0.1 Modules

Let $(R, 0, 1, +, \cdot)$ or simply R be a ring.

Definition 0.1. (a) A left R-module $(M, 0, +, \cdot)$ or simply M is an abelian group $(M, 0, +)$, together with an operation $\cdot : R \times M \to M, (r, m) \mapsto r \cdot m = rm$, such that for all $a, b \in R, m, n \in M$

(M1) $a(m + n) = am + an$ and $(a + b)m = am + bm$

(M2) $a(b \cdot m) = (ab) \cdot m$

(M3) $1 \cdot m = m$

(b) Let M, N be left R-modules. A map $\varphi : M \to N$ is called R-linear or a left R-module homomorphism $:\iff \varphi : (M, 0, +) \to (N, 0, +)$ is a group homomorphism, and $\forall a \in R, m \in M : \varphi(am) = a\varphi(m)$. Define $\mathrm{Hom}_R(M, N) = \{\varphi : M \to N \mid \varphi \text{ is } R\text{-linear}\}$.

Facts 0.2 (Excers.)**.** $\forall x \in M, a \in R : 0_R \cdot x = 0_M, a \cdot 0_M = 0_M, (-1) \cdot x = -x$

Remark 0.3 (Excers.)**.** (a) $\mathrm{Hom}_R(M, N)$ is an abelian group with $0 =$ the map $M \to \{0_N\}$ and $\varphi + \psi : M \to N, m \mapsto \varphi(m) + \psi(m)$.

(b) If R is commutative, then $\mathrm{Hom}_R(M, N)$ is an R-module via

$$r \cdot \varphi : M \to N, m \mapsto r \cdot \varphi(m)$$

(c) If an abelian group $(M, 0, +)$ carries an operation $\cdot : M \times R \to M, (m, r) \mapsto m \cdot r$ such that:

(M1') $(m + n) \cdot a = m \cdot a + n \cdot a, m \cdot (a + b) = ma + mb$

(M2') $(m \cdot a) \cdot b = m \cdot (ab)$

(M3') $m \cdot 1 = m$

then $(M, 0, +, \cdot)$ is called a right R-module. Analogously we can define right R-module homomorphisms.

Convention 0.4. We shall use the term R-module for left R-module, since we will mainly work with these. In fact right R-modules are left R^{op}-modules.

Definition 0.5. The opposite ring (Gegenring) of $(R, 0, 1, +, \cdot)$ is $R^{\mathrm{op}} = (R, 0, 1, +, \cdot^{\mathrm{op}})$ with $a \cdot^{\mathrm{op}} b = b \cdot a$

Facts 0.6 (Excersize)**.** (a) R^{op} is a ring

(b) $\mathrm{id}_R : R \to R$ is a ring homomorphism $\iff R$ is commutative.

(c) $\mathrm{id}_R : R \to (R^{\mathrm{op}})^{\mathrm{op}}$ is an isomorphism.
In particular: If R is commutative, then left R-modules are right R-modules.

Remark 0.7 (Excersize)**.** Let $(M, 0, +)$ be an abelian group.

(a) The abelian group $\mathrm{End}_{\mathbb{Z}}(M) = \mathrm{Hom}_{\mathbb{Z}}(M, M)$ is a ring with composition as multiplication.

(b) There is a bijection $\{$operations $* : R \times M \to M \mid (M, 0, +, *)$ is an R-module$\} \leftrightarrow \{$ring homomorphisms $\varphi : R \to \mathrm{End}_{\mathbb{Z}}(M)\}$ via

$$* \mapsto \varphi_* : R \to \mathrm{End}_{\mathbb{Z}}(M), r \mapsto (\varphi_*(r) : m \mapsto r \cdot m)$$

figure out an inverse.

(c) If M is an R-module, then $\mathrm{End}_R(M) \subseteq \mathrm{End}_{\mathbb{Z}}(M)$ is a subring

(d) The map $R^{\mathrm{op}} \to \mathrm{End}_R(R), r \mapsto \rho_r : a \mapsto a \cdot r$ is a ring isomorphism. The inverse is $\mathrm{End}_R(R) \to R^{\mathrm{op}}, \varphi \mapsto \varphi(1)$

Example 0.8. (a) Let K be a field, K-modules are K-vector spaces and vice versa.

(b) If $(M, 0, +)$ is an abelian group, it is in a unique way a $\mathbb{Z}$-module.

(c) Let K be a field, $R = M_{n\times n}(K), n > 1, V_n(K) =$ column $Z_n(K)$ row vectors of length n over K, then:

- $V_n(K)$ is a left R-module.
- $Z_n(K)$ is a right R-module.

(d) R is a left R-module and right R module with multiplication.

(e) If M_1 and M_2 are R-modules, we can define on $M_1 \times M_2$ a R-module structure via

$$r \cdot (m_1, m_2) := (rm_1, rm_2)$$

(group structure from Algebra 1)

(f) $\mathrm{Hom}_R(R, M) \to M, \varphi : \varphi(1)$ is an isomorphism of abelian groups, and if R is commutative, then also an isomorphism of R-modules.

Definition 0.9. An R-linear map $\varphi : M \to M'$ is called a monomorphism/epimorphism/isomorphism $\iff$ φ is injective/surjective/bijective respectively. We say R-modules M, M' are isomorphic if there exists an isomorphism $M \to M'$.

Remark. φ is an R-linear isomorphism $\iff$ φ^{-1} is an R-linear isomorphism.

Definition 0.10. (a) Let M be an R-module. A subset $N \subseteq M$ is an R-submodule if it is a subgroup and $\forall a \in R, n \in N : a \cdot n \in N$ (i.e. $R \cdot N \subseteq N$)

(b) An R-submodule $I \subseteq R$ is called a left ideal.

