Algebra 2 Lecture Notes from Prof. Gebhard Böckle

Yousef Khell

April 23, 2024

Chapter 1

Modules

1.1 Modules

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

Definition 1.1. (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 1.2 (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 1.3 (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 1.4. 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 1.5. 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 1.6 (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 1.7 (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 $\{\text{operations } * : R \times M \to M \mid (M, 0, +, *) \text{ is an } R\text{-module}\} \leftrightarrow \{\text{ring homomorphisms } \varphi : R \to \mathrm{End}_{\mathbb{Z}}(M)\}$ 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 1.8. (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, $R = M_{n \times n}(K), n > 1, V_n(K) = \text{column } Z_n(K) \text{ row vectors of length } n \text{ over } K$, 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 1.9. 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 1.10. (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 1.11. (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.

Quotient Modules

Definition 1.12. 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 1.13. 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 1.14 (Homomorphism theorem)**.** *Let $\varphi : M \to M'$ be an R-linear map, then*

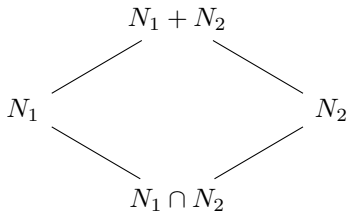
(a) $\forall$ submodules $N \subseteq \ker(\varphi) : \exists! R$-linear map $\overline{\varphi} : M/N \to M', m + N \mapsto \varphi(m)$ such that $\varphi = \overline{\varphi} \circ \pi_{N \subseteq M}$

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

Theorem 1.15. *(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.



Theorem 1.16 (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:

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

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

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

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

Direct sums and products

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

Definition 1.17. (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 1.18 (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 1.19 (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 $M \cong M'$*

1.1.1 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 $M^r := M^{\{1,\dots,r\}}$, so if I is finite then $M^I = M^{\#I} = M^{(I)}$

Definition 1.20. 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 1.21. 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 1.22. *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

$$R^{n_1} \xrightarrow{\cong} R^{n_2} \twoheadrightarrow R^{n_2} \Big/ \mathfrak{m}^{n_2}$$
$$\rho$$

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

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

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

□

Definition 1.23. If M is free and finitely generated, then define $\operatorname{rank}(M)$ (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 $R = \operatorname{End}_K(K[X])$)

1.1.2 Exact sequences

Definition 1.24. (a) A diagram of R-modules

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

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

(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 $\overset{\text{Exercise}}{\iff}$ f is injective.
- $M \xrightarrow{g} M'' \to 0$ is exact $\overset{\text{Exercise}}{\iff}$ g is surjective.

(0 stands for the 0-module $\{0\}$)

Example 1.25. Let $f : M \to N$ be an R-module homomorphism. Then one defines

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

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

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

is exact. Subexamples:

- If f is injective, then $0 \to M \xrightarrow{f} N \to \operatorname{coker}(f) \to 0$ 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 $\operatorname{coker}(\alpha) \cong M/\operatorname{im}(\alpha) \to M''$

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

Proposition 1.26 (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 1.27 (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

$$\begin{array}{ccc} .M_1 & \xrightarrow{f} & M_2 \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g'} \\ M_3 & \xrightarrow[f']{} & M_4 \end{array}$$

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

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

Theorem-Definition 1.28. *For a short exact sequence of R-modules*

$$0 \longrightarrow M' \underset{s}{\overset{f}{\rightleftarrows}} M \underset{t}{\overset{g}{\rightleftarrows}} M'' \longrightarrow 0 \qquad (*)$$

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.

- $(a) \Longrightarrow (b)$: 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 $g : M \to M''$:

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

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

  - $\mathrm{im}(\psi) = M$: 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.

- $(c) \Longrightarrow (b)$ 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:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow[m' \mapsto (f(m'),0)]{f'} & \mathrm{im}(f) \oplus N & \xrightarrow[(b,n)\mapsto g(n)]{g'} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{M'}} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{id}_{M''}} & & \\ 0 & \longrightarrow & M' & \xrightarrow[?]{f} & M & \xrightarrow[?]{g} & M'' & \longrightarrow & 0 \end{array}$$

  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

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

- 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. □

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. One also has short exact sequences for groups

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

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

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