if $j = (M' \hookrightarrow M_1)$, then $i' = i \circ j = (M' \hookrightarrow M)$, and thus $i' \otimes E$ is a monomorphism by **A**₀. If

$$z' = \sum_{\nu=1}^n a_\nu \otimes e_\nu \in M' \otimes_R E, \quad \text{then } (i' \otimes E)(z') = (i \otimes E) \circ (j \otimes E)(z') = (i \otimes E)(z) = 0,$$

hence $z' = 0$, and thus also $z = (j \otimes E)(z') = 0$. Consequently, $i \otimes E$ is a monomorphism. $\square[\mathbf{A}_0]$

Proof of A. CASE 1: M is finitely generated and free. We use induction on $n = \text{rk}(M)$. If $n = 1$, we may assume that $M = R$, and then a finitely generate right R -submodule of R is a finitely generated right ideal. Hence there is nothing to do.

Suppose that $n > 1$. Then $M = M_1 \dot{+} M_2$, where, for $i \in \{1, 2\}$, $M_i \subset M$ is a free R -submodule of rank $\text{rk}(M_i) < n$. Let $M' \subset M$ be a finitely generated R -submodule. It induces a commutative diagram with exact rows

$$\begin{array}{ccccccccc} \mathbf{0} & \longrightarrow & M'_1 & \xrightarrow{\varepsilon'} & M' & \xrightarrow{p'} & M'_2 & \longrightarrow & \mathbf{0} \\ & & i_1 \downarrow & & \downarrow i & & \downarrow i_2 & & \\ \mathbf{0} & \longrightarrow & M_1 & \xrightarrow{\varepsilon} & M & \xrightarrow{p} & M_2 & \longrightarrow & \mathbf{0} \end{array}$$

where ε is the injection and p the projection of the internal direct sum, $M'_1 = M_1 \cap M'$, $\varepsilon' = \varepsilon|_{M'_1}$, $p' = p|_{M'}$, $M'_2 = p(M')$, and i_1, i, i_2 are the injections. Since the bottom sequence splits, tensoring with E induces a commutative diagram with exact rows

$$\begin{array}{ccccccccc} M'_1 \otimes_R E & \xrightarrow{\varepsilon' \otimes E} & M' \otimes_R E & \xrightarrow{p' \otimes E} & M'_2 \otimes_R E & \longrightarrow & \mathbf{0} \\ i_1 \otimes E \downarrow & & \downarrow i \otimes E & & \downarrow i_2 \otimes E & & \\ \mathbf{0} & \longrightarrow & M_1 \otimes_R E & \xrightarrow{\varepsilon \otimes E} & M \otimes_R E & \xrightarrow{p \otimes E} & M_2 \otimes_R E & \longrightarrow & \mathbf{0} \end{array},$$

and the Snake Lemma yields an exact sequence $\text{Ker}(i_1 \otimes E) \rightarrow \text{Ker}(i \otimes E) \rightarrow \text{Ker}(i_2 \otimes E)$. By the induction hypothesis, $i_1 \otimes E$ and $(i_2 \otimes E)$ are monomorphisms, and therefore $i \otimes E$ is a monomorphism.

CASE 2: M is free with an arbitrary basis $(u_j)_{j \in J}$. Let $M' \subset M$ be a finitely generated submodule and $i: M' \hookrightarrow M$ the injection. Then there is a finite subset $J_0 \subset J$ such that

$$M' \subset M_0 = \sum_{i \in J_0} u_i R \subseteq M.$$

Then we obtain $i = i_0 \circ i'$, where $i' = (M' \hookrightarrow M_0)$ and $i_0 = (M_0 \hookrightarrow M)$. As i_0 splits, the induced homomorphism $i_0 \otimes E: M_0 \otimes E \rightarrow M \otimes E$ is a (split) monomorphism, and as M_0 is finitely generated and free, $i' \otimes E: M' \otimes_R E \rightarrow M_0 \otimes_R E$ is a monomorphism by CASE 1. Hence $i \otimes E = (i_0 \otimes E) \circ (i' \otimes E)$ is a monomorphism.

CASE 3: M is any right R -module. Let $M' \subset M$ be an R -submodule, $i: M' \hookrightarrow M$ the injection, F a free right R -module and $p: F \rightarrow M$ an R -epimorphism. Then $K = \text{Ker}(p) = p^{-1}(\mathbf{0}) \subset p^{-1}(M')$, and we obtain the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} \mathbf{0} & \longrightarrow & K & \xrightarrow{j'} & p^{-1}(M') & \xrightarrow{p'} & M' & \longrightarrow & \mathbf{0} \\ & & \text{id}_K \downarrow & & \downarrow i_1 & & \downarrow i & & \\ \mathbf{0} & \longrightarrow & K & \xrightarrow{j} & F & \xrightarrow{p} & M & \longrightarrow & \mathbf{0} \end{array},$$

where $p' = p|_{p^{-1}(M')}$, j, j', i_1 and i are injections. By CASE 2, applied with F instead of M , j and i_1 induce a monomorphism $j \otimes E: K \otimes_R E \rightarrow F \otimes_R E$ and $i_1 \otimes E: p^{-1}(M') \otimes_R E \rightarrow F \otimes_R E$. Tensoring with E yields the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} K \otimes_R E & \xrightarrow{j' \otimes E} & p^{-1}(M') \otimes_R E & \xrightarrow{(p|_{p^{-1}(M')}) \otimes E} & M' \otimes_R E & \longrightarrow & \mathbf{0} \\ \text{id}_{K \otimes_R E} \downarrow & & \downarrow i_1 \otimes E & & \downarrow i \otimes E & & \\ \mathbf{0} & \longrightarrow & K \otimes_R E & \xrightarrow{j \otimes E} & F \otimes_R E & \xrightarrow{p \otimes E} & M \otimes_R E & \longrightarrow & \mathbf{0} \end{array},$$

The Snake Lemma yields an exact sequence $\mathbf{0} = \text{Ker}(i_1 \otimes E) \rightarrow \text{Ker}(i \otimes E) \rightarrow \text{Coker}(\text{id}_{K \otimes_R E}) = \mathbf{0}$, and therefore $i \otimes E$ is a monomorphism.

2. Let $\mathfrak{a} \subset R$ be a right ideal. For $i \in I$, let $\mu_i = \mu_{\mathfrak{a}}^{E_i}: \mathfrak{a} \otimes_R E_i \rightarrow E_i$ the multiplication homomorphism, and define

$$\mu: \mathfrak{a} \otimes_R E = \mathfrak{a} \otimes \bigoplus_{i \in I} E_i \xrightarrow{\sim} \bigoplus_{i \in I} (\mathfrak{a} \otimes_R E_i) \xrightarrow{(\mu_i)_{i \in I}} \bigoplus_{i \in I} E_i = E$$

For $a \in \mathfrak{a}$ and $e = (e_i)_{i \in I} \in E$, we obtain $\mu(a \otimes e) = (\mu_i(a \otimes e_i))_{i \in I} = ae$, and thus $\mu = \mu_{\mathfrak{a}}^E$. Hence $\mu_{\mathfrak{a}}^E$ is a monomorphism if and only if all $\mu_{\mathfrak{a}}^{E_i}$ are monomorphisms. Therefore E is flat if and only if all E_i are flat.

3. Let $\mathfrak{a} \subset R$ is a right ideal. Then $\mu_{\mathfrak{a}}^R = (\mathfrak{a} \otimes_R R \xrightarrow{\sim} \mathfrak{a} \hookrightarrow R)$ is a monomorphism, and therefore R is flat. By 2., every free R -module and thus also every projective R -module is flat. \square

Theorem 1.2.8. *Let $R \rightarrow A$ be a flat R -algebra.*

1. *Let $\mathfrak{a}, \mathfrak{b} \subset R$ be ideals. Then $(\mathfrak{a} \cap \mathfrak{b})A = \mathfrak{a}A \cap \mathfrak{b}A$.*
2. *Let M, N be R -modules, and suppose that M is finitely presented. Then the A -homomorphism $\Phi: A \otimes_R \text{Hom}_R(M, N) \rightarrow \text{Hom}_A(A \otimes_R M, A \otimes_R N)$ introduced in Theorem 1.2.6 is an isomorphism.*

PROOF. 1. The exact sequence $\mathbf{0} \rightarrow \mathfrak{a} \cap \mathfrak{b} \xrightarrow{i} R \rightarrow R/\mathfrak{a} \oplus R/\mathfrak{b}$ induces the following commutative diagram, where the upper row is exact and the vertical arrows are isomorphisms, where all arrays are the natural one.

$$\begin{array}{ccccccc} \mathbf{0} & \longrightarrow & (\mathfrak{a} \cap \mathfrak{b}) \otimes_R A & \xrightarrow{i \otimes A} & R \otimes_R A & \xrightarrow{\rho} & (R/\mathfrak{a} \otimes_R A) \oplus (R/\mathfrak{b} \otimes_R A) \\ & & \mu_{\mathfrak{a} \cap \mathfrak{b}}^A \downarrow & & \Phi \downarrow \cong & & \cong \downarrow \Phi_0 \\ \mathbf{0} & \longrightarrow & (\mathfrak{a} \cap \mathfrak{b})A & \xrightarrow{j} & A & \xrightarrow{\rho_0} & A/\mathfrak{a}A \oplus A/\mathfrak{b}A \end{array}$$

Note that, for all $r \in R$ and $a \in A$, $(\rho_0 \circ \Phi)(r \otimes a) = (ra + \mathfrak{a}A, ra + \mathfrak{b}A)$, and

$$(\Phi_0 \circ \rho)(r \otimes a) = \Phi_0((r + \mathfrak{a}) \otimes a, (r + \mathfrak{b}) \otimes a) = (ra + \mathfrak{a}A, ra + \mathfrak{b}A) = (\rho_0 \circ \Phi)(r \otimes a).$$

Hence the bottom row is exact, and $(\mathfrak{a} \cap \mathfrak{b})A = \text{Ker}(\rho_0) = \mathfrak{a}A \cap \mathfrak{b}A$.

2. As M is finitely presented, there is an exact sequence $F_2 \xrightarrow{\pi'} F_1 \xrightarrow{\pi} M \rightarrow \mathbf{0}$, where F_1 and F_2 are finitely generated free R -modules. Since A is flat and Hom is left-exact, we obtain the following commutative diagram with exact rows.

$$\begin{array}{ccccccc} \mathbf{0} & \longrightarrow & A \otimes_R \text{Hom}_R(M, N) & \longrightarrow & A \otimes_R \text{Hom}_R(F_1, N) & \longrightarrow & A \otimes_R \text{Hom}_R(F_2, N) \\ & & \Phi \downarrow & & \downarrow \Phi_1 & & \downarrow \Phi_2 \\ \mathbf{0} & \longrightarrow & \text{Hom}_A(A \otimes_R M, A \otimes_R N) & \longrightarrow & \text{Hom}_A(A \otimes_R F_1, A \otimes_R N) & \longrightarrow & \text{Hom}_A(A \otimes_R F_2, A \otimes_R N) \end{array}$$

By Theorem 1.2.6, Φ_1 and Φ_2 are isomorphisms, and by an easy diagram chasing it follows that also Φ is an isomorphism. \square

1.3. Basics of homological algebra

Let R be a ring.

Definitions and Remarks.

1. A *(chain) complex* (in $R\text{-Mod}$) is a sequence of (R -)homomorphisms $(d_n: K_n \rightarrow K_{n-1})_{n \in \mathbb{Z}}$ such that $d_n \circ d_{n+1} = 0$ for all $n \in \mathbb{Z}$. We write it in the form

$$K_\bullet = (K_\bullet, d_\bullet) : \dots \rightarrow K_{n+1} \xrightarrow{d_{n+1}} K_n \xrightarrow{d_n} K_{n-1} \rightarrow \dots$$

Then $\text{Im}(d_{n+1}) \subset \text{Ker}(d_n)$, and we call $H_n(K_\bullet) = \text{Ker}(d_n)/\text{Im}(d_{n+1})$ the n -th *homology group* of K_\bullet . For every $n \in \mathbb{Z}$, there is an exact sequence

$$\begin{array}{c} \mathbf{0} \rightarrow H_n(K_\bullet) = \text{Ker}(d_n)/\text{Im}(d_{n+1}) \hookrightarrow \text{Coker}(d_{n+1}) = K_n/\text{Im}(d_{n+1}) \\ \xrightarrow{\bar{d}_n} \text{Ker}(d_{n-1}) \xrightarrow{\pi_{n-1}} \text{Ker}(d_{n-1})/\text{Im}(d_n) = H_{n-1}(K_\bullet) \rightarrow \mathbf{0}, \end{array}$$

where $\bar{d}_n(x + \text{Im}(d_{n+1})) = d_n(x)$ for $x \in K_n$, and π_{n-1} is the residue class homomorphism. A complex K_\bullet is called *positive* if $K_n = \mathbf{0}$ for all $n < 0$. A complex K_\bullet is an exact sequence if and only if $H_n(K_\bullet) = \mathbf{0}$ for all $n \in \mathbb{Z}$.

2. Let $(K_\bullet, d_\bullet), (K'_\bullet, d'_\bullet)$ be complexes. A *morphism* $f_\bullet: K_\bullet \rightarrow K'_\bullet$ is a sequence of R -homomorphisms $(f_n: K_n \rightarrow K'_n)_{n \in \mathbb{Z}}$ such that $f_{n-1} \circ d_n = d'_n \circ f_n$ for all $n \in \mathbb{Z}$. If $f_\bullet, g_\bullet: K_\bullet \rightarrow K'_\bullet$ are morphisms, then $f_\bullet + g_\bullet = (f_n + g_n)_{n \in \mathbb{Z}}$ is also a morphism. $0 = (0: K_n \rightarrow K'_n)_{n \in \mathbb{Z}}$ and $\text{id}_{K_\bullet} = (\text{id}_{K_n})_{n \in \mathbb{Z}}$ are morphisms, and if $f_\bullet: K_\bullet \rightarrow K'_\bullet$ and $g_\bullet: K'_\bullet \rightarrow K''_\bullet$ are morphisms, then $g_\bullet \circ f_\bullet = (g_n \circ f_n)_{n \in \mathbb{Z}}: K_\bullet \rightarrow K''_\bullet$ is again a morphism. Consequently, the class of complexes in $R\text{-Mod}$ together with its morphisms is an additive category, denoted by \mathbf{C}_R .

If $f_\bullet: (K_\bullet, d_\bullet) \rightarrow (K'_\bullet, d'_\bullet)$ is a morphism of complexes, then

$$f_n(\text{Ker}(d_n)) \subset \text{Ker}(d'_n) \quad \text{and} \quad f_n(\text{Im}(d_{n+1})) \subset \text{Im}(d'_{n+1}) \quad \text{for all } n \in \mathbb{Z}.$$

Indeed, if $x \in \text{Ker}(d_n)$, then $d'_n \circ f_n(x) = f_{n-1} \circ d_n(x) = 0$, and if $x = d_{n+1}(y) \in \text{Im}(d_{n+1})$, then $f_n(x) = f_n \circ d_{n+1}(y) = d'_{n+1} \circ f_{n+1}(y) \in \text{Im}(d'_{n+1})$. Consequently, f_\bullet induces a family of homomorphisms $(H_n(f_\bullet): H_n(K_\bullet) \rightarrow H_n(K'_\bullet))_{n \in \mathbb{Z}}$, and the following commutative diagram connecting the exact sequences mentioned above.

$$\begin{array}{ccccccc} \mathbf{0} & \longrightarrow & H_n(K_\bullet) & \longrightarrow & \text{Coker}(d_{n+1}) & \longrightarrow & \text{Ker}(d_{n-1}) & \longrightarrow & H_{n-1}(K_\bullet) & \longrightarrow & \mathbf{0} \\ & & H_n(f_\bullet) \downarrow & & \downarrow \bar{f}_n & & \downarrow f_{n-1} & & \downarrow H_{n-1}(f_\bullet) & & \\ \mathbf{0} & \longrightarrow & H_n(K'_\bullet) & \longrightarrow & \text{Coker}(d'_{n+1}) & \longrightarrow & \text{Ker}(d'_{n-1}) & \longrightarrow & H_{n-1}(K'_\bullet) & \longrightarrow & \mathbf{0} \end{array}$$

For $n \in \mathbb{Z}$, $H_n: \mathbf{C}_R \rightarrow \mathbf{Ab}$ is an additive functor. Indeed, $H_n(f_\bullet + g_\bullet) = H_n(f_\bullet) + H_n(g_\bullet)$ for morphisms $f_\bullet, g_\bullet: K_\bullet \rightarrow K'_\bullet$, and $H_n(g_\bullet \circ f_\bullet) = H_n(g_\bullet) \circ H_n(f_\bullet)$ for morphisms $f_\bullet: K_\bullet \rightarrow K'_\bullet$ and $g_\bullet: K'_\bullet \rightarrow K''_\bullet$.

3. A sequence $\mathbf{0} \rightarrow K'_\bullet \xrightarrow{f_\bullet} K_\bullet \xrightarrow{g_\bullet} K''_\bullet \rightarrow \mathbf{0}$ of morphisms in \mathbf{C}_R is called *exact* if, for all $n \in \mathbb{Z}$, the sequence $\mathbf{0} \rightarrow K'_n \xrightarrow{f_n} K_n \xrightarrow{g_n} K''_n \rightarrow \mathbf{0}$ is exact.

Theorem 1.3.1. *For every exact sequence $\mathbf{0} \rightarrow K'_\bullet \xrightarrow{f_\bullet} K_\bullet \xrightarrow{g_\bullet} K''_\bullet \rightarrow \mathbf{0}$ in \mathbf{C}_R there exists a family of homomorphisms $(\omega_n: H_n(K''_\bullet) \rightarrow H_{n-1}(K'_\bullet))_{n \in \mathbb{Z}}$ such that the long homology sequence*

$$\dots \xrightarrow{\omega_{n+1}} H_n(K'_\bullet) \xrightarrow{H_n(f_\bullet)} H_n(K_\bullet) \xrightarrow{H_n(g_\bullet)} H_n(K''_\bullet) \xrightarrow{\omega_n} H_{n-1}(K'_\bullet) \xrightarrow{H_{n-1}(f_\bullet)} H_{n-1}(K_\bullet) \rightarrow \dots$$

is exact. It is functorial in the given short exact sequence. Explicitly, a commutative diagram of complexes with exact rows

$$\begin{array}{ccccccccc} \mathbf{0} & \longrightarrow & K'_\bullet & \longrightarrow & K_\bullet & \longrightarrow & K''_\bullet & \longrightarrow & \mathbf{0} \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \mathbf{0} & \longrightarrow & L'_\bullet & \longrightarrow & L_\bullet & \longrightarrow & L''_\bullet & \longrightarrow & \mathbf{0} \end{array}$$

induces the following commutative diagram connecting the long homology sequences.

$$\begin{array}{ccccccccccc} \dots & \xrightarrow{\omega_{n+1}} & H_n(K'_\bullet) & \longrightarrow & H_n(K_\bullet) & \longrightarrow & H_n(K''_\bullet) & \xrightarrow{\omega_n} & H_{n-1}(K'_\bullet) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \dots & \xrightarrow{\omega_{n+1}} & H_n(L'_\bullet) & \longrightarrow & H_n(L_\bullet) & \longrightarrow & H_n(L''_\bullet) & \xrightarrow{\omega_n} & H_{n-1}(L'_\bullet) & \longrightarrow & \dots \end{array}$$

PROOF. Let $\mathbf{0} \rightarrow K'_\bullet \xrightarrow{f_\bullet} K_\bullet \xrightarrow{g_\bullet} K''_\bullet \rightarrow \mathbf{0}$ be an exact sequence of complexes (K'_\bullet, d'_\bullet) , (K_\bullet, d_\bullet) and $(K''_\bullet, d''_\bullet)$. For every $n \in \mathbb{Z}$, we have the commutative diagram

$$\begin{array}{ccccccccc} \mathbf{0} & \longrightarrow & K'_{n-1} & \xrightarrow{f_{n-1}} & K_{n-1} & \xrightarrow{g_{n-1}} & K''_{n-1} & \longrightarrow & \mathbf{0} \\ & & d'_{n-1} \downarrow & & \downarrow d_{n-1} & & \downarrow d''_{n-1} & & \\ \mathbf{0} & \longrightarrow & K'_n & \xrightarrow{f_n} & K_n & \xrightarrow{g_n} & K''_n & \longrightarrow & \mathbf{0} \end{array}$$

and the Snake Lemma induces exact sequences $\mathbf{0} \rightarrow \text{Ker}(d'_{n-1}) \xrightarrow{f_{n-1}} \text{Ker}(d_{n-1}) \xrightarrow{g_{n-1}} \text{Ker}(d''_{n-1})$ and $\text{Coker}(d'_{n+1}) \xrightarrow{\bar{f}_{n+1}} \text{Coker}(d_{n+1}) \xrightarrow{\bar{g}_{n+1}} \text{Coker}(d''_{n+1}) \rightarrow \mathbf{0}$. Hence we obtain the the following commutative diagram with exact columns, in which the two middle rows are exact.

$$\begin{array}{ccccccccc} & & \mathbf{0} & & \mathbf{0} & & \mathbf{0} & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & H_n(K'_\bullet) & \xrightarrow{H_n(f_\bullet)} & H_n(K_\bullet) & \xrightarrow{H_n(g_\bullet)} & H_n(K''_\bullet) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \text{Coker}(d'_{n+1}) & \xrightarrow{\bar{f}_{n+1}} & \text{Coker}(d_{n+1}) & \xrightarrow{\bar{g}_{n+1}} & \text{Coker}(d''_{n+1}) & \longrightarrow & \mathbf{0} \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \mathbf{0} & \longrightarrow & \text{Ker}(d'_{n-1}) & \xrightarrow{f_{n-1}} & \text{Ker}(d_{n-1}) & \xrightarrow{g_{n-1}} & \text{Ker}(d''_{n-1}) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & H_{n-1}(K'_\bullet) & \xrightarrow{H_{n-1}(f_\bullet)} & H_{n-1}(K_\bullet) & \xrightarrow{H_{n-1}(g_\bullet)} & H_{n-1}(K''_\bullet) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \mathbf{0} & & \mathbf{0} & & \mathbf{0} & & \end{array}$$

By the Snake Lemma, it induces an exact sequence

$$H_n(K'_\bullet) \xrightarrow{H_n(f_\bullet)} H_n(K'_\bullet) \xrightarrow{H_n(g_\bullet)} H_n(K''_\bullet) \xrightarrow{\omega} H_{n-1}(K'_\bullet) \xrightarrow{H_{n-1}(f_\bullet)} H_{n-1}(K'_\bullet) \xrightarrow{H_{n-1}(g_\bullet)} H_{n-1}(K''_\bullet).$$

It is easily checked that the whole construction is functorial in the given short exact sequence. \square

Definition. Let (K_\bullet, d_\bullet) and (K'_\bullet, d'_\bullet) be complexes.

1. Two morphisms $f_\bullet, g_\bullet: K_\bullet \rightarrow K'_\bullet$ are called *homotopic*, $f \sim g$, if there exists a sequence of homomorphisms $(h_n: K_n \rightarrow K'_{n+1})_{n \in \mathbb{Z}}$ such that $f_n - g_n = d'_{n+1} \circ h_n + h_{n-1} \circ d_n$ for all $n \in \mathbb{Z}$.
2. A morphism $f_\bullet, g_\bullet: K_\bullet \rightarrow K'_\bullet$ is called a *homotopy equivalence* if there exists a morphism $g_\bullet: K'_\bullet \rightarrow K_\bullet$ such that $g_\bullet \circ f_\bullet \sim \text{id}_{K_\bullet}$ and $f_\bullet \circ g_\bullet \sim \text{id}_{K'_\bullet}$. The complexes K_\bullet and K'_\bullet are called *homotopy equivalent* if there exists a homotopy equivalence $f_\bullet: K_\bullet \rightarrow K'_\bullet$.

Theorem 1.3.2. Let (K_\bullet, d_\bullet) and (K'_\bullet, d'_\bullet) be complexes and $f_\bullet, g_\bullet: K_\bullet \rightarrow K'_\bullet$ morphisms such that $f_\bullet \sim g_\bullet$. Then $H_n(f_\bullet) = H_n(g_\bullet): H_n(K_\bullet) \rightarrow H_n(K'_\bullet)$ for all $n \in \mathbb{Z}$. In particular, if f_\bullet is a homotopy equivalence, then $H_n(f_\bullet)$ is an isomorphism for all $n \in \mathbb{Z}$.

PROOF. Let $(h_n: K_n \rightarrow K'_{n+1})_{n \in \mathbb{Z}}$ be a sequence of homomorphisms such that

$$f_n - g_n = d'_{n+1} \circ h_n + h_{n-1} \circ d_n \quad \text{for all } n \in \mathbb{Z},$$

and consider the maps $H_n(f_\bullet) - H_n(g_\bullet): H_n(K_\bullet) = \text{Ker}(d_n)/\text{Im}(d_{n+1}) \rightarrow \text{Ker}(d'_n)/\text{Im}(d'_{n+1}) = H_n(K'_\bullet)$. If $x \in \text{Ker}(d_n)$, then

$$(H_n(f_\bullet) - H_n(g_\bullet))(x + \text{Im}(d_{n+1})) = f_n(x) - g_n(x) + \text{Im}(d'_{n+1}) = d'_{n+1} \circ h_n(x) + h_{n-1} \circ d_n(x) + \text{Im}(d'_{n+1}) = 0,$$

and thus $H_n(f_\bullet) = H_n(g_\bullet)$.

Assume not that $f_\bullet: K_\bullet \rightarrow K'_\bullet$ is a homotopy equivalence, and let $g_\bullet: K'_\bullet \rightarrow K_\bullet$ be a morphism such that $g_\bullet \circ f_\bullet = \text{id}_{K_\bullet}$ and $f_\bullet \circ g_\bullet = \text{id}_{K'_\bullet}$. Then we obtain $\text{id}_{H_n(K_\bullet)} = H_n(g_\bullet \circ f_\bullet) = H_n(g_\bullet) \circ H_n(f_\bullet)$, and $\text{id}_{H_n(K'_\bullet)} = H_n(f_\bullet \circ g_\bullet) = H_n(f_\bullet) \circ H_n(g_\bullet)$. \square

Theorem and Definition 1.3.3. Let M be an R -module.

A *projective resolution* $(P_\bullet, d_\bullet, \varepsilon)$ of M is a positive complex (P_\bullet, d_\bullet) of projective modules such that $H_n(P_\bullet) = \mathbf{0}$ for all $n \neq 0$, together with an epimorphism $\varepsilon: P_0 \rightarrow M$ such that $\text{Ker}(\varepsilon) = \text{Im}(d_1)$. Equivalently, a projective resolution of M is an exact sequence $\dots \rightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \rightarrow \mathbf{0}$, which (due to $d_0 = 0$) induces an isomorphism $\varepsilon_0: H_0(P_\bullet) = P_0/\text{Im}(d_1) \xrightarrow{\sim} M$.

1. Let $\varphi: M \rightarrow M'$ be a homomorphism of R -modules, $(P_\bullet, d_\bullet, \varepsilon)$ a projective resolution of M and $(P'_\bullet, d'_\bullet, \varepsilon')$ a projective resolution of M' . Then there exists up to homotopy a unique morphism $f_\bullet: P_\bullet \rightarrow P'_\bullet$ such that $\varepsilon' \circ f_0 = \varphi \circ \varepsilon: P_0 \rightarrow M'$.
2. M possesses a projective resolution. If $(P_\bullet, d_\bullet, \varepsilon)$ and $(P'_\bullet, d'_\bullet, \varepsilon')$ are projective resolutions of M , then there exists a homotopy equivalence $f_\bullet: P_\bullet \rightarrow P'_\bullet$ such that $\varepsilon' \circ f_0 = \varepsilon: P_0 \rightarrow M$.

PROOF. 1. *Existence.* We must establish the following commutative diagram with exact rows:

$$\begin{array}{ccccccccccccccc} \dots & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{d_n} & P_{n-1} & \xrightarrow{d_{n-1}} & P_{n-2} & \xrightarrow{d_{n-2}} & \dots & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & \mathbf{0} \\ & & f_n \downarrow & & f_{n-1} \downarrow & & f_{n-2} \downarrow & & & & f_0 \downarrow & & \varphi \downarrow & & \\ \dots & \xrightarrow{d'_{n+1}} & P'_n & \xrightarrow{d'_n} & P'_{n-1} & \xrightarrow{d'_{n-1}} & P'_{n-2} & \xrightarrow{d'_{n-2}} & \dots & \xrightarrow{d'_1} & P'_0 & \xrightarrow{\varepsilon'} & M' & \longrightarrow & \mathbf{0} \end{array}$$

We construct recursively a sequence of homomorphisms $(f_n: P_n \rightarrow P'_n)_{n \in \mathbb{Z}}$ satisfying $f_{n-1} \circ d_n = d'_n \circ f_n$ for all $n \in \mathbb{Z}$ and $\varepsilon' \circ f_0 = \varepsilon$. For $n < 0$ we set $f_0 = 0$. Since P_0 is projective, the diagram

$$\begin{array}{c} P_0 \\ \downarrow \varphi \circ \varepsilon \\ P'_0 \xrightarrow{\varepsilon'} M' \longrightarrow \mathbf{0} \end{array}$$

induces a homomorphism $f_0: P_0 \rightarrow P'_0$ such that $\varphi \circ \varepsilon = \varepsilon' \circ f_0$. Since $\varepsilon' \circ f_0 \circ d_1 = \varphi \circ \varepsilon \circ d_1 = 0$, we get $\text{Im}(f_0 \circ d_1) \subset \ker(\varepsilon') = \text{Im}(d'_1)$, and since P_1 is projective, the diagram

$$\begin{array}{ccc} & P_1 & \\ & \downarrow f_0 \circ d_1 & \\ P'_1 & \xrightarrow{d'_1} \text{Im}(d'_1) & \longrightarrow \mathbf{0} \end{array}$$

induces a homomorphism $f_1: P_1 \rightarrow P'_1$ such that $d'_1 \circ f_1 = f_0 \circ d_1$.

Assume now that $n \geq 2$, and that we have already constructed homomorphisms f_{n-2}, f_{n-1} such that $d'_{n-1} \circ f_{n-1} = f_{n-2} \circ d_{n-1}$. Then we get $d'_{n-1} \circ f_{n-1} \circ d_n = f_{n-2} \circ d_{n-1} \circ d_n = 0$, and consequently $\text{Im}(f_{n-1} \circ d_n) \subset \text{Ker}(d'_{n-1}) = \text{Im}(d'_n)$, since $H_n(P'_\bullet) = \mathbf{0}$. Since P_n is projective, the diagram

$$\begin{array}{ccc} & P_n & \\ & \downarrow f_{n-1} \circ d_n & \\ P'_n & \xrightarrow{d'_n} \text{Im}(d'_n) & \longrightarrow \mathbf{0} \end{array}$$

induces a homomorphism $f_n: P_n \rightarrow P'_n$ such that $d'_n \circ f_n = f_{n-1} \circ d_n$.

Uniqueness up to homotopy. Let $f_\bullet, g_\bullet: P_\bullet \rightarrow P'_\bullet$ be morphisms such that $\varepsilon' \circ f_0 = \varepsilon' \circ g_0 = \varphi \circ \varepsilon$. We construct a sequence of homomorphisms $(h_n: P_n \rightarrow P'_{n+1})_{n \in \mathbb{Z}}$ such that $f_n - g_n = d'_{n+1} \circ h_n + h_{n-1} \circ d_n$ for all $n \in \mathbb{Z}$. For $n < 0$ we have $d'_{n+1} = d_n = 0$, and we set $h_n = 0$. Since $\varepsilon' \circ (f_0 - g_0) = 0$, we obtain $\text{Im}(f_0 - g_0) \subset \text{Ker}(\varepsilon') = \text{Im}(d'_1)$, and since P_0 is projective, the diagram

$$\begin{array}{ccc} & P_0 & \\ & \downarrow f_0 - g_0 & \\ P'_1 & \xrightarrow{d'_1} \text{Im}(d'_1) & \longrightarrow \mathbf{0} \end{array}$$

induces a homomorphism $h_0: P_0 \rightarrow P'_1$ such that $f_0 - g_0 = d'_1 \circ h_0 = d'_1 \circ h_0 + h_{-1} \circ d_0$.

Thus assume that $n \geq 1$ and that we have already constructed homomorphisms h_{n-2}, h_{n-1} . Then

$$\begin{aligned} d'_n \circ (f_n - g_n - h_{n-1} \circ d_n) &= (f_{n-1} - g_{n-1}) \circ d_n - d'_n \circ h_{n-1} \circ d_n \\ &= (d'_n \circ h_{n-1} + h_{n-2} \circ d_{n-1}) \circ d_n - d'_n \circ h_{n-1} \circ d_n = 0, \end{aligned}$$

hence $\text{Im}(f_n - g_n - h_{n-1} \circ d_n) \subset \text{Ker}(d'_n) = \text{Im}(d'_{n+1})$. Since P_n is projective, the diagram

$$\begin{array}{ccc} & P_n & \\ & \downarrow f_n - g_n - h_{n-1} \circ d_n & \\ P'_{n+1} & \xrightarrow{d'_{n+1}} \text{Im}(d'_{n+1}) & \longrightarrow \mathbf{0} \end{array}$$

induces a homomorphism $h_n: P_n \rightarrow P'_{n+1}$ such that $f_n - g_n - h_{n-1} \circ d_n = d'_{n+1} \circ h_n$.

2. We construct an exact sequence $\dots \rightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \rightarrow \mathbf{0}$ with free (hence projective) modules P_n for all $n \geq 0$. Again, we proceed recursively. Clearly, there exists an epimorphism $\varepsilon: P_0 \rightarrow M$ with a free R -module P_0 , and there exists an epimorphism $d_1: P_1 \rightarrow \text{Ker}(\varepsilon) \subset P_0$ with a free R -module P_1 . Then $P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \rightarrow \mathbf{0}$ is exact. Assume now that $n \geq 1$, and that we have already constructed an exact sequence $P_{n-1} \xrightarrow{d_{n-1}} P_{n-2} \rightarrow \dots \rightarrow P_0 \xrightarrow{\varepsilon} M \rightarrow \mathbf{0}$ with free R -modules P_0, \dots, P_{n-1} . Then there exists an epimorphism $d_n: P_n \rightarrow \text{Ker}(d_{n-1}) \subset P_{n-1}$ with a free R -module P_n and we may append the homomorphism $d_n: P_n \rightarrow P_{n-1}$ to extend our sequence.

Assume not that (P_\bullet, ε) and $(P'_\bullet, \varepsilon')$ are projective resolutions of M . By 1., there exist morphisms $f_\bullet: P_\bullet \rightarrow P'_\bullet$ and $g_\bullet: P'_\bullet \rightarrow P_\bullet$ such that $\varepsilon' \circ f_0 = \varepsilon$ and $\varepsilon \circ g_0 = \varepsilon'$. Then $g_\bullet \circ f_\bullet: P_\bullet \rightarrow P_\bullet$ and $\text{id}_{P_\bullet}: P_\bullet \rightarrow P_\bullet$, are morphisms satisfying $\varepsilon \circ (g_0 \circ f_0) = \varepsilon \circ \text{id}_{P_0} = \varepsilon$, and 1. implies that $g_\bullet \circ f_\bullet \sim \varepsilon_{P_\bullet}$. Similarly, we obtain $f_\bullet \circ g_\bullet \sim \varepsilon_{P'_\bullet}$, and therefore P_\bullet and P'_\bullet are homotopy equivalent. \square

Definition. In the sequel we fix for every left and every right R -module a projective resolution. Let N be an R -module and M a right R -module.

a. Let $(Q_\bullet, d_\bullet, \eta)$ be a projective resolution of N . Then $M \otimes_R Q_\bullet = (M \otimes_R Q_n \xrightarrow{M \otimes d_n} M \otimes_R Q_{n-1})_{n \in \mathbb{Z}}$ is a complex, and we define

$$'Tor_n^R(M, N) = H_n(M \otimes_R Q_\bullet) \quad \text{for all } n \in \mathbb{Z}.$$

If $f: M \rightarrow M'$ is a homomorphism of right R -modules, then $f \otimes Q_\bullet: M \otimes_R Q_\bullet \rightarrow M' \otimes_R Q_\bullet$ is a complex homomorphism, and we define

$$'Tor_n^R(f, N) = H_n(f \otimes Q_\bullet): 'Tor_n^R(M, N) \rightarrow 'Tor_n^R(M', N) \quad \text{for all } n \in \mathbb{Z}.$$

These settings define a sequence of additive functors $({}'Tor_n^R(-, N): \mathbf{Mod}\text{-}R \rightarrow \mathbf{Ab})_{n \in \mathbb{Z}}$, called the *Tor functors* in the first variable. By definition, $'Tor_n^R(-, N) = \mathbf{0}$ for $n < 0$, and the exact sequence

$$M \otimes_R Q_1 \xrightarrow{M \otimes d_1} M \otimes_R Q_0 \xrightarrow{M \otimes \eta} M \otimes_R N \rightarrow \mathbf{0},$$

together with $d_0 = 0$, induces an isomorphism

$$'Tor_0^R(M, N) = H_0(M \otimes_R Q_\bullet) = M \otimes_R Q_0 / \text{Im}(M \otimes d_1) = M \otimes_R Q_0 / \text{Ker}(M \otimes \eta) \xrightarrow{\sim} M \otimes_R N,$$

which is functorial in M , and we identify $'Tor_0^R(-, N) = - \otimes_R N$ by means of this isomorphism.

b. Let $(P_\bullet, d_\bullet, \varepsilon)$ be a projective resolution of M . Then $P_\bullet \otimes_R N = (P_n \otimes_R N \xrightarrow{d_n \otimes N} P_{n-1} \otimes_R N)_{n \in \mathbb{Z}}$ is a complex, and we define

$$''Tor_n^R(M, N) = H_n(P_\bullet \otimes_R N) \quad \text{for all } n \in \mathbb{Z}.$$

If $f: N \rightarrow N'$ is a homomorphism of R -modules, then $P_\bullet \otimes f: P_\bullet \otimes_R N \rightarrow P_\bullet \otimes_R N'$ is a complex homomorphism, and we define

$$''Tor_n^R(M, f) = H_n(P_\bullet \otimes f): ''Tor_n^R(M, N) \rightarrow ''Tor_n^R(M, N') \quad \text{for all } n \in \mathbb{Z}.$$

These settings define a sequence of additive functors $(''Tor_n^R(M, -): R\text{-}\mathbf{Mod} \rightarrow \mathbf{Ab})_{n \in \mathbb{Z}}$, called the *Tor functors* in the second variable. By definition, $''Tor_n^R(M, -) = \mathbf{0}$ for $n < 0$, and the exact sequence

$$P_1 \otimes_R N \xrightarrow{d_1 \otimes N} P_0 \otimes_R N \xrightarrow{\varepsilon \otimes N} M \otimes_R N \rightarrow \mathbf{0},$$

together with $d_0 = 0$, induces an isomorphism

$$''Tor_0^R(M, N) = H_0(P_\bullet \otimes_R N) = P_0 \otimes_R N / \text{Im}(d_1 \otimes N) = P_0 \otimes_R N / \text{Ker}(\varepsilon \otimes N) \xrightarrow{\sim} M \otimes_R N,$$

which is functorial in N , and we identify $''Tor_0^R(M, -) = M \otimes_R -$ by means of this isomorphism.

Theorem and Definition 1.3.4. *Let M be a right R -module and N an R -module. Up to functorial isomorphisms, we have $'Tor_n^R(M, N) = ''Tor_n^R(M, N)$ for all $n \in \mathbb{Z}$.*

We define $\text{Tor} = \text{Tor}' = \text{Tor}''$.

For the proof of Theorem 1.3.4 we introduce the notion of double complexes and a first simple Spectral Theorem.

Definitions and Remarks. A *double complex* $(K_{\bullet\bullet}, d'_{\bullet\bullet}, d''_{\bullet\bullet})$ consists of a double sequence of R -homomorphisms

$$(K_{p,q}, d'_{p,q}: K_{p,q} \rightarrow K_{p-1,q}, d''_{p,q}: K_{p,q} \rightarrow K_{p,q-1})$$

satisfying $d'_{p-1,q} \circ d'_{p,q} = 0$, $d''_{p,q-1} \circ d''_{p,q} = 0$ and $d''_{p-1,q} \circ d'_{p,q} = d'_{p,q-1} \circ d''_{p,q}$ for all $p, q \in \mathbb{Z}$. If there is no doubt, in which dimensions the morphisms act, we write the conditions in the form $d' \circ d' = 0$, $d'' \circ d'' = 0$ and $d'' \circ d' = d' \circ d''$. Associated with the double complex $(K_{\bullet\bullet}, d'_{\bullet\bullet}, d''_{\bullet\bullet})$, we define the associated *total complex* (K_\bullet, d_\bullet) by

$$K_n = \bigoplus_{p+q=n} K_{p,q},$$

where $(d_n: K_n \rightarrow K_{n-1})_{n \in \mathbb{Z}}$ is defined as follows. If $n \in \mathbb{Z}$ and $a = (a_{n-i,i})_{i \in \mathbb{Z}}$, where $a_{n-i,i} \in K_{n-i,i}$ for all $i \in \mathbb{Z}$, then $d_n a = ((d_n a)_{n-i-1,i})_{i \in \mathbb{Z}}$, where

$$(d_n a)_{n-i-1,i} = d' a_{n-i,i} + (-1)^{n-i-1} d'' a_{n-i-1,i+1} \in K_{n-i-1,i} \quad \text{for all } i \in \mathbb{Z}.$$

We must verify that $d_{n+1} \circ d_n = 0$ for all $n \in \mathbb{Z}$. Indeed, let $n \in \mathbb{Z}$ and $a = (a_{n+1-i,i})_{i \in \mathbb{Z}} \in K_{n+1}$. If $i \in \mathbb{Z}$, then

$$(d_{n+1} a)_{n-i,i} = d' a_{n+1-i,i} + (-1)^{n-i} d'' a_{n-i,i+1},$$

and, observing $d' \circ d' = d'' \circ d'' = 0$ and $d' \circ d'' = d'' \circ d'$, we obtain

$$\begin{aligned} d_n(d_{n+1} a)_{n-i-1,i} &= d'(d_{n+1} a)_{n-i,i} + (-1)^{n-i-1} d''(d_{n+1} a)_{n-i-i,i+1} \\ &= (-1)^{n-i} d' \circ d'' a_{n-i,i+1} + (-1)^{n-i-1} d'' \circ d' a_{n-i,i+1} = 0. \end{aligned}$$

For $p, q \in \mathbb{Z}$, we call $(K_{p,\bullet}, d''_{p,\bullet})$ the p -th row complex and $(K_{\bullet,q}, d'_{\bullet,q})$ the q -th column complex of $K_{\bullet\bullet}$. Then $d''_{p,\bullet}: K_{p,\bullet} \rightarrow K_{p-1,\bullet}$ and $d'_{\bullet,q}: K_{\bullet,q} \rightarrow K_{\bullet,q-1}$ are complex morphisms.

Let $(K_{\bullet\bullet}, d''_{\bullet\bullet}, d'_{\bullet\bullet})$ be a positive double complex (that means, $K_{p,q} = \mathbf{0}$ if $p < 0$ or $q < 0$). Then the associated total complex and all row and column complexes of $K_{\bullet\bullet}$ are also positive complexes. We define

$$X'_p = H_0(K_{p,\bullet}) = K_{p,0}/\text{Im}(d''_{p,1}) \quad \text{and} \quad X''_q = H_0(K_{\bullet,q}) = K_{0,q}/\text{Im}(d'_{1,q}).$$

Then $\delta'_p = H_0(d''_{p,\bullet}): X'_p \rightarrow X'_{p-1}$ and $\delta''_q = H_0(d'_{\bullet,q}): X''_q \rightarrow X''_{q-1}$ are homomorphisms, given by $\delta'_p(a_{p,0} + \text{Im}(d''_{p,1})) = d''_{p,0}(a_{p,0}) + \text{Im}(d''_{p-1,1})$ and $\delta''_q(a_{0,q} + \text{Im}(d'_{1,q})) = d'_{0,q}(a_{0,q}) + \text{Im}(d'_{1,q-1})$ for all $a_{p,0} \in K_{p,0}$ and $a_{0,q} \in K_{0,q}$. The $(X'_\bullet, \delta'_\bullet)$ and $(X''_\bullet, \delta''_\bullet)$ are positive complexes, called the right and lower edge complex of $X_{\bullet\bullet}$. The situation is coded in the following commutative diagram :

$$\begin{array}{ccccccc} & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \dots & \longrightarrow & K_{2,2} & \xrightarrow{d''_{2,2}} & K_{2,1} & \xrightarrow{d''_{2,1}} & K_{2,0} & \longrightarrow & X'_2 & \longrightarrow & \mathbf{0} \\ & & d'_{2,2} \downarrow & & d'_{2,1} \downarrow & & d'_{2,0} \downarrow & & \downarrow \delta'_1 & & \\ \dots & \longrightarrow & K_{1,2} & \xrightarrow{d''_{1,2}} & K_{1,1} & \xrightarrow{d''_{1,1}} & K_{1,0} & \longrightarrow & X'_1 & \longrightarrow & \mathbf{0} \\ & & d'_{1,2} \downarrow & & d'_{1,1} \downarrow & & d'_{1,0} \downarrow & & \downarrow \delta'_0 & & \\ \dots & \longrightarrow & K_{0,2} & \xrightarrow{d''_{0,2}} & K_{0,1} & \xrightarrow{d''_{0,1}} & K_{0,0} & \longrightarrow & X'_0 & \longrightarrow & \mathbf{0} \\ & & \downarrow & & \downarrow & & \downarrow & & & & \\ \dots & \longrightarrow & X''_2 & \xrightarrow{\delta''_2} & X''_1 & \xrightarrow{\delta''_1} & X''_0 & & & & \\ & & \downarrow & & \downarrow & & & & & & \\ & & \mathbf{0} & & \mathbf{0} & & & & & & \end{array}$$

For $n \in \mathbb{Z}$, we define $\Phi'_n: K_n \rightarrow X'_n$ and $\Phi''_n: K_n \rightarrow X''_n$ by

$$\Phi'_n(a) = a_{n,0} + \text{Im}(d''_{n,1}) \quad \text{and} \quad \Phi''_n(a) = a_{0,n} + \text{Im}(d'_{1,n}) \quad \text{if } a = (a_{n-i,i})_{i \in \mathbb{Z}} \in K_n = \bigoplus_{i \in \mathbb{Z}} K_{n-i,i}.$$

Then the following Spectral Theorem connects the homology of the total complex with the homology of the edge complexes.

Spectral Theorem.

- $\Phi'_\bullet: K_\bullet \rightarrow X'_\bullet$ is a complex morphism which is functorial in $K_{\bullet\bullet}$. If $H_q(K_{p,\bullet}) = \mathbf{0}$ for all $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, then $H_n(\Phi'_\bullet): H_n(K_\bullet) \xrightarrow{\sim} H_n(X'_\bullet)$ is an isomorphism for all $n \in \mathbb{Z}$.
- $\Phi''_\bullet: K_\bullet \rightarrow X''_\bullet$ is a complex morphism which is functorial in $K_{\bullet\bullet}$. If $H_p(K_{\bullet,q}) = 0$ for all $q \in \mathbb{Z}$ and $p \in \mathbb{N}$, then $H_n(\Phi''_\bullet): H_n(K_\bullet) \xrightarrow{\sim} H_n(X''_\bullet)$, is an isomorphism for all $n \in \mathbb{Z}$.

PROOF OF THE SPECTRAL THEOREM. It suffices to prove the first assertion (concerning the right edge complex)

A. Φ'_\bullet is a complex morphism, that means, $\delta'_n \circ \Phi'_n = \Phi'_{n-1} \circ d_n: K_n \rightarrow X'_n$ for all $n \in \mathbb{Z}$.

Let $n \in \mathbb{Z}$ and $a = (a_{n-i,i})_{i \in \mathbb{Z}} \in K_n$. $\delta'_n \circ \Phi'_n(a) = \delta'_n(a_{n,0} + \text{Im}(d''_{n,1})) = d'a_{n,0} + \text{Im}(d''_{n-1,1})$, and $\Phi'_{n-1} \circ d_n(a) = d_n(a)_{n-1,0} + \text{Im}(d''_{n-1,1}) = d'a_{n,0} + (-1)^{n-1}d''a_{n-1,1} + \text{Im}(d''_{n-1,1}) = d'a_{n,0} + \text{Im}(d''_{n-1,1})$. $\square[\mathbf{A.}]$

Suppose now that $H_q(K_{p,\bullet}) = \mathbf{0}$ for all $q \in \mathbb{Z}$ and $p \in \mathbb{N}$.

B. $H_n(\Phi'_\bullet): H_n(K_\bullet) \rightarrow H_n(X'_\bullet)$ is a monomorphism for all $n \in \mathbb{Z}$.

Let $n \in \mathbb{Z}$, and suppose that $x = a + \text{Im}(d_{n+1}) \in \text{Ker}(H_n(\Phi'_\bullet)) \subset H_n(K_\bullet) = \text{Ker}(d_n)/\text{Im}(d_{n+1})$, where $a = (a_{n-i,i})_{i \in \mathbb{Z}} \in \text{Ker}(d_n) \subset K_n$. Then $0 = d_n a = d'a_{n-i,i} + (-1)^{n-i-1}d''a_{n-i-1,i+1}$, and therefore $d'a_{n-i,i} = (-1)^{n-i}d''a_{n-i-1,i+1}$ for all $i \in \mathbb{Z}$. By assumption, $H_n(\Phi'_\bullet)(x) = \Phi'_n(a) + \text{Im}(\delta'_{n+1}) = 0$, which implies that $\Phi'_n(a) = a_{n,0} + \text{Im}(d''_{n,1}) \in \text{Im}(\delta'_{n+1})$, say

$$a_{n,0} + \text{Im}(d''_{n,1}) = \delta'_{n+1}(c_{n+1,0}) + \text{Im}(d''_{n+1,1}) = d'_{n+1,0}(c_{n+1,0}) + \text{Im}(d''_{n,1}) \quad \text{for some } c_{n+1,0} \in K_{n+1,0}.$$

Hence there exists some $c_{n,1} \in K_{n,1}$ such that $a_{n,0} = d'c_{n+1,0} + (-1)^n d''c_{n,1}$.

We shall prove that there exists some $c = (c_{n+1-i,i})_{i \in \mathbb{Z}} \in K_{n+1}$ such that $a = d_{n+1}c \in \text{Im}(d_{n+1})$, that is, $a_{n-i,i} = d'c_{n-i+1,i} + (-1)^{n-i}d''c_{n-i,i+1}$ for all $i \in \mathbb{Z}$. Then it follows that $x = 0$. We proceed recursively to construct the elements $c_{n-i+1,i} \in K_{n-i+1,i}$. For $i < 0$, we set $c_{n+1-i,i} = 0$, and the elements $c_{n+1,0}$ and $c_{n,1}$ as constructed above satisfy the requirement. Thus suppose that $i \geq 0$ and there exist elements $c_{n-i+1,i} \in K_{n-i+1,i}$ and $c_{n-i,i+1} \in K_{n-i,i+1}$ such that

$$a_{n-i,i} = d'c_{n-i+1,i} + (-1)^{n-i}d''c_{n-i,i+1}.$$

Then $d'a_{n-i,i} = (-1)^{n-i}d''d'c_{n-i,i+1} = (-1)^{n-i}d''d'c_{n-i,i+1}$, and since $d'a_{n-i,i} = (-1)^{n-i}d''a_{n-i-1,i+1}$ (as above), it follows that $a_{n-i-1,i+1} - d'c_{n-i,i} \in \text{Ker}(d''_{n-i-1,i+1}) = \text{Im}(d''_{n-i-1,i+2})$, since (by assumption) $H_{i+1}(K_{n-i-1,\bullet}) = \text{Ker}(d''_{n-i-1,i+1})/\text{Im}(d''_{n-i-1,i+2}) = \mathbf{0}$. If $c_{n-i-1,i+2} \in K_{n-i-1,i+2}$ is such that $a_{n-i-1,i+1} - d'c_{n-i,i} = (-1)^{n-i-1}d''c_{n-i-1,i+2}$, then $a_{n-i-1,i+1} = d'c_{n-i,i} + (-1)^{n-i-1}d''c_{n-i-1,i+2}$. $\square[\mathbf{B.}]$

C. $H_n(\Phi'_\bullet): H_n(K_\bullet) \rightarrow H_n(X'_\bullet)$ is an epimorphism for all $n \in \mathbb{Z}$.

Let $n \in \mathbb{Z}$, and suppose that $x \in H_n(X'_\bullet) = \text{Ker}(\delta'_n)/\text{Im}(\delta'_{n+1})$, say $x = b + \text{Im}(\delta'_{n+1})$, where $b = a_{n,0} + \text{Im}(d''_{n,1}) \in \text{Ker}(\delta'_n) \subset X_n = K_{n,0}/\text{Im}(d''_{n,1})$. Then $0 = \delta'_n(b) = d'a_{n,0} + \text{Im}(d''_{n-1,1})$, hence $d'a_{n,0} = (-1)^n d''a_{n-1,1}$ for some $a_{n-1,1} \in K_{n-1,1}$.

We shall prove that there exists some $a = (a_{n-i,i})_{i \in \mathbb{Z}} \in K_n$ such that $d'a_{n-i,i} = (-1)^{n-i}d''a_{n-i-1,i+1}$ for all $i \in \mathbb{Z}$. Then it follows that $a \in \text{Ker}(d_n)$, and

$$\begin{aligned} H_n(\Phi'_\bullet)(a + \text{Im}(d_{n+1})) &= \Phi'_n(a) + \text{Im}(\delta'_{n+1}) = (a_{n,0} + \text{Im}(d''_{n,1})) + \text{Im}(\delta'_{n+1}) \\ &= b + \text{Im}(\delta'_{n+1}) = x \in \text{Im}(H_n(K_\bullet)). \end{aligned}$$

We proceed recursively to construct the elements $a_{n-i,i} \in K_{n-i,i}$. For $i < 0$, we set $a_{n-i,i} = 0$, and the elements $a_{n,0}$ and $a_{n-1,1}$ constructed above satisfy our requirements. Thus suppose that $i \geq 0$ and there exist elements $a_{n-i,i} \in K_{n-i,i}$ and $a_{n-i-1,i+1} \in K_{n-i-1,i+1}$ such that $d'a_{n-i,i} = (-1)^{n-i}d''a_{n-i-1,i+1}$. Then we obtain $d''d'a_{n-i-1,i+1} = d'd''a_{n-i-1,i+1} = (-1)^{n-i}d'd'a_{n-i,i} = 0$, and therefore it follows that $d'a_{n-i-1,i+1} \in \text{Ker}(d''_{n-i-2,i+1}) = \text{Im}(d''_{n-i-2,i+2})$, since (by assumption) $H_{i+1}(K_{n-i-2,\bullet}) = \text{Ker}(d''_{n-i-2,i+1})/\text{Im}(d''_{n-i-2,i+2}) = \mathbf{0}$. Hence there exists some $a_{n-i-2,i+2} \in K_{n-i-2,i+2}$ such that $d'a_{n-i-1,i+1} = (-1)^{n-i-1}d''a_{n-i-2,i+2}$. \square

Proof of Theorem 1.3.4. Let $(P_\bullet, d'_\bullet, \varepsilon)$ be a projective resolution of M , $(Q_\bullet, d''_\bullet, \eta)$ a projective resolution of N , and consider the double complex

$$K_{\bullet\bullet} = (K_{p,q} = P_p \otimes_R Q_q, d'_p \otimes Q_q, P_p \otimes d''_q).$$

For $p \in \mathbb{Z}$, the p -th row complex $K_{p,\bullet} = P_p \otimes_R Q_\bullet$ induces an exact sequence

$$\rightarrow P_p \otimes_R Q_1 \xrightarrow{P_p \otimes d''_1} P_p \otimes Q_0 \xrightarrow{P_p \otimes \eta} P_p \otimes N \rightarrow \mathbf{0}$$

which yields $H_q(K_{p,\bullet}) = \mathbf{0}$ for all $q \in \mathbb{N}$ and $p \in \mathbb{Z}$, $X'_p = H_0(K_{p,\bullet}) = P_p \otimes_R Q_0 / \text{Im}(P_p \otimes d''_1) = P_p \otimes N$, and consequently $H_n(X'_\bullet) = {}''\text{Tor}_n^R(M, N)$ for all $n \in \mathbb{Z}$. Similarly, we obtain $H_n(X''_\bullet) = {}'\text{Tor}_n^R(M, N)$ for all $n \in \mathbb{Z}$, and the Spectral Theorem implies a family of isomorphisms ${}''\text{Tor}_n^R(M, N) \xrightarrow{\sim} {}'\text{Tor}_n^R(M, N)$, by means of which we identify these groups. \square

Theorem 1.3.5.

1. For all $n \in \mathbb{Z}$, $\text{Tor}_n^R: \mathbf{Mod}\text{-}R \times R\text{-}\mathbf{Mod} \rightarrow \mathbf{Ab}$ is an additive functor in both variables, $\text{Tor}_n^R(-, -) = \mathbf{0}$ if $n < 0$, and (up to functorial isomorphisms) $\text{Tor}_n^R(M, N) = \text{Tor}_n^{R^{\text{op}}}(N, M)$ for all $n \in \mathbb{Z}$ and $\text{Tor}_0^R(M, N) = M \otimes_R N$ for all right R -modules M and all R -modules N ,
2. If R is commutative and M, N are R -modules, then for all $n \in \mathbb{Z}$ (up to functorial isomorphisms) $\text{Tor}_n^R(M, N) = \text{Tor}_n^R(M, N)$ are R -modules. They are finitely generated provided that R is noetherian and both M and N are finitely generated.
3. For every short exact sequence $\mathbf{0} \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow \mathbf{0}$ of right R -modules and every R -module N , there is a long exact sequence

$$\begin{aligned} \dots \rightarrow \text{Tor}_2^R(M, N) \rightarrow \text{Tor}_2^R(M'', N) \rightarrow \text{Tor}_1^R(M', N) \rightarrow \text{Tor}_1^R(M, N) \rightarrow \\ \rightarrow \text{Tor}_1^R(M'', N) \rightarrow M' \otimes_R N \rightarrow M \otimes_R N \rightarrow M'' \otimes_R N \rightarrow \mathbf{0} \end{aligned}$$

which is functorial both in N and the original short exact sequence.

4. For every short exact sequence $\mathbf{0} \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow \mathbf{0}$ of R -modules and every right R -module M there is a long exact sequence

$$\begin{aligned} \dots \rightarrow \text{Tor}_2^R(M, N) \rightarrow \text{Tor}_2^R(M, N'') \rightarrow \text{Tor}_1^R(M, N') \rightarrow \text{Tor}_1^R(M, N) \rightarrow \\ \rightarrow \text{Tor}_1^R(M, N'') \rightarrow M \otimes_R N' \rightarrow M \otimes_R N \rightarrow M \otimes_R N'' \rightarrow \mathbf{0} \end{aligned}$$

which is functorial both in M and the original short exact sequence.

PROOF. 1. and 2. follows by tracing through the definitions.

3. Let $\mathbf{0} \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow \mathbf{0}$ be a short exact sequence of right R -modules and (Q_\bullet, η) a projective resolution of N . Then $\mathbf{0} \rightarrow M' \otimes_R Q_\bullet \rightarrow M \otimes_R Q_\bullet \rightarrow M'' \otimes_R Q_\bullet \rightarrow \mathbf{0}$ is an exact sequence of complexes (since the modules Q_n are projective and thus flat for all $n \in \mathbb{Z}$). Now the assertion follows by Theorem 1.3.1.

4. Apply 3. for R^{op} . \square

Theorem 1.3.6. For an R -module E , the following assertions are equivalent:

- (a) E is flat.
- (b) $\text{Tor}_n^R(M, E) = \mathbf{0}$ for every right R -module M and all $n \in \mathbb{N}$.
- (c) $\text{Tor}_1^R(M, E) = \mathbf{0}$ for every right R -module M .
- (d) $\text{Tor}_1^R(R/\mathfrak{a}, E) = \mathbf{0}$ for every right ideal $\mathfrak{a} \subset R$.
- (e) For every short exact sequence of R -modules $\mathbf{0} \rightarrow N' \rightarrow N \rightarrow E \rightarrow \mathbf{0}$ and every right R -module M , the sequence $\mathbf{0} \rightarrow M \otimes_R N' \rightarrow M \otimes_R N \rightarrow M \otimes_R E \rightarrow \mathbf{0}$ is exact.

PROOF. (a) \Rightarrow (b) Let M be a right R -module and (P_\bullet, ε) be a projective resolution of M . Since E is flat, it induces an exact sequence $\rightarrow P_n \otimes_R E \rightarrow P_{n-1} \otimes_R E \rightarrow \dots \rightarrow P_0 \otimes_R E \rightarrow M \otimes_R E \rightarrow \mathbf{0}$, which shows that $\text{Tor}_n^R(M, E) = \mathbf{0}$ for all $n \in \mathbb{N}$.

(b) \Rightarrow (c) \Rightarrow (d) Obvious.

(d) \Rightarrow (a) By Theorem 1.2.7 we must prove: For every finitely generated right ideal, the multiplication homomorphism $\mu_\mathfrak{a}^E: \mathfrak{a} \otimes_R E \rightarrow E$ is a monomorphism. If $j = (\mathfrak{a} \hookrightarrow R)$ denotes the injection, then $\mu_\mathfrak{a}^E = (\mathfrak{a} \otimes_R E \xrightarrow{j \otimes E} R \otimes_R E \xrightarrow{\sim} E)$, and thus it suffices that $j \otimes E$ is a monomorphism. However, the exact sequence $\mathbf{0} \rightarrow \mathfrak{a} \xrightarrow{j} R \rightarrow R/\mathfrak{a} \rightarrow \mathbf{0}$ induces the exact sequence $\mathbf{0} = \text{Tor}_1^R(R/\mathfrak{a}, E) \rightarrow \mathfrak{a} \otimes_R E \xrightarrow{j \otimes E} R \otimes_R E$, and thus $j \otimes E$ is a monomorphism.

(c) \Rightarrow (e) Let $\mathbf{0} \rightarrow N' \rightarrow N \rightarrow E \rightarrow \mathbf{0}$ be an exact sequence of R -modules and M a right R -module. Then we obtain the exact sequence $\mathbf{0} = \text{Tor}_1^R(M, E) \rightarrow M \otimes_R N' \rightarrow M \otimes_R N \rightarrow M \otimes_R E \rightarrow \mathbf{0}$.

(e) \Rightarrow (c) Since every free R -module is projective and thus flat, there exists an exact sequence of R -modules $\mathbf{0} \rightarrow N' \xrightarrow{j} N \rightarrow E \rightarrow \mathbf{0}$, where N is flat. If M is a right R -module, we obtain the exact sequence $\text{Tor}_1^R(M, N) \rightarrow \text{Tor}_1^R(M, E) \rightarrow M \otimes_R N' \xrightarrow{M \otimes f} M \otimes_R N \rightarrow M \otimes_R E \rightarrow \mathbf{0}$. The implication (a) \Rightarrow (c) shows that $\text{Tor}_1^R(M, N) = \mathbf{0}$, and by assumption $M \otimes f$ is a monomorphism. Hence the exact sequence $\mathbf{0} \rightarrow \text{Tor}_1^R(M, E) \rightarrow \text{Ker}(M \otimes f) = \mathbf{0}$ implies $\text{Tor}_1^R(M, E) = \mathbf{0}$ \square

Definitions and Remarks.

1. Let (K_\bullet, d_\bullet) be a complex in $R\text{-Mod}$. For $n \in \mathbb{Z}$, we set

$$K^n = K_{-n} \quad \text{and} \quad d^n = d_{-n}: K^n \rightarrow K^{n+1}.$$

The sequence $K^\bullet = (K^\bullet, d^\bullet) = (d^n: K^n \rightarrow K^{n+1})_{n \in \mathbb{Z}}$ is called a *cochain complex* or *cocomplex* in $R\text{-Mod}$. The groups $H^n(K^\bullet) = H_{-n}(K_\bullet) = \text{Ker}(d^n)/\text{Im}(d^{n-1})$ are called the *cohomology groups* of K^\bullet . For a complex morphism $f_\bullet: K_\bullet \rightarrow K'_\bullet$, we set $f^\bullet = (f^n: K^n \rightarrow K'^n)_{n \in \mathbb{Z}}$, where $f^n = f_{-n}$, and $H^n(f^\bullet) = H_{-n}(f_\bullet)$ for all $n \in \mathbb{Z}$. With these definitions, the cocomplexes in $R\text{-Mod}$ form a category \mathbf{C}^R , and $(H^n: \mathbf{C}^R \rightarrow \mathbf{Ab})_{n \in \mathbb{Z}}$ is a sequence of additive functors. A cocomplex K^\bullet is called *positive* if $K^n = \mathbf{0}$ for all $n < 0$.

2. For every exact sequence $\mathbf{0} \rightarrow K'^\bullet \xrightarrow{f^\bullet} K^\bullet \xrightarrow{g^\bullet} K''^\bullet \rightarrow \mathbf{0}$ in \mathbf{C}^R there exists a family of homomorphisms $(\omega^n: H^n(K''^\bullet) \rightarrow H^{n+1}(K'^\bullet))_{n \in \mathbb{Z}}$ such that the long cohomology sequence

$$\dots \xrightarrow{\omega^{n-1}} H^n(K'^\bullet) \xrightarrow{H^n(f^\bullet)} H^n(K^\bullet) \xrightarrow{H^n(g^\bullet)} H^n(K''^\bullet) \xrightarrow{\omega^n} H^{n+1}(K'^\bullet) \rightarrow \dots$$

is exact and functorial in the short exact sequence.

3. Let M be an R -module. An *injective resolution* $(I^\bullet, d^\bullet, \nu)$ of M is a positive cocomplex I^\bullet of injective modules such that $H^n(I^\bullet) = \mathbf{0}$ for all $n \neq 0$, together with a monomorphism $\nu: M \rightarrow I^0$ such that $\text{Im}(\nu) = \text{Ker}(d^0)$. Equivalently, an injective resolution of M is an exact sequence $\mathbf{0} \rightarrow M \xrightarrow{\nu} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \rightarrow \dots$ and induces an isomorphism $\nu^0: M \xrightarrow{\sim} H^0(I^\bullet) = \text{Ker}(d^0)$.
4. Let $\varphi: M \rightarrow M'$ be an R -homomorphism, (I^\bullet, ν) an injective resolution of M and (I'^\bullet, ν') an injective resolution of M' . Then there exists up to homotopy a unique morphism $f^\bullet: I^\bullet \rightarrow I'^\bullet$ such that $\nu' \circ \varphi = f^0 \circ \nu: M \rightarrow I'^0$.
5. Every R -module M has an injective resolution. If (I^\bullet, ν) and (I'^\bullet, ν') are injective resolutions of M , then there exists a homotopy equivalence $f^\bullet: I^\bullet \rightarrow I'^\bullet$ such that $f^0 \circ \nu = \nu': M \rightarrow I'^0$.

Definition. We fix for every R -module a projective and an injective resolution. Let M and N be R -modules.

a. Let $(I^\bullet, d^\bullet, \nu)$ be an injective resolution of N , say $\mathbf{0} \rightarrow N \xrightarrow{\nu} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} \dots$. Then $(\text{Hom}_R(M, I^\bullet), d_*^\bullet)$ (where $d_*^\bullet: \text{Hom}_R(M, I^n) \rightarrow \text{Hom}_R(M, I^{n+1})$ is the homomorphism induced by d^n) is a cocomplex, and we define

$${}^R\text{Ext}_R^n(M, N) = H^n(\text{Hom}_R(M, I^\bullet)) \quad \text{for all } n \in \mathbb{Z}.$$

If $f: M \rightarrow M'$ is a homomorphism of R -modules, then $\text{Hom}(f, I^\bullet): \text{Hom}_R(M', I^\bullet) \rightarrow \text{Hom}_R(M, I^\bullet)$ is a cocomplex homomorphism, and we define

$${}^R\text{Ext}_R^n(f, N) = H^n(\text{Hom}(f, I^\bullet)): {}^R\text{Ext}_R^n(M', N) \rightarrow {}^R\text{Ext}_R^n(M, N) \quad \text{for all } n \in \mathbb{Z}.$$

These settings define a sequence of (contravariant) additive functors $({}^R\text{Ext}_R^n(-, N): \mathbf{Mod}\text{-}R^{\text{op}} \rightarrow \mathbf{Ab})_{n \in \mathbb{Z}}$, called the *Ext functors* in the first variable. By definition, ${}^R\text{Ext}_R^n(-, N) = \mathbf{0}$ for $n < 0$, and the exact sequence $\mathbf{0} \rightarrow \text{Hom}_R(M, N) \xrightarrow{\nu_*} \text{Hom}_R(M, I^0) \xrightarrow{d_*^0} \text{Hom}_R(M, I^1)$ induces an isomorphism

$${}^R\text{Ext}_R^0(M, N) = H^0(\text{Hom}_R(M, I^\bullet) = \text{Ker}(d_*^0) = \text{Im}(\nu_*) \xrightarrow{\sim} \text{Hom}_R(M, N),$$

which is functorial in M , and we identify ${}^{\prime}\text{Ext}_R^0(-, N) = \text{Hom}_R(-, N)$ by means of this isomorphism.

b. Let $(P_{\bullet}, d_{\bullet}, \varepsilon)$ be a projective resolution of M , say $\dots \rightarrow P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \rightarrow \mathbf{0}$. For $n \in \mathbb{Z}$, we set $\text{Hom}_R(P, N)^n = \text{Hom}_R(P_n, N)$ and $d^n = (d_{n+1})^*: \text{Hom}_R(P_n, N) \rightarrow \text{Hom}_R(P_{n+1}, N)$. Then $(\text{Hom}_R(P, N)^{\bullet}, d^{\bullet})$ is a cocomplex, and we define

$${}^{\prime\prime}\text{Ext}_R^n(M, N) = H^n(\text{Hom}_R(P, N)^{\bullet}).$$

If $f: N \rightarrow N'$ is a homomorphism of R -modules, then $(\text{Hom}(P_q, f))_{q \in \mathbb{Z}}$ defines a cocomplex homomorphism $\text{Hom}(P, f)^{\bullet}: \text{Hom}_R(P, N)^{\bullet} \rightarrow \text{Hom}_R(P, N')^{\bullet}$, and we define

$${}^{\prime\prime}\text{Ext}_R^n(M, f) = H^n(\text{Hom}(P, f)^{\bullet}): {}^{\prime\prime}\text{Ext}_R^n(M, N) \rightarrow {}^{\prime\prime}\text{Ext}_R^n(M, N') \quad \text{for all } n \in \mathbb{Z}.$$

These settings define a sequence of additive functors $({}^{\prime\prime}\text{Ext}_R^n(M, -): \mathbf{Mod}\text{-}R \rightarrow \mathbf{Ab})_{n \in \mathbb{Z}}$, called the *Ext functors* in the second variable. By definition, ${}^{\prime\prime}\text{Ext}_R^n(M, -) = \mathbf{0}$ for $n < 0$, and the exact sequence $\mathbf{0} \rightarrow \text{Hom}_R(M, N) \xrightarrow{\varepsilon^*} \text{Hom}_R(M, P_0) \xrightarrow{d_1^*} \text{Hom}_R(M, P^1)$ induces an isomorphism

$${}^{\prime\prime}\text{Ext}_R^0(M, N) = H^0(\text{Hom}_R(P, N)^{\bullet} = \text{Ker}(d^0) = \text{Ker}(d_*^1) \xrightarrow{\sim} \text{Hom}_R(M, N),$$

which is functorial in N , and we identify ${}^{\prime\prime}\text{Ext}_R^0(M, -) = \text{Hom}_R(M, -)$ by means of this isomorphism.

Theorem and Definition 1.3.7. *Let M and N be R -modules. Up to functorial isomorphisms, we have ${}^{\prime}\text{Ext}_R^n(M, N) = {}^{\prime\prime}\text{Ext}_R^n(M, N)$ for all $n \in \mathbb{Z}$.*

We define $\text{Ext} = \text{Ext}' = \text{Ext}''$.

PROOF. (Sketch) Take a projective resolution $(P_{\bullet}, \varepsilon)$ of M , an injective resolution (I^{\bullet}, ν) of N and apply the Spectral Theorem to the double cocomplex built by the groups $\text{Hom}_R(P_p, I^q)$. \square

Theorem 1.3.8.

1. For all $n \in \mathbb{Z}$, $\text{Ext}_R^n: R\text{-Mod}^{\text{op}} \times R\text{-Mod} \rightarrow \mathbf{Ab}$ is an additive functor in both variables, $\text{Ext}_R^n(-, -) = \mathbf{0}$ if $n < 0$, and (up to functorial isomorphisms) $\text{Ext}_R^0(M, N) = \text{Hom}_R(M, N)$ for all R -modules M and N .
2. If R is commutative and M, N are R -modules, then the groups $\text{Ext}_R^n(M, N)$ are R -modules, and they are finitely generated provided that R is noetherian and both M and N are finitely generated.
3. For every short exact sequence $\mathbf{0} \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow \mathbf{0}$ of R -modules and every R -module N there is a long exact sequence

$$\begin{aligned} \mathbf{0} \rightarrow \text{Hom}_R(M'', N) \rightarrow \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M', N) \rightarrow \text{Ext}_R^1(M'', N) \rightarrow \text{Ext}_R^1(M, N) \rightarrow \\ \rightarrow \text{Ext}_R^1(M', N) \rightarrow \text{Ext}_R^2(M'', N) \rightarrow \text{Ext}_R^2(M, N) \rightarrow \dots \end{aligned}$$

which is functorial both in N and the original short exact sequence.

4. For every short exact sequence $\mathbf{0} \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow \mathbf{0}$ of R -modules and every R -module M there is a long exact sequence

$$\begin{aligned} \mathbf{0} \rightarrow \text{Hom}_R(M, N') \rightarrow \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M, N'') \rightarrow \text{Ext}_R^1(M, N') \rightarrow \text{Ext}_R^1(M, N) \rightarrow \\ \rightarrow \text{Ext}_R^1(M, N'') \rightarrow \text{Ext}_R^2(M, N') \rightarrow \text{Ext}_R^2(M, N) \rightarrow \dots \end{aligned}$$

which is functorial both in M and the original short exact sequence.

PROOF. 1. and 2. follows by tracing through the definitions.

3. Let $\mathbf{0} \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow \mathbf{0}$ be a short exact sequence of R -modules and N an R -module. Let (I^{\bullet}, ν) be an injective resolution of N . Then $\mathbf{0} \rightarrow \text{Hom}_R(M'', I^{\bullet}) \rightarrow \text{Hom}_R(M, I^{\bullet}) \rightarrow \text{Hom}_R(M', I^{\bullet}) \rightarrow \mathbf{0}$ is an exact sequence of cocomplexes, and the assertion follows from the long cohomology sequence.

4. Let $\mathbf{0} \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow \mathbf{0}$ be a short exact sequence of R -modules and M an R -module. Let $(P_{\bullet}, \varepsilon)$ be a projective resolution of M , and observe that $\text{Hom}_R(P, -)^{\bullet} = \text{Hom}_R(P_{\bullet}, -)$. Then $\mathbf{0} \rightarrow \text{Hom}_R(P, N')^{\bullet} \rightarrow \text{Hom}_R(P, N)^{\bullet} \rightarrow \text{Hom}_R(P, N'')^{\bullet}$ is an exact sequence of cocomplexes, and the assertion follows from the long cohomology sequence. \square

Theorem 1.3.9.

1. For an R -module P , the following assertions are equivalent:
 - (a) P is projective.
 - (b) $\text{Ext}_R^n(P, N) = \mathbf{0}$ for all R -modules N and all $n \in \mathbb{N}$.
 - (c) $\text{Ext}_R^1(P, N) = \mathbf{0}$ for all R -modules N .
2. For an R -module Q , the following assertions are equivalent:
 - (a) Q is injective.
 - (b) $\text{Ext}_R^n(M, Q) = \mathbf{0}$ for all R -modules M and all $n \in \mathbb{N}$.
 - (c) $\text{Ext}_R^1(M, Q) = \mathbf{0}$ for all R -modules M .

PROOF. 1. (a) \Rightarrow (b) $\dots \rightarrow \mathbf{0} \rightarrow \mathbf{0} \xrightarrow{d_1} P \xrightarrow{\text{id}_P} P \rightarrow \mathbf{0}$ is a projective resolution of P . If N is an R -module, then the exact sequence $\dots \rightarrow \mathbf{0} = \text{Hom}_R(\mathbf{0}, N) \xrightarrow{d_1^*} \text{Hom}_R(P, N) \xrightarrow{\text{id}_P^*} \text{Hom}_R(P, N) \rightarrow \mathbf{0}$ shows that $\text{Ext}_R^n(P, N) = \mathbf{0}$ for all $n \in \mathbb{N}$.

(b) \Rightarrow (c) Obvious.

(c) \Rightarrow (a) We must prove that every R -epimorphism $M \rightarrow P$ splits. Thus let $g: M \rightarrow P$ be an R -epimorphism and $M' = \text{Ker}(g)$. The exact sequence $\mathbf{0} \rightarrow M' \hookrightarrow M \xrightarrow{g} P \rightarrow \mathbf{0}$ yields the exact sequence $\dots \rightarrow \text{Hom}_R(P, M) \xrightarrow{g_*} \text{Hom}_R(P, P) \rightarrow \text{Ext}_R^1(P, M') = \mathbf{0}$. Hence there exists some $\psi \in \text{Hom}_R(P, M)$ such that $g_*(\psi) = g \circ \psi = \text{id}_P$. Hence g splits.

2. (a) \Rightarrow (b) $\mathbf{0} \rightarrow Q \xrightarrow{\text{id}_Q} Q \xrightarrow{d^0} \mathbf{0} \xrightarrow{d^1} \mathbf{0} \rightarrow \dots$ is an injective resolution of P . If N is an R -module, then the exact sequence $\mathbf{0} \rightarrow \text{Hom}_R(N, Q) \xrightarrow{\text{id}_Q^*} \text{Hom}_R(N, Q) \rightarrow \mathbf{0} \rightarrow \mathbf{0} \rightarrow \dots$ shows that $\text{Ext}_R^n(P, N) = \mathbf{0}$ for all $n \in \mathbb{N}$.

(b) \Rightarrow (c) Obvious.

(c) \Rightarrow (a) We must prove that every R -monomorphism $Q \rightarrow M$ splits. Thus let $f: Q \rightarrow M$ be an R -monomorphism and $M'' = \text{Coker}(f)$. The exact sequence $\mathbf{0} \rightarrow Q \xrightarrow{f} M \rightarrow M'' \rightarrow \mathbf{0}$ yields the exact sequence $\dots \rightarrow \text{Hom}_R(M, Q) \xrightarrow{f^*} \text{Hom}_R(Q, Q) \rightarrow \text{Ext}_R^1(M'', Q) = \mathbf{0}$. Hence there exists some $\varphi \in \text{Hom}_R(M, Q)$ such that $f^*(\varphi) = \varphi \circ f = \text{id}_Q$. Hence f splits. \square

Remarks. Let $T: R\text{-Mod} \rightarrow \mathbf{Ab}$ be an additive exact functor.

1. Let $M' \subset M$ be an R -submodule, and consider the exact sequence $\mathbf{0} \rightarrow M' \xrightarrow{j} M \xrightarrow{\pi} M/M' \rightarrow \mathbf{0}$, where $j = (M' \hookrightarrow M)$ is the embedding and $\pi: M \rightarrow M/M'$ is the residue class homomorphism. Then the sequence $\mathbf{0} \rightarrow TM' \xrightarrow{Tj} TM \xrightarrow{T\pi} T(M/M') \rightarrow \mathbf{0}$ is exact and induces isomorphisms $Tj: TM' \xrightarrow{\sim} \text{Im}(Tj) \subset TM$ and $(T\pi)^*: TM/\text{Im}(Tj) \xrightarrow{\sim} T(M/M')$. We may identify the modules by means of these isomorphisms and obtain $TM' \subset TM$ and $T(M/M') = TM/IM'$.
2. Let $f: M \rightarrow M'$ be a homomorphism of R -modules. Then the exact sequences

$$\mathbf{0} \rightarrow \text{Ker}(f) \hookrightarrow M \xrightarrow{f} M' \quad \text{and} \quad M \xrightarrow{f} M' \rightarrow M'/\text{Im}(f) \rightarrow \mathbf{0}$$

induce the exact sequences

$$\mathbf{0} \rightarrow T(\text{Ker}(f)) \rightarrow TM \xrightarrow{Tf} TM' \quad \text{and} \quad TM \xrightarrow{Tf} TM' \rightarrow T(M'/\text{Im}(f)) \rightarrow \mathbf{0}.$$

Due to the identifications made above, we obtain $\text{Ker}(Tf) = T(\text{Ker}(f))$ and

$$TM'/T(\text{Im}(f)) = T(M'/\text{Im}(f)) = TM'/\text{Im}(Tf), \quad \text{and therefore} \quad T(\text{Im}(f)) = \text{Im}(Tf).$$

Conversely, if T is any additive functor preserving kernels and images, then T is exact.

3. Let K^\bullet be a complex in $R\text{-Mod}$. Then TK^\bullet is a complex, and, due to the above identifications, $H_n(TK^\bullet) = TH_n(K^\bullet)$ for all $n \in \mathbb{Z}$.

Exercise 1. Let $R \rightarrow A$ be a flat commutative R -algebra, and let M, N be R -modules.

1. For every $n \in \mathbb{Z}$, There is an A -isomorphism $A \otimes_R \operatorname{Tor}_n^R(M, N) \xrightarrow{\sim} \operatorname{Tor}_n^A(A \otimes_R M, A \otimes_R N)$, functorial in both M and N .
2. Let M be finitely presented [that means, there is an exact sequence $F' \rightarrow F \rightarrow M \rightarrow \mathbf{0}$ with finitely generated free R -modules. Then the A -homomorphism

$$\Phi: A \otimes_R \operatorname{Hom}_R(M, N) \rightarrow \operatorname{Hom}_A(A \otimes_R M, A \otimes_R N)$$

introduced in Theorem 1.2.6 is an isomorphism.

3. Let R be noetherian, M finitely generated and $n \in \mathbb{Z}$. Then there is an A -isomorphism $A \otimes_R \operatorname{Ext}_R^n(M, N) \xrightarrow{\sim} \operatorname{Ext}_A^n(A \otimes_R M, A \otimes_R N)$, functorial in both M and N .

Ring Theory

2.1. Local rings, Quotients, Localization, Prime and primary ideals

Theorem and Definition 2.1.1. *Let $R \neq \mathbf{0}$ be a ring.*

A subset $T \subset R$ is called multiplicatively closed if $1 \in T$ and $TT \subset T$ [then $TT = T$]. A subset $\mathfrak{a} \subset R$ is called a *maximal left ideal* [*maximal right ideal*, *maximal ideal*] if it is maximal among those distinct from R .

1. *Let $T \subset R$ be a multiplicatively closed subset, $\mathfrak{a} \subset R$ a left ideal [a right ideal, an ideal] such that $\mathfrak{a} \cap T = \emptyset$, and let Ω be the set of all left ideals [right ideals, ideals] $\mathfrak{c} \subset R$ such that $\mathfrak{a} \subset \mathfrak{c}$ and $\mathfrak{c} \cap T = \emptyset$. Then Ω contains maximal elements, and if R is commutative, then every maximal element of Ω is a prime ideal.*

In particular ($T = \{1\}$): If $R \neq \mathbf{0}$, then R contains maximal left ideals, maximal right ideals and maximal ideals.

2. *For a subset $J \subset R$, the following assertions are equivalent:*

- (a) *J is the intersection of all maximal left ideals of R .*
- (b) *J is the intersection of all maximal right ideals of R .*
- (c) *J is the greatest left ideal [right ideal, ideal] of R such that $1 + J \subset R^\times$.*

*If J satisfies these conditions, then $J = J(R)$ is an ideal of R . It is called the *Jacobson radical* of R .*

3. *The following assertions are equivalent:*

- (a) *$R \setminus R^\times \triangleleft R$.*
- (b) *$J(R) = R \setminus R^\times$.*
- (c) *R has a greatest left ideal [right ideal] (namely $J(R)$).*
- (d) *$R/J(R)$ is a division ring.*

*If these conditions are fulfilled, then the ring R is called *local*. Every division ring is local.*

In particular, let R be commutative. Then R is local if and only if R has a unique maximal ideal \mathfrak{m} , and then $\mathfrak{m} = J(R) = R \setminus R^\times$.

4. *An element $u \in R$ is called *nilpotent* if $u^n = 0$ for some $n \in \mathbb{N}$. If every $u \in R \setminus R^\times$ is nilpotent, then R is local.*

PROOF. 1. $\mathfrak{a} \in \Omega$, and the union of every chain in Ω belongs to Ω . By Zorn's Lemma, Ω has a maximal element.

If R is commutative and $\mathfrak{p} \in \Omega$ is a maximal element, then \mathfrak{p} is a prime ideal. Indeed, if $a, b \in R \setminus \mathfrak{p}$, then $(\mathfrak{p} + aR) \cap T \neq \emptyset$ and $(\mathfrak{p} + bR) \cap T \neq \emptyset$. Hence there exist elements $p, q \in \mathfrak{p}$ and $u, v \in R$ such that $p + au \in T$ and $q + bv \in T$. But then $y = (p + au)(q + bv) \in T$, and as $y \equiv abuv \pmod{\mathfrak{p}}$, it follows that $ab \notin \mathfrak{p}$.

2. Let \mathcal{L} be the set of all maximal left ideals of R , and

$$J = \bigcap_{\mathfrak{m} \in \mathcal{L}} \mathfrak{m}.$$

We shall prove the following three assertions:

- A.** $J \triangleleft R$.
B. $1 + J \subset R^\times$.
C. If $\mathfrak{a} \subset R$ is a left ideal such that $1 + \mathfrak{a} \subset R^\times$, then $\mathfrak{a} \subset J$.

Suppose that **A**, **B** and **C** hold. Then J is the greatest left ideal (and thus also the greatest ideal) such that $1 + J \subset R^\times$. Hence a) \Leftrightarrow c). b) \Leftrightarrow c) is proved in the same way.

Proof of A. For $\mathfrak{m} \in \mathfrak{L}$, let $\mathfrak{m}^* = \text{Ann}_R(R/\mathfrak{m}) = \{x \in R \mid xR \subset \mathfrak{m}\}$. Then $\mathfrak{m}^* \triangleleft R$, $\mathfrak{m}^* \subset \mathfrak{m}$, and we set

$$J^* = \bigcap_{\mathfrak{m} \in \mathfrak{L}} \mathfrak{m}^*.$$

Then $J^* \triangleleft R$, $J^* \subset J$, and we assert that $J^* = J$ (then **A** holds).

Assume to the contrary that $x \in J \setminus J^*$. Then there exist some $\mathfrak{m} \in \mathfrak{L}$ and $u \in R$ such that $xu \notin \mathfrak{m}$, and consequently $Rxu \not\subset \mathfrak{m}$. Hence $\mathfrak{m} + Rxu = R$, and there exist elements $y \in R$ and $m \in \mathfrak{m}$ such that $m + yxu = u$, and thus $(1 - yx)u = m \in \mathfrak{m}$.

CASE 1: $R(1 - yx) = R$. Let $v \in R$ be such that $v(1 - yx) = 1$. Then $u = v(1 - yx)u = vm \in \mathfrak{m}$, and thus $xu \in \mathfrak{m}$, a contradiction.

CASE 2: $R(1 - yx) \subsetneq R$. Then there exists some $\mathfrak{n} \in \mathfrak{L}$ such that $R(1 - yx) \subset \mathfrak{n}$, hence $1 - yx \in \mathfrak{n} \subset J$, and as $x \in J$, this implies that $1 \in J$, a contradiction.

Proof of B. Let $y \in J$. We assert that $R(1 - yx) = R$ for all $x \in R$. Indeed, assume that there is some $x \in R$ such that $R(1 - yx) \subsetneq R$, and let $\mathfrak{n} \in \mathfrak{L}$ be such that $R(1 - yx) \subset \mathfrak{n}$. Then $1 - yx \in \mathfrak{n} \subset J$, and as $y \in J$, we obtain $1 \in J$, a contradiction.

In particular, $R(1 + y) = R$, and there exists some $u \in R$ such that $u(1 + y) = 1$. Since $u = 1 - uy$, we obtain also $Ru = R$, and there is some $v \in R$ such that $vu = 1$. As u has both a left and a right inverse, it follows that $u \in R^\times$ and thus $1 + y = u^{-1} \in R^\times$.

Proof of C. Let $\mathfrak{a} \subset R$ be a left ideal such that $1 + \mathfrak{a} \subset R^\times$. We must prove that $\mathfrak{a} \subset \mathfrak{m}$ for all $\mathfrak{m} \in \mathfrak{L}$. Suppose at the contrary that there is some $\mathfrak{m} \in \mathfrak{L}$ such that $\mathfrak{a} \not\subset \mathfrak{m}$. Then $\mathfrak{a} + \mathfrak{m} = R$, hence $a + m = 1$ for some $a \in \mathfrak{a}$ and $m \in \mathfrak{m}$. But then $m = 1 - a \in 1 + \mathfrak{a} \subset R^\times$, a contraction.

3. (a) \Rightarrow (b) \Rightarrow (c) If $R \setminus R^\times$ is an ideal, then it is the greatest (and thus the only maximal) left ideal [right ideal] of R , and $J(R) = R \setminus R^\times$.

(c) \Rightarrow (d) We must prove that $(R/J(R))^\bullet$ is a group, that is, every $\xi \in (R/J(R))^\bullet$ has a left-inverse. Let $\xi = x + J(R) \in (R/J(R))^\bullet$, where $x \in R \setminus J(R)$. Then $J(R) + Rx = R$, and there exist $y \in J(R)$ and $u \in R$ such that $y + ux = 1$. If $\eta = u + J(R)$, then $\eta\xi = 1 \in R/J(R)$.

(d) \Rightarrow (b) It suffices to prove that $R \setminus J(R) \subset R^\times$. Indeed, once this is done, then $R \setminus J(R) = R^\times$, and $R \setminus R^\times = J(R) \triangleleft R$. If $a \in R \setminus J(R)$, then $a + J(R) \in (R/J(R))^\times$, and thus there is some $u \in R$ such that $au \in 1 + J(R) \subset R^\times$, and thus $a \in R^\times$.

4. It suffices to prove that $R \setminus R^\times \subset J(R)$ (then $R \setminus R^\times = J(R)$). Let $u \in R \setminus R^\times$ and $n \in \mathbb{N}$ minimal such that $u^n = 0$. We shall prove that $1 + Ru \subset R^\times$, for then $u \in Ru \subset J(R)$. If $a \in R$, then $y = -au \notin R^\times$ for otherwise $yu^{n-1} = -au^n = 0$ implies $u^{n-1} = 0$, a contradiction. Hence $y^k = 0$ for some $k \in \mathbb{N}$, and $1 = 1 - y^k = (1 - y)(1 + y + \dots + y^{k-1}) = (1 + y + \dots + y^{k-1})(1 - y)$ implies $1 - y = 1 + au \in R^\times$ \square

Example (Origin of the terminology "local"). Let X be a topological space, $x_0 \in X$, $\mathcal{U} = \mathcal{U}(x_0)$ the system of neighborhoods of x_0 in X and Ω the set of all pairs (U, f) , where $U \in \mathcal{U}$ and $f: U \rightarrow \mathbb{R}$ is a continuous function. For $(U_1, f_1), (U_2, f_2) \in \Omega$, we define $(U_1, f_1) \sim (U_2, f_2)$ if there exists some $U \in \mathcal{U}$ such that $U \subset U_1 \cap U_2$ and $f_1|_U = f_2|_U$. Then \sim is an equivalence relation on Ω , and if $(U, f) \in \Omega$, then the equivalence class $[U, f]$ of (U, f) is called the *germ* of f in x_0 . The set $\mathcal{O} = \mathcal{O}_{X, x_0} = \Omega / \sim$ of all germs of continuous functions in x_0 is made into a ring by means of $[U_1, f_1] \dot{+} [U_2, f_2] = [U_0, f_0]$ if $f_1|_U \dot{+} f_2|_U = f_0|_U$ for some $U \in \mathcal{U}$ such that $U \subset U_0 \cap U_1 \cap U_2$. The map

$$\varepsilon: \mathcal{O} \rightarrow \mathbb{R}, \quad \text{defined by } \varepsilon([U, f]) = f(x_0),$$

is a ring epimorphism, and $\mathcal{O} \setminus \text{Ker}(\varepsilon) = \{[U, f] \in \mathcal{O} \mid f(x_0) \neq 0\} = \mathcal{O}^\times$ [indeed, if $[U, f] \in \mathcal{O}$ and $f(x_0) \neq 0$, then there is some $U_0 \in \mathcal{U}$ such that $U_0 \subset U$ and $f(x) \neq 0$ for all $x \in U_0$, which implies $[U, f] \cdot [U_0, 1/f] = 1_{\mathcal{O}}$]. Hence $\text{Ker}(\varepsilon) = \mathcal{O} \setminus \mathcal{O}^\times \triangleleft \mathcal{O}$, and thus \mathcal{O} is local.

Theorem 2.1.2 (Nakayama's Lemma). *Let $R \neq \mathbf{0}$ be a ring, M an R -module and $\mathfrak{a} \subset \text{J}(R)$ and ideal of R .*

1. *Let $M' \subset M$ be an R -submodule such that M/M' is finitely generated. If $M = M' + \mathfrak{a}M$, then $M = M'$. In particular ($M' = \mathbf{0}$): If M is finitely generated and $M = \mathfrak{a}M$, then $M = \mathbf{0}$.*
2. *Let M be finitely generated, $n \in \mathbb{N}$ and $u_1, \dots, u_n \in M$.*
 - (a) *$M = {}_R\langle u_1, \dots, u_n \rangle$ if and only if $M/\mathfrak{a}M = {}_{R/\mathfrak{a}}\langle u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M \rangle$.*
 - (b) *Suppose that M is finitely presented and $u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M$ is an R/\mathfrak{a} -basis of $M/\mathfrak{a}M$. If the multiplication homomorphism $\mu_{\mathfrak{a}}: \mathfrak{a} \otimes_R M \rightarrow M$ is a monomorphism, then (u_1, \dots, u_n) is an R -basis of M .*

PROOF. 1. Assume first that $M' = \mathbf{0}$, and let (u_1, \dots, u_n) be a minimal system of generators of M . We assert that $\mathfrak{a}M = \{a_1u_1 + \dots + a_nu_n \mid a_1, \dots, a_n \in \mathfrak{a}\}$.

Indeed, \supset follows by the very definition. Conversely, if $x \in \mathfrak{a}M$, then $x = c_1m_1 + \dots + c_km_k$, where $k \in \mathbb{N}$, $c_1, \dots, c_k \in \mathfrak{a}$ and $m_1, \dots, m_k \in M$. For $j \in [1, k]$, there exist $b_{j,1}, \dots, b_{j,n} \in R$ such that

$$m_j = \sum_{\nu=1}^n b_{j,\nu}u_\nu, \quad \text{and then} \quad x = \sum_{\nu=1}^n a_\nu u_\nu, \quad \text{where} \quad a_\nu = \sum_{i=1}^k c_i b_{i,\nu} \in \mathfrak{a} \quad \text{for all } \nu \in [1, n].$$

In particular, $M = \mathfrak{a}M$ implies $u_1 = a_1u_1 + \dots + a_nu_n$ for some $a_1, \dots, a_n \in \mathfrak{a}$. Hence it follows that $(1 - a_1)u_1 = a_2u_2 + \dots + a_nu_n$, and since $1 - a_1 \in 1 + \mathfrak{a} \subset R^\times$, we obtain $u_1 \in {}_R\langle u_2, \dots, u_n \rangle$ and $M = {}_R\langle u_2, \dots, u_n \rangle$, which contradicts the assumption that (u_1, \dots, u_n) is a minimal system of generators.

2. (a) If $M = {}_R\langle u_1, \dots, u_n \rangle$, then $M/\mathfrak{a}M = {}_R\langle u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M \rangle = {}_{R/\mathfrak{a}}\langle u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M \rangle$. Conversely, assume that $M/\mathfrak{a}M = {}_{R/\mathfrak{a}}\langle u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M \rangle = {}_R\langle u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M \rangle$, and set $M' = {}_R\langle u_1, \dots, u_n \rangle$. Then $(M' + \mathfrak{a}M)/\mathfrak{a}M = {}_R\langle u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M \rangle = M/\mathfrak{a}M$, hence $M' + \mathfrak{a}M = M$, and thus $M' = M$ by 1.

(b) By assumption, $M/\mathfrak{a}M = {}_{R/\mathfrak{a}}\langle u_1 + \mathfrak{a}M, \dots, u_n + \mathfrak{a}M \rangle$, and thus $M = {}_R\langle u_1, \dots, u_n \rangle$ by (a). Let F be a free R -module with basis (e_1, \dots, e_n) , let $p: F \rightarrow M$ be the unique epimorphism satisfying $p(e_i) = u_i$ for all $i \in [1, n]$, $K = \text{Ker}(p)$ and $j = (K \hookrightarrow F)$. We shall prove that $K = \mathbf{0}$ (then p is an isomorphism and M is free). $F/\mathfrak{a}F$ is a free R/\mathfrak{a} -module with basis $(e_1 + \mathfrak{a}F, \dots, e_n + \mathfrak{a}F)$, and therefore p induces an isomorphism $p^*: F/\mathfrak{a}F \rightarrow M/\mathfrak{a}M$ satisfying $p^*(e_i + \mathfrak{a}F) = u_i + \mathfrak{a}M$ for all $i \in [1, n]$. We obtain the following commutative diagram with exact rows.

$$\begin{array}{ccccccc} \mathfrak{a} \otimes_R K & \xrightarrow{\mathfrak{a} \otimes j} & \mathfrak{a} \otimes_R F & \xrightarrow{\mathfrak{a} \otimes p} & \mathfrak{a} \otimes_R M & \longrightarrow & \mathbf{0} \\ \mu_{\mathfrak{a}}^K \downarrow & & \mu_{\mathfrak{a}}^F \downarrow & & \mu_{\mathfrak{a}}^M \downarrow & & \\ \mathbf{0} & \longrightarrow & K & \xrightarrow{j} & F & \xrightarrow{p} & M & \longrightarrow & \mathbf{0}. \end{array}$$

By the Snake Lemma, we obtain an exact sequence

$$\mathbf{0} = \text{Ker}(\mu_{\mathfrak{a}}^M) \rightarrow \text{Coker}(\mu_{\mathfrak{a}}^K) = K/\mathfrak{a}K \xrightarrow{j^*} \text{Coker}(\mu_{\mathfrak{a}}^F) = F/\mathfrak{a}F \xrightarrow{p^*} \text{Coker}(\mu_{\mathfrak{a}}^M) = M/\mathfrak{a}M \rightarrow \mathbf{0},$$

and as p^* is an isomorphism, this implies $K/\mathfrak{a}K = \mathbf{0}$ and thus $K = \mathfrak{a}K$. Since M is finitely presented, the Corollary to Theorem 1.1.4 implies that K is finitely generated, and therefore $K = \mathbf{0}$. \square

Corollary. *Let R be a local ring, $\mathfrak{m} = \text{J}(R) = R \setminus R^\times$ and M an R -module.*

1. *Let M be finitely generated, $n \in \mathbb{N}$ and $u_1, \dots, u_n \in M$. Then (u_1, \dots, u_n) is a minimal system of generators of M if and only if $(u_1 + \mathfrak{m}M, \dots, u_n + \mathfrak{m}M)$ is an R/\mathfrak{m} -basis of $M/\mathfrak{m}M$. In particular, any two minimal systems of generators of M have the same length.*

2. Let M be finitely presented, $u_1, \dots, u_n \in M$, and assume that the multiplication homomorphism $\mu_{\mathfrak{m}}^M: \mathfrak{m} \otimes_R M \xrightarrow{\sim} \mathfrak{m}M$ is an isomorphism. Then (u_1, \dots, u_n) is an R -basis of M if and only if $(u_1 + \mathfrak{m}M, \dots, u_n + \mathfrak{m}M)$ is an R/\mathfrak{m} -basis of $M/\mathfrak{m}M$.
3. Consider the following assertions:
 - (a) M is free.
 - (b) M is projective.
 - (c) M is flat.
 - (d) The multiplication homomorphism $\mu_{\mathfrak{m}}^M: \mathfrak{m} \otimes_R M \rightarrow M$ is a monomorphism.
 Then (a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d), and if M is finitely presented, then (d) \Rightarrow (a).

PROOF. 1. By Theorem 2.1.2, (u_1, \dots, u_n) is a minimal system of generators of M if and only if $(u_1 + \mathfrak{m}M, \dots, u_n + \mathfrak{m}M)$ is a minimal system of generators of the R/\mathfrak{m} -module $M/\mathfrak{m}M$, but the latter holds if and only if $(u_1 + \mathfrak{m}M, \dots, u_n + \mathfrak{m}M)$ is an R/\mathfrak{m} -basis of $M/\mathfrak{m}M$, since $M/\mathfrak{m}M$ is a vector space over R/\mathfrak{m} .

2. Obvious.

3. (a) \Rightarrow (b) \Rightarrow (c) Obvious.

(c) \Rightarrow (d) If $i = (\mathfrak{m} \hookrightarrow R)$, then $\mu_{\mathfrak{m}}^M: \mathfrak{m} \otimes_R M \xrightarrow{i \otimes M} R \otimes_R M \xrightarrow{\sim} M$ is a monomorphism, since $i \otimes M$ is a monomorphism.

(d) \Rightarrow (a) By Theorem 2.1.2, since $M/\mathfrak{m}M$ is a vector space over R/\mathfrak{m} . □

Definitions and Remarks. Let R be a ring and M an R -module.

1. M is called *indecomposable* if $M \neq \mathbf{0}$, and $M = M_1 \dot{+} M_2$ for some submodules $M_1, M_2 \subset M$ implies $M_1 = \mathbf{0}$ or $M_2 = \mathbf{0}$.
2. We call $l(M) = \sup\{n \in \mathbb{N}_0 \mid \text{there exist submodules } M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_n = \mathbf{0}\}$ the *length* of M . By definition, $l(M) \in \mathbb{N}_0 \cup \{\infty\}$, and if $l(M) < \infty$, then M is called a *module of finite length*. $l(M) = 0$ if and only if $M = \mathbf{0}$, and M is called *simple* if $l(M) = 1$ [equivalently, $M \cong R/\mathfrak{a}$ for some maximal left ideal $\mathfrak{a} \subset R$].

Example: Let K be a field, R a finite-dimensional K -algebra and M a finitely generated R -module. Then $l(M) < \infty$ [indeed, M is a finite-dimensional vector space over K , and every R -submodule of M is a K -subspace].

3. A finite sequence of submodules $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_n = \mathbf{0}$ is called a *composition series* if M_i/M_{i-1} is simple for all $i \in [1, n]$. The following assertions are equivalent:
 - M is both noetherian and artinian (that is, it satisfies the ACC and the DCC on submodules).
 - M possesses a composition series.
 - M is a module of finite length.
4. (Theorem or Jordan-Hölder) If $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_n = \mathbf{0}$ and $M = M'_0 \supsetneq M'_1 \supsetneq \dots \supsetneq M'_m$ are two composition series, then $m = n = l(M)$, and there is some permutation $\sigma \in \mathfrak{S}_n$ such that $M'_{i-1}/M'_i \cong M_{\sigma(i-1)}/M_{\sigma(i)}$ for all $i \in [1, n]$.

Theorem 2.1.3. Let R be a ring, $M \neq \mathbf{0}$ an R -module and $E = \text{End}_R(M)$.

1. (Fitting's Lemma) If $l(M) < \infty$ and $f \in E$, then $M = \text{Ker}(f^n) \dot{+} \text{Im}(f^n)$ for all sufficiently large $n \in \mathbb{N}$.
2. If M is indecomposable and $l(M) < \infty$, then E is a local ring.
3. (Krull-Schmidt Theorem)
 - (a) Suppose that M is either artinian or noetherian. Then there exists some $r \in \mathbb{N}$ and indecomposable submodules $M_1, \dots, M_r \subset M$ such that $M = M_1 \dot{+} M_2 \dot{+} \dots \dot{+} M_r$ into.

- (b) Suppose that $l(M) < \infty$, and $M = M_1 \dot{+} M_2 \dot{+} \dots \dot{+} M_r = N_1 \dot{+} N_2 \dot{+} \dots \dot{+} N_s$, where $r, s \in \mathbb{N}$, and $M_1, \dots, M_r, N_1, \dots, N_s \subset M$ are indecomposable submodules. Then $r = s$, and there is a permutation $\sigma \in \mathfrak{S}_r$ such that $M_i \cong N_{\sigma(i)}$ for all $i \in [1, r]$.

PROOF. 1. Since $M \supset \text{Im}(f) \supset \text{Im}(f^2) \supset \dots$, $\mathbf{0} \subset \text{Ker}(f) \subset \text{Ker}(f^2) \subset \dots$ and M satisfies both the ACC and the DCC, there exists some $m \in \mathbb{N}$ such that $\text{Im}(f^n) = \text{Im}(f^m)$ and $\text{Ker}(f^n) = \text{Ker}(f^m)$ for all $n \geq m$. Assume now that $n \geq m$, and let $c \in M$. Then $f^n(c) \in \text{Im}(f^n) = \text{Im}(f^{2n})$, and therefore $f^n(c) = f^{2n}(d)$ for some $d \in M$. Since $f^n(c - f^n(d)) = f^n(c) - f^{2n}(d) = 0$, we get $c = (c - f^n(d)) + f^n(d) \in \text{Ker}(f^n) + \text{Im}(f^n)$. If $x \in \text{Ker}(f^n) \cap \text{Im}(f^n)$, then $x = f^n(y)$ for some $y \in M$. But $0 = f^n(x) = f^{2n}(y)$ implies $y \in \text{Ker}(f^{2n}) = \text{Ker}(f^n)$, and therefore $x = 0$. Hence $M = \text{Ker}(f^n) \dot{+} \text{Im}(f^n)$.

2. Let M be indecomposable and $l(M) < \infty$. By Theorem 2.1.1.4 it suffices to prove that every $f \in E \setminus E^\times$ is nilpotent. Thus let $f \in E \setminus E^\times$ and $n \in \mathbb{N}$ such that $M = \text{Ker}(f^n) \dot{+} \text{Im}(f^n)$. Then either $\text{Ker}(f^n) = \mathbf{0}$ or $\text{Im}(f^n) = \mathbf{0}$. If $\text{Im}(f^n) = \mathbf{0}$, then $f^n = 0$. If $\text{Ker}(f^n) = \mathbf{0}$, then $\text{Im}(f^n) = M$, hence f^n and thus also f is an isomorphism, which implies $f \in E^\times$.

3. (a) Assume the contrary. We construct two sequences of R -submodules $(M_i)_{i \geq 0}$, $(M'_i)_{i \geq 1}$ of M such that $M_0 = M$, and for all $i \geq 0$ the following assertions hold: M_i is not a direct sum of indecomposable submodules, $M_i = M_{i+1} \dot{+} M'_{i+1}$, $M_{i+1} \neq \mathbf{0}$ and $M'_{i+1} \neq \mathbf{0}$. We proceed recursively. Set $M_0 = M$, and suppose that $i \geq 0$ and $M_i \subset M$ is not a direct sum of indecomposable submodules. Then $M_i = M_{i+1} \dot{+} M'_{i+1}$, where $M_{i+1} \neq \mathbf{0}$, $M'_{i+1} \neq \mathbf{0}$ and M_{i+1} is not a direct sum of indecomposable submodules. If $i \geq 0$, then it follows by an easy induction on j that $M_i = M_{i+j} \dot{+} M'_{i+j} \dot{+} M'_{i+j-1} \dot{+} \dots \dot{+} M'_{i+1}$. Hence we obtain $M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$ and $M'_1 \subsetneq M'_1 \dot{+} M'_2 \subsetneq M'_1 \dot{+} M'_2 \dot{+} M'_3 \subsetneq \dots$, contradicting the assumption that M is either noetherian or artinian.

(b) We may assume that $r \geq s$, and we proceed by induction on s . If $s = 1$, then M is indecomposable and $r = 1$.

$s \geq 2$, $s - 1 \rightarrow s$: For $i \in [1, r]$, let $p_i \in \text{Hom}_R(M, M_i)$ such that $p_i | M_i = \text{id}_{M_i}$ and $p_i | M_j = 0$ for all $j \in [1, r] \setminus \{i\}$. For $i \in [1, s]$ let $q_i \in \text{Hom}_R(M, N_i)$ such that $q_i | N_i = \text{id}_{N_i}$ and $q_i | N_j = 0$ for all $j \in [1, s] \setminus \{i\}$. Then

$$\text{id}_M = \sum_{i=1}^s q_i, \quad \text{hence} \quad p_1 = \sum_{i=1}^s p_1 \circ q_i \quad \text{and} \quad \text{id}_{M_1} = p_1 | M_1 = \sum_{i=1}^s p_1 \circ q_i | M_1$$

Since $E_1 = \text{End}_R(M_1)$ is local, $E_1 \setminus E_1^\times \subset E_1$ is an ideal, and thus there is some $i \in [1, s]$ such that $p_1 \circ q_i | M_1 \in E_1^\times$, say $i = 1$. Then $p_1 \circ q_1 | M_1: M_1 \rightarrow M_1$ is an isomorphism, hence $q_1 | M_1: M_1 \rightarrow N_1$ is a monomorphism, $g = (p_1 \circ q_1 | M_1)^{-1} \circ p_1 | N_1: N_1 \rightarrow M_1$ is a homomorphism, and $g \circ q_1 | M_1 = \text{id}_{M_1}$. Hence $q_1 | M_1: M_1 \rightarrow N_1$ splits, and therefore $q_1(M_1) \in N_1$. Since $q_1(M_1) \neq \mathbf{0}$ and N_1 is indecomposable, it follows that $q_1(M_1) = N_1$, and $q_1 | M_1: M_1 \rightarrow N_1$ is an isomorphism. Now we assert:

A. $M = M_1 \dot{+} N_2 \dot{+} \dots \dot{+} N_s$.

Proof of A. We first show that $N_1 \subset M_1 + N_2 + \dots + N_s$. If $a \in N_1 = q_1(M_1)$, then $a = q_1(b)$ for some $b \in M_1$, and $q_1(a - b) = q_1(a) - q_1(b) = a - a = 0$. Hence $a - b \in \text{Ker}(q_1) = N_2 + \dots + N_s$, and therefore $a = b + (a - b) \in M_1 + N_2 + \dots + N_s$. Hence it follows that $M = M_1 + (N_2 \dot{+} \dots \dot{+} N_s)$, and we assert that the sum is direct. Indeed, if $a \in M_1 \cap (N_2 + \dots + N_s)$, then $q_1(a) \in N_1$, and since $q_1 | N_2 + \dots + N_s = 0$, we obtain $q_1(a) = 0$ and therefore $a = 0$, since $q_1 | M_1$ is injective. \square [A]

Since $M = M_1 \dot{+} M_2 \dot{+} \dots \dot{+} M_r$ and $M = M_1 \dot{+} N_2 \dot{+} \dots \dot{+} N_s$ we obtain

$$M/M_1 \cong M_2 \dot{+} \dots \dot{+} M_r \cong N_2 \dot{+} \dots \dot{+} N_s, \quad \text{and let} \quad \Phi: M_2 \dot{+} \dots \dot{+} M_r \xrightarrow{\sim} N_2 \dot{+} \dots \dot{+} N_s$$

be an isomorphism. Then $\Phi(M_2) \dot{+} \dots \dot{+} \Phi(M_r) = N_2 \dot{+} \dots \dot{+} N_s$, and the Theorem follows from the induction hypothesis. \square

Definition (Power series rings). Let R be a ring, $r \in \mathbb{N}$ and (e_1, \dots, e_r) the canonical basis of \mathbb{Z}^r . We denote by $R^{[r]}$ the set of all maps $f: \mathbb{N}_0^r \rightarrow R$ and by $R^{[r]}$ the set of all $f \in R^{[r]}$ satisfying

$f(\mathbf{n}) = 0$ for almost all $\mathbf{n} \in \mathbb{N}_0^r$. Then $R^{[r]} \subset R^{\llbracket r \rrbracket}$ are R -modules under pointwise addition and scalar multiplication. We define a multiplication on $R^{\llbracket r \rrbracket}$ by

$$(f \cdot g)(\mathbf{k}) = \sum_{\substack{(\mathbf{m}, \mathbf{n}) \in \mathbb{N}_0^r \times \mathbb{N}_0^r \\ \mathbf{m} + \mathbf{n} = \mathbf{k}}} f(\mathbf{m})g(\mathbf{n}).$$

Then $R^{\llbracket r \rrbracket}$ is a ring, and $R^{[r]} \subset R^{\llbracket r \rrbracket}$ is a subring. We define $\nu: R \rightarrow R^{[r]}$ and $\mu: R^{\llbracket r \rrbracket} \rightarrow R$ by

$$\nu(c)(\mathbf{k}) = c\delta_{\mathbf{k}, \mathbf{0}} = \begin{cases} c & \text{if } \mathbf{k} = \mathbf{0}, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad \mu(f) = f(\mathbf{0}) \quad \text{for all } c \in R \text{ and } f \in R^{\llbracket r \rrbracket}.$$

Then $\mu: R^{\llbracket r \rrbracket} \rightarrow R$ is a ring epimorphism, called *augmentation*, $\nu: R \rightarrow R^{[r]}$ is a ring monomorphism, and we identify R with $\nu(R)$. Then $R \subset R^{[r]} \subset R^{\llbracket r \rrbracket}$ are subrings. For $i \in [1, r]$, we define $X_i \in R^{[r]}$ by $X_i(\mathbf{k}) = \delta_{\mathbf{k}, \mathbf{e}_i}$, and for $\mathbf{n} = (n_1, \dots, n_r) \in \mathbb{N}_0^r$ we set $\mathbf{X}^{\mathbf{n}} = X_1^{n_1} \cdots X_r^{n_r}$. Then it follows (by an easy induction on $n_1 + \dots + n_r$) that $\mathbf{X}^{\mathbf{n}}(\mathbf{k}) = \delta_{\mathbf{n}, \mathbf{k}}$ for all $\mathbf{n}, \mathbf{k} \in \mathbb{N}_0^r$, $\mathbf{X}^{\mathbf{n}} \cdot \mathbf{X}^{\mathbf{m}} = \mathbf{X}^{\mathbf{n} + \mathbf{m}}$ for all $\mathbf{m}, \mathbf{n} \in \mathbb{N}_0^r$, and

$$f = \sum_{\mathbf{k} \in \mathbb{N}_0^r} f(\mathbf{k})\mathbf{X}^{\mathbf{k}} \quad \text{for all } f \in R^{\llbracket r \rrbracket}$$

(note that pointwise this formally infinite sum reduces to a single summand). Hence every $f \in R^{\llbracket r \rrbracket}$ has a unique representation

$$f = \sum_{(k_1, \dots, k_r) \in \mathbb{N}_0^r} f_{k_1, \dots, k_r} X_1^{k_1} \cdots X_r^{k_r}$$

with coefficients $f_{k_1, \dots, k_r} \in R$, and we obtain $f \in R^{[r]}$ if and only if $f_{k_1, \dots, k_r} = 0$ for almost all $(k_1, \dots, k_r) \in \mathbb{N}_0^r$. In particular, $R^{[r]} = R[X_1, \dots, X_r]$ is a polynomial ring in (X_1, \dots, X_r) over R .

If $r, s \in \mathbb{N}$, then there is an isomorphism $\Phi: (R^{\llbracket r \rrbracket})^{\llbracket s \rrbracket} \xrightarrow{\sim} R^{\llbracket r+s \rrbracket}$, given by $\Phi(f)(\mathbf{m}, \mathbf{n}) = f(\mathbf{m})(\mathbf{n})$ for all $\mathbf{m} \in \mathbb{N}_0^r$ and $\mathbf{n} \in \mathbb{N}_0^s$. It satisfies $\Phi(R^{\llbracket r \rrbracket})^{\llbracket s \rrbracket} = R^{\llbracket r+s \rrbracket}$, and we identify $(R^{\llbracket r \rrbracket})^{\llbracket s \rrbracket} = R^{\llbracket r+s \rrbracket}$ and $(R^{\llbracket r \rrbracket})^{\llbracket s \rrbracket} = R^{\llbracket r+s \rrbracket}$ by means of Φ .

We call $R[[X_1, \dots, X_r]] = R^{\llbracket r \rrbracket}$ the *power series ring* or *ring of formal power series* in (X_1, \dots, X_r) over R . If $r \geq 2$, then it follows that $R[[X_1, \dots, X_r]] = R[[X_1, \dots, X_{r-1}]] [[X_r]] \supset R[[X_1, \dots, X_{r-1}]]$, $R[[X_1, \dots, X_r]] = R[[X_1, \dots, X_{r-1}]] [X_r] \supset R[[X_1, \dots, X_{r-1}]]$, and the augmentation maps behave transitively. Explicitly, if

$$\mu': R[[X_1, \dots, X_{r+1}]] = R[[X_1, \dots, X_r]] [[X_{r+1}]] \rightarrow R[[X_1, \dots, X_r]] \quad \text{and} \quad \mu: R[[X_1, \dots, X_r]] \rightarrow R$$

are the (partial) augmentation maps, then $\mu \circ \mu': R[[X_1, \dots, X_{r+1}]] \rightarrow R$ is the (total) augmentation map.

In particular, if $r = 1$ and $X = X_1$, then every $f \in R[[X]]$ has a unique representation

$$f = \sum_{n=0}^{\infty} f_n X^n, \quad \text{where } f_n \in R \text{ for all } n \geq 0,$$

and $f \in R[X]$ if and only if $f_n = 0$ for almost all $n \geq 0$. If $f \in R[[X]]$ is as above, then $\mu(f) = f_0$, and we call

$$\text{ord}(f) = \inf\{n \in \mathbb{N}_0 : f_n \neq 0\} \in \mathbb{N}_0 \cup \{\infty\} \quad \text{the order of } f.$$

If $f \neq 0$ then f has a unique representation $f = X^{\text{ord}(f)} f_1$, where $f_1 \in R[[X]]$ and $\mu(f_1) \neq 0$. If $f, g \in R[[X]]$, then $\text{ord}(f) = \infty$ if and only if $f = 0$, $\text{ord}(f + g) \geq \min\{\text{ord}(f), \text{ord}(g)\}$ with equality if $\text{ord}(f) \neq \text{ord}(g)$, and $\text{ord}(fg) \geq \text{ord}(f) + \text{ord}(g)$ with equality if R has no zero divisors. In particular, if R has no zero divisors, the same is true for $R[[X]]$.

For $f, g \in R[[X]]$, we define $\delta(f, g) = e^{-\text{ord}(f-g)}$ (with $e^{-\infty} = 0$). Then δ is a metric on $R[[X]]$. If $f \in \mathbb{R}[[X]]$, then $\text{ord}(f) = -\log \delta(f, 0)$ (where $-\log 0 = \infty$), and the sets

$$f + X^n R[[X]] = \{g \in R[[X]] \mid \text{ord}(g - f) \geq n\} = \{g \in R[[X]] \mid \delta(g, f) \leq e^{-n}\} \quad (\text{for } n \in \mathbb{N})$$

are a fundamental system of neighborhoods of f . Consequently, if

$$f = \sum_{n=0}^{\infty} f_n X^n \in R[[X]], \quad \text{then} \quad f = \lim_{k \rightarrow \infty} \sum_{n=0}^k f_n X^n.$$

If R has no zero divisors, then it follows by induction that, for every $r \in \mathbb{N}$, the power series ring $R[[X_1, \dots, X_r]]$ has no zero divisors. In particular, if K is a field, then $K[[X_1, \dots, X_r]]$ is a domain. We denote by $K((X_1, \dots, X_r))$ the quotient field of $K[[X_1, \dots, X_r]]$ and call it the *field of formal Laurent series* in (X_1, \dots, X_r) over K .

Theorem 2.1.4. *Let R be a ring, $r \in \mathbb{N}$, $R[[X_1, \dots, X_r]]$ the power series ring in (X_1, \dots, X_r) over R , $\mu: R[[X_1, \dots, X_r]] \rightarrow R$ the augmentation map and $f \in R[[X_1, \dots, X_r]]$.*

1. $f \in R[[X_1, \dots, X_r]]^\times$ if and only if $\mu(f) \in R^\times$.
2. If R is local with maximal ideal \mathfrak{m} , then $R[[X_1, \dots, X_r]]$ is local with maximal ideal $\mathfrak{M} = \mu^{-1}(\mathfrak{m})$. In particular, if $r = 1$ and $X = X_1$, then

$$f = \sum_{n=0}^{\infty} f_n X^n \in R[[X]]^\times \quad \text{if and only if} \quad f_0 \in R^\times,$$

and if R is a division ring, then every $f \in R[[X]]$ has a unique representation $f = X^n h$, where $n \in \mathbb{N}_0$ and $h \in R[[X]]^\times$.

PROOF. 1. If $f \in R[[X_1, \dots, X_r]]^\times$, the $\mu(f) \in R^\times$, since μ is a ring homomorphism. For the converse, we use induction on r .

$r = 1$, $X = X_1$: Assume that

$$f = \sum_{n=0}^{\infty} f_n X^n \in R[[X]] \quad \text{and} \quad f_0 = \mu(f) \in R^\times.$$

We define a sequence $(g_n)_{n \geq 0}$ in R recursively by

$$g_0 = f_0^{-1}, \quad g_n = -f_0^{-1} \sum_{\nu=1}^n f_\nu g_{n-\nu} \quad \text{for all } n \geq 1, \quad \text{and set} \quad g = \sum_{n=0}^{\infty} g_n X^n$$

Then

$$fg = \sum_{n=0}^{\infty} \left(f_0 g_n + \sum_{\nu=1}^n f_\nu g_{n-\nu} \right) X^n = 1.$$

Hence f has a right-inverse, and, by the same reason, f has a left-inverse. Hence $f \in R[[X]]^\times$.

$r \geq 2$, $r - 1 \rightarrow r$: By the induction hypothesis, $R' = R[[X_1, \dots, X_{r-1}]]$ is local with maximal ideal $\mathfrak{M}' = \mu'^{-1}(\mathfrak{m})$, where $\mu': R' \rightarrow R$ denotes the augmentation map. Hence $\bar{R} = R[[X_1, \dots, X_r]] = R'[[X_r]]$ is local with maximal ideal $\mathfrak{M} = \tilde{\mu}^{-1}(\mathfrak{M}')$, where $\tilde{\mu}: R'[[X_r]] \rightarrow R'$ denotes the augmentation. Since $\mu = \mu' \circ \tilde{\mu}$, it follows that $\mathfrak{M} = \mu^{-1}(\mathfrak{m})$.

2. $R[[X_1, \dots, X_r]] \setminus R[[X_1, \dots, X_r]]^\times = \{f \in R[[X_1, \dots, X_r]] \mid \mu(f) \in R \setminus R^\times\} = \mu^{-1}(\mathfrak{m})$ is an ideal of $R[[X_1, \dots, X_r]]$. \square

Theorem 2.1.5. *Let R be a commutative ring.*

1. (Cohen's Theorem) *If every prime ideal of R is finitely generated, then R is noetherian.*
2. *Let $R[[X]]$ be the power series ring, $\mu: R[[X]] \rightarrow R$ the augmentation, $\mathfrak{p} \subset R[[X]]$ a prime ideal, $m \in \mathbb{N}$ and $f_1, \dots, f_m \in \mathfrak{p}$. Then $\mu(\mathfrak{p}) \subset R$ is an ideal, and if $\mu(\mathfrak{p}) = {}_R\langle \mu(f_1), \dots, \mu(f_m) \rangle$, then*

$$\mathfrak{p} = \begin{cases} {}_{R[[X]]}\langle f_1, \dots, f_m \rangle & \text{if } X \notin \mathfrak{p}, \\ {}_{R[[X]]}\langle \mu(f_1), \dots, \mu(f_m), X \rangle & \text{if } X \in \mathfrak{p}. \end{cases}$$

3. *Let $r \in \mathbb{N}$. Then the power series ring $R[[X_1, \dots, X_n]]$ is noetherian if and only if R is noetherian.*

PROOF. 1. Suppose that every prime ideal of R is finitely generated, but R is not noetherian. Let Ω be the set of all not finitely generated ideals of R . Then $\Omega \neq \emptyset$, and the union of every chain in Ω belongs to Ω . By Zorn's Lemma, Ω has a maximal element \mathfrak{q} , and we shall prove that $\mathfrak{q} \subset R$ is a prime ideal (which contradicts our assumption that every prime ideal is finitely generated).

Assume to the contrary that there exist $a, b \in R \setminus \mathfrak{q}$ such that $ab \in \mathfrak{q}$. Then $\mathfrak{q} \subsetneq \mathfrak{q} + aR \triangleleft R$ and $\mathfrak{q} \subsetneq \mathfrak{q} + bR \subset (\mathfrak{q} : aR) = \{x \in R \mid xa \in \mathfrak{q}\}$. Hence the ideals $\mathfrak{q} + aR$ and $(\mathfrak{q} : aR)$ are finitely generated, say $\mathfrak{q} + aR = {}_R\langle q_1 + ax_1, \dots, q_n + ax_n \rangle$ and $(\mathfrak{q} : aR) = {}_R\langle z_1, \dots, z_m \rangle$, where $m, n \in \mathbb{N}$, $q_1, \dots, q_n \in \mathfrak{q}$ and $x_1, \dots, x_n, z_1, \dots, z_m \in R$. Then ${}_R\langle q_1, \dots, q_n, az_1, \dots, az_m \rangle \subset \mathfrak{q}$, and we assert that equality holds (this contradicts the fact that $\mathfrak{q} \in \Omega$ is not finitely generated). Indeed, if $z \in \mathfrak{q} \subset \mathfrak{q} + aR$, then there exist $b_1, \dots, b_n \in R$ such that

$$z = \sum_{\nu=1}^n b_\nu(q_\nu + ax_\nu) = \sum_{\nu=1}^n b_\nu q_\nu + a \sum_{\nu=1}^n b_\nu x_\nu, \quad \text{and therefore} \quad a \sum_{\nu=1}^n b_\nu x_\nu = z - \sum_{\nu=1}^n b_\nu q_\nu \in \mathfrak{q}.$$

Hence

$$\sum_{\nu=1}^n b_\nu x_\nu \in (\mathfrak{q} : aR) = {}_R\langle z_1, \dots, z_m \rangle, \quad \text{and} \quad z = \sum_{\nu=1}^n b_\nu q_\nu + a \sum_{\nu=1}^n b_\nu x_\nu \in {}_R\langle q_1, \dots, q_n, az_1, \dots, az_m \rangle.$$

2. $\mu(\mathfrak{p}) \subset R$ is an ideal, since μ is an epimorphism. Suppose that $\mu(\mathfrak{p}) = {}_R\langle \mu(f_1), \dots, \mu(f_m) \rangle$, and set

$$f_j = \sum_{n \geq 0} f_{j,n} X^n, \quad \text{where } f_{j,n} \in R \text{ for all } j \in [1, m] \text{ and } n \geq 0$$

CASE 1: $X \in \mathfrak{p}$. Obviously ${}_R[X]\langle \mu(f_1), \dots, \mu(f_m), X \rangle \subset \mathfrak{p}$, since $f_j \in \mu(f_j) + XR[X]$ for all $j \in [1, m]$. Conversely, if $h \in \mathfrak{p}$, then $h = \mu(h) + Xh_1$ for some $h_1 \in R[X]$, and therefore we obtain $h \in \mu(\mathfrak{p}) + XR[X] = {}_R[X]\langle \mu(f_1), \dots, \mu(f_m), X \rangle$.

CASE 2: $X \notin \mathfrak{p}$. It suffices to prove that $\mathfrak{p} \subset {}_R[X]\langle f_1, \dots, f_m \rangle$. Let $h \in \mathfrak{p}$. For $j \in [1, m]$ and $n \geq 0$, we construct elements $g_{j,n} \in R$ such that, for all $n \geq 0$,

$$h - \sum_{j=1}^m \left(\sum_{\nu=0}^{n-1} g_{j,\nu} X^\nu \right) f_j \in X^n R[X], \quad \text{and for } j \in [1, m] \text{ s we set } g_j = \sum_{\nu \geq 0} g_{j,\nu} X^\nu \in R[X].$$

Then it follows that

$$h - \sum_{j=1}^m g_j f_j \in \bigcap_{n \geq 0} X^n R[X] = \mathbf{0}, \quad \text{and therefore } h \in {}_R[X]\langle f_1, \dots, f_m \rangle.$$

We perform our construction by recursion on n . For $n = 0$, there is nothing to do. Thus suppose that $n \geq 0$, and there exist elements $g_{j,\nu}$ for all $j \in [1, m]$ and $\nu \in [0, n-1]$ such that

$$h - \sum_{j=1}^m \left(\sum_{\nu=0}^{n-1} g_{j,\nu} X^\nu \right) f_j = X^n q, \quad \text{where } q = \sum_{\nu \geq 0} q_\nu X^\nu \in R[X].$$

Then $X^n q \in \mathfrak{p}$, and as $X \notin \mathfrak{p}$, it follows that $q \in \mathfrak{p}$ and $q_0 = \mu(q) \in {}_R\langle \mu(f_1), \dots, \mu(f_m) \rangle$. Hence there exist $g_{1,n}, \dots, g_{m,n} \in R$ such that

$$q_0 = - \sum_{j=1}^m g_{j,n} \mu(f_j) = - \sum_{j=1}^m g_{j,n} f_{j,0},$$

and we obtain

$$h - \sum_{j=1}^m \left(\sum_{\nu=0}^n g_{j,\nu} X^\nu \right) f_j = X^n \sum_{\nu \geq 0} q_\nu X^\nu + X^n \sum_{j=1}^m g_{j,n} f_j = X^n \left(q_0 + \sum_{j=1}^m g_{j,n} f_{j,0} \right) + X^{n+1} g^* \in X^{n+1} g^*$$

for some $g^* \in R[X]$, which completes the construction.

3. Since $R[X_1, \dots, X_r] = R[X_1, \dots, X_{r-1}][X_r]$ if $r \geq 2$, the assertion follows by induction on r , once we have given the proof for $r = 1$. Thus let $R[X]$ be a power series ring. If $R[X]$ is noetherian,

then R is noetherian, since $\mu: R[[X]] \rightarrow R$ is an epimorphism. Thus suppose that R is noetherian. By 2., every prime ideal of $R[[X]]$ is finitely generated, and thus $R[[X]]$ is noetherian by 1. \square

Definitions and Remarks (Recapitulation: Quotients). Let R be a commutative ring, $T \subset R$ a multiplicatively closed subset and M an R -module.

1. On $T \times M$ we define an equivalence relation by $(t, x) \sim (t', x')$ if there exists some $s \in T$ such that $st'x = stx'$. We set $T^{-1}M = T \times M / \sim$, denote by $\frac{x}{t} \in T^{-1}M$ the equivalence class of (t, x) and call $T^{-1}M$ the *quotient module* of M with T . By definition, if $x \in M$ and $t \in T$, then

$$\frac{x}{t} = \frac{sx}{st} \quad \text{for all } s \in T, \quad \text{and} \quad \frac{x}{t} = \frac{0}{1} \quad \text{if and only if } sx = 0 \text{ for some } s \in T.$$

For any $n \in \mathbb{N}$ and $z_1, \dots, z_n \in T^{-1}M$, there exist $x_1, \dots, x_n \in M$ and $t \in T$ such that $z_i = \frac{x_i}{t}$ for all $i \in [1, n]$.

2. We make $T^{-1}M$ into an abelian group by means of

$$\frac{x}{t} + \frac{x'}{t'} = \frac{t'x + tx'}{tt'} \quad \text{check details!},$$

and we define the *quotient homomorphism* $j: M \rightarrow T^{-1}M$ by $j(x) = \frac{x}{1}$ for all $x \in M$. By definition,

$$\text{Ker}(j) = \{x \in M \mid xt = 0 \text{ for some } t \in T\} = \{x \in M \mid T \cap \text{Ann}_R(x) \neq \emptyset\}.$$

If $0 \in T$, then $T^{-1}M = \mathbf{0}$. If M is torsion-free and $0 \notin T$, then $j: M \rightarrow T^{-1}M$ is a monomorphism.

If $M' \subset M$ is an R -submodule, then $T^{-1}M' \subset T^{-1}M$ is a subgroup [indeed, if \sim' denotes the defining equivalence relation on $T \times M'$, then $\sim' = \sim \cap (T \times M')$, and therefore we may identify, for every $(t, x) \in T \times M'$, the equivalence class $\frac{x}{t} \in M'$ with the equivalence class $\frac{x}{t} \in M$].

3. Now we consider the special case $M = R$ and define a multiplication on $T^{-1}R$ by

$$\frac{a}{t} \frac{a'}{t'} = \frac{aa'}{tt'}.$$

With this definition, $T^{-1}R$ is a commutative ring, called the *quotient ring* of R with respect to T , and the quotient homomorphism $j: R \rightarrow T^{-1}R$ is a ring homomorphism. Consequently $T^{-1}R$ is an R -algebra.

Let $\mathfrak{z}(R)$ be the set of zero divisors of R . Then $R \setminus \mathfrak{z}(R)$ is a multiplicatively closed subset of R , and $\mathfrak{q}(R) = (R \setminus \mathfrak{z}(R))^{-1}R$ is called the *total quotient ring* of R . The quotient homomorphism $j: R \rightarrow \mathfrak{q}(R)$ is a monomorphism, we identify R with $j(R)$ (we set $x = \frac{x}{1}$ for every $x \in R$), and for every multiplicatively closed subset $T \subset R \setminus \mathfrak{z}(R)$, we may assume that $T^{-1}R \subset \mathfrak{q}(R)$. If R is a domain, then $\mathfrak{q}(R)$ is just the usual quotient field. If $T \subset R^\times$, then $T^{-1}R = R$ and $T^{-1}M = M$ for every R -module M .

4. Let M be an R -module. Then $T^{-1}M$ is a $T^{-1}R$ -module by means of

$$\frac{a}{t} \frac{x}{t'} = \frac{ax}{tt'} \quad \text{for all } a \in R, x \in M \text{ and } t, t' \in T. \quad \text{Check details!}$$

If $j: M \rightarrow T^{-1}M$ is the quotient homomorphism, and $M = {}_R\langle E \rangle$, then $T^{-1}M = {}_{T^{-1}R}\langle j(E) \rangle$. In particular, if M is a finitely generated R -module, then $T^{-1}M$ is a finitely generated $T^{-1}R$ -module.

If $M' \subset M$ is an R -submodule, then $T^{-1}M' \subset T^{-1}M$ is a $T^{-1}R$ -submodule, and the map

$$\Phi: T^{-1}M/T^{-1}M' \rightarrow T^{-1}(M/M'), \quad \text{defined by} \quad \Phi\left(\frac{x}{t} + T^{-1}M'\right) = \frac{x + M'}{t}$$

for all $x \in M$ and $t \in T$, is a $T^{-1}R$ -module isomorphism by which we usually identify these two modules: $T^{-1}(M/M') = T^{-1}M/T^{-1}M'$.

In particular, $T^{-1}M$ is also an R -module by means of the quotient homomorphism $j: R \rightarrow T^{-1}R$. For all $r \in R$, $m \in M$ and $t \in T$, we have

$$r \frac{m}{t} = \frac{r}{1} \frac{m}{t} = \frac{rm}{t}.$$

5. Let $f: M \rightarrow M'$ be a homomorphism of R -modules. Then there is a unique homomorphism $T^{-1}f: T^{-1}M \rightarrow T^{-1}M'$ of $T^{-1}R$ -modules such that

$$T^{-1}f\left(\frac{x}{t}\right) = \frac{f(x)}{t} \quad \text{for all } x \in M \text{ and } t \in T,$$

It satisfies $T^{-1}\text{id}_M = \text{id}_{T^{-1}M}$, $T^{-1}(g+f) = T^{-1}g + T^{-1}f$ if $g: M \rightarrow M'$ is another R -homomorphism, $T^{-1}(g \circ f) = T^{-1}g \circ T^{-1}f$ if $g: M' \rightarrow M''$ is an R -homomorphism,

$$\text{Ker}(T^{-1}f) = T^{-1}\text{Ker}(f) \subset T^{-1}M \quad \text{and} \quad \text{Im}(T^{-1}f) = T^{-1}\text{Im}(f) \subset M'.$$

In particular, the assignment $(M \mapsto T^{-1}M, f \mapsto T^{-1}f)$ defines an additive and exact functor $R\text{-Mod} \rightarrow T^{-1}R\text{-Mod}$ (it carries exact sequences into exact sequences).

6. Let $\varepsilon: R \rightarrow A$ be an R -algebra. On $T^{-1}A$, we define a multiplication by

$$\frac{a}{t} \frac{a'}{t'} = \frac{aa'}{tt'} \quad \text{for all } a, a' \in A \text{ and } t, t' \in T.$$

Then $T^{-1}A$ is a $T^{-1}R$ -algebra with structural homomorphism $T^{-1}\varepsilon: T^{-1}R \rightarrow T^{-1}A$.

If A is commutative, then $\varepsilon(T) \subset A$ is multiplicatively closed, and if N is an A -module, then N is an R -module, and $T^{-1}N = \varepsilon(T)^{-1}N$.

Theorem 2.1.6. *Let R be a commutative ring, $T \subset R$ a multiplicatively closed subset and M an R -module. Then there is a $T^{-1}R$ -isomorphism*

$$\Phi: T^{-1}R \otimes_R M \xrightarrow{\sim} T^{-1}M \quad \text{such that} \quad \Phi\left(\frac{r}{t} \otimes m\right) = \frac{rm}{t} \quad \text{for all } r \in R, m \in M \text{ and } t \in T.$$

It is functorial in M , and if M is an R -algebra, then Φ is an isomorphism of $T^{-1}R$ -algebras. In particular, $T^{-1}R$ is a flat R -algebra.

PROOF. We define $F: T^{-1}R \times M \rightarrow T^{-1}M$ by

$$F\left(\frac{r}{t}, m\right) = \frac{rm}{t} \quad \text{for all } r \in R, t \in T, m \in M,$$

and we assert that this definition does not depend on representatives, that means, $\frac{r}{t} = \frac{r'}{t'}$ implies $\frac{rm}{t} = \frac{r'm}{t'}$ for all $r, r' \in R$, $t, t' \in T$ and $m \in M$. Indeed, if $\frac{r}{t} = \frac{r'}{t'}$, then $st'r = str'$ for some $s \in T$, hence $st'rm = str'm$, and therefore $\frac{rm}{t} = \frac{r'm}{t'}$. Obviously, F is R -bilinear, and thus it induces a group homomorphism $\Phi: T^{-1}R \otimes_R M \rightarrow T^{-1}M$ such that $\Phi\left(\frac{r}{t} \otimes m\right) = \frac{rm}{t}$ for all $r \in R$, $m \in M$ and $t \in T$.

It is easily checked that Φ is in fact a $T^{-1}R$ -homomorphism, that it is functorial in M , and that it is a homomorphism of T^{-1} -algebras if M is an R -algebra.

To prove that Φ is bijective, define $\Psi: T^{-1}M \rightarrow T^{-1}R \otimes_R M$ by $\Psi\left(\frac{m}{t}\right) = \frac{1}{t} \otimes m$ for all $m \in M$ and $t \in T$, and we assert that this definition does not depend on representatives, that means, $\frac{m}{t} = \frac{m'}{t'}$ implies $\frac{1}{t} \otimes m = \frac{1}{t'} \otimes m'$ for all $m, m' \in M$ and $t, t' \in T$. Indeed, if $\frac{m}{t} = \frac{m'}{t'}$, then $st'm = stm'$ for some $s \in T$, and we obtain

$$\frac{1}{t} \otimes m = \frac{1}{stt'} st' \otimes m = \frac{1}{stt'} \otimes st'm = \frac{1}{stt'} \otimes stm' = \frac{1}{stt'} st \otimes m' = \frac{1}{t'} \otimes m'.$$

If $M' \rightarrow M \rightarrow M''$ is an exact sequence in $R\text{-Mod}$, then the commutative diagram

$$\begin{array}{ccccc} T^{-1}M' & \longrightarrow & T^{-1}M & \longrightarrow & T^{-1}M'' \\ \cong \downarrow & & \downarrow \cong & & \downarrow \cong \\ T^{-1}R \otimes_R M' & \longrightarrow & T^{-1}R \otimes_R M & \longrightarrow & T^{-1}R \otimes_R M'' \end{array}$$

shows that the sequence $T^{-1}R \otimes_R M' \rightarrow T^{-1}R \otimes_R M \rightarrow T^{-1}R \otimes_R M''$ is also exact. Hence $T^{-1}R$ is flat over R . \square

Definition. Let R be a commutative ring. We denote by $\text{spec}(R)$ be the set of all prime ideals and by $\text{max}(R)$ the set of all maximal ideals of R . Note that $\text{max}(R) \subset \text{spec}(R)$, and R is local if and only if $|\text{max}(R)| = 1$ [then $\text{max}(R) = \{R \setminus R^\times\}$].

If $\mathfrak{p} \in \text{spec}(R)$, then $R \setminus \mathfrak{p} \subset R$ is a multiplicatively closed subset, and for an R -module M we call $M_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}M$ the *localization* of M at \mathfrak{p} . In particular, if R is a domain, then $\mathbf{0} \in \text{spec}(R)$, and $R_{\mathbf{0}} = \mathfrak{q}(R)$. For an R -module homomorphism $f: M \rightarrow N$, we set $f_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}f: M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$.

Remark and Definition. Let $\varepsilon: R \rightarrow A$ be an R -algebra. For an ideal $\mathfrak{a} \subset R$, we call $\mathfrak{a}A = {}_A\langle \varepsilon(\mathfrak{a}) \rangle$ the *extension* of \mathfrak{a} to A , and for an ideal $\mathfrak{A} \subset A$ we call $\varepsilon^{-1}(\mathfrak{A}) \subset R$ the *contraction* of \mathfrak{A} to R . Obviously, $\mathfrak{a} \subset \varepsilon^{-1}(\mathfrak{a}A)$ and $\varepsilon^{-1}(\mathfrak{A})A \subset \mathfrak{A}$ for all ideals $\mathfrak{a} \triangleleft R$ and $\mathfrak{A} \triangleleft A$, and the maps

$$\{\mathfrak{a}A \mid \mathfrak{a} \triangleleft R\} \rightleftharpoons \{\varepsilon^{-1}\mathfrak{A} \mid \mathfrak{A} \triangleleft A\}, \quad \text{given by } \mathfrak{A} \mapsto \varepsilon^{-1}\mathfrak{A} \text{ and } \mathfrak{a} \mapsto \mathfrak{a}A,$$

are mutually inverse bijections from the set of extension ideals in A onto the set of contraction ideals of R . If $\mathfrak{P} \in \text{spec}(A)$, then $\varepsilon^{-1}(\mathfrak{P}) \in \text{spec}(R)$.

Theorem 2.1.7. *Let $T \subset R$ be a multiplicatively closed subset and $j: R \rightarrow T^{-1}R$ the quotient homomorphism.*

1. *If $\mathfrak{a} \triangleleft R$, then $\mathfrak{a}T^{-1}R = T^{-1}\mathfrak{a}$, and $T^{-1}\mathfrak{a} = T^{-1}R$ if and only if $T \cap \mathfrak{a} \neq \emptyset$.*
2. *If $\mathfrak{A} \triangleleft T^{-1}R$, then $\mathfrak{A} = T^{-1}j^{-1}(\mathfrak{A})$. In particular, $\{T^{-1}\mathfrak{a} \mid \mathfrak{a} \triangleleft R\}$ is the set of all ideals of $T^{-1}R$, and if R is noetherian, then $T^{-1}R$ is also noetherian.*
3. *If $\mathfrak{p} \in \text{spec}(R)$ and $T \cap \mathfrak{p} = \emptyset$, then $T^{-1}\mathfrak{p} \in \text{spec}(T^{-1}R)$, $\mathfrak{p} = j^{-1}(T^{-1}\mathfrak{p})$,*

$$T^{-1}R \setminus T^{-1}\mathfrak{p} = \left\{ \frac{s}{t} \mid s \in R \setminus \mathfrak{p}, t \in T \right\},$$

and there is a ring isomorphism

$$R_{\mathfrak{p}} \xrightarrow{\sim} (T^{-1}R)_{T^{-1}\mathfrak{p}}, \quad \text{given by } \frac{a}{t} \mapsto \frac{\frac{a}{t}}{\frac{1}{t}} \text{ for all } a \in R \text{ and } t \in R \setminus \mathfrak{p}.$$

4. *The maps*

$$\{\mathfrak{p} \in \text{spec}(R) \mid \mathfrak{p} \cap T = \emptyset\} \rightleftharpoons \text{spec}(T^{-1}R), \quad \mathfrak{p} \mapsto T^{-1}\mathfrak{p} \text{ and } \mathfrak{P} \mapsto j^{-1}(\mathfrak{P})$$

are mutually inverse bijections.

5. *If $\mathfrak{p} \in \text{spec}(R)$, then $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$, and there is an isomorphism $\mathfrak{q}(R/\mathfrak{p}) = (R/\mathfrak{p})_{\mathfrak{p}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.*

PROOF. 1. $j(\mathfrak{a}) = \{\frac{a}{1} \mid a \in \mathfrak{a}\} \subset T^{-1}\mathfrak{a}$, and $T^{-1}\mathfrak{a} \triangleleft T^{-1}R$, hence $\mathfrak{a}T^{-1}R = {}_{T^{-1}R}\langle j(\mathfrak{a}) \rangle \subset T^{-1}\mathfrak{a}$. Conversely, if $\frac{a}{t} \in T^{-1}\mathfrak{a}$, where $t \in T$ and $a \in \mathfrak{a}$, then $\frac{a}{t} = a\frac{1}{t} \in \mathfrak{a}T^{-1}R$.

If $T^{-1}\mathfrak{a} = T^{-1}R$, then there exist $a \in \mathfrak{a}$ and $t \in T$ such that $\frac{a}{t} = \frac{1}{1}$, and thus there is some $s \in T$ such that $sa = st \in \mathfrak{a} \cap T$. Conversely, if $s \in \mathfrak{a} \cap T$, then $\frac{s}{s} = \frac{1}{1} \in T^{-1}\mathfrak{a}$, which implies $T^{-1}\mathfrak{a} = T^{-1}R$.

2. Obviously, $T^{-1}j^{-1}(\mathfrak{A}) = j^{-1}(\mathfrak{A})T^{-1}R \subset \mathfrak{A}$. Conversely, suppose that $\frac{a}{s} \in \mathfrak{A}$, where $a \in R$ and $s \in T$. Then $j(a) = \frac{a}{1} = \frac{s}{1}\frac{a}{s} \in \mathfrak{A}$, hence $\frac{a}{1} \in j^{-1}(\mathfrak{A})$ and $\frac{a}{s} \in T^{-1}j^{-1}(\mathfrak{A})$. Consequently, $\{T^{-1}\mathfrak{a} \mid \mathfrak{a} \triangleleft R\}$ is the set of all ideals of $T^{-1}R$. If $\mathfrak{a} \triangleleft R$ is a finitely generated ideal of R , then $T^{-1}\mathfrak{a}$ is a finitely generated ideal of $T^{-1}R$. Hence, if R is noetherian, then $T^{-1}R$ is also noetherian.

3. $T^{-1}\mathfrak{p}$ is a prime ideal: Let $\frac{a}{s}, \frac{b}{t} \in T^{-1}R$ (where $a, b \in R$ and $s, t \in T$), $\frac{a}{s}\frac{b}{t} \in T^{-1}\mathfrak{p}$ and $\frac{b}{t} \notin T^{-1}\mathfrak{p}$. Then $b \notin \mathfrak{p}$, and $\frac{ab}{st} = \frac{c}{w}$ for some $c \in \mathfrak{p}$ and $w \in T$. Hence there is some $v \in T$ such that $vwab = vstc \in \mathfrak{p}$, and since $vwb \notin \mathfrak{p}$, it follows that $a \in \mathfrak{p}$ and $\frac{a}{s} \in T^{-1}\mathfrak{p}$.

$\mathfrak{p} = j^{-1}(T^{-1}\mathfrak{p})$: Obviously, $\mathfrak{p} \subset j^{-1}(\mathfrak{p}T^{-1}R) = j^{-1}(T^{-1}\mathfrak{p})$. To prove the reverse inclusion, let $a \in j^{-1}(T^{-1}\mathfrak{p})$. Then $j(a) = \frac{a}{1} = \frac{c}{t}$ for some $c \in \mathfrak{p}$ and $t \in T$. Then there is some $s \in T$ such that $sta = sc \in \mathfrak{p}$, and $st \in T \subset R \setminus \mathfrak{p}$ implies $a \in \mathfrak{p}$.

$T^{-1}R \setminus T^{-1}\mathfrak{p} = \{\frac{s}{t} \mid s \in R \setminus \mathfrak{p}, t \in T\}$: It suffices to prove that, for all $a \in R$ and $t \in T$ we have $\frac{a}{t} \in T^{-1}\mathfrak{p}$ if and only if $a \in \mathfrak{p}$. By definition, $a \in \mathfrak{p}$ implies $\frac{a}{t} \in T^{-1}\mathfrak{p}$. Conversely, suppose that $\frac{a}{t} \in T^{-1}\mathfrak{p}$, say $\frac{a}{t} = \frac{c}{s}$, where $c \in \mathfrak{p}$ and $s \in T$. Then there is some $w \in T$ such that $wsa = wtc \in \mathfrak{p}$, and $ws \in T \subset R \setminus \mathfrak{p}$ implies $a \in \mathfrak{p}$.

Finally, we prove that there is a ring isomorphism $\Phi: R_{\mathfrak{p}} \xrightarrow{\sim} (T^{-1}R)_{T^{-1}\mathfrak{p}}$ as asserted. Thus define

$$\Phi: R_{\mathfrak{p}} \rightarrow (T^{-1}R)_{T^{-1}\mathfrak{p}} \quad \text{by} \quad \Phi\left(\frac{a}{t}\right) = \frac{\frac{a}{t}}{\frac{1}{1}} \quad \text{for all } a \in R \text{ and } t \in R \setminus \mathfrak{p}$$

(observe that $t \in R \setminus \mathfrak{p}$ implies $\frac{t}{1} \in T^{-1}R \setminus T^{-1}\mathfrak{p}$). We assert that this definition does not depend on representatives. Indeed, suppose that $\frac{a}{t} = \frac{a'}{t'}$, where $a, a' \in R$ and $t, t' \in R \setminus \mathfrak{p}$. Then there is some $s \in R \setminus \mathfrak{p}$ such that $st'a = sta'$, and since $\frac{s}{1}, \frac{t}{1}, \frac{t'}{1} \in T^{-1}R \setminus T^{-1}\mathfrak{p}$ and $\frac{s}{1} \frac{t'}{1} \frac{a}{1} = \frac{s}{1} \frac{t}{1} \frac{a'}{1}$, we get

$$\frac{\frac{a}{t}}{\frac{1}{1}} = \frac{\frac{a'}{t'}}{\frac{1}{1}}. \quad \text{Since} \quad \frac{\frac{a}{t}}{\frac{v}{st}} = \frac{\frac{at}{st}}{\frac{sv}{st}} = \frac{\frac{at}{sv}}{\frac{1}{1}} = \Phi\left(\frac{at}{sv}\right) \quad \text{for all } a \in R, s, v \in R \setminus \mathfrak{p} \text{ and } t \in T,$$

it follows that Φ is surjective. Obviously, Φ is a ring homomorphism. Suppose that $\frac{a}{t} \in \text{Ker}(\Phi)$, where $a \in R$ and $t \in T$. Then there exists some $\frac{s}{v} \in T^{-1}R \setminus T^{-1}\mathfrak{p}$ (where $s \in R \setminus \mathfrak{p}$ and $v \in T$) such that $\frac{s}{v} \frac{a}{t} = \frac{0}{1}$. Then there is some $w \in R \setminus \mathfrak{p}$ such that $wsa = 0$, and therefore $\frac{a}{t} = \frac{0}{1}$.

4. Obvious by 2. and 3.

5. Let $\mathfrak{p} \in \text{spec}(R)$. Then $\{\mathfrak{a}R_{\mathfrak{p}} \mid \mathfrak{a} \triangleleft R\}$ is the set of all ideals of $R_{\mathfrak{p}}$, and if $\mathfrak{a} \triangleleft R$, then $\mathfrak{a}R_{\mathfrak{p}} \subsetneq R_{\mathfrak{p}}$ is equivalent to $\mathfrak{a} \subset \mathfrak{p}$ and thus to $\mathfrak{a}R_{\mathfrak{p}} \subset \mathfrak{p}R_{\mathfrak{p}}$. Hence $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$. If $\pi: R \rightarrow R/\mathfrak{p}$ denotes the residue class homomorphism, then

$$R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} = (R/\mathfrak{p})_{\mathfrak{p}} = \pi(R \setminus \mathfrak{p})^{-1}R/\mathfrak{p} = (R/\mathfrak{p})^{\bullet-1}R/\mathfrak{p} = \mathfrak{q}(R/\mathfrak{p}). \quad \square$$

Theorem 2.1.8. *Let D be a domain, $K = \mathfrak{q}(D)$ and $T \subset D^{\bullet}$ a multiplicatively closed subset (then $D \subset T^{-1}D \subset K$).*

1. *Let $J, J' \subset K$ be D -submodules. Then $T^{-1}(JJ') = (T^{-1}J)(T^{-1}J')$, and if for every $T^{-1}D$ -submodule $\tilde{J} \subset K$ we set $\tilde{J}_{[T^{-1}D]}^{-1} = \{z \in K \mid z\tilde{J} \subset T^{-1}D\}$, then $T^{-1}J^{-1} \subset (T^{-1}J)_{[T^{-1}D]}^{-1}$, and if J is a finitely generated D -module, then equality holds.*
2. *Let $J \subset K$ be a (D -)invertible fractional ideal. Then $T^{-1}J$ is ($T^{-1}D$ -)invertible.*

PROOF. 1. If $x \in T^{-1}(JJ')$, then there exist $n \in \mathbb{N}$, $t \in T$, $a_1, \dots, a_n \in J$ and $a'_1, \dots, a'_n \in J'$ such that

$$x = \frac{1}{t} \sum_{i=1}^n a_i b_i = \sum_{i=1}^n \frac{a_i}{t} \frac{b_i}{1} \in (T^{-1}J)(T^{-1}J').$$

Conversely, if $x \in (T^{-1}J)(T^{-1}J')$, then

$$x = \sum_{i=1}^n \frac{a_i}{t_i} \frac{a'_i}{t'_i}, \quad \text{where } a_i \in J, a'_i \in J' \text{ and } t_i, t'_i \in T \text{ for all } i \in [1, n], \quad \text{and we set } t = \prod_{i=1}^n t_i t'_i.$$

Then

$$x = \frac{1}{t} \sum_{i=1}^n a_i^* a'_i, \quad \text{where } a_i^* = \left(\prod_{\substack{j=1 \\ j \neq i}}^n t_j t'_j \right) a_i \in J \text{ for all } i \in [1, n],$$

and therefore $x \in T^{-1}(JJ')$.

If $z \in T^{-1}J^{-1}$, then $z = \frac{u}{t}$, where $uJ \subset D$ and $t \in T$. Then $z(T^{-1}J) \subset T^{-1}uJ \subset T^{-1}D$, and therefore $z \in (T^{-1}J)_{[T^{-1}D]}^{-1}$. Assume now that $J = {}_D\langle a_1, \dots, a_n \rangle$ and $z \in (T^{-1}J)_{[T^{-1}D]}^{-1}$. Since $T^{-1}D = {}_{T^{-1}D}\langle a_1, \dots, a_n \rangle$, we obtain $za_i \in T^{-1}D$ for all $i \in [1, n]$, and therefore there exist $c_1, \dots, c_n \in D$

and $t \in T$ such that $za_i = \frac{c_i}{t}$ for all $i \in [1, n]$, and thus $tza_i \in D$ for all $i \in [1, n]$. Thus we obtain $tzJ \subset D$, $tz \in J^{-1}$ and $z = \frac{tz}{t} \in T^{-1}J^{-1}$.

2. Let J be invertible. Then $(T^{-1}J)(T^{-1}J^{-1}) = T^{-1}(JJ^{-1}) = T^{-1}D$, and therefore $T^{-1}J$ is $T^{-1}D$ -invertible. \square

Theorem 2.1.9. *Let R be a commutative ring and M an R -module.*

1. *If $x \in M$, then $x = 0$ if and only if $\frac{x}{1} = \frac{0}{1} \in M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \max(R)$. In particular, $M = \mathbf{0}$ if and only if $M_{\mathfrak{p}} = \mathbf{0}$ for all $\mathfrak{p} \in \text{spec}(R)$.*
2. *Let $f: M \rightarrow N$ be an R -module homomorphism. Then f is a monomorphism [an epimorphism, an isomorphism] if and only if, for all $\mathfrak{p} \in \max(R)$, $f_{\mathfrak{p}}: M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is a monomorphism [an epimorphism, an isomorphism].*
3. *Let R be a domain, $K = \mathfrak{q}(R)$, V a K -vector space and $M \subset V$ an R -submodule. Then $M \subset T^{-1}M \subset V$ for all multiplicatively closed subset $T \subset R^{\bullet}$, and*

$$M = \bigcap_{\mathfrak{p} \in \max(R)} M_{\mathfrak{p}}.$$

PROOF. 1. Clearly, $x = 0$ implies $\frac{x}{1} = \frac{0}{1} \in \mathfrak{p}$ for all $\mathfrak{p} \in \max(R)$. If $x \neq 0$, then $\mathfrak{a} = \text{Ann}_R(x) \subsetneq R$, and there exists some $\mathfrak{p} \in \max(R)$ such that $\mathfrak{a} \subset \mathfrak{p}$. Hence $sx \neq 0$ for all $s \in R \setminus \mathfrak{p}$, and $\frac{x}{1} \neq \frac{0}{1} \in R_{\mathfrak{p}}$.

2. If $\mathfrak{p} \in \max(R)$, then $\text{Ker}(f_{\mathfrak{p}}) = \text{Ker}(f)_{\mathfrak{p}}$ and $\text{Im}(f_{\mathfrak{p}}) = \text{Im}(f)_{\mathfrak{p}}$. Hence the assertion follows by 1.

3. Since $\text{Ann}_R(x) = \mathbf{0}$ for all $x \in M^{\bullet}$, it follows that $M \subset T^{-1}M \subset T^{-1}V = V$, since $T \subset K^{\times}$. By definition

$$M \subset \overline{M} = \bigcap_{\mathfrak{p} \in \max(R)} M_{\mathfrak{p}} \quad \text{and} \quad \overline{M} \subset M_{\mathfrak{p}} \quad \text{for all } \mathfrak{p} \in \max(R).$$

Hence $M_{\mathfrak{p}} = \overline{M}_{\mathfrak{p}}$ and therefore $(\overline{M}/M)_{\mathfrak{p}} = \overline{M}_{\mathfrak{p}}/M_{\mathfrak{p}} = \mathbf{0}$ for all $\mathfrak{p} \in \max(R)$. Hence $\overline{M}/M = \mathbf{0}$ and $\overline{M} = M$. \square

2.2. Valuation domains and Prüfer domains

Throughout, let D be a domain and $K = \mathfrak{q}(D)$.

Definitions and Remarks. Let $\Gamma = (\Gamma, +)$ be an additive abelian group.

1. Let \leq be a total ordering of Γ . Then $\Gamma = (\Gamma, \leq)$ is called an *ordered abelian group* if $a \leq b$ implies $a + c \leq b + c$ for all $a, b, c \in \Gamma$.

If Γ is a totally ordered abelian group, then Γ is torsion-free. Indeed, if $\gamma \in \Gamma$ and $n \in \mathbb{N}$, then $n\gamma \geq \gamma > 0$ if $\gamma > 0$, and $n\gamma \leq \gamma < 0$ if $\gamma < 0$.

Assume that $\Gamma_{>0}$ has no smallest element. If $\gamma \in \Gamma_{>0}$ and $n \in \mathbb{N}$, then there exists some $\delta \in \Gamma_{>0}$ such that $n\delta < \gamma$. Indeed, this is obvious for $n = 1$, and we use induction on n . Suppose that $n \geq 2$, let $\delta_1 \in \Gamma_{>0}$ be such that $(n-1)\delta_1 < \gamma$, and let $\delta \in \Gamma_{>0}$ be such that $\delta < \min\{\delta_1, \gamma - (n-1)\delta_1\}$. Then $n\delta = (n-1)\delta + \delta < (n-1)\delta_1 + \delta < \gamma$.

For an ordered abelian group we consider the extension $\Gamma \cup \{\infty\}$, where $\infty \notin \Gamma$, $\gamma \leq \infty$ and $\gamma + \infty = \infty$ for all $\gamma \in \Gamma \cup \{\infty\}$.

2. Let K be a field and Γ an ordered abelian group. A *valuation* of K with *value group* Γ is a surjective map $v: K \rightarrow \Gamma \cup \{\infty\}$ such that the following assertions hold for all $x, y \in K$:
 - $v(x) = \infty$ if and only if $x = 0$.
 - $v(xy) = v(x) + v(y)$.
 - $v(x + y) \geq \min\{v(x), v(y)\}$.

A *discrete valuation* is a valuation with value group \mathbb{Z} .

If $v: K \rightarrow \Gamma \cup \{\infty\}$ is a valuation, then $v|K^\times: K^\times \rightarrow \Gamma$ is a group epimorphism.

If $x \in \mu(K)$, then $v(x) = 0$. Indeed, if $x \in \mu(K)$, $n \in \mathbb{N}$ and $x^n = 1$, then $0 = v(x^n) = nv(x)$, and thus $v(x) = 0$. In particular, $v(-1) = 0$ and $v(-x) = v(-1) + v(x) = v(x)$ for all $x \in K$.

If $x, y \in K$ and $v(x) \neq v(y)$, then $v(x+y) = \min\{v(x), v(y)\}$. Indeed, let $v(x) < v(y)$. Then $v(x) = v(x+y+(-y)) \geq \min\{v(x+y), v(-y)\} \geq \min\{v(x), v(y)\} = v(x)$, and therefore $\min\{v(x+y), v(y)\} = v(x) < v(y)$, which implies $v(x+y) = v(x)$.

3. Let $v: K \rightarrow \Gamma \cup \{\infty\}$ be a valuation with value group Γ , $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ and $\mathfrak{m}_v = \{x \in K \mid v(x) > 0\}$. Then it is easily checked that \mathcal{O}_v is a local domain with maximal ideal \mathfrak{m}_v , $\mathcal{O}_v \setminus \mathfrak{m}_v = \{x \in K \mid v(x) = 0\} = \mathcal{O}_v^\times = \text{Ker}(v|K^\times)$, $\mathfrak{q}(\mathcal{O}_v) = K$, and v induces an isomorphism $v^*: K^\times/\mathcal{O}_v^\times \xrightarrow{\sim} \Gamma$. Moreover, \mathfrak{m}_v is a principal ideal if and only if $\Gamma_{>0}$ has a smallest element. \mathcal{O}_v is called the *valuation ring* and \mathfrak{m}_v is called the *valuation ideal* of v .
4. D is called a *valuation domain* if $D = \mathcal{O}_v$ for some valuation v of K , and D is called a *discrete valuation domain* or *dv-domain* if $D = \mathcal{O}_v$ for some discrete valuation v of K .
5. Let $v_0: D^\bullet \rightarrow \Gamma_{>0}$ be a surjective map such that the following assertions hold for all $x, y \in D$:
 - $v_0(x) = \infty$ if and only if $x = 0$.
 - $v_0(xy) = v_0(x) + v_0(y)$.
 - $v_0(x+y) \geq \min\{v_0(x), v_0(y)\}$.

Then there exists a unique valuation $v: K \rightarrow \Gamma \cup \{\infty\}$ such that $v|D^\bullet = v_0$. In particular, there exists a unique discrete valuation $\omega: K((X)) \rightarrow \mathbb{Z} \cup \{\infty\}$ such that $\omega|K[[X]] = \text{ord}$. Every $f \in K((X))^\times$ has a unique representation $f = X^{\omega(f)}f_0$, where $f_0 \in K[[X]]^\times$, and $\mathcal{O}_\omega = K[[X]]$.

Theorem 2.2.1.

1. *The following assertions are equivalent:*
 - (a) D is a valuation domain.
 - (b) D is local, and every finitely generated ideal of D is a principal ideal.
 - (c) For all $a, b \in D$, either $a \in bD$ or $b \in aD$.
 - (d) For all $x \in K^\times$, either $x \in D$ or $x^{-1} \in D$.
 - (e) For all D -submodules $A, B \subset K$, either $A \subset B$ or $B \subset A$. In particular, the set of D -submodules of K is a chain with respect to \subset .
 - (f) For all $a, b \in K$, either $a \in bD$ or $b \in aD$.
2. *Let D be a valuation domain.*
 - (a) *Let $D \subset E \subset K$ be a domain. Then E is a valuation domain, and if $\mathfrak{m} = E \setminus E^\times$ is its maximal ideal, then $\mathfrak{p} = \mathfrak{m} \cap D \in \text{spec}(D)$, and $\overline{D} = D_{\mathfrak{p}}$.*
 - (b) *If $\mathfrak{p} \in \text{spec}(D)$, then D/\mathfrak{p} is a valuation domain.*

PROOF. 1. (a) \Rightarrow (b) Let v be a valuation of K such that $D = \mathcal{O}_v$. Then D is local with maximal ideal $\mathfrak{m} = \mathfrak{m}_v = D \setminus D^\times$. Let $\mathfrak{a} = {}_D\langle a_1, \dots, a_n \rangle \subset D$ be a finitely generated ideal. After renumbering if necessary, we may assume that $v(a_1) \leq v(a_2) \leq \dots \leq v(a_n) < \infty$. For all $i \in [2, n]$, it follows that $v(a_1^{-1}a_i) = -v(a_1) + v(a_i) \geq 0$, hence $a_1^{-1}a_i \in D$ and $a_i \in a_1D$. Thus we obtain $\mathfrak{a} = a_1D$.

(b) \Rightarrow (c) We may assume that $a, b \in D^\bullet$. Then $\langle a, b \rangle = aD + bD = dD$ for some $d \in D^\bullet$. Since $a \in dD$ and $b \in dD$, we get $d^{-1}a, d^{-1}b \in D$, and ${}_D\langle d^{-1}a, d^{-1}b \rangle = D$. Hence there exist $u, v \in D$ such that $1 = d^{-1}au + d^{-1}bv$, and therefore $d^{-1}a$ and $d^{-1}b$ cannot both lie in the maximal ideal of D . If $d^{-1}a \in D^\times$, then $Da = Dd = Da + Db \supset Db$. Similarly, if $d^{-1}b \in D^\times$, then $Db \supset Da$.

(c) \Rightarrow (d) Suppose that $x = a^{-1}b \in K^\times$, where $a, b \in D^\bullet$. If $b \in aD$, then $x \in D$, and if $a \in bD$, then $x^{-1} \in D$.

(d) \Rightarrow (e) Let $A, B \subset K$ be D -submodules, $A \not\subset B$ and $a \in A \setminus B$. Then it follows that $B \subset A$. Indeed, if $b \in B^\bullet$, then $bD \subset B$, hence $a \notin bD$ and $b^{-1}a \notin D$, which implies $a^{-1}b \in D$ and $b \in aD \subset A$.

(e) \Rightarrow (f) Obvious.

(f) \Rightarrow (a) Let $\Gamma = K^\times/D^\times$, written additively, that is $aD^\times \boxplus bD^\times = abD^\times$ for all $a, b \in K^\times$. Define \leq on Γ by $aD^\times \leq bD^\times$ if $bD \subset aD$, and note that $aD^\times = bD^\times$ if and only if $aD = bD$. By (f), \leq is a total ordering on Γ , and obviously (Γ, \leq) is an ordered abelian group with $0_\Gamma = D^\times$. Now we define $v: K \rightarrow \Gamma \cup \{\infty\}$ by $v(a) = aD^\times$ if $a \in K^\times$, and $v(0) = \infty$. We assert that v is a valuation. Indeed, if $a, b \in K$, then $v(ab) = v(a) \boxplus v(b)$ by the very definition of \boxplus . For the proof of $v(a+b) \geq \min\{v(a), v(b)\}$ we may assume that $a, b, a+b \in K^\times$ and $v(a) \leq v(b)$. Then $bD \subset aD$, hence $(a+b)D \subset aD$, and $v(a+b) = (a+b)D^\times \geq aD^\times = v(a)$. If $a \in K^\times$, then $v(a) = aD^\times \geq 0_\Gamma = D^\times$ if and only if $a \in D$, and therefore $D = \mathcal{O}_v$.

2. (a) If $x \in K \setminus E$, then $x \notin D$, and thus $x^{-1} \in D \subset E$. Hence E is a valuation domain, and if \mathfrak{m} is its maximal ideal, then $\mathfrak{p} = \mathfrak{m} \cap D \in \text{spec}(D)$, and $D \setminus \mathfrak{p} \subset E \setminus \mathfrak{m} = E^\times$, which implies $D_{\mathfrak{p}} \subset E$. Suppose that there is some $z \in E \setminus D_{\mathfrak{p}}$. Then $z \notin D$, hence $z^{-1} \in D$, and therefore $z^{-1} \in E^\times$. Since $z = (z^{-1})^{-1} \notin D_{\mathfrak{p}}$, it follows that $z^{-1} \in \mathfrak{p} \subset \mathfrak{m}$, a contradiction.

(b) Let $\mathfrak{p} \in \text{spec}(D)$. As the ideals of D form a chain, the same holds true for the ideals of D/\mathfrak{p} , and thus D/\mathfrak{p} is a valuation domain. \square

Theorem 2.2.2. *Let $\mathfrak{p} \in \text{spec}(D)$ and $L \supset K$ an extension field. Then there exists a valuation domain $V \subset L$ with maximal ideal \mathfrak{m} such that $L = \mathfrak{q}(V)$ and $\mathfrak{m} \cap D = \mathfrak{p}$.*

PROOF. The proof depends on the following Lemma.

L. Let $R \subset S$ be commutative rings, $u \in S^\times$ and $\mathfrak{a} \subsetneq R$ an ideal. Then \mathfrak{a} survives in $R[u]$ or in $R[u^{-1}]$, that means, either $\mathfrak{a}R[u] \subsetneq R[u]$ or $\mathfrak{a}R[u^{-1}] \subsetneq R[u^{-1}]$.

We first prove the Theorem using **L**. Let Ω be the set of all intermediate domains $R_{\mathfrak{p}} \subset S \subset L$ satisfying $\mathfrak{p}S \neq S$. The $R_{\mathfrak{p}} \in \Omega$, and we assert that the union of every chain in Ω belongs to Ω . Indeed, let $\Sigma \subset \Omega$ be a chain and $S^* = \bigcup \Sigma$. Then $R_{\mathfrak{p}} \subset S^* \subset L$ is an intermediate domain, and we assume that, contrary to our assertion, $\mathfrak{p}S^* = S^*$. Then there exist $m \in \mathbb{N}$, $a_1, \dots, a_m \in \mathfrak{p}$ and $x_1, \dots, x_m \in S^*$ such that $a_1x_1 + \dots + a_mx_m = 1$. Since Σ is a chain, there exists some $S \in \Sigma$ such that $x_j \in S$ for all $j \in [1, m]$, whence $\mathfrak{p}S = S$, a contradiction.

By Zorn's Lemma, Ω possesses a maximal element V . We assert that V is a valuation domain, and $\mathfrak{q}(V) = L$, and we prove that, for every $x \in L^\times$, either $x \in V$ or $x^{-1} \in V$. Let $x \in L^\times$. Since $\mathfrak{p}V \neq V$, **L** implies $\mathfrak{p}V[x] \neq V[x]$ or $\mathfrak{p}V[x^{-1}] \neq V[x^{-1}]$, and thus $V[x] \in \Omega$ or $V[x^{-1}] \in \Omega$. As V was a maximal element in Ω , this yields $x \in V$ or $x^{-1} \in V$. Let \mathfrak{m} be the maximal ideal of V . Then $\mathfrak{p}V \subset \mathfrak{m}$, and therefore $\mathfrak{p}D_{\mathfrak{p}} \subset \mathfrak{m} \cap D_{\mathfrak{p}} \subsetneq D_{\mathfrak{p}}$. Hence $\mathfrak{m} \cap D_{\mathfrak{p}} = \mathfrak{p}D_{\mathfrak{p}}$, and $\mathfrak{m} \cap D = \mathfrak{m} \cap D_{\mathfrak{p}} \cap D = \mathfrak{p}D_{\mathfrak{p}} \cap D = \mathfrak{p}$.

Proof of L. We assert that every $z \in \mathfrak{a}R[u]$ has a representation in the form

$$z = \sum_{i=0}^n a_i u^i, \quad \text{where } n \in \mathbb{N} \text{ and } a_1, \dots, a_n \in \mathfrak{a}.$$

Indeed, if $z \in \mathfrak{a}R[u]$, then

$$z = \sum_{j=1}^m c_j x_j, \quad \text{where } m \in \mathbb{N}, c_1, \dots, c_m \in \mathfrak{a} \text{ and } x_1, \dots, x_m \in R[u].$$

For all $j \in [1, m]$,

$$x_j = \sum_{i=0}^n b_{j,i} u^i, \quad \text{where } n \in \mathbb{N} \text{ and } b_{j,1}, \dots, b_{j,n} \in R.$$

Hence it follows that

$$z = \sum_{i=0}^n a_i u^i, \quad \text{where } a_i = \sum_{j=1}^m c_j b_{j,i} \in \mathfrak{a}.$$

Assume now that, contrary to our assertion, $\mathfrak{a}R[u] = R[u]$ and $\mathfrak{a}R[u^{-1}] = R[u^{-1}]$. Then there exist relations

$$1 = \sum_{i=0}^n a_i u^i = \sum_{j=0}^m b_j u^{-j}, \quad \text{where } m, n \in \mathbb{N} \text{ and } a_1, \dots, a_n, b_1, \dots, b_m \in \mathfrak{a}.$$

Among all these relations we choose one, for which $m + n$ is minimal, and we assume that $m \leq n$ (otherwise we interchange m and n). Then we obtain

$$(1 - b_0)u^m = \sum_{j=1}^m b_j u^{m-j} \quad \text{and} \quad 1 - b_0 = \sum_{i=0}^n a_i (1 - b_0)u^i = \sum_{i=0}^{n-1} a_i (1 - b_0)u^i + a_n u^{n-m} \sum_{j=1}^m b_j u^{m-j}$$

and therefore

$$1 = [b_0 + a_0(1 - b_0)] + \sum_{i=1}^{n-1} C_i u^i \quad \text{for some } C_1, \dots, C_{n-1} \in \mathfrak{a},$$

contradicting the minimal choice of $m + n$. □

Remarks (Recapitulation: Integrality). Let $R \subset S$ be commutative rings.

1. An element $x \in S$ is called *integral* over R if it satisfies one of the following equivalent conditions:
 - There exists a monoid polynomial $f \in R[X] \setminus R$ such that $f(x) = 0$.
 - There exist $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in R$ such that $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ (such a relation is called an *integral equation* of x over R).
 - $R[x]$ is a finitely generated R -module.
 - There exists a finitely generated R -module $M \subset S$ such that $xM \subset M$ and, for all $g \in R[X]$, $g(x)M = \mathbf{0}$ implies $g(x) = 0$.
2. $\text{cl}_S(R) = \{x \in S \mid x \text{ is integral over } R\}$ is called the *integral closure* of R in S . If $\text{cl}_S(R) = S$, then S is called *integral* over R , and if $\text{cl}_S(R) = R$, then R is called *integrally closed* in S . $\text{cl}_S(R)$ is a subring of S which is integral over R and integrally closed in S .
3. If $T \subset R$ is a multiplicatively closed subset, then $\text{cl}_{T^{-1}S}(T^{-1}R) = T^{-1}\text{cl}_S(R)$, and S is integral over R if and only if $S_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \max(R)$.
4. If $R \subset S \subset \bar{S}$ are commutative rings, then \bar{S} is integral over R if and only if \bar{S} is integral over S and S is integral over R .
5. A domain D is called *integrally closed* if it is integrally closed in $K = \mathfrak{q}(D)$. Every factorial domain is integrally closed, and the intersection of any family of integrally closed domains between D and K is integrally closed. In particular, D is integrally closed if and only if $D_{\mathfrak{p}}$ is integrally closed for every $\mathfrak{p} \in \max(D)$.
6. Let D be an integrally closed domain, $K = \mathfrak{q}(D)$ and L/K an algebraic field extension. Then $S = \text{cl}_L(D)$ is an integrally closed domain, and $L = KS = \mathfrak{q}(S)$. If $x \in L$ and $f \in K[X]$ is the minimal polynomial of x over K , then $x \in S$ if and only if $f \in D[X]$.

Theorem 2.2.3. *Let Ω the set of all valuation domains V such that $D \subset V \subset K$. Then*

$$\text{cl}_K(D) = \bigcap_{V \in \Omega} V.$$

In particular, every valuation domain is integrally closed, and if D is integrally closed, then D is the intersection of all valuation domains V such that $D \subset V \subset K$.

PROOF. We show first that every valuation domain is integrally closed. Let D be a valuation domain with maximal ideal \mathfrak{m} , and assume that $x \in K \setminus D$ is integral over D . Let $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ be an integral equation of x over D . Then $1 = -(a_{n-1}^{-1} + \dots + a_1^{-(n-1)} + a_0^{-n})$, and since $x^{-1} \in \mathfrak{m}$ it follows that $1 \in \mathfrak{m}$, a contradiction.

Now let D be any domain, Ω the set of all valuation domains between D and K , and

$$D' = \bigcap_{V \in \Omega} V \supset D.$$

Then D' is an integrally closed domain, and $D \subset \text{cl}_K(D) \subset \text{cl}_K(D') = D'$. Thus we must prove that every $x \in D'$ is integral over D . Thus suppose that $x \in D'$.

CASE 1: $x^{-1}D[x^{-1}] = D[x^{-1}]$. Then $1 = x^{-1}(a_0 + a_1x^{-1} + \dots + a_nx^{-n})$ for some $n \in \mathbb{N}$ and $a_0, \dots, a_n \in D$, and therefore $x^{n+1} - a_0x^n - a_1x^{n-1} - \dots - a_n = 0$, which shows that x is integral over D .

CASE 2: $x^{-1}D[x^{-1}] \subsetneq D[x^{-1}]$. Let $\mathfrak{p} \in \text{spec}(D[x^{-1}])$ be such that $x^{-1}D[x^{-1}] \subset \mathfrak{p}$. By Theorem 2.2.2, there exists a valuation domain V with maximal ideal \mathfrak{m} such that $D[x^{-1}] \subset V \subset K$ and $\mathfrak{m} \cap D[x^{-1}] = \mathfrak{p}$. Then $V \in \Omega$, $x^{-1} \in \mathfrak{m}$ and therefore $x \notin V$, a contradiction. \square

Theorem 2.2.4. *Suppose that $D \neq K$. Then the following assertions are equivalent:*

- (a) D is a *dv-domain*.
- (b) D is a *noetherian valuation domain*.
- (c) D is a *local principal ideal domain*.
- (d) D is a *factorial domain* and possesses (up to associates) *exactly one prime element*.

PROOF. (a) \Rightarrow (b) Let $v: K \rightarrow \mathbb{Z} \cup \{\infty\}$ be a discrete valuation such that $D = \mathcal{O}_v$. We prove that D is a principal ideal domain. Let $\mathbf{0} \neq \mathfrak{a} \triangleleft D$, $n = \min v(\mathfrak{a}) \in \mathbb{N}_0$ and $n = v(a)$, where $a \in \mathfrak{a}$. Then $aD \subset \mathfrak{a}$, and we assert that equality holds. Indeed, if $x \in \mathfrak{a}$, then $v(x) \geq v(a)$, hence $v(a^{-1}x) = -v(a) + v(x) \geq 0$, and therefore $a^{-1}x \in D$, whence $x \in aD$.

(b) \Rightarrow (c) Being a valuation domain, D is local and every finitely generated ideal is principal. By assumption, D is noetherian and thus every ideal is principal.

(c) \Rightarrow (d) Since D is a principal ideal domain, it follows that D is factorial and every non-zero prime ideal is maximal. Hence the maximal ideal pD of D is the unique non-zero prime ideal, and therefore p is up to associates the only prime element of D .

(d) \Rightarrow (a) Let p be a prime element of D . Then every $x \in K^\times$ has a unique representation $x = p^n u$, where $n \in \mathbb{Z}$, $u \in D^\times$, and we set $v(x) = n$. We define $v(0) = \infty$. Then $v: K \rightarrow \mathbb{Z} \cup \{\infty\}$ is a discrete valuation, and $D = \mathcal{O}_v$. \square

Theorem and Definition 2.2.5.

1. *The following assertions are equivalent:*

- (a) *Every finitely generated non-zero ideal of D is invertible.*
- (b) *For all $\mathfrak{p} \in \text{spec}(D)$, $D_{\mathfrak{p}}$ is a valuation domain.*
- (c) *For all $\mathfrak{p} \in \text{max}(D)$, $D_{\mathfrak{p}}$ is a valuation domain.*

If these conditions are fulfilled, then D is called a *Prüfer domain*. If $D_{\mathfrak{p}}$ is a *dv-domain* for all $\mathbf{0} \neq \mathfrak{p} \in \text{spec}(D)$, then D is called an *almost Dedekind domain*.

2. *If D is a Prüfer domain, then D is integrally closed, and if D is an almost Dedekind domain, then every non-zero prime ideal is maximal.*
3. *Let D be a Prüfer domain and $D \subset E \subset K$ a domain. Then E is a Prüfer domain, and if $\mathfrak{q} \in \text{spec}(E)$, then $\mathfrak{p} = \mathfrak{q} \cap D \in \text{spec}(D)$, and $D_{\mathfrak{p}} = E_{\mathfrak{q}}$, and $\mathfrak{q} = \mathfrak{p}D_{\mathfrak{p}} \cap E$.*
4. *Let D be a Prüfer domain and $\mathfrak{p} \in \text{spec}(D)$. Then D/\mathfrak{p} is a Prüfer domain.*

PROOF. 1. (a) \Rightarrow (b) If $\mathfrak{p} \in \text{spec}(D)$, then $D_{\mathfrak{p}}$ is a local domain, and by Theorem 2.2.1.1(b) it suffices to prove that every finitely generated ideal of $D_{\mathfrak{p}}$ is principal. Let $\mathbf{0} \neq \mathfrak{A} = {}_{D_{\mathfrak{p}}}\langle \frac{a_1}{t_1}, \dots, \frac{a_n}{t_n} \rangle \subset D_{\mathfrak{p}}$ be a finitely generated ideal. If $\mathfrak{a} = {}_D\langle a_1, \dots, a_n \rangle$, then $\mathfrak{a}_{\mathfrak{p}} = {}_{D_{\mathfrak{p}}}\langle a_1, \dots, a_n \rangle = \mathfrak{A}$. Hence $\mathfrak{a} \neq \mathbf{0}$, \mathfrak{a} is invertible, and thus \mathfrak{a} is D -projective. Since $\mathfrak{A} = \mathfrak{a}_{\mathfrak{p}} \cong D_{\mathfrak{p}} \otimes_D \mathfrak{a}$, it follows that \mathfrak{A} is $D_{\mathfrak{p}}$ -projective by Theorem 1.2.5.3, and since $D_{\mathfrak{p}}$ is local, the Corollary to Theorem 2.1.2 implies that \mathfrak{A} is free and thus a principal ideal.

(b) \Rightarrow (c) Obvious.

(c) \Rightarrow (a) Let $\mathbf{0} \neq \mathbf{a}$ be a finitely generated ideal of D , and suppose that \mathbf{a} is not invertible. Then $\mathbf{a}\mathbf{a}^{-1} \subsetneq D$, and thus there is some $\mathfrak{p} \in \max(D)$ such that $\mathbf{a}\mathbf{a}^{-1} \subset \mathfrak{p}$. Now Theorem 2.1.8 implies $\mathfrak{a}_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}})^{-1} = \mathfrak{a}_{\mathfrak{p}}(\mathbf{a}^{-1})_{\mathfrak{p}} = (\mathbf{a}\mathbf{a}^{-1})_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}} \subsetneq D_{\mathfrak{p}}$, and thus $\mathfrak{a}_{\mathfrak{p}}$ is not $D_{\mathfrak{p}}$ -invertible. However, $\mathfrak{a}_{\mathfrak{p}}$ is a finitely generated ideal of $D_{\mathfrak{p}}$, hence principal and thus $D_{\mathfrak{p}}$ -invertible, a contradiction.

2. If D is a Prüfer domain, then $D_{\mathfrak{p}}$ is integrally closed for all $\mathfrak{p} \in \max(D)$. Hence D is integrally closed. If D is an almost Dedekind domain, $\mathbf{0} \neq \mathfrak{p} \in \text{spec}(D)$ and $\mathfrak{m} \in \max(D)$ such that $\mathfrak{p} \subset \mathfrak{m}$, then $\mathbf{0} \neq \mathfrak{p}D_{\mathfrak{m}} \subset \mathfrak{m}D_{\mathfrak{m}}$ are prime ideals. As $D_{\mathfrak{m}}$ is a dv-domain, it follows that $\mathfrak{p}D_{\mathfrak{m}} = \mathfrak{m}D_{\mathfrak{p}}$, and therefore $\mathfrak{p} = \mathfrak{m}$ is maximal.

3. If $\mathfrak{q} \in \text{spec}(E)$, then $\mathfrak{p} = \mathfrak{q} \cap D \in \text{spec}(D)$, and $D \setminus \mathfrak{p} \subset E \setminus \mathfrak{q}$ implies $D_{\mathfrak{p}} \subset E_{\mathfrak{q}}$. Since $D_{\mathfrak{p}}$ is a valuation domain, Theorem 2.2.1.2 implies that $E_{\mathfrak{q}}$ is a valuation domain, $\mathfrak{q}E_{\mathfrak{q}} \cap D_{\mathfrak{p}} \in \text{spec}(D_{\mathfrak{p}})$, and $E_{\mathfrak{q}} = (D_{\mathfrak{p}})_{\mathfrak{q}E_{\mathfrak{q}} \cap D_{\mathfrak{p}}}$. In particular, E is a Prüfer domain. Since $\mathfrak{q}E_{\mathfrak{q}} \cap D_{\mathfrak{p}} \cap D = \mathfrak{q} \cap D = \mathfrak{p} = \mathfrak{p}D_{\mathfrak{p}} \cap D$, it follows that $\mathfrak{q}E_{\mathfrak{q}} \cap D_{\mathfrak{p}} = \mathfrak{p}D_{\mathfrak{p}}$, and therefore $E_{\mathfrak{q}} = (D_{\mathfrak{p}})_{\mathfrak{p}D_{\mathfrak{p}}} = D_{\mathfrak{p}}$. Hence $\mathfrak{p}D_{\mathfrak{p}} = \mathfrak{q}E_{\mathfrak{q}}$, and therefore $\mathfrak{q} = \mathfrak{p}D_{\mathfrak{p}} \cap E$.

4. If $\mathfrak{Q} \in \text{spec}(D/\mathfrak{p})$, then $\mathfrak{Q} = \mathfrak{q}/\mathfrak{p}$ for some prime ideal $\mathfrak{q} \in \text{spec}(D)$ such that $\mathfrak{p} \subset \mathfrak{q}$, and $(D/\mathfrak{p})_{\mathfrak{Q}} = (D/\mathfrak{p})_{\mathfrak{q}} = D_{\mathfrak{q}}/\mathfrak{p}_{\mathfrak{q}}$ is a valuation domain by Theorem 2.2.1. \square

Theorem and Definition 2.2.6. *The following assertions are equivalent:*

- (a) D is a noetherian Prüfer domain.
- (b) D is noetherian, and for all $\mathbf{0} \neq \mathfrak{p} \in \text{spec}(D)$, $D_{\mathfrak{p}}$ is a dv-domain.
- (c) D is noetherian, integrally closed, and every non-zero prime ideal is maximal.
- (d) Every non-zero ideal of D is invertible.

If these conditions are fulfilled, then D is called a *Dedekind domain*.

PROOF. (a) \Rightarrow (b) If $\mathbf{0} \neq \text{spec}(D)$, then $D_{\mathfrak{p}} \neq K$ is a noetherian valuation domain and thus a dv-domain.

(b) \Rightarrow (a) Obvious.

(a) and (b) \Rightarrow (c) Since D is a Prüfer domain, it is integrally closed. By (b), D is an almost Dedekind domain, and thus every non-zero prime ideal is maximal.

(c) \Rightarrow (d) It suffices to prove the following assertions: If $\mathbf{0} \neq \mathbf{a} \triangleleft D$, then

- a.** There exist $r \in \mathbb{N}$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \max(D)$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathbf{a}$.
- b.** If $\mathfrak{p} \in \max(D)$, then $\mathbf{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$.

Suppose that **a.** and **b.** hold, and not every non-zero ideal of D is invertible. Let \mathbf{a} be maximal among not invertible ideals and $\mathfrak{p} \in \max(D)$ such that $\mathbf{a} \subset \mathfrak{p}$. Then $\mathbf{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset D$ by **b.** Hence $\mathfrak{a}\mathfrak{p}^{-1}$ is invertible, and there exists a fractional ideal \mathfrak{b} such that $\mathfrak{a}\mathfrak{p}^{-1}\mathfrak{b} = D$. Hence $\mathfrak{p}^{-1}\mathfrak{b} \subset \mathfrak{a}^{-1}$, and $D = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{b} \subset \mathfrak{a}\mathfrak{a}^{-1} \subset D$ implies $\mathfrak{a}\mathfrak{a}^{-1} = D$, a contradiction.

Proof of a. Assume the contrary. Then there exists a maximal non-zero ideal $\mathbf{a} \subset D$ which does not contain a product of maximal ideal. Since every non-zero prime ideal is maximal, \mathbf{a} is not a prime ideal, and there exist $x, y \in D \setminus \mathbf{a}$ such that $xy \in \mathbf{a}$. Then $\mathbf{a} \subsetneq \mathbf{a} + xD$ and $\mathbf{a} \subsetneq \mathbf{a} + yD$, and there exist $r, s \in \mathbb{N}$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s \in \max(D)$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathbf{a} + xD$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathbf{a} + yD$. It follows that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset (\mathbf{a} + xD)(\mathbf{a} + yD) \subset \mathbf{a} + xyD = \mathbf{a}$, a contradiction. \square [a.]

Proof of b. Since $D \subset \mathfrak{p}^{-1}$, we obtain $\mathbf{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$, and we assume that, contrary to our assertion, $\mathbf{a} = \mathfrak{a}\mathfrak{p}^{-1}$. If $x \in \mathfrak{p}^{-1}$, then $x\mathbf{a} \subset \mathbf{a}$, hence x is integral over D , and therefore $x \in D$. Thus we obtain $\mathfrak{p}^{-1} = D$. Suppose that $0 \neq a \in \mathfrak{p}$, and let $r \in \mathbb{N}$ be minimal such that there exist $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \max(D)$ satisfying $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset aD \subset \mathfrak{p}$ (such an r exists by **a.**). There exist some $i \in [1, r]$ such that $\mathfrak{p}_i \subset \mathfrak{p}$, say $i = 1$. Hence $\mathfrak{p} = \mathfrak{p}_1$, and by the minimal choice of r there exists some $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus aD$. In particular, $a^{-1}b \notin D$ and $b\mathfrak{p} \subset aD$, hence $a^{-1}b\mathfrak{p} \subset D$, and therefore $a^{-1}b \in \mathfrak{p}^{-1} \setminus D$. \square [b.]

(d) \Rightarrow (a) Obvious, since every invertible ideal is finitely generated. \square

2.3. Integer-valued polynomials

Throughout, let D be a domain and $K = \mathfrak{q}(D)$.

Definition. The domain

$$\text{Int}(D) = \{f \in K[X] \mid f(D) \subset D\}$$

is called the *domain of integer-valued polynomials* over D , and for an ideal $\mathfrak{a} \subset D$, we set

$$\text{Int}(D, \mathfrak{a}) = \{f \in K[X] \mid f(D) \subset \mathfrak{a}\}.$$

Then $D[X] \subset \text{Int}(D) \subset K[X]$, $\text{Int}(D) \cap K = D$, $\text{Int}(D, \mathfrak{a}) \subset \text{Int}(D)$ is an ideal, and $\text{Int}(D, \mathfrak{a}) \cap K = \mathfrak{a}$.

Theorem 2.3.1. *Let $T \subset D^\bullet$ be a multiplicatively closed subset.*

1. *If $f \in K[X]$, then $T^{-1}D \langle f(D) \rangle = T^{-1}D \langle f(T^{-1}D) \rangle$.*
2. *$T^{-1}\text{Int}(D) \subset \text{Int}(T^{-1}D)$, and if D is noetherian, then equality holds.*

PROOF. 1. If $f \in K[X]$, then obviously $f(D) \subset f(T^{-1}D) \subset T^{-1}D \langle f(T^{-1}D) \rangle$, and therefore it follows that $T^{-1}D \langle f(D) \rangle \subset T^{-1}D \langle f(T^{-1}D) \rangle$. Hence it suffices to prove that $f(T^{-1}D) \subset T^{-1}D \langle f(D) \rangle$, and we use induction on $n = \deg(f)$. If f is constant, there is nothing to do. Thus suppose that $n > 0$ and the assertion holds for all polynomials of smaller degree. Suppose that $a \in D$, $t \in T$, and consider the polynomial $g = t^n f - f(tX) \in K[X]$. Then $\deg(g) < n$, and by the induction hypothesis we get $g(T^{-1}D) \subset T^{-1}D \langle g(D) \rangle \subset T^{-1}D \langle f(D) \rangle$. Hence it follows that

$$t^n f\left(\frac{a}{t}\right) = g\left(\frac{a}{t}\right) + f(a) \in g(T^{-1}D) + f(D) \subset T^{-1}D \langle f(D) \rangle, \quad \text{and thus} \quad f\left(\frac{a}{t}\right) \in T^{-1}D \langle f(D) \rangle.$$

2. If $f \in \text{Int}(D)$ and $t \in T$, then $(t^{-1}f)(T^{-1}D) \subset T^{-1}D \langle f(T^{-1}D) \rangle = T^{-1}D \langle f(D) \rangle \subset T^{-1}D$ by 1., and therefore $t^{-1}f \in \text{Int}(T^{-1}D)$.

Let now D be noetherian, $f \in \text{Int}(T^{-1}D)$ and $C \subset K$ the D -module generated by the coefficients of f . Then $D \langle f(D) \rangle \subset T^{-1}D \cap C$ is a finitely generated submodule of $T^{-1}D$, and therefore there exists some $t \in T$ such that $tf(D) \subset D$, hence $tf \in \text{Int}(D)$ and $f \in T^{-1}\text{Int}(D)$. \square

Theorem 2.3.2.

1. *Let $f \in K[X]$, $\deg(f) = n \in \mathbb{N}$ and $a_0, \dots, a_n \in D$ such that $f(a_i) \in D$ for all $i \in [0, n]$. If*

$$d = \prod_{0 \leq i < j \leq n} (a_i - a_j), \quad \text{then} \quad df \in D[X].$$

2. *Let $\mathfrak{p} \in \text{spec}(D)$ be a prime ideal such that D/\mathfrak{p} is infinite. Then $\text{Int}(D)_{\mathfrak{p}} = \text{Int}(D_{\mathfrak{p}}) = D_{\mathfrak{p}}[X]$.*
3. *Let $\Omega \subset \text{spec}(D)$ be a set of prime ideals such that $|D/\mathfrak{p}| = \infty$ for all $\mathfrak{p} \in \Omega$.*

$$\text{Then} \quad D = \bigcap_{\mathfrak{p} \in \Omega} D_{\mathfrak{p}} \quad \text{implies} \quad \text{Int}(D) = D[X].$$

PROOF. 1. If

$$f = \sum_{\nu=0}^n c_{\nu} X^{\nu}, \quad \text{then} \quad \sum_{\nu=0}^n c_{\nu} a_i^{\nu} = f(a_i) \quad \text{for all } i \in [0, n], \quad \text{and} \quad d = \det(a_i^{\nu})_{i, \nu \in [0, n]}.$$

By Cramer's rule, it follows that $dc_{\nu} \in D$ for all $\nu \in [0, n]$, and thus $df \in D[X]$.

2. It suffices to prove that $\text{Int}(D) \subset D_{\mathfrak{p}}[X]$.

Indeed, then $D[X] \subset \text{Int}(D) \subset D_{\mathfrak{p}}[X]$ implies $D_{\mathfrak{p}}[X] = D[X]_{\mathfrak{p}} \subset \text{Int}(D)_{\mathfrak{p}} \subset D_{\mathfrak{p}}[X]$ and thus $\text{Int}(D)_{\mathfrak{p}} = D_{\mathfrak{p}}[X] \subset \text{Int}(D_{\mathfrak{p}})$. Now we replace (D, \mathfrak{p}) by $(D_{\mathfrak{p}}, \mathfrak{p}D_{\mathfrak{p}})$ and observe that $(D_{\mathfrak{p}})_{\mathfrak{p}D_{\mathfrak{p}}} = D_{\mathfrak{p}}$ and $D_{\mathfrak{p}}/\mathfrak{p}D_{\mathfrak{p}} = \mathfrak{q}(D/\mathfrak{p})$ is infinite. Hence we get $\text{Int}(D_{\mathfrak{p}}) \subset D_{\mathfrak{p}}[X]$ and are done.

Thus let $f \in \text{Int}(D)$ and $n = \deg(f) \in \mathbb{N}$. Then there exist $a_0, \dots, a_n \in D$ such that $a_i - a_j \notin \mathfrak{p}$ for all $i, j \in [0, n]$ such that $i \neq j$. Then

$$d = \prod_{0 \leq i < j \leq n} (a_i - a_j) \in D \setminus \mathfrak{p},$$

$df \in D[X]$ by 1., and thus $f \in D_{\mathfrak{p}}[X]$.

3. By 2., it follows that

$$\text{Int}(D) \subset \bigcap_{\mathfrak{p} \in \Omega} D_{\mathfrak{p}}[X] = D[X]. \quad \square$$

Theorem and Definition 2.3.3. An ideal $\mathfrak{a} \subset D$ is called a *conductor ideal* if $\mathfrak{a} = xD \cap D$ for some $x \in K^\times$. By definition, every principal ideal is a conductor ideal.

1. If $x \in K$, then $xD \cap D = D$ if and only if $x \neq 0$ and $x^{-1} \in D$.
2. Let $\mathfrak{a} \subsetneq D$ be an ideal which is maximal among proper conductor ideals. Then \mathfrak{a} is a prime ideal.
3. If $\mathfrak{a} \subsetneq D$ is a conductor ideal such that D/\mathfrak{a} is finite, then $D[X] \subsetneq \text{Int}(D)$.
4. If D is noetherian and $D[X] \subsetneq \text{Int}(D)$, then there exists some $\mathfrak{p} \in \text{spec}(D)$ such that D/\mathfrak{p} is finite and \mathfrak{p} is a conductor ideal.
5. Let D be a valuation domain with maximal ideal \mathfrak{m} . Then $D[X] \subsetneq \text{Int}(D)$ if and only if \mathfrak{m} is principal and D/\mathfrak{m} is finite.

PROOF. 1. If $x \in K$, then $xD \cap D = D$ if and only if $D \subset xD$, and this is equivalent to $x \neq 0$ and $x^{-1} \in x^{-1}D \subset D$.

2. Suppose that $\mathfrak{a} = xD \cap D$ for some $x \in K^\times$. Let $a, b \in D^\bullet$ be such that $ab \in \mathfrak{a}$ and $a \notin \mathfrak{a}$. Since $\mathfrak{a} \subset xD \subset b^{-1}xD$ and $a \in b^{-1}\mathfrak{a} \subset b^{-1}xD$, it follows that $\mathfrak{a} \subsetneq \mathfrak{a} + aD \subset b^{-1}xD \cap D$. By the maximality of \mathfrak{a} , we obtain $b^{-1}xD = D$, hence $xD = bD$, and $b \in xD = \mathfrak{a}$.

3. Let $\mathfrak{a} \subsetneq D$ be a conductor ideal such that D/\mathfrak{a} is finite, and let $x \in K^\times$ be such that $\mathfrak{a} = xD \cap D$. Let $\{u_1, \dots, u_r\} \subset D$ be a set of representatives for D/\mathfrak{a} , and set $f = x^{-1}(X - u_1) \cdots (X - u_r) \in K[X]$. Then $f(D) \subset x^{-1}\mathfrak{a} \subset D$, hence $f \in \text{Int}(D)$, and $\mathfrak{a} \subsetneq D$ implies $x^{-1} \notin D$ and therefore $f \notin D[X]$.

4. Let D be noetherian and $f \in \text{Int}(D) \setminus D[X]$. Then f has a coefficient $x \in K \setminus D$, and the conductor ideal $x^{-1}D \cap D$ is contained in a maximal conductor ideal \mathfrak{p} which is a prime ideal ideal by 2. We assert that D/\mathfrak{p} is finite. Assume the contrary. Then $\text{Int}(D) \subset D_{\mathfrak{p}}[X]$ by Theorem 2.3.2.2, and therefore there exists some $t \in D \setminus \mathfrak{p}$ such that $tf \in D[X]$. In particular, it follows that $tx \in D$ and $t \in x^{-1}D \cap D = \mathfrak{p}$, a contradiction.

5. If \mathfrak{m} is principal and D/\mathfrak{m} is finite, then $D[X] \subsetneq \text{Int}(D)$ by 3. If $|D/\mathfrak{m}| = \infty$, then Theorem 2.3.2.2 implies $\text{Int}(D) \subset D_{\mathfrak{m}}[X] = D[X]$. Thus suppose that \mathfrak{m} is not principal, and yet there is some $f \in \text{Int}(D) \setminus D[X]$. Let $v: K \rightarrow \Gamma \cup \{\infty\}$ be the valuation defining D , E the set of all coefficients of f and $\min\{v(c) \mid c \in E\} = -\gamma$, where $\gamma \in \Gamma_{>0}$. Since \mathfrak{m} is not principal, $\Gamma_{>0}$ has no smallest element, and thus there exist $a_0, \dots, a_n \in \mathfrak{m}$ such that $v(a_0), \dots, v(a_n)$ are distinct, and $\binom{n}{2}v(a_i) < \gamma$ for all $i \in [0, n]$.

$$\text{If } d = \prod_{1 \leq i < j \leq n} (a_j - a_i), \text{ then } df \in D[X] \text{ by Theorem 2.3.2.1,}$$

hence $v(cd) = v(c) + v(d) \geq 0$ for all $c \in E$, and therefore $v(d) \geq \gamma$. On the other hand,

$$v(d) = \sum_{1 \leq i < j \leq n} v(a_j - a_i) = \sum_{1 \leq i < j \leq n} \min\{v(a_j), v(a_i)\} < \gamma, \quad \text{a contradiction.} \quad \square$$

Theorem 2.3.4. Let $\mathfrak{P} \in \text{spec}(\text{Int}(D))$ be such that $\mathfrak{P} \cap D = \mathfrak{m} \in \text{max}(D)$ is principal and D/\mathfrak{m} is finite. Then $\mathfrak{P} \in \text{max}(\text{Int}(D))$, $\text{Int}(D, \mathfrak{m}) \subset \mathfrak{P}$, and the inclusion $D \hookrightarrow \text{Int}(D)$ induces an isomorphism $D/\mathfrak{m} \xrightarrow{\sim} \text{Int}(D)/\mathfrak{P}$ (we identify).

PROOF. Let $\mathfrak{m} = tD$ and $\{u_1, \dots, u_r\}$ be a set of representatives of D/\mathfrak{m} . If $f \in \text{Int}(D, \mathfrak{m})$, then $f(D) \subset tD$, hence $f \in t \text{Int}(D) = \mathfrak{m} \text{Int}(D) \subset \mathfrak{P}$, and thus $\text{Int}(D, \mathfrak{m}) \subset \mathfrak{P}$. For every $f \in \text{Int}(D)$, we have

$$\prod_{i=1}^r (f - u_i) \in \text{Int}(D, \mathfrak{m}) \subset \mathfrak{P},$$

hence $f - u_i \in \mathfrak{P}$ for some $i \in [1, r]$, and therefore $\text{Int}(D)/\mathfrak{P} = \{u_1 + \mathfrak{P}, \dots, u_r + \mathfrak{P}\}$. \square

Remarks (Topology of discrete valuation domains). Let D be a dv-domain, $v: K \rightarrow \mathbb{Z} \cup \{\infty\}$ the defining valuation of K and $t \in K$ such that $v(t) = 1$.

1. $D = \{x \in K \mid v(x) \geq 0\}$, and $\mathfrak{m} = tD = \{x \in K \mid v(x) > 0\}$ is the unique maximal ideal of D . Every $z \in K^\times$ has a unique representation $z = t^k u$, where $k \in \mathbb{Z}$ and $u \in D^\times$ (in fact, $k = v(z)$). In particular, D is factorial, and (up to associates) t is the unique prime element of D .
2. Fix some $\rho \in (0, 1)$, and let $|\cdot| = |\cdot|_{v, \rho}: K \rightarrow \mathbb{R}_{\geq 0}$ the absolute value with basis ρ associated with v , defined by $|a| = \rho^{v(a)}$ for all $a \in K$ (where $\rho^\infty = 0$). Then $|K| = \langle \rho \rangle \cup \{0\}$, and the map $d: K \times K \rightarrow \mathbb{R}_{> 0}$, defined by $d(x, y) = |x - y| = \rho^{v(x-y)}$, is a metric. The topology induced on K by d is called the v -topology. If $a \in K$ and $n \in \mathbb{N}$, then

$$\begin{aligned} a + \mathfrak{m}^n &= a + t^n D = \{x \in K \mid v(x - a) \geq n\} = \{x \in K \mid d(x, a) \leq \rho^n\} \\ &= \{x \in K \mid v(x - a) > n - 1\} = \{x \in K \mid d(x, a) < \rho^{n-1}\}. \end{aligned}$$

Hence $\{a + \mathfrak{m}^n \mid n \in \mathbb{N}\}$ is a fundamental system of neighborhoods of a , and the v -topology does not depend on ρ . Since $||x| - |y|| \leq |x - y|$ for all $x, y \in K$, then map $|\cdot|: K \rightarrow \langle \rho \rangle \cup \{0\} \hookrightarrow \mathbb{R}_{\geq 0}$ is uniformly continuous, and therefore the sets $a + \mathfrak{m}^n$ for $a \in K$ and $n \in \mathbb{N}_0$ are clopen.

We endow $\mathbb{Z} \cup \{\infty\}$ with the topology induced by the extended real line $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$. Then $\{a\}$ is open for every $a \in \mathbb{Z}$, and the sets $N_n = \{g \in \mathbb{N} \mid g \geq n\}$ for $n \in \mathbb{N}$ are a fundamental system of neighborhoods of ∞ . The map $\theta: \mathbb{Z} \cup \{\infty\} \rightarrow \langle \rho \rangle \cup \{\infty\}$ is a homeomorphism, and therefore $v = \theta^{-1} \circ |\cdot|: K \rightarrow \mathbb{Z} \cup \{\infty\}$ is continuous.

Let $(x_n)_{n \geq 0}$ be a sequence in K and $x \in K$. Then $(x_n)_{n \geq 0} \rightarrow x$ if and only if $(|x_n - x|)_{n \geq 0} \rightarrow 0$ if and only if $(v(x_n - x))_{n \geq 0} \rightarrow \infty$, and then either $(x_n)_{n \geq 0} \rightarrow 0$ and $v(x_n)_{n \geq 0} \rightarrow \infty$, or $v(x_n) = v(x)$ for all $n \gg 1$. If $x, y \in K$ and $(x_n)_{n \geq 0}, (y_n)_{n \geq 0}$ are sequences in K such that $(x_n)_{n \geq 0} \rightarrow x$ and $(y_n)_{n \geq 0} \rightarrow y$, then $(x_n + y_n)_{n \geq 0} \rightarrow x + y$, $(x_n y_n)_{n \geq 0} \rightarrow xy$, and if $x \neq 0$, then $x_n \neq 0$ for all $n \gg 1$, and $(x_n^{-1})_{n \gg 1} \rightarrow x^{-1}$. Hence K is a topological field under the v -topology.

For every $n \in \mathbb{N}$, there is an isomorphism $D/\mathfrak{m} \xrightarrow{\sim} \mathfrak{m}^n/\mathfrak{m}^{n+1}$, given by $u + \mathfrak{m} \mapsto t^n u + \mathfrak{m}^{n+1}$. By induction on n , we obtain $|D/\mathfrak{m}^n| = |D/\mathfrak{m}|^n$ for all $n \in \mathbb{N}$.

3. A sequence $(a_n)_{n \geq 0}$ in K is a Cauchy sequence if and only if $(v(a_{n+1} - a_n))_{n \geq 0} \rightarrow \infty$. Indeed, if $m > n \geq 0$, then

$$v(a_m - a_n) = v\left(\sum_{j=n}^{m-1} (a_{j+1} - a_j)\right) \geq \min\{v(a_{j+1} - a_j) \mid j \in [n, m-1]\} \rightarrow \infty.$$

Every convergent sequence is a Cauchy sequence, and K is called *complete* if every Cauchy sequence in K converges. If $(a_n)_{n \geq 0}$ is a Cauchy sequence, then either $(v(a_n))_{n \geq 0} \rightarrow \infty$ or $(v(a_n))_{n \geq 0}$ is ultimately constant, and in any case there exists some $c \in D^\bullet$ such that $ca_n \in D$ for all $n \geq 0$. Then $(ca_n)_{n \geq 0}$ is also a Cauchy sequence, and $(ca_n)_{n \geq 0}$ converges if and only if $(a_n)_{n \geq 0}$ converges. Hence K is complete if and only if every Cauchy sequence in D converges, and then we call D a *complete dv-domain*.

4. Let K be complete and $(a_n)_{n \geq 0}$ is a sequence in K . Then

$$\sum_{n \geq 0} a_n \text{ converges if and only if } (a_n)_{n \geq 0} \rightarrow 0.$$

Let R be a set of representatives for $D/\mathfrak{m} = D/tD$. Then every $a \in D$ has a unique representation

$$a = \sum_{n=0}^{\infty} a_n t^n, \quad \text{where } a_n \in R \text{ for all } n \geq 0.$$

If R is equipped with the discrete topology, then the map

$$\Theta: R^{\mathbb{N}_0} \rightarrow D, \quad \text{defined by } \Theta((a_n)_{n \geq 0}) = \sum_{n=0}^{\infty} a_n t^n,$$

is a homeomorphism. In particular, if D/\mathfrak{m} is finite, then D is compact by Tychonoff's Theorem.

5. A field \widehat{K} with a discrete valuation $\widehat{v}: \widehat{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ is called a *completion* of K if \widehat{K} is complete, $K \subset \widehat{K}$ is a dense subfield and $\widehat{v}|_K = v$. Then $\widehat{D} = \{x \in \widehat{K} \mid \widehat{v}(x) \geq 0\}$ is a complete dv-domain, \widehat{D} is the (topological) closure of D in \widehat{K} , and if $t \in D$ is such that $v(t) = 1$, then $\widehat{\mathfrak{m}} = t\widehat{D}$ is the maximal ideal of \widehat{D} . For every $n \in \mathbb{N}$, $\widehat{\mathfrak{m}}^n = t^n \widehat{D} = \{x \in \widehat{D} \mid \widehat{v}(x) \geq n\}$ is the (topological) closure of \mathfrak{m}^n , $\mathfrak{m}^n = \widehat{\mathfrak{m}}^n \cap D$, and the inclusion $D \hookrightarrow \widehat{D}$ induces an isomorphism $D/\mathfrak{m}^n \xrightarrow{\sim} \widehat{D}/\widehat{\mathfrak{m}}^n$ (we identify these residue class rings). We call \widehat{D} a *completion* of D .

Every discrete valued field has a completion which is unique up to a unique isomorphism. Explicitly, if $(\widehat{K}, \widehat{v})$ and $(\widetilde{K}, \widetilde{v})$ are completions of (K, v) , then there is a unique isomorphism $\Phi: \widehat{K} \rightarrow \widetilde{K}$ such that $\Phi|_K = \text{id}_K$ and $\widetilde{v} \circ \Phi = \widehat{v}$.

Definitions and Remarks. Let D be a dv-domain with maximal ideal $\mathfrak{m} = tD$, $|D/\mathfrak{m}| = q \in \mathbb{N}$ and $v: K \rightarrow \mathbb{Z} \cup \{\infty\}$ the defining valuation. For $g \in \mathbb{Z}$, we define $\text{ord}_q(g) = \{\sup\{n \in \mathbb{N}_0 \mid q^n \mid g\} \in \mathbb{N}_0 \cup \{\infty\}\}$.

1. A sequence $(u_n)_{n \geq 0}$ in D is called *well distributed* if $v(u_m - u_n) = \text{ord}_q(m - n)$ for all $m, n \in \mathbb{N}_0$.

If $(u_n)_{n \geq 0}$ is well distributed and $k \in \mathbb{N}_0$, then $(u_{k+n})_{n \geq 0}$ is also well distributed, and, for every $r \in \mathbb{N}$, the set $\{u_i \mid i \in [k, k + q^r - 1]\} \subset D$ is a set of representatives for D/\mathfrak{m}^r .

Proof. Let $k \in \mathbb{N}_0$ and $r \in \mathbb{N}$. By the very definition, $(u_{k+n})_{n \geq 0}$ is well distributed. If $i, j \in [k, k + q^r - 1]$ and $i \neq j$, then $0 < |i - j| < q^r$, hence $\text{ord}_q(i - j) < r$ and therefore $v(u_i - u_j) < r$, which implies $u_i \not\equiv u_j \pmod{\mathfrak{m}^r}$. Since $|[k, k + q^r - 1]| = q^r = |D/\mathfrak{m}^r|$, it follows that $\{u_i \mid i \in [k, k + q^r - 1]\} \subset D$ is a set of representatives for D/\mathfrak{m}^r . \square

2. Let $\{u_0, \dots, u_{q-1}\} \subset D$ be a set of representatives for D/\mathfrak{m} . For $n \in \mathbb{N}$, let

$$n = \sum_{i=0}^{\infty} n_i q^i, \quad \text{where } n_i \in [0, q-1] \text{ for all } i \geq 0, \text{ and } n_i = 0 \text{ for almost all } i \geq 0$$

be the q -adic digit expansion, and set

$$u_n = \sum_{i=0}^{\infty} u_{n_i} t^i.$$

If $n_i = 0$ for all $i \geq l$, then

$$\sum_{i \geq 0} u_{n_i} t^i = \sum_{i=0}^{l-1} u_{n_i} t^i + \frac{u_0 t^l}{t-1} \in D.$$

The sequence $(u_n)_{n \geq 0}$ is well distributed.

Proof. Let $m, n \in \mathbb{N}_0$. We must prove that $v(u_m - u_n) = \text{ord}_q(m - n)$, and we may assume that $m \neq n$. Then

$$m - n = \sum_{i=0}^{\infty} (m_i - n_i) q^i \quad \text{and} \quad u_m - u_n = \sum_{i=0}^{\infty} (m_i - n_i) t^i$$

If $k = \min\{i \in \mathbb{N}_0 \mid m_i \neq n_i\}$, then $m_i - n_i \not\equiv 0 \pmod{q}$, and $v(u_m - u_n) = k = \text{ord}_q(m - n)$. \square

3. For $n \in \mathbb{N}_0$, we define

$$\mathfrak{w}_q(n) = \sum_{l=1}^n \text{ord}_q(n), \quad \text{and we assert that} \quad \mathfrak{w}_q(n) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{q^k} \right\rfloor.$$

(note that $\mathfrak{w}_q(n) = \mathfrak{v}_q(n!)$ if $q \in \mathbb{P}$). For all $m, n \in \mathbb{N}_0$, we have $\mathfrak{w}_q(m+n) \geq \mathfrak{w}_q(m) + \mathfrak{w}_q(n)$.

Proof. For $n = 0$, there is nothing to do. Suppose that $n \in \mathbb{N}$. For $k \in \mathbb{N}_0$,

$$\left\lfloor \frac{n}{q^k} \right\rfloor \quad \text{is the number of integers } l \in [1, n] \text{ such that } q^k \mid l,$$

and therefore

$$\left\lfloor \frac{n}{q^k} \right\rfloor - \left\lfloor \frac{n}{q^{k+1}} \right\rfloor = |\{l \in [1, n] \mid \text{ord}_q(l) = k\}|.$$

Hence we obtain

$$\sum_{l=0}^n \text{ord}_q(l) = \sum_{k=1}^{\infty} k \left(\left\lfloor \frac{n}{q^k} \right\rfloor - \left\lfloor \frac{n}{q^{k+1}} \right\rfloor \right) = \sum_{k=1}^{\infty} k \left\lfloor \frac{n}{q^k} \right\rfloor - \sum_{k=1}^{\infty} (k-1) \left\lfloor \frac{n}{q^k} \right\rfloor = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{q^k} \right\rfloor.$$

For $x, y \in \mathbb{R}$, we have $\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$. If $m, n \in \mathbb{N}_0$, then

$$\mathfrak{w}_q(m+n) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{m+n}{q^k} \right\rfloor \geq \sum_{k=1}^{\infty} \left\lfloor \frac{m}{q^k} \right\rfloor + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{q^k} \right\rfloor = \mathfrak{w}_q(m) + \mathfrak{w}_q(n) \right).$$

Theorem and Definition 2.3.5. *Let D be a dv-domain with maximal ideal \mathfrak{m} , $|D/\mathfrak{m}| = q < \infty$, and let $(u_n)_{n \geq 0}$ be a well distributed sequence in D . For $n \geq 0$, define*

$$g_n = \prod_{i=0}^{n-1} (X - u_i) \in D[X] \quad \text{and} \quad f_n = \frac{g_n}{g_n(u_n)} = \prod_{i=0}^{n-1} \frac{X - u_i}{u_n - u_i} \in K[X] \quad (f_0 = 1).$$

1. For all $x \in D$ and $n \in \mathbb{N}$ we have $v(g_n(x)) \geq v(g_n(u_n)) = \text{ord}_q(n!)$.
2. $\text{Int}(D)$ is a free D -module with basis $(f_n)_{n \geq 0}$.
 $(f_n)_{n \geq 0}$ is called the *regular basis* associated with the well distributed sequence $(u_n)_{n \geq 0}$.
3. Let $f \in \text{Int}(D)$, $\deg(f) < q^h$ for some $h \in \mathbb{N}$ and $a, b \in D$. Then $v(f(a) - f(b)) \geq v(a-b) - h + 1$.
In particular, f is uniformly continuous on D .

PROOF. 1. Let $x \in D$, $n \in \mathbb{N}$, and assume first that $x \notin \{u_0, \dots, u_{n-1}\}$. Then $g_n(x) \neq 0$, we set $v(g_n(x)) = s \in \mathbb{N}_0$ and let $m \in \mathbb{N}$ be such that $u_m \equiv x \pmod{\mathfrak{m}^{s+1}}$. Then $g_n(u_m) - g_n(x) = (u_m - x)h(x)$ for some $h \in D[X]$, which implies $v(g_n(u_m) - g_n(x)) \geq v(u_m - x) > s = v(g_n(x))$, hence $v(g_n(u_m)) = s$ and thus $m \geq n$. Now we calculate

$$\begin{aligned} v(g_n(x)) &= v(g_n(u_m)) = \sum_{k=0}^{n-1} v(u_m - u_k) = \sum_{k=0}^{n-1} \text{ord}_q(m - k) \\ &= \sum_{k=0}^m \text{ord}_q(k) - \sum_{k=0}^{m-n} \text{ord}_q(k) = \mathfrak{w}_q(m) - \mathfrak{w}_q(m-n) \geq \mathfrak{w}_q(n) \end{aligned}$$

with equality if $m = n$. In particular, it follows that $v(g_n(x)) \geq v(g_n(u_n)) = \mathfrak{w}_q(n)$, and obviously this also holds for $x \in \{u_0, \dots, u_{n-1}\}$ since then $g_n(x) = 0$.

2. By 1. we obtain $v(f_n(x)) = v(g_n(x)) - v(g_n(u_n)) \geq 0$ for all $x \in D$, hence $f_n(D) \subset D$ and thus $f_n \in \text{Int}(D)$. Since $\deg(f_n) = n$, it follows that $(f_n)_{n \geq 0}$ is a K -basis of $K[X]$. If $f \in \text{Int}(D)$, then

$$f = \sum_{n \geq 0} c_n f_n, \quad \text{where } c_n \in K \text{ for all } n \geq 0, \text{ and } c_n = 0 \text{ for almost all } n \geq 0,$$

and prove by induction on n that $c_n \in D$ for all $n \geq 0$. Thus suppose that $n \geq 0$ and $c_i \in D$ for all $i \in [0, n-1]$. Then

$$g = f - \sum_{i=0}^{n-1} c_i f_i = \sum_{i=n}^{\infty} c_i f_i \in \text{Int}(D), \quad \text{and} \quad g(u_n) = c_n f_n(u_n) = c_n \in D.$$

3. We assume that $u_0 = 0$, and we set $g = f(b+X) - f(b)$ and $d = a - b$. Then $g \in \text{Int}(D)$, $\deg(g) = \deg(f) < q^h$ and $f(a) - f(b) = g(d)$. Hence we must prove that $v(g(d)) \geq v(d) - h + 1$. By 2.,

$$g = \sum_{n=0}^{\infty} c_n f_n, \quad \text{where} \quad c_n \in D \text{ for all } n \geq 0, \text{ and } c_n = 0 \text{ for all } n \geq q^h.$$

Then $c_0 = g(u_0) = g(0) = 0$, and therefore $v(g(d)) \geq \min\{v(f_n(d)) \mid n \in [1, q^h - 1]\}$. Hence it suffices to prove that $v(f_n(d)) \geq v(d) - h + 1$ for all $n \in [1, q^h - 1]$. If $n \in [1, q^h - 1]$, then

$$f_n(d) = \prod_{i=0}^{n-1} \frac{d - u_i}{u_n - u_i} = \frac{d}{u_n} \prod_{i=1}^{n-1} \frac{d - u_i}{u_n - u_i}.$$

Since $(u_{i+1})_{i \geq 0}$ is a well distributed sequence, it follows by 1. that

$$\tilde{f}_n = \prod_{i=1}^{n-1} \frac{X - u_i}{u_n - u_i} \in \text{Int}(D), \quad \text{and therefore} \quad v(f_n(d)) = v(d) - v(u_n) + v(\tilde{f}_n(d)) \geq v(d) - v(u_n).$$

Since $v(u_n) = v(u_n - u_0) = \text{ord}_q(n) \leq h - 1$, the assertion follows. \square

Theorem 2.3.6 (Stone-Weierstrass Theorem for integer-valued polynomials). *Let D be a dv -domain with maximal ideal $\mathfrak{m} = tD$ and $|D/\mathfrak{m}| = q < \infty$. Let \widehat{D} be a completion of D , $\widehat{\mathfrak{m}} = t\widehat{D}$ its maximal ideal and \widehat{v} the defining valuation of \widehat{D} . Let $\varphi: \widehat{D} \rightarrow \widehat{D}$ a continuous function and $k \in \mathbb{N}$. Then there exists some $f \in \text{Int}(D)$ such that $v(\varphi(x) - f(x)) \geq k$ for all $x \in \widehat{D}$.*

PROOF. We first prove the following two assertions.

A. There exists some $h \in \mathbb{N}$ with the following property: If $N = q^h - 1$, $\{u_0, \dots, u_N\} \subset D$ is a set of representatives for $D/\mathfrak{m}^h = \widehat{D}/\widehat{\mathfrak{m}}^h$, and $\widehat{U}_i = u_i + \widehat{\mathfrak{m}}^h$ for all $i \in [0, N]$, then there exist $c_0, \dots, c_N \in D$ such that

$$\left(\varphi - \sum_{i=0}^N c_i \mathbf{1}_{\widehat{U}_i}\right)(x) \in \widehat{\mathfrak{m}} \quad \text{for all } x \in \widehat{D}.$$

B. Let $h \in \mathbb{N}$, $N = q^h - 1$, $u \in D$ and $\widehat{U} = u + \widehat{\mathfrak{m}}^h$. Then there exists some $f \in \text{Int}(D)$ such that

$$(\mathbf{1}_{\widehat{U}} - f)(x) \in \widehat{\mathfrak{m}} \quad \text{for all } x \in \widehat{D}.$$

Proof of A. Since \widehat{D} is compact, it follows that φ is uniformly continuous, and therefore there exists some $h \in \mathbb{N}$ such that, for all $x, y \in \widehat{D}$, $\widehat{v}(x - y) \geq h$ implies $\varphi(x) - \varphi(y) \in \widehat{\mathfrak{m}}$. Set now $N = q^h - 1$, and let $\{u_0, \dots, u_N\} \subset D$ be a set of representatives for $D/\mathfrak{m}^h = \widehat{D}/\widehat{\mathfrak{m}}^h$. For $i \in [0, N]$, set $\widehat{U}_i = u_i + \widehat{\mathfrak{m}}^h$, and let $c_i \in D$ be such that $\varphi(u_i) - c_i \in \widehat{\mathfrak{m}}$. If $x \in \widehat{U}_i$, then $x - u_i \in \widehat{\mathfrak{m}}^h$, hence $\varphi(x) - \varphi(u_i) \in \widehat{\mathfrak{m}}$, and therefore $\varphi(x) - c_i = \varphi(x) - \varphi(u_i) + \varphi(u_i) - c_i \in \widehat{\mathfrak{m}}$. Since

$$\widehat{D} = \bigsqcup_{i=0}^N \widehat{U}_i, \quad \text{it follows that} \quad \left(\varphi - \sum_{i=0}^N c_i \mathbf{1}_{\widehat{U}_i}\right)(x) \in \widehat{\mathfrak{m}} \quad \text{for all } x \in \widehat{D}. \quad \square[\mathbf{A}]$$

Proof of B. Let $v = \widehat{v}|_D$, $(u_i)_{i \geq 0}$ a well distributed sequence in D and $(f_n)_{n \geq 0}$ the associated regular basis. For $i \in [0, N]$, set $U_i = u_i + \mathfrak{m}^h$. Then

$$D = \bigsqcup_{i=0}^N U_i, \quad \text{and therefore} \quad f_n = \sum_{i=0}^N f_n \mathbf{1}_{U_i} \quad \text{for all } n \geq 0.$$

Assume not that $n \in [0, N]$. Then $\deg(f_n) < q^h$, and therefore $v(f_n(x) - f_n(y)) \geq v(x - y) - h + 1$ for all $x, y \in D$. In particular, if $i \in [0, N]$ and $x \in U_i$, then $v(x - u_i) \geq h$, and therefore $f_n(x) - f_n(u_i) \in \mathfrak{m}$. It follows that the function

$$\psi_n = f_n - \sum_{i=0}^N f_n(u_i) \mathbf{1}_{U_i}: D \rightarrow D \quad \text{satisfies} \quad \psi_n(x) \in \mathfrak{m} \quad \text{for all } x \in D.$$

We gather these equations for $n \in [0, N]$ into a matrix equation

$$(f_0, \dots, f_N) = (\mathbf{1}_{U_0}, \dots, \mathbf{1}_{U_N})T + (\psi_0, \dots, \psi_N), \quad \text{where} \quad T = (f_n(u_i))_{n,i \in [0,N]} \in \mathbf{M}_{N+1}(D).$$

Since $f_n(u_i) = 0$ if $i < n$ and $f_n(u_n) = 1$, it follows that $T \in \mathbf{GL}_n(D)$, and we obtain

$$(\mathbf{1}_{U_0}, \dots, \mathbf{1}_{U_N}) = (f_0, \dots, f_N)T^{-1} + (\tilde{\psi}_0, \dots, \tilde{\psi}_N), \quad \text{where} \quad (\tilde{\psi}_0, \dots, \tilde{\psi}'_N) = -(\psi_0, \dots, \psi_N)T^{-1},$$

and $\tilde{\psi}_i: D \rightarrow D$ satisfy $\tilde{\psi}_i(D) \subset \mathfrak{m}$ for all $i \in [0, N]$. In particular, for every $i \in [0, N]$ we obtain $\mathbf{1}_{U_i} = g_i + \tilde{\psi}_i$ for some $g_i \in \text{Int}(D)$.

After these preparations, we can do the proof of **B**. If $U = u + \mathfrak{m}^h$, then there is some $i \in [0, N]$ such that $U = U_i$. Then $\widehat{U} = u + \widehat{\mathfrak{m}}^h$ is the (topological) closure of U , $U = \widehat{U} \cap D$, and there exists some $f \in \text{Int}(D)$ such that $(\mathbf{1}_U - f)(x) = (\mathbf{1}_{\widehat{U}} - f)(x) \in \mathfrak{m}$ for all $x \in D$. Since $\widehat{U} \subset \widehat{D}$ is clopen, its characteristic function $\mathbf{1}_{\widehat{U}}$ is continuous. Hence $\mathbf{1}_{\widehat{U}} - f: \widehat{D} \rightarrow \widehat{D}$ is continuous, and $(\mathbf{1}_{\widehat{U}} - f)(D) \subset \mathfrak{m}$ implies $(\mathbf{1}_{\widehat{U}} - f)(\widehat{D}) \subset \widehat{\mathfrak{m}}$. $\square[\mathbf{B}]$

Now we prove the Theorem by induction on k . We must prove that, for all $k \in \mathbb{N}$, there exists some $f \in \text{Int}(D)$ such that $\varphi - f = t^k \psi$ for some continuous function $\psi: \widehat{D} \rightarrow \widehat{D}$.

$k = 1$: By **A**, there exist $h, N \in \mathbb{N}$, $c_0, \dots, c_N \in D$ and $u_0, \dots, u_N \in D$ such that, if $\widehat{U}_i = u_i + \widehat{\mathfrak{m}}^h$ for all $i \in [0, N]$, then

$$\left(\varphi - \sum_{i=0}^N c_i \mathbf{1}_{\widehat{U}_i} \right)(x) \in \mathfrak{m} \quad \text{for all } x \in \widehat{D}.$$

For every $i \in [0, N]$, **B** implies that there exists some $g_i \in \text{Int}(D)$ such that $(\mathbf{1}_{\widehat{U}_i} - g_i)(x) \in \widehat{\mathfrak{m}}$ for all $x \in \widehat{D}$. Then

$$f = \sum_{i=0}^N c_i g_i \in \text{Int}(D), \quad \text{and} \quad (\varphi - f)(x) = \left(\varphi - \sum_{i=0}^N c_i \mathbf{1}_{\widehat{U}_i} \right)(x) + \left(\sum_{i=0}^N c_i (\mathbf{1}_{\widehat{U}_i} - g_i) \right)(x) \in \widehat{\mathfrak{m}} \quad \text{for all } x \in \widehat{D},$$

and therefore $\varphi - f = t\psi$ for some continuous function $\psi: \widehat{D} \rightarrow \widehat{D}$.

$k \geq 1$, $k \rightarrow k + 1$: Let $f \in \text{Int}(D)$ be such that $\varphi - f = t^k \psi$ for some continuous function $\psi: \widehat{D} \rightarrow \widehat{D}$. Let $f_1 \in \text{Int}(D)$ be such that $\psi - f_1 = t\psi_1$ for some continuous function $\psi_1: \widehat{D} \rightarrow \widehat{D}$. Then $f + t^k f_1 \in \text{Int}(D)$, and $\varphi - (f + t^k f_1) = t^k(\psi - f_1) = t^{k+1}\psi_1$.

Corollary. *Let D be a dv -domain with maximal ideal \mathfrak{m} such that D/\mathfrak{m} is finite. Let \widehat{D} be a completion of D and \widehat{v} the defining valuation of \widehat{D} . Let $r \in \mathbb{N}$, $n_1, \dots, n_r \in \mathbb{Z}$ and $U_1, \dots, U_r \subset \widehat{D}$ disjoint clopen subsets such that*

$$\widehat{D} = \bigsqcup_{i=1}^r U_i.$$

Then there exists some $f \in K[X]$ such that $\widehat{v}(f(x)) = n_i$ for all $i \in [1, r]$ and $x \in U_i$, and even $f \in \text{Int}(D)$ provided that $n_i \geq 0$ for all $i \in [1, r]$.

PROOF. Let $t \in D$ be such that $\widehat{v}(t) = 1$, and assume first that $n_i \geq 0$ for all $i \in [1, r]$. Let $\varphi: \widehat{D} \rightarrow \widehat{D}$ be the locally constant function defined by $\varphi(x) = t^{n_i}$ if $i \in [1, r]$ and $x \in U_i$. Then φ is continuous. Suppose that $n \in \mathbb{N}$, $n > \max\{n_1, \dots, n_r\}$, and let $f \in \text{Int}(D)$ such that $\widehat{v}(f(x) - \varphi(x)) > n$ for all $x \in \widehat{D}$. Then it follows that $\widehat{v}(f(x)) = n_i$ for all $i \in [1, r]$ and $x \in U_i$.

If $n_1, \dots, n_r \in \mathbb{Z}$ are arbitrary, let $m \in \mathbb{N}$ be such that $m + n_i \geq 0$ for all $i \in [1, r]$, and let $f_1 \in \text{Int}(D)$ be such that $\widehat{v}(f_1(x)) = m + n_i$ for all $i \in [1, r]$ and $x \in U_i$. Then $f = t^{-m} f_1 \in K[X]$ fulfills our requirements. \square

Theorem 2.3.7. *Let D be a dv-domain with maximal ideal \mathfrak{m} such that D/\mathfrak{m} is finite. Let \widehat{D} be a completion of D and $\widehat{\mathfrak{m}}$ the maximal ideal of \widehat{D} .*

1. *For $\alpha \in \widehat{D}$, let $\mathfrak{M}_\alpha = \{f \in \text{Int}(D) \mid f(\alpha) \in \widehat{\mathfrak{m}}\}$. Then $\mathfrak{M}_\alpha \in \max(\text{Int}(D))$ is not finitely generated, $\mathfrak{M}_\alpha \cap D = \mathfrak{m}$, $\text{Int}(D, \mathfrak{m}) \subset \mathfrak{M}_\alpha$, $\text{Int}(D)/\mathfrak{M}_\alpha = D/\mathfrak{m}$, and the map*

$$\widehat{D} \rightarrow \{\mathfrak{P} \in \text{spec}(\text{Int}(D)) \mid \mathfrak{P} \cap D = \mathfrak{m}\}, \quad \alpha \mapsto \mathfrak{M}_\alpha,$$

is bijective.

2. *For an irreducible monic polynomial $g \in K[X]$, let $\mathfrak{P}_g = gK[X] \cap \text{Int}(D)$. Then the map*

$$\Theta: \{g \in K[X] \mid g \text{ monic and irreducible}\} \rightarrow \{\mathfrak{P} \in \text{spec}(\text{Int}(D)) \mid \mathfrak{P} \neq \mathbf{0}, \mathfrak{P} \cap D = \mathbf{0}\},$$

defined by $\Theta(g) = \mathfrak{P}_g$, is bijective. If $g \in K[X]$ is monic and irreducible and $\alpha \in \widehat{D}$, then $\mathfrak{P}_g \subset \mathfrak{M}_\alpha$ if and only if $g(\alpha) = 0$.

PROOF. 1. Let $q = |D/\mathfrak{m}|$ and \widehat{v} be the defining valuation of \widehat{D} . By definition, $\mathfrak{M}_\alpha \in \text{spec}(\text{Int}(D))$, and $\mathfrak{M}_\alpha \cap D = \mathfrak{m}$ is principal. By Theorem 2.3.4 we obtain $\mathfrak{M}_\alpha \in \max(\text{Int}(D))$, $\text{Int}(D, \mathfrak{m}) \subset \mathfrak{M}_\alpha$ and $\text{Int}(D)/\mathfrak{M}_\alpha = D/\mathfrak{m}$.

If $\alpha, \beta \in \widehat{D}$ and $\alpha \neq \beta$, then there exists a continuous function $\varphi: \widehat{D} \rightarrow \widehat{D}$ such that $\varphi(\alpha) = 0$ and $\varphi(\beta) = 1$. Let $f \in \text{Int}(D)$ be such that $\widehat{v}(f(x) - \varphi(x)) \geq 1$ for all $x \in \widehat{D}$. Then $f(\alpha) \in \widehat{\mathfrak{m}}$ and $f(\beta) \in 1 + \widehat{\mathfrak{m}}$, hence $f \in \mathfrak{M}_\alpha \setminus \mathfrak{M}_\beta$, and thus $\mathfrak{M}_\alpha \neq \mathfrak{M}_\beta$.

Assume now that, contrary to our assertion, there exists some $\mathfrak{P} \in \text{spec}(\text{Int}(D))$ such that $\mathfrak{P} \cap D = \mathfrak{m}$, hence $\text{Int}(D, \mathfrak{m}) \subset \mathfrak{P}$ by Theorem 2.3.4, and $\mathfrak{P} \neq \mathfrak{M}_\alpha$ for all $\alpha \in \widehat{D}$. Consequently, for all $\alpha \in \widehat{D}$, there exists some function $f_\alpha \in \mathfrak{P}$ such that $f_\alpha(\alpha) \notin \widehat{\mathfrak{m}}$. Since $\widehat{D} \setminus \widehat{\mathfrak{m}}$ is open, there exists a clopen neighborhood U_α of α in \widehat{D} such that $f_\alpha(x) \notin \widehat{\mathfrak{m}}$ for all $x \in U_\alpha$. Since \widehat{D} is compact, the open covering $(U_\alpha)_{\alpha \in \widehat{D}}$ has a finite subcovering. Hence there exist open subsets $U_1, \dots, U_m \subset \widehat{D}$ and polynomials $f_1, \dots, f_m \in \mathfrak{P}$ such that $\widehat{D} = U_1 \cup \dots \cup U_m$ and $f_j(x) \notin \widehat{\mathfrak{m}}$ for all $j \in [1, m]$ and $x \in U_j$. For $j \in [1, m]$, we set $g_j = f_j^{q-1}$. Then $g_j \in \mathfrak{P}$, $g_j(x) \equiv 0$ or $1 \pmod{\widehat{\mathfrak{m}}}$ for all $x \in \widehat{D}$, and $g_j(x) \equiv 1 \pmod{\widehat{\mathfrak{m}}}$ for all $x \in U_j$. Now we obtain

$$g = 1 - \prod_{j=1}^m (1 - g_j) \in \mathfrak{P}, \quad \text{and} \quad g(x) - 1 \in \widehat{\mathfrak{m}} \quad \text{for all } x \in \widehat{D}.$$

Hence it follows that $g - 1 \in \text{Int}(D, \mathfrak{m}) \subset \mathfrak{P}$, a contradiction.

It remains to prove that the ideals \mathfrak{M}_α are not finitely generated. Indeed, assume to the contrary that $\alpha \in \widehat{D}$ and $\mathfrak{M}_\alpha = \text{Int}(D)\langle f_1, \dots, f_m \rangle$. Then $f_j(\alpha) \in \widehat{\mathfrak{m}}$ for all $j \in [1, m]$, and as $\widehat{\mathfrak{m}} \subset \widehat{D}$ is open and $f_j: \widehat{D} \rightarrow \widehat{D}$ is continuous for all $j \in [1, m]$, it follows that there is some $k \in \mathbb{N}$ with the following property: If $\beta \in \widehat{D}$ and $\widehat{v}(\beta - \alpha) \geq k$, then $f_j(\beta) \in \widehat{\mathfrak{m}}$ for all $j \in [1, m]$, and thus $f_j \in \mathfrak{M}_\beta$ for all $j \in [1, m]$, a contradiction if $\beta \neq \alpha$.

2. Since $K[X] = D^{\bullet-1}\text{Int}(D) = \text{Int}(D)_{\mathbf{0}}$, the map

$$\{\mathfrak{P} \in \text{spec}(\text{Int}(D)) \mid \mathfrak{P} \cap D = \mathbf{0}\} \rightarrow \text{spec}(K[X]), \quad \mathfrak{P} \mapsto \mathfrak{P}K[X],$$

is bijective, and its inverse is given by $\mathfrak{Q} \mapsto \mathfrak{Q} \cap \text{Int}(D)$. Since the map

$$\{g \in K[X] \mid g \text{ monic and irreducible}\} \rightarrow \text{spec}(K[X]) \setminus \{\mathbf{0}\}, \quad g \mapsto gK[X]$$

is also bijective, it follows that Θ is bijective.

Let now $g \in K[X]$ be monic and irreducible and $\alpha \in \widehat{D}$. If $g(\alpha) = 0$, then $f(\alpha) = 0$ for all $f \in \mathfrak{P}_g$, and thus $\mathfrak{P}_g \subset \mathfrak{M}_\alpha$. Thus suppose that $g(\alpha) \neq 0$, let $d \in D^\bullet$ be such that $dg \in D[X]$, and set $\widehat{v}(dg(\alpha)) = n \in \mathbb{N}_0$. Since $\widehat{v} \circ g: \widehat{D} \rightarrow \mathbb{N}_0 \cup \{\infty\}$ is continuous, there exists some clopen neighborhood $U \subset \widehat{D}$ of α such that $\widehat{v}(dg(x)) = n$ for all $x \in U$. By the Corollary to Theorem 2.3.6, there exists some

$h \in K[X]$ such that $\widehat{v}(h(x)) = -n$ for all $x \in U$, and $\widehat{v}(h(x)) = 0$ for all $x \in \widehat{D} \setminus U$. Then $\widehat{v}(dg(x)h(x)) = 0$ for all $x \in U$, and $\widehat{v}(dg(x)h(x)) = \widehat{v}(dg(x)) \geq 0$ for all $x \in \widehat{D} \setminus U$. Hence $dgqh \in \text{Int}(D)$, hence $dgh \in \mathfrak{P}_g$, but $dgh(\alpha) \neq 0$ and therefore $dgh \notin \mathfrak{M}_\alpha$. \square

Theorem 2.3.8 (Prime ideals of $\text{Int}(\mathbb{Z})$). *For a prime $p \in \mathbb{P}$, let $\mathbb{Z}_{(p)} = \mathbb{Z}_{p\mathbb{Z}}$ the domain of p -integral rational numbers and $\mathbb{Z}_p = \widehat{\mathbb{Z}_{(p)}}$ the domain of p -adic numbers. For $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$, we set $\mathfrak{M}_{p,\alpha} = \{f \in \text{Int}(\mathbb{Z}) \mid f(\alpha) \in p\mathbb{Z}_p\}$, and for a monic irreducible polynomial $g \in \mathbb{Q}[X]$, we set $\mathfrak{P}_g = g\mathbb{Q}[X \cap \text{Int}(\mathbb{Z})]$.*

1. For every prime $p \in \mathbb{P}$, the map

$$\mathbb{Z}_p \rightarrow \{\mathfrak{P} \in \text{spec}(\text{Int}(\mathbb{Z})) \mid \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}\}, \quad \alpha \mapsto \mathfrak{M}_{p,\alpha},$$

is bijective, and the ideals $\mathfrak{M}_{p,\alpha}$ are maximal and not finitely generated.

2. Then the map

$$\Theta: \{g \in \mathbb{Q}[X] \mid g \text{ monic and irreducible}\} \rightarrow \{\mathfrak{P} \in \text{spec}(\text{Int}(\mathbb{Z})) \mid \mathfrak{P} \neq \mathbf{0}, \mathfrak{P} \cap \mathbb{Z} = \mathbf{0}\},$$

defined by $\Theta(g) = \mathfrak{P}_g$, is bijective. If $g \in \mathbb{Q}[X]$ is monic and irreducible, $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$, then $\mathfrak{P}_g \subset \mathfrak{M}_{p,\alpha}$ if and only if $g(\alpha) = 0$.

3. $\max(\text{Int}(\mathbb{Z})) = \{\mathfrak{M}_{p,\alpha} \mid p \in \mathbb{P}, \alpha \in \mathbb{Z}_p\}$, and the minimal non-zero prime ideals of $\text{Int}(\mathbb{Z})$ are the ideals \mathfrak{P}_g for monic irreducible polynomials $g \in \mathbb{Q}[X]$ and the ideals $\mathfrak{M}_{p,\alpha}$, where $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$ is not algebraic over \mathbb{Q} . In particular, $\dim(\text{Int}(\mathbb{Z})) = 2$.

PROOF. 1. Let $p \in \mathbb{P}$. By Theorem 2.3.1, $\text{Int}(\mathbb{Z}) \subset \text{Int}(\mathbb{Z})_{p\mathbb{Z}} = \text{Int}(\mathbb{Z}_{(p)})$, and therefore the map

$$\text{spec}(\text{Int}(\mathbb{Z}_{(p)})) \rightarrow \{\mathfrak{P} \in \text{spec}(\text{Int}(\mathbb{Z})) \mid \mathfrak{P} \cap \mathbb{Z} \subset p\mathbb{Z}\}, \quad \overline{\mathfrak{P}} \mapsto \overline{\mathfrak{P}} \cap \text{Int}(\mathbb{Z}),$$

is bijective. If $\overline{\mathfrak{P}} \in \text{spec}(\text{Int}(\mathbb{Z}_{(p)}))$ and $\mathfrak{P} = \overline{\mathfrak{P}} \cap \text{Int}(\mathbb{Z})$, then $\overline{\mathfrak{P}} = \mathfrak{P}_{(p)}$, and $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ if and only if $\overline{\mathfrak{P}} \cap \mathbb{Z}_{(p)} = p\mathbb{Z}_{(p)}$. Hence we obtain a bijective map

$$\{\overline{\mathfrak{P}} \in \text{spec}(\text{Int}(\mathbb{Z}_{(p)})) \mid \overline{\mathfrak{P}} \cap \mathbb{Z}_{(p)} = p\mathbb{Z}_{(p)}\} \rightarrow \{\mathfrak{P} \in \text{spec}(\text{Int}(\mathbb{Z})) \mid \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}\}, \quad \overline{\mathfrak{P}} \mapsto \overline{\mathfrak{P}} \cap \text{Int}(\mathbb{Z}).$$

By Theorem 2.3.7.1, the assignment $\alpha \mapsto \overline{\mathfrak{M}}_{p,\alpha} = \{f \in \text{Int}(\mathbb{Z}_{(p)}) \mid f(\alpha) \in \mathbb{Z}_p\}$ defines a bijective map $\mathbb{Z}_p \rightarrow \{\overline{\mathfrak{P}} \in \text{spec}(\text{Int}(\mathbb{Z}_{(p)})) \mid \overline{\mathfrak{P}} \cap \mathbb{Z}_{(p)} = p\mathbb{Z}_{(p)}\}$, and since $\overline{\mathfrak{M}}_{p,\alpha} \cap \text{Int}(\mathbb{Z}) = \mathfrak{M}_{p,\alpha}$, we obtain a bijective map

$$\mathbb{Z}_p \rightarrow \{\mathfrak{P} \in \text{spec}(\text{Int}(\mathbb{Z})) \mid \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}\}, \quad \alpha \mapsto \mathfrak{M}_{p,\alpha}.$$

The ideals $\overline{\mathfrak{M}}_{p,\alpha}$ are not finitely generated and maximal ideals of $\text{Int}(\mathbb{Z}_{(p)})$. Since $\overline{\mathfrak{M}}_{p,\alpha} = (\mathfrak{M}_{p,\alpha})_{(p)}$, the ideals $\mathfrak{M}_{p,\alpha}$ are likewise not finitely generated maximal ideals of $\text{Int}(\mathbb{Z})$.

2. Since $\mathbb{Q}[X] = \mathbb{Z}^{\bullet-1}\text{Int}(\mathbb{Z}) = \text{Int}(\mathbb{Z})_{\mathbf{0}}$, the map

$$\{\mathfrak{P} \in \text{spec}(\text{Int}(\mathbb{Z})) \mid \mathfrak{P} \cap \mathbb{Z} = \mathbf{0}\} \rightarrow \text{spec}(\mathbb{Q}[X]), \quad \mathfrak{P} \mapsto \mathfrak{P}\mathbb{Q}[X],$$

is bijective, and its inverse is given by $\mathfrak{Q} \mapsto \mathfrak{Q} \cap \text{Int}(\mathbb{Z})$. Since the map

$$\{g \in \mathbb{Q}[X] \mid g \text{ monic and irreducible}\} \rightarrow \text{spec}(\mathbb{Q}[X]) \setminus \{\mathbf{0}\}, \quad g \mapsto g\mathbb{Q}[X]$$

is also bijective, it follows that Θ is bijective.

Assume now that $g \in \mathbb{Q}[X]$ is monic and irreducible, $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$. Then we obtain

$$\overline{\mathfrak{M}}_{p,\alpha} = \{f \in \text{Int}(\mathbb{Z}_{(p)}) \mid f(\alpha) \in p\mathbb{Z}_p\} = (\mathfrak{M}_{p,\alpha})_{(p)} \quad \text{and} \quad \overline{\mathfrak{P}}_g = g\mathbb{Q}[X] \cap \text{Int}(\mathbb{Z}_{(p)}) = (\mathfrak{P}_g)_{(p)}.$$

Hence $\mathfrak{P}_g \subset \mathfrak{M}_{p,\alpha}$ if and only if $\overline{\mathfrak{P}}_g \subset \overline{\mathfrak{M}}_{p,\alpha}$, and by Theorem 2.3.7 this holds if and only if $g(\alpha) = 0$.

3. If $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$, then $\mathfrak{M}_{p,\alpha} \in \max(\text{Int}(\mathbb{Z}))$ by 1. If α is algebraic over \mathbb{Q} and $g \in \mathbb{Q}[X]$ is its minimal polynomial, then $\mathfrak{P}_g \subset \mathfrak{M}_{p,\alpha}$ by 2., and if α is not algebraic over \mathbb{Q} , then $\mathfrak{M}_{p,\alpha}$ is a minimal non-zero prime ideal of $\text{Int}(\mathbb{Z})$. It therefore remains to prove that the ideals \mathfrak{P}_g for monic and irreducible $g \in \mathbb{Q}[X]$ are not maximal.

Thus let $g \in \mathbb{Q}[X]$ be monic and irreducible. We shall prove that there exist infinitely many primes p such that $g(\alpha) = 0$ for some $\alpha \in \mathbb{Z}_p$ (and then $\mathfrak{P}_g \subset \mathfrak{M}_{p,\alpha}$). Let $d \in \mathbb{N}$ be such that $g_1 = dg \in \mathbb{Z}[X]$, and let E be the (finite) set of all primes dividing d or the discriminant of g_1 . If $p \in \mathbb{P} \setminus E$, then the

residue class polynomial $\bar{g}_1 = g_1 + p\mathbb{Z}[X] \in \mathbb{F}_p[X]$ has no multiple roots. If $z \in \mathbb{F}_p$ is a root of \bar{g}_1 , then Hensel's Lemma implies that there is some $\alpha \in \mathbb{Z}_p$ such that $g_1(\alpha) = 0$, hence $g(\alpha) = 0$, and $\alpha + p\mathbb{Z}_p = z$. Hence it suffices to prove that the set $F = \{p \in \mathbb{P} \setminus E \mid g_1(a) \in p\mathbb{Z} \text{ for some } a \in \mathbb{Z}\}$ is infinite. Let $g_1 = a_0 + a_1X + \dots + a_dX^d$, where $d \in \mathbb{N}$ and $a_0, \dots, a_d \in \mathbb{Z}$. If $a_0 = 0$, then $g_1(p) \in p\mathbb{Z}$ for all $p \in \mathbb{P}$. Thus suppose that $a_0 \neq 0$, and let F be finite. If $s \geq 2$ is any product of primes, then there is some $k \in \mathbb{N}$ such that $g_1(a_0s^k) \neq \pm a_0$, and then $g_1(a_0s^k) = a_0(1 + s^kb)$ for some $b \in \mathbb{Z}$ such that $1 + s^kb \neq \pm 1$. If $p \in \mathbb{P}$ and $p \mid 1 + s^kb$, then $p \nmid s$ and yet $g_1(a_0s^k) \in p\mathbb{Z}$, a contradiction. \square

Theorem 2.3.9.

1. Let D be an almost Dedekind domain such that D/\mathfrak{m} is finite and $\text{Int}(D)_{\mathfrak{m}} = \text{Int}(D_{\mathfrak{m}})$ for all $\mathfrak{m} \in \max(D)$. Then $\text{Int}(D)$ is a Prüfer domain. In particular, if D is a Dedekind domain with finite residue class fields, then $\text{Int}(D)$ is a Prüfer domain.
2. If $\text{Int}(D)$ is a Prüfer domain, then D is an almost Dedekind domain, and D/\mathfrak{m} is finite for every non-zero prime ideal of D .

PROOF. 1. We assume first that D is a dv-domain with maximal ideal \mathfrak{m} such that D/\mathfrak{m} is finite. Let \hat{D} be a completion of D and \hat{v} the defining valuation of \hat{D} . We show that every finitely generated non-zero ideal of $\text{Int}(D)$ is invertible. Thus let $\mathfrak{0} \neq \mathfrak{A} \subset \text{Int}(D)$ be a finitely generated ideal.

CASE 1: $\mathfrak{A} \cap D \neq \mathfrak{0}$. Assume that \mathfrak{A} is not invertible. Then there exists some $\mathfrak{M} \in \max(\text{Int}(D))$ such that $\mathfrak{A} \subset \mathfrak{A}\mathfrak{A}^{-1} \subset \mathfrak{M}$, and since $\mathfrak{0} \neq \mathfrak{A} \cap D \subset \mathfrak{M} \cap D$, we get $\mathfrak{M} \cap D = \mathfrak{m}$, and therefore $\mathfrak{M} = \mathfrak{M}_{\alpha}$ for some $\alpha \in \hat{D}$. Suppose that $\mathfrak{A} = \langle f_1, \dots, f_r \rangle_{\text{Int}(D)}$, and let $n = \min\{\hat{v}(f(\alpha)) \mid f \in \mathfrak{A}\}$. Then it follows that $\hat{v}(f_0(\alpha)) = n$ for some $f_0 \in \mathfrak{A}$, and $\hat{v}(f_i(\alpha)) \geq n$ for all $i \in [1, r]$. Since $f_1, \dots, f_r: \hat{D} \rightarrow \hat{D}$ are continuous, there exists a clopen set $U \subset D$ such that $\alpha \in U$ and $f_i(x) \geq n$ for all $i \in [1, r]$ and $x \in U$. By the Corollary to Theorem 2.3.6, there exists some $h \in K[X]$ such that $\hat{v}(h(x)) = -n$ if $x \in U$, and $\hat{v}(h(x)) = 0$ if $x \in \hat{D} \setminus U$. Then $\hat{v}(f_i(x)h(x)) = \hat{v}(f_i(x)) + \hat{v}(h(x)) \geq 0$ for all $x \in D$, hence $f_i h \in \text{Int}(D)$ for all $i \in [1, r]$, and therefore $h \in \mathfrak{A}^{-1}$. In particular, $f_0 h \in \mathfrak{A}\mathfrak{A}^{-1}$, but $\hat{v}(f_0(\alpha)h(\alpha)) = 0$ and therefore $f_0 h \notin \mathfrak{M}_{\alpha}$.

CASE 2: $\mathfrak{A} \cap D = \mathfrak{0}$. Then $\mathfrak{A}K[X] = gK[X]$ for some $g \in \mathfrak{A} \setminus K$, and since \mathfrak{A} is finitely generated, there is some $d \in D^{\bullet}$ such that $d\mathfrak{A} \subset g \text{Int}(D)$. Then $g^{-1}d\mathfrak{A} \subset \text{Int}(D)$ is a finitely generated ideal, and $d \in g^{-1}d\mathfrak{A} \cap D$. By CASE 1, $g^{-1}d\mathfrak{A}$ is invertible, and therefore \mathfrak{A} is also invertible.

Now we do the general case. Let D be an almost Dedekind domain such that, for all $\mathfrak{m} \in \max(D)$, D/\mathfrak{m} is finite and $\text{Int}(D)_{\mathfrak{m}} = \text{Int}(D_{\mathfrak{m}})$. We must prove that $\text{Int}(D)_{\mathfrak{M}}$ is a valuation domain for all $\mathfrak{M} \in \max(\text{Int}(D))$. If $\mathfrak{M} \in \max(\text{Int}(D))$, then either $\mathfrak{M} \cap D = \mathfrak{0}$ or $\mathfrak{M} \cap D = \mathfrak{m} \in \max(D)$. In the first case, $K[X] \subset \text{Int}(D)_{\mathfrak{M}}$. Hence $\text{Int}(D)_{\mathfrak{M}}$ is a local Prüfer domain and thus a valuation domain. In the second case, $D_{\mathfrak{m}}$ is a dv-domain with finite residue class field $D_{\mathfrak{m}}/\mathfrak{m}D_{\mathfrak{m}} = D/\mathfrak{m}$, hence $\text{Int}(D_{\mathfrak{m}})$ is a Prüfer domain, and therefore $\text{Int}(D)_{\mathfrak{M}} = (\text{Int}(D)_{\mathfrak{m}})_{\mathfrak{M} \cap D} = \text{Int}(D_{\mathfrak{m}})_{\mathfrak{M} \cap D}$ is also a Prüfer domain.

2. Let $\text{Int}(D)$ be a Prüfer domain. The assignment $f \mapsto f(0)$ defines an epimorphism $\text{Int}(D) \rightarrow D$. Hence D is a Prüfer domain. If $\mathfrak{0} \neq \mathfrak{p} \in \text{spec}(D)$, then $D_{\mathfrak{p}}$ is a valuation domain with maximal ideal $\mathfrak{p}D_{\mathfrak{p}}$ and residue class field $D_{\mathfrak{p}}/\mathfrak{p}D_{\mathfrak{p}} = \mathfrak{q}(D/\mathfrak{p})$. If either $D_{\mathfrak{p}}/\mathfrak{p}D_{\mathfrak{p}}$ is infinite or $\mathfrak{p}D_{\mathfrak{p}}$ is not principal, then $\text{Int}(D_{\mathfrak{p}}) = D_{\mathfrak{p}}[X]$ by Theorem 2.3.3.5. By Theorem 2.3.1, $\text{Int}(D) \subset \text{Int}(D)_{\mathfrak{p}} \subset \text{Int}(D_{\mathfrak{p}}) = D_{\mathfrak{p}}[X]$, and thus $D_{\mathfrak{p}}[X]$ is a Prüfer domain, a contradiction. It remains to prove that $D_{\mathfrak{p}}$ is a principal ideal domain, and therefore it suffices to prove that $\mathfrak{p}D_{\mathfrak{p}}$ is the only non-zero prime ideal. Thus suppose that $\mathfrak{0} \neq \bar{\mathfrak{q}} \subset \mathfrak{p}D_{\mathfrak{p}}$ is a prime ideal of $D_{\mathfrak{p}}$. Then $\bar{\mathfrak{q}} = \mathfrak{q}D_{\mathfrak{p}}$ for some prime ideal $\mathfrak{q} \subset D$ such that $\mathfrak{0} \neq \mathfrak{q} \subset \mathfrak{p}$. But then $\mathfrak{p}/\mathfrak{q}$ is an ideal of D/\mathfrak{q} , which is finite and thus a field. Hence $\mathfrak{p} = \mathfrak{q}$ and $\bar{\mathfrak{q}} = \mathfrak{p}D_{\mathfrak{p}}$. \square