(c) $I \subseteq R$ is called a two sided ideal iff it is a left ideal and $I \cdot R \subseteq I$

Example 0.11. (a) If $N' \subseteq N$ and $M' \subseteq M$ are R-submodules of R-modules M and N and if $\varphi : M \to N$ is an R-linear map, then:

$$\varphi(M') \subseteq N \text{ and } \varphi^{-1}(N') \subseteq M$$

are R-submodules. In particular $\ker(\varphi) \leq M$ and $im(\varphi) \leq N$ are submodules.

(b) If $(M_i)_{i\in I}$ is a family of submodules of M, then $\bigcap_{i\in I} M_i \subseteq M$ is the largest submodule of M contained in all M_i, and

$$\sum_{i\in I} M_i = \{\sum_{i\in I} m_i \mid m_{i\in M)i}, \#\{i \mid m_{i\neq 0}\} < \infty\}$$

is the smallest submodule of M containing all M_i.

(c) 2-sided ideals of $M_{n\times n}(R)$ are of the form $M_{n\times n}(I)$ for $I \subseteq R$ a 2-sided ideal.

0.2 Quotient Modules

Definition 0.12. Let $N \subseteq N$ be a submodule. From linear algebra $(M/N, \overline{0}, \overline{+})$ is an abelian group. ($\overline{m} = m + N$ are the equivalence classes and $\overline{m} + \overline{m}' = \overline{m + m'}$). This is an R-module (exercise) via

$$\bar{\cdot} : R \times {}^{M}\!\big/_{N} \to {}^{M}\!\big/_{N} : (r, m+N) \mapsto rm + N$$

We call M/N (with $\overline{0}, \overline{+}, \bar{\cdot}$) the quotient module of M by N, and we write

$$\pi_{N\subseteq M} : M \twoheadrightarrow {}^{M}\!\big/_{N}, m \mapsto m + N$$

Definition 0.13. If $I \subseteq R$ is a 2-sided ideal of R, then

(a) $I \cdot M := \{\sum_{i\in I} a_i \cdot m_i \mid I \text{ finite}, a_{i\in I, m_i \in M}\}$ is an R-submodule of M (M an R-module)

(b) $(R/I, \overline{0}, \overline{1}, \overline{+}, \bar{\cdot})$ is a ring, and $M/I \cdot M$ is an R/I-module.

The following 3 results are proved as for groups:

Theorem 0.14 (Homomorphism theorem)**.** *Let $\varphi : M \to M'$ be an R-linear map, then*

(a) $\forall$ submodules $N \subseteq \ker(\varphi)$: $\exists!R$-linear map $\overline{\varphi} : M/N \to M', m+N \mapsto \varphi(m)$ such that $\varphi = \overline{\varphi} \circ \pi_{N\subseteq M}$

(b) For $N = \ker(\varphi)$, the map $\overline{\varphi} : M/\ker(\varphi) \to im(\varphi)$ is an R-module isomorphism.

Theorem 0.15. *(First isomorphism theorem) Let M be an R-module and $N_1, N_2 \leq M$ be R-submodules. Then the map*

$${}^{N_1}\!\big/_{N_1 \cap N_2} \to {}^{N_1 + N_2}\!\big/_{N_2}, n_1 + N_1 \cap N_2 \mapsto n_1 + N_2$$

is a well-defined R-linear isomorphism.

$$\begin{tikzcd}
 & N_1 + N_2 \arrow[dl, dash] \arrow[dr, dash] & \\
N_1 \arrow[dr, dash] & & N_2 \arrow[dl, dash] \\
 & N_1 \cap N_2 &
\end{tikzcd}$$

Theorem 0.16 (Second isomorphism theorem)**.** *Let M be an R-module and $N \leq M$ an R-submodule. Then*

(a) The following maps are bijective and mutually inverse to each other:

$$\{N' \subseteq M \text{ submodule} \mid N \subseteq N'\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{\overline{N} \subseteq {}^{M}\big/_{N} \text{ submodule}\}$$

$$\varphi : N \mapsto {}^{N'}\big/_{N} \qquad \pi^{-1}_{N \subseteq M}(\overline{N}) \hookleftarrow \overline{N} : \psi$$

(b) For $N' \subseteq M$ a submodule with $N \subseteq N'$ we have the R-linear isomorphism:

$${}^{(M/N)}\big/_{(N'/N)} \to {}^{M}\big/_{N'}, \overline{m} + {}^{N'}\big/_{M} \mapsto m + N'$$

0.3 Direct sums and products

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

Definition 0.17. (a) $\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i, \forall i \in I\}$ is an R-module with component-wise operations:

$$(m_i)_{i \in I} + (n_i)_{i \in I} = (m_i + n_i)_{i \in I}$$

$$r \cdot (m_i)_{i \in I} = (r \cdot m_i)_{i \in I}, \quad r \in R$$

is called the (direct) product of $(M_i)_{i \in I}$. One has the projection maps (R-module epimorphisms):

$$\pi_{i_0} : \prod_{i \in I} M_i \to M_{i_0}, (m_i) \mapsto m_{i_0}$$

(b) $\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \in \prod_{i \in I} M_i \mid \{i \mid m_i \neq 0\} < \infty\}$ is an R-submodule of $\prod_{i \in I} M_i$. It is called the direct sum of $(M_i)_{i \in I}$. One has R-module monomorphisms

$$\iota_{i_0} : M_{i_0} \to \bigoplus_{i \in I} M_i, m_{i_0} \mapsto (\iota_{i_0}(m_{i_0}))$$

where the i-th component of $\iota_{i_0}(m_{i_0})$ is given by $\begin{cases} m_{i_0}, & i = i_0, \\ 0, & \text{otherwise} \end{cases}$

Theorem 0.18 (Universal property of the direct product/sum)**.** *(a) $\forall R$-modules M, the map*

$$\mathrm{Hom}_R(M, \prod_{i \in I} M_i) \xrightarrow{\cong} \prod_{i \in I} \mathrm{Hom}_R(M, M_i), \varphi \mapsto (\pi_i \circ \varphi)_{i \in I}$$

is well defined, bijective and a group isomorphism.

(b) $\forall R$-modules M, the map

$$\mathrm{Hom}_R(\bigoplus_{i \in I} M_i, M) \xrightarrow{\cong} \prod_{i \in I} \mathrm{Hom}_R(M_i, M), \psi \mapsto (\psi \cdot \iota_i)_{i \in I}$$

is well defined, bijective and a group isomorphism.

Proof. (a) The inverse map is given by sending

$$\underline{\varphi} := (\varphi_i : M \to M_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_R(M, M_i)$$

to

$$\pi_{\underline{\varphi}} : M \to \prod_{i\in I} M_i, m \mapsto (\varphi_i(m))_{i\in I}$$

now check: $\underline{\varphi} \mapsto \pi_{\underline{\varphi}}$ is inverse to the map in (a).

(b) The map is given by sending $\overline{\varphi} = (\varphi_i : M_i \to M)_{i\in I}$ to

$$\coprod_{\overline{\varphi}} : \bigoplus_{i\in I} : M_i \to M, (m_i)_{i\in I} \mapsto \sum_{i\in I} \varphi_i(m_i)$$

□

Corollary 0.19 (Important special case)**.** *Let I be finite, then:*

(a) $M := \prod_{i\in I} M_i \overset{!}{=} \bigoplus_{i\in I} M_i$

(b) The maps $M_i \underset{\pi_i}{\overset{\iota_i}{\rightleftarrows}} M$ *satisfy*

$$\pi_i \circ \iota_j = \begin{cases} \mathrm{id}_{M_i}, & i = j, \\ 0, & \textit{otherwise} \end{cases} \quad \textit{and} \quad \sum_{i\in I} \iota_i \circ \pi_i = \mathrm{id}_M$$

(c) If M' is a module with maps $M_i \underset{\pi_i'}{\overset{\iota_i'}{\rightleftarrows}} M'$ *such that the formulas above hold, then* $M \cong M'$

0.4 Generators and bases

From now onwards let R be a unitary ring and M, M', N be R-modules.

Notation.

- For I a set we write $M^I := \prod_{i\in I} M$ and $M^{(I)} := \bigoplus_{i\in I} M$ (where $M_i = M, \forall i \in I$).
- For $r \in \mathbb{N}$ we will write $M^r := M^{\{1,\ldots,r\}}$, so if I is finite then $M^I = M^{\#I} = M^{(I)}$

Definition 0.20. For $\underline{m} = (m_i)_{i\in I} \in M^{(I)}$ we define a map $\varphi_{\underline{m}} : R^{(I)} \to M, (r_i) \mapsto \sum_{i\in I} r_i \cdot m_i$ where r_i is non-zero only for finitely many i. We can also define $\varphi_{\underline{m}}$ via the universal property of $R^{(I)}$ using maps $R \to M, r \mapsto r \cdot m_i$ at component $i \in I$.

(a) $\underline{m}$ is a generating set of $M \iff \varphi_{\underline{m}}$ is surjective.

(b) $\underline{m}$ is a basis of $M \iff \varphi_{\underline{m}}$ is an isomorphism.

(c) M is a free R-module $\iff M$ has a basis.

(d) $\underline{m}$ is finitely generated $\iff$ it has a finite generating set.

(e) $\underline{m}$ is linearly independent $\iff$ $\varphi_{\underline{m}}$ is injective.

Remark. Let $\iota_j : R \to R^{(I)}$ be the inclusion of the component $j \in I$ (1.18) and set $e_j := \iota_j(1)$. Then we call $(e_j)_{j\in I}$ the standard basis of $R^{(I)}$.

Example. (a) If K is a field, then any K-vector space has a basis.

(b) If $R = \mathbb{Z}$, then $M = \mathbb{Z}/(3)$ is finitely generated but not free (exercise).

Remark 0.21. Every R-module is a quotient of a free R-module.

Proof. Let $R^{(M)}$ be the free R-module over the index set M, then

$$\varphi_{\underline{m}} : R^{(M)} \to M, (r_m)_{m\in M} \mapsto \sum_{m\in M} r_m \cdot m$$

is surjective for $\underline{m} = (m)_{m\in M}$. □

Theorem 0.22. *Let R be commutative, then for $n_1, n_2 \in \mathbb{N}_0$, then we have $R^{n_1} \cong R^{n_2} \iff n_1 = n_2$.*

Proof.
- " $\Longleftarrow$ ": (By induction to linear algebra.) Let $\mathfrak{m} \subseteq R$ be a maximal ideal. (Axiom of choice) Consider for $n \in \mathbb{N}$ the map $\varphi_n : R^n \to (R/\mathfrak{m})^n, (r_1, \dots r_n) \mapsto (r_i \mod n)_{i\in\{1,\dots,n\}}$. Then φ_n is surjective with kernel $\mathfrak{m}^n \in R^n \implies R^n/\mathfrak{m}^n \cong (R/\mathfrak{m})^n$ by the homomorphism theorem. Now suppose $\psi : R^{n_1} \to R^{n_2}$ is an isomorphism. We show $n_1 \geq n_2$ (by symmetry of argument we get $n_1 = n_2$). Consider the map

$$\begin{tikzcd} R^{n_1} \arrow[r, "\cong"] \arrow[rr, bend right, "\rho"'] & R^{n_2} \arrow[r, two heads] & R^{n_2}\big/\mathfrak{m}^{n_2} \end{tikzcd}$$

  this map is surjective and contains $\mathfrak{m}^{n_1}$ in its kernel (check this). By the homomorphism theorem we get a surjective homomorphism

$$\left(R\big/\mathfrak{m}\right)^{n_1} = R^{n_1}\big/\mathfrak{m}^{n_1} \to R^{n_2}\big/\mathfrak{m}^{n_2} = \left(R\big/\mathfrak{m}\right)^{n_2}$$

  by linear algebra we conclude that $n_1 \geq n_2$.

□

Definition 0.23. If M is free and finitely generated, then define $\mathrm{rank}(M)$ (the rank of M) as the unique $n \in \mathbb{N}_0$ such that $M \cong R^n$.

Remark. If R is non-commutative, then the rank of the finitely generated R-modules is not well-defined. (Jantzen Schwermer Bsp VII.4.2: $R \cong M \cong R^2$ for $R = \mathrm{End}_K(K[X])$)

0.5 Exact sequences

Definition 0.24. (a) A diagram of R-modules

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is called exact (at M) $:\Longleftrightarrow$ $\ker(g) = \mathrm{im}(f)$

(b) An exact sequence of R-modules is a family $(f_j)_{j\in J}$ of R-module homomorphisms $f_j : M_j \to M_{j+1}$ index of an interval $J \subseteq \mathbb{Z}$, such that $\forall j \in J : j+1 \in J$, the sequence

$$M_j \xrightarrow{f_j} M_{j+1} \xrightarrow{f_{j+1}} M_{j+2}$$

is exact (at M_{j+1}). Other notation:

$$M_{j_0} \xrightarrow{f_{j_0}} M_{j_0+1} \xrightarrow{f_{j_0+1}} \cdots \to M_{j+2}$$

(c) An exact sequence $0 \to M' \to M \to M'' \to 0$ is called a short exact sequence (s.e.s.)

Remark.
- $0 \to M' \xrightarrow{f} M$ is exact $\overset{\text{Exercise}}{\Longleftrightarrow}$ f is injective.
- $M \xrightarrow{g} M'' \to 0$ is exact $\overset{\text{Exercise}}{\Longleftrightarrow}$ g is surjective.
  (0 stands for the 0-module $\{0\}$)

Example 0.25. Let $f : M \to N$ be an R-module homomorphism. Then one defines

$$\mathrm{coker}(f) := N \big/ \mathrm{im}(f)$$

as the cokernel of f , it comes toether with an R-module epimorphism $\pi : N \to \mathrm{coker}(f)$. As an exercise: The sequence

$$0 \to \ker(f) \xrightarrow{i} M \xrightarrow{f} N \xrightarrow{\pi} \mathrm{coker}(f) \to 0$$

is exact. Subexamples:

- If f is injective, then $0 \to M \xrightarrow{f} N \to \mathrm{coker}(f) \to 0$ is exact.
- If f is surjective, then $0 \to \ker(f) \to M \xrightarrow{f} N \to 0$ is exact.

Remark. For R-module homomorphisms $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ with $\beta \circ \alpha = 0$, the following are equivalent:

(i) $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ is a s.e.s.

(ii) β is surjective and $\alpha : M' \to \ker(\beta)$ is an isomorphism.

(iii) α is injective and the homomorphism theorem induces an isomorphism $\mathrm{coker}(\alpha) \cong M/\mathrm{im}(\alpha) \to M''$

($\beta \circ \alpha = 0 \iff \mathrm{im}(\alpha) \subseteq \ker(\beta)$)

Proposition 0.26 (Exercise)**.** *(a) Let $0 \to M_i' \to M_i \to M_i'' \to 0$ be short exact sequences $\forall i \in I$, then we get short exact sequences*

$$0 \to \bigoplus_{i\in I} M_i' \to \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} M_i'' \to 0$$

$$0 \to \prod_{i\in I} M_i' \to \prod_{i\in I} M_i \to \prod_{i\in I} M_i'' \to 0$$

(b) Suppose $0 \to V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} V_n \to 0$ is an exact sequence of finite dimensional K-vector spaces, then:

$$\sum (-1)^i \dim_K(V_i) = 0.$$

Notation 0.27 (Commutativity of diagrams)**.** A diagram of R-modules is a directed graph, where any vertex is an R-module and any arrow is an R-linear map from the module at its source to the module at its target. We call two arrows composable if the target of the first arrow is the source of the second; then the correspoding maps can be composed. So to any chain of composable arrows, the composition of maps defines a map from the source of the first to the target of the last arrow in the chain. A diagram is **commutative** if for any two chains of arrows with the same source and target, the resulting two maps agree.

Example. (a) To say that the diagram

$$\begin{tikzcd} .M_1 \arrow[r, "f"] \arrow[d, "g"'] & M_2 \arrow[d, "g'"] \\ M_3 \arrow[r, "f'"'] & M_4 \end{tikzcd}$$

commutes means that $g' \circ f = f' \circ g$.

(b) $M \underset{g}{\overset{f}{\rightleftarrows}} N$ commutes $\iff$ $g = h$

Theorem-Definition 0.28. *For a short exact sequence of R-modules*

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] \arrow[l, dashed, bend left, "s"] & M'' \arrow[r] \arrow[l, dashed, bend left, "t"] & 0 \end{tikzcd} \qquad (*)$$

the following are equivalent:

(a) $\exists R$-linear map $t : M'' \to M$ such that $g \circ t = \mathrm{id}_{M''}$

(b) $\exists$ submodule $N \subseteq M$ such that

$$\psi : \mathrm{im}(f) \oplus N \to M, (b, n) \mapsto b + n$$

is an isomorphism.

(c) $\exists R$-linear map $s : M \to M'$ such that $s \circ f = \mathrm{id}_{M'}$.

In this case (if (a) - (c) hold), then the sequence $(*)$ is called a split exact sequence. (simply $(*)$ is split or splits), and t (or s) is called a splitting of g (or of f respectively).

Proof.

- $(a) \implies (b)$: Given t, define $N := \mathrm{im}(t)$ and ψ as above, i.e. $\psi : \mathrm{im}(f) \oplus N \to M, (b, n) \mapsto b + n$
  - $\ker(\psi) = 0$: Let $(b, n) \in \ker(\psi)$, i.e. $n = t(m'')$, for some $m'' \in M''$ and $b = f(m')$ for some $m' \in M'$ and $n + b = 0$ ($\psi(b, n) = 0$).
  - Apply $g : M \to M''$:

$$\underbrace{g(n+b)}_{0} = \underbrace{g(t(m''))}_{g \circ t = \mathrm{id}_{M''}} + \underbrace{g(f(m'))}_{g \circ f = 0} = m'' + 0$$

$$\implies m'' = 0 \implies n = t(m'') = 0 \underset{n+b=0}{\implies} b = 0 \implies (b, n) = (0, 0)$$

  - $\mathrm{im}(\psi) = M$: Let $m \in M$, define $n = t(g(m))$ and $b = m - n$. So $n \in N = \mathrm{im}(f)$. $b \in \mathrm{im}(f)$?, to show $b \in \ker(g)$. For this $g(b) = g(m - n) = g(m) - \underbrace{g(t(g(m)))}_{g \circ t = \mathrm{id}_{M''}} = g(m) - g(m) = 0$, so $(b, n) \in \mathrm{im}(f) \oplus N$ and $\psi(b, n) = b + n = m$ by definition of b.

- $(c) \implies (b)$ analogous. Define $N = \ker(s)$ ($M' \underset{s}{\overset{f}{\rightleftarrows}} M$). We want to show $\mathrm{im}(f) \oplus N \to M, (b, n) \to b + n$ is an isomorphism.
  - $\ker(\psi) = 0$: Check.
  - $\mathrm{im}(\psi) = M$: For $m \in M$ observe that

$$\underbrace{f \circ s(m)}_{\in \mathrm{im}(f)} + \underbrace{(m - f \circ s(m))}_{\in \ker(s) \text{ check.}} = m$$

- $(b) \to (a)$ and (c): Consider the diagram:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f'", "m' \mapsto (f(m'), 0)"'] \arrow[d, "\mathrm{id}_{M'}"] & \mathrm{im}(f) \oplus N \arrow[r, "g'", "(b,n) \mapsto g(n)"'] \arrow[d, "\psi"] \arrow[l, bend right, dashed] & M'' \arrow[r] \arrow[d, "\mathrm{id}_{M''}"] & 0 \\
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] \arrow[l, bend left, dashed, "?"] & M'' \arrow[r] \arrow[l, bend left, dashed, "?"] & 0
\end{tikzcd}$$

The diagram commutes. $\psi \circ f' = f, g \circ \psi = g'$, e.g:

$$\psi \circ f'(m') = \psi(f(m'), 0) = f(m') + 0 = f(m')$$

and

$$g \circ \psi(b, n) = g(b + n) = \underbrace{g(b)}_{=0} = g(n) = g(n) = g'(b, n)$$

($g(b) = 0$ is because $b \in \mathrm{im}(f) = \ker(g)$).

- For s: $f : M' \to \mathrm{im}(f)$ is an isomorphism (f is injective) $\implies$ $f^{-1} : \mathrm{im}(f) \to M'$ is an isomorphism. Check

$$s = (f^{-1}, 0) \circ \psi^{-1} : \ M \xrightarrow{\psi^{-1}} \mathrm{im}(f) \oplus N \xrightarrow{(b,n)\mapsto f^{-1}(b)} M'$$

- For t: Check that $s : N \to M''$ is an isomorphism using (b). Set $t := i \circ g^{-1}$ for i the inclusion so
$$t : M'' \to N \hookrightarrow M$$
Check. $\square$

Remark. $M' \underset{s}{\overset{f}{\rightleftarrows}} M$ and $M'' \underset{g}{\overset{t}{\rightleftarrows}} M$ satisfy the condition from corollary 1.19, namely:

- $s \circ f = \mathrm{id}_{M'}$
- $g \circ t = \mathrm{id}_{M''}$
- $t \circ g + f \circ s = \mathrm{id}_M$

shows again: the sequence is split if $M \cong M' \oplus M''$ (for the "right maps")

Remark 0.29. One also has short exact sequences for groups

$$1 \to \ker(\pi) \overset{s}{\leftrightarrows} G \underset{\pi}{\overset{t}{\leftrightarrows}} \overline{G} \to 1$$

Here one has to be careful what splitting means. Having a t is not equivalent to having an s.

$$\exists t \iff G \cong \ker(\pi) \rtimes \overline{G}$$
$$\exists s \iff G \cong \ker(\pi) \times \overline{G}$$

0.6 Projective Modules

Definition 0.30. An R-module P is called projective $\iff$ it has the following lifting property (LP; Hochhebungseigenschaft): In every diagram of R-modules

$$\begin{tikzcd} & P \arrow[dl, dashed, "\widehat{\varphi}"'] \arrow[d, "\varphi"] & \\ M \arrow[r, "\pi"] & M' \arrow[r] & 0 \end{tikzcd}$$

with π surjective, there exists a lifting $\widehat{\varphi} : P \to M$ such that $\pi \circ \widehat{\varphi} = \varphi$.

Proposition 0.31. *(a) Every free R-module is projective.*

(b) For an R-module P TFAE:

(i) P is projective

(ii) every s.e.s. $0 \to M' \to M \to P \to 0$ of R-modules splits.

(iii) P is a direct summand of a free module, i.e. $\exists R$-module Q, such that $P \oplus Q$ is a free R-module.

Proof. (a) Let $P = R^{(I)}$ for a set I. Consider the diagram

$$\begin{tikzcd} & R^{(I)} \arrow[dl, dashed, "\widehat{\varphi}"'] \arrow[d, "\varphi"] & \\ M \arrow[r, "\pi"] & M' \arrow[r] & 0 \end{tikzcd}$$

Denote by $(e_i)_{i\in I}$ the standard basis of $R^{(I)}$. φ is characterized by $m_i' := \varphi(e_i)$ for all $i \in I$. (by universal property of $R^{(I)} = \bigoplus_{i\in I} R$). Because π is surjective, we can choose a preimage $m_i \in M$ with $\pi(m_i) = m_i'$. Define $\widehat{\varphi} : R^{(I)} \to M$ as the unique R-module-homomorphism with $\widehat{\varphi}(e_i) = m_i$. Then $(\pi \circ \widehat{\varphi})(e_i) = \pi(m_i) = m_i' = \varphi(e_i) \implies \pi \circ \widehat{\varphi} = \varphi$.

(b)
- (i) $\implies$ (ii): Let P be projective, consider a s.e.s.

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] & M \arrow[r, "\pi"] & P \arrow[r] & 0 \\ & & & P \arrow[u, "\mathrm{id}_P"'] \arrow[ul, dashed, "\psi"] & \end{tikzcd}$$

  By the lifting property $\exists \psi : P \to M$ such that $\pi \circ \psi = \mathrm{id}_P$, i.e. ψ is a splitting $\implies$ the s.e.s. splits.

- (ii) $\implies$ (iii): From Remark 21 we have an R-module epimorphism $R^{(I)} \xrightarrow{\pi} P$ (for $I = P$). Take $Q := \ker \pi$ ($\implies$ s.e.s. $0 \to Q \to R^{(I)} \to P \to 0$) By splitness $R^{(I)} = P \oplus Q$ (by Theorem 28).
- (iii) $\implies$ (i): Start with a diagram

$$\begin{tikzcd} & P \arrow[d, "\varphi"] & \\ M \arrow[r, "\pi"] & M' \arrow[r] & 0 \end{tikzcd}$$

  and assume $\exists R$-module Q such that $P \oplus Q = R^{(I)}$ (really $\cong$). Extend φ to

$$P \oplus Q \xrightarrow{\widetilde{\varphi}} M', (p, q) \mapsto \varphi(p) + 0$$

  By (a) $\exists \widehat{\widetilde{\varphi}} : P \oplus Q \to M$ with $\pi \circ \widehat{\widetilde{\varphi}} = \widetilde{\varphi}$.

$$\begin{tikzcd} & P \oplus Q \arrow[dl, dashed, "\widehat{\widetilde{\varphi}}"'] \arrow[d, "\widetilde{\varphi}"] \\ M \arrow[r, "\pi"] & M' \end{tikzcd}$$

  Set $\widehat{\varphi} := \widehat{\widetilde{\varphi}}|_{P\oplus Q} : P \to M$, check $\pi \circ \widehat{\varphi} = \varphi$. $\square$

Corollary 0.32. *Let $0 \to M' \to M \to M'' \to 0$ be a s.e.s. of R-modules.*

(a) M'' projective $\implies$ ($M \cong M' \oplus M''$ and M is projective $\iff$ M' projective).

(b) If M' and M'' are free R-modules, then so is M.

(c) If $M' \cong R^{(I)}$ and $M'' \cong R^{(I'')}$, then $M \cong R^{(I' \cup I'')}$. In particular, $rank(M) = rank(M') + rank(M'')$ if $I' \cup I''$ is finite.

Proof. (c) clear: $R^{(I')} \oplus R^{(I'')} \cong R^{I' \cup I''}$

(c) Follows from (a)

(c)
- First assertion in (a) ($M'' \implies M \cong M' \oplus M''$) from Proposition 31.
- Second assertion: we know $M \cong M' \oplus M''$.
- Suppose first: M is projective. Then by 31(b)(iii): $\exists Q$ an R-module such that $M \oplus Q$

□

Theorem 0.33 (Horse shoe lemma)**.** *Given a diagra of R-modules with P', P'' projective, and the first row exact*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \\
& P' \arrow[u, "\alpha"] & & P'' \arrow[u, "\gamma"'] &
\end{tikzcd}$$

(a) The diagram can be completed by the dotted part to a commutative diagram, for a suitable $\beta : P' \oplus P'' \to M$, so that:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \\
0 \arrow[r, dashed] & P' \arrow[u, "\alpha"] \arrow[r, dashed, "f' : p' \mapsto (p', 0)"'] & P' \oplus P'' \arrow[u, dashed, "\beta"] \arrow[r, dashed, "g' : (p', p'') \mapsto p''"'] & P'' \arrow[u, "\gamma"'] \arrow[r, dashed] & 0
\end{tikzcd}$$

and the second row is then also exact.

(b) If α and γ are surjective, then so is β.

Proof. (a) Construction of β: Use the lifting property of P'' to complete

$$\begin{tikzcd}
M \arrow[r, "g"] & M'' \arrow[r] & 0 \\
& P'' \arrow[u, "\gamma"'] \arrow[ul, dashed, "\widehat{\gamma}"] &
\end{tikzcd}$$

By the diagonal arrow $\widehat{\gamma} : P'' \to M$ to a commutative diagram. Define

$$\beta : P' \oplus P'' \to M, (x', x'') \mapsto f \circ \alpha(x') + \widehat{\gamma}(x'')$$

Check commutativities:

- $\beta \circ f' \stackrel{?}{=} f \circ \alpha$:

$$\beta \circ f'(x') = \beta(x', 0) = f \circ \alpha(x') + \widehat{\gamma}(0)$$

- $\gamma \circ g' \stackrel{?}{=} g \circ \beta$:

$$g \circ \beta(x', x'') = g(f \circ \alpha(x') + \widehat{\gamma}(x'')) = TODO$$

(b) Diagram chase:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \alpha\Big\uparrow & & \beta\Big\uparrow & & \Big\uparrow\gamma & & \\ 0 & \longrightarrow & P' & \xrightarrow{f'} & P & \xrightarrow{g'} & P'' & \longrightarrow & 0 \end{array} \quad TODO$$

To show: β is surjective. Let $m \in M$, γ surjective $\implies \exists x'' \in P'' : \gamma(x'') = g(m)$. g' surjective $\implies \exists x \in P : g'(x) = x'$.

Compare m with $\beta(x)$, consider $m - \beta(x)$. Observe: $g(m - \beta(x)) = g(m) - g \circ \beta(x) = \gamma(x'') - g(x'') = 0$ TODO

□

0.7 Finite generation, exact sequences and $\oplus$

Corollary 0.34. *Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be a s.e.s. of R-modules, then*

(a) If M is finitely generated as R-module, then so is M''

(b) If M' and M'' are finitely generated (as R-modules), then so is M.

Proof. (a) M finitely generated R-module means $\exists$ finite set I and R-module epimorphism $\pi : R^{(I)} \to M \implies R^{(I)} \to M''$ is given by $g \circ \pi$ is an epimorphism
$impM''$ is finitely generated as an R-module.

(b) Suppose we know R-module epimorphisms $\alpha : R^{(I')} \to M'$ and $\gamma : R^{(I'')} \to M''$, then Theorem 33 gives an R-module epimorphism

$$\beta : R^{(I')} \oplus R^{(I'')} \to M$$

$\implies M$ is finitely generated. □

Remark. M is finitely generated as an R-module $\not\Longrightarrow$ $M' \leq M$ is finitely generated. Example: let $R = M = K[X_i \mid i \in \mathbb{N}]$ and consider

$$g : M \to K, X_i \mapsto 0, \forall i$$

The kernel is the ideal I of R generated by $\{X_i \mid i \in \mathbb{N}\}$. We can check: I is not a finitely generated R-module. If $I = (f_1, \dots, f_m)$ say $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ TODO

Corollary 0.35 (exer)**.** *Let $M_1, \dots, M_n$ be R-modules, then*

(a) $M = \bigoplus_{1 \leq i \leq n} M_i$ is finitely generated $\iff$ M_i is finitely generated $\forall i$

(b) Suppose $M_0 \subseteq \cdots \subseteq M_n$ with M_i/M_{i-1} finitely generated for all $i \in \{1, \dots, n\}$. Then M_n is finitely generated.

Theorem 0.36 (Snake lemma)**.** *Suppose we are given the following commutative diagram of R-modules with exact rows.*

$$\begin{array}{ccccccccc} & & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \Big\downarrow\varphi' & & \Big\downarrow\varphi & & \Big\downarrow\varphi'' & & \\ 0 & \longrightarrow & N' & \xrightarrow{f'} & N & \xrightarrow{g'} & N'' & & \end{array}$$

Then:

(a) $\exists R$-linear map δ (called the connecting homomorphism) from $\ker(\varphi'')$ *to* $\operatorname{coker}(\varphi')$*, such that the following sequence of R-modules is exact: TODO*

(b) If f is injective, then so is f.

(c) If g' is surjective, then so is

Proof. Construction of δ: Given $m'' \in \ker \varphi''$ map it to $m'' \in M''$ not $\varphi''(m'') = 0$

□

Theorem 0.37 (5-lemma). *Suppose we are given the following commutative diagram of R-modules with exact rows*

$$\begin{tikzcd}
M_1 \arrow[r, "\alpha"] \arrow[d, two heads, "\varphi_1"] & M_2 \arrow[r, "\beta"] \arrow[d, "\varphi_2"] & M_3 \arrow[r, "\gamma"] \arrow[d, "\varphi_3"] & M_4 \arrow[r, "\delta"] \arrow[d, "\varphi_4"] & M_5 \arrow[d, hook, "\varphi_5"] \\
N_1 \arrow[r, "\alpha'"] & N_2 \arrow[r, "\beta'"] & N_3 \arrow[r, "\gamma'"] & N_4 \arrow[r, "\delta'"] & N_5
\end{tikzcd}$$

and suppose that φ_1 is surjective, φ_5 is injective, and φ_2 and φ_4 are isomorphisms, then φ_3 is also an isomorphism.

Proof. (in parts) Exercise.

1. version: diagram chase.
2. version: break up the diagram into 3 diagrams to which the snake lemma applies. □

0.8 Noetherian and Artinian modules and rings

Let R be a ring, M, M', M'', M_i R-modules. A sequence $(M_i)_{i\in\mathbb{N}}$ is said to *become stationary* if $\exists i_0 : \forall i \geq i_0 : M_i = M_{i_0}$.

Definition 0.38. M is called

(a) noetherian: $\iff$ each ascending chain of submodules

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq \cdots \subseteq M$$

becomes stationary (ACC for ascending chain condition)

(b) artinian: $\iff$ each descending chain of submodules

$$M \supseteq M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

becomes stationary (DCC for descending chain condition)

and R is called

(c) left noetherian: $\iff$ it is noetherian as a left R-module

(d) left artinian: $\iff$ it is artinian as a left R-module

analogously one defines right artinian/noetherian rings and modules.

Examples 0.39. (a) $\mathbb{Z}$ is noetherian but not artinian.

(b) Finite dimensional K-vector spaces are noetherian and artinian (use the dimension-function)

(c) (Exersize) Let D be a skew field (division algebra), then any D-module is a free D-module. If a D-module is finitely generated, it is artinian and noetherian.*In the present case one has a well-defined dimension for finitely generated D-modules.*

(d) Every field and every skew field is left and right artinian and noetherian. (D^{op} is a skew field if D is a skew field)

Definition 0.40. (a) The center of R is $Z(R) := \{r \in R \mid \forall r' \in R : r \cdot r' = r' \cdot r\}$, $Z(R)$ is a commutative subring (exersize)

(b) Let S be any commutative ring and $\varphi : S \to R$ be a ring homomorphism such that $\varphi(S) \subseteq Z(R)$, then R is called an S-algebra (via φ).

Examples. (a) Every ring is a $\mathbb{Z}$-algebra (in a unique way)

(b) $K[X]$ is a K-algebra.

(c) If R is finite dimensional K-algebra, then R is left and right noetherian and artinian. (exercise) For instance, if M is a finite monoid (or a finite group), then the monoid ring $K[M]$ is left and right artinian and noetherian.

(d) $S = \mathbb{Q}$-subalgebra of 2×2 matrices over $\mathbb{Q}$ generated by $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \implies S$ is commutative, but $MM_{2\times 2}(\mathbb{Q})$ over S is not an S-algebra.

Facts 0.41 (Exercise; compare to linear algebra 2 (or Jantzen-Schwermer Ch. VIII.))**.**

(a) For M the following are equivalent:

  (i) Each subset of submodules of M contains a maximal element.

  (ii) Each submodule of M is finitely generated.

(b) For M the following are equivalent:

  (i) M is artinian

  (ii) Each subset of submodules of M contains a minimal element.

