CHAPTER 3

Modules

3.1. Some generalities about modules

The concept of module generalizes the idea of both vector spaces and ideals. The essential idea is simple: a module is like a vector space where we replace the base field by an arbitrary ring.

3.1.1. Basic definitions.

DEFINITION 3.1.1. Let R be a ring (commutative, with unity). An ***R–module*** is an abelian group $(M, +)$ together with an action of R, i.e a map

$$\begin{array}{rcl} R \times M & \longrightarrow & M \\ (r, m) & \longmapsto & r * m =: rm \in M \end{array}$$

satisfying the following conditions:

M1 **Distributivity:** $r(m + n) = rm + rn$ for all $r \in R$, $m, n \in M$.
M2 **Distributivity:** $(r + s)m = rm + sm$ for all $r, s \in R$, $m \in M$.
M3 **Pseudoassociativity:** $(rs)m = r(sm)$ for all $r, s \in R$, $m \in M$.
M4 **Modularity:** For all $m \in M$ one has $1m = m$.

If this is the case, we will also say that M is a ***module over*** R. When we want to emphasize the R–module structure of M, we will write it as ${}_RM$.

EXAMPLES 3.1.2.

(1) Let $\mathbb{F}$ be a field, then an $\mathbb{F}$–module is precisely a vector space over $\mathbb{F}$.
(2) Let $(M, +)$ be an abelian group. Define the map

$$\begin{array}{rcl} \mathbb{Z} \times M & \longrightarrow & M \\ (r, m) & \longmapsto & rm := \begin{cases} m + m + \overset{(r)}{\cdots} + m & \text{if } r > 0, \\ (-m) + (-m) + \overset{(-r)}{\cdots} + (-m) & \text{if } r < 0, \\ 0 & \text{if } r = 0. \end{cases} \end{array}$$

From the group axioms it can be asily deduced that the previous map defines a $\mathbb{Z}$–action on M. In other words, every abelian group is a $\mathbb{Z}$–module. The converse is also true, if $(M, +)$ is a $\mathbb{Z}$–module the for any $r > 0$ in $\mathbb{Z}$ one has $r = 1 + 1 + \overset{(r)}{\cdots} + 1$, and thus

$$rm = (1 + \cdots + 1)m = 1m + \overset{(r)}{\cdots} + 1m = m + \overset{(r)}{\cdots} + m,$$

and for $r < 0$ one has $r = (-1)+$ thus $\mathbb{Z}$–modules are precisely abelian groups.
(3) Let R be a ring. Define an action of R on $(R, +)$ by $r * s := rs$. By the ring laws this action makes R into an R–module. This action is called the ***(left) regular action*** of R on itself. When we want to refer to R as a module over itself rather than as a ring we will write it as ${}_RR$.

(4) Let R, S be rings, $\varphi : R \to S$ a ring homomorphism, ${}_SM$ an S–module. Consider the map

$$\begin{array}{rcl} R \times M & \longrightarrow & M \\ (r, m) & \longmapsto & r * m := \varphi(r)m. \end{array}$$

The ring morphism axioms, together with the fact that M is an S–module, ensure that this action provides an R–module structure on M. This is called the ***R–module structure induced by*** φ.

In particular, if $R \leq S$ subring, then every S–module is automatically an R–module with the action given by ***restriction of scalars***.

(5) Let V be a vector space over a field $\mathbb{F}$, and $\alpha : V \to V$ a linear map. Define the map

$$\begin{array}{rcl} \mathbb{F}[x] \times V & \longrightarrow & V \\ (x, v) & \longmapsto & x * v := \alpha(v) \end{array}$$

extending to $x^n * v := \alpha^n(v) = \alpha(\alpha(\overset{(n)}{\cdots}\alpha(v)))$ and $(\sum a_i x^i) * v := \sum a_i \alpha^i(v)$. It is an easy exercise to check that under this action V becomes an $\mathbb{F}[x]$–module.

Conversely, if V is a module over the polynomial ring $\mathbb{F}[x]$, since $\mathbb{F} \leq \mathbb{F}[x]$, by the previous example V is automatically an $\mathbb{F}$–module, thus a vector space over $\mathbb{F}$. Now, define $\alpha : V \to V$ by $\alpha(v) := x * v$. By the module axioms, α is an $\mathbb{F}$–linear map, and thus there is a one to one correspondence between $\mathbb{F}[x]$–modules and vector spaces V over $\mathbb{F}$ endowed with a linear map $\alpha : V \to V$.

(6) Let R be any commutative ring. The set $M_n(R)$ of all $n \times n$ matrices with coefficients in R is an R–module under the action $r * (a_{ij}) := (ra_{ij})$.

REMARK. This is a particular case of example 4, with $M = S = M_n(R)$ and $\varphi : R \to S$ given by $\alpha(r) := r \cdot \mathrm{Id}$.

DEFINITION 3.1.3. Let ${}_RM$ be an R–module. A subset $p \subseteq M$ is said to be a ***submodule*** of M if:

(1) P is a subgroup of $(M, +)$, i.e. $P \neq \varnothing$, for all $a, b \in P$ one has $a + b$ in P and $-a \in P$.
(2) For all $r \in R$, and for all $m \in P$ one has $rm \in P$.

If P is a submodule of M we will denote that by $P \leq M$. In this case, P is also an R–module in its own right.

REMARK 3.1.4. P is a submodule of M if and only if for all $m, n \in P$ and for all $r, s \in R$ one has $rm + sn \in P$. The proof is left as an exercise.

EXAMPLