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.

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

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

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

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

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*

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

is a well-defined R-linear isomorphism.

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

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:

$$\{N' \subseteq M \text{ submodule} \mid N \subseteq N'\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{\overline{N} \subseteq {}^{M}\!\diagup_{N} \text{ submodule}\}$$

$$\varphi : N \mapsto {}^{N'}\!\diagup_{N} \qquad \pi^{-1}_{N \subseteq M}(\overline{N}) \leftarrow\!\shortmid \overline{N} : \psi$$

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

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

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

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

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* $M \cong M'$