Lemma 0.42. *For submodules $N, P_1, P_2 \subseteq M$ with*

(i) $P_1 \supseteq P_2$

(ii) $P_1 + N = P_2 + N$

(iii) $P_1 \cap N = P_2 \cap N$

it follows that $P_1 = P_2$.

Proof. We need to show that $P_1 \subseteq P_2$. Take $m_1 \in P_1 \underset{(ii)}{\Longrightarrow} \exists m_2 \in P_2, n \in N$ such that $m_1 = m_2 + n$. $\Longrightarrow n = m_1 - m_2 \underset{P_2 \subseteq P_1}{\in} P_1 \cap N \underset{(iii)}{=} P_2 \cap N$. $\Longrightarrow m_1 = m_2 + \underbrace{n}_{\in P_2 \cap N} \in P_2$. □

Theorem 0.43. *Let $N \subseteq M$ be a submodule, then*

(a) M is noetherian (artinian) $\Longrightarrow$ N and M/N are noetherian (artinian).

(b) N and M/N are noetherian $\Longleftrightarrow$ M is noetherian (artinian).

Proof. (a) For N: use directly the characterization (ii) from Facts 41. For M/N: use the homomorphism theorem to identify submodules of M/N with those of M containing N and apply again (ii) from 41.

(b) Proof only in the artinian case: assume that N and M/N are artinian. Let $M \supseteq M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$ be a descending chain. Then by hypothesis:

$$M \cap N \supseteq M_0 \cap N \supseteq M_1 \cap N \supseteq \cdots \supseteq M_n \cap N \supseteq \cdots$$

becomes stationary, as does

$$M + N \supseteq M_0 + N \supseteq M_1 + N \supseteq \cdots \supseteq M_n + N \supseteq \cdots$$

$\Longrightarrow \exists i_0 : \forall i \geq i_0 : M_i + N = M_{i_0} + N$ and $M_i \cap N = M_{i_0} \cap N$, we also have $M_i \subseteq M_{i_0}$, so by lemma 42 we have $M_i = M_{i_0} \Longrightarrow (M_i)$ becomes stationary. □

Corollary 0.44 (Exercise)**.**

(a) Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Then M is noetherian (artinian) $\Longleftrightarrow$ M' and M'' are noetherian (artinian).

(b) If I is a finite set and $M := \bigoplus_{i \in I} M_i$, then M is noetherian (artinian) $\Longleftrightarrow$ all M_i are noetherian (artinian).

Note: R left-right noetherian (artinian) $\Longrightarrow$ R^n is also left-right noetherian (artinian) R-module.

Corollary 0.45. *Let R be left noetherian (artinian) and M a finitely generated R-module, then M is noetherian (artinian).*

Proof. $\exists$ an epimorphism $R^n \to M$. Now apply 44(a). □

Corollary 0.46. *Let R be left noetherian (artinian) and $I \subseteq R$ a two-sided ideal, then the ring R/I is also left noetherian (artinian).*

Proof. R/I is a ring (because I is a two-sided ideal). R/I is left noetherian (artinian) as an R-module by 44(a) $\Longrightarrow$ R/I is left noetherian (artinian) as an R/I-module. □

Remark. R is noetherian and $S \subseteq R$ a subring $\not\Longrightarrow$ S is noetherian because not every integral domain is noetherian, but its fraction field certainly is.

Proposition 0.47. *Suppose we have $M \cong M \oplus N$ for some R-module $N \neq 0$. Then M is neither noetherian nor artinian.*

proof sketch. 1. $M \neq 0$ because $N \neq 0$ is a direct summand of it.

2. $M \cong M \oplus N \cong (M \oplus N) \oplus N \cong ((M \oplus N) \oplus N) \oplus N \cong \cdots$.

- ∞ ascending chain:

$$0 \oplus N \subsetneq (0 \oplus N) \oplus N \subsetneq ((0 \oplus N) \oplus N) \oplus N \subsetneq \cdots$$

$\implies M$ is not noetherian.

- ∞ descending chain:

$$M \supsetneq (M \oplus 0) \supsetneq (M \oplus 0) \oplus 0 \supsetneq ((M \oplus 0) \oplus 0) \oplus 0 \supsetneq \cdots$$

$\implies M$ is not artinian. $\square$

Corollary 0.48 (Exercise from 42 and 45)**.** *Suppose $R \neq 0$ is left noetherian (artinian), then for $n_1, n_2 \in \mathbb{N}_0 : R^{n_1} \cong R^{n_2} \implies n_1 = n_2$ (In particular a rank of free finitely generated R-modules is defined.)*

Proof. Assume $\exists n_1, n_2 \in \mathbb{N}_0$ such that $R^{n_1} \cong R^{n_2}$, then $R^{n_1} \cong R^{n_1} \oplus R^{n_2 + n_1} \implies R^{n_1}$ not left noetherian (artinian). But 45 implies that R^{n_1} is left noetherian (artinian) because R has these properties. $\square$

Theorem 0.49 (Hilbert's basis theorem)**.** *If R is left noetherian, then $R[X]$ is left noetherian (here X commutes with elements of R).*

Proof. TODO $\square$

0.9 Simple modules

Let R be a ring, M, M', M'', M_i R-modules.

Definition 0.50. M is called simple (or irreducibile) if $M \neq 0$ and 0 and M are the only R-submodules of M.

Examples 0.51. (a) Simple K-vector spaces are the 1-dimensional K-vectorspaces.

(b) Simple $\mathbb{Z}$-modules are $\mathbb{Z}/p\mathbb{Z}$ for p a prime.

(c) A simple $M_{n \times n}(K)$-module is $V_n(K)$ (space of column vectors).

Definition 0.52. M is said to have a composition series $\iff \exists$ finite descending chain of submodules

$$M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

such that $\forall i \in \{1, \ldots, n\}$: the quotients M_i/M_{i-1} are simple. The index n is called the *length* of M and the quotients M_i/M_{i-1} are called the *factors* of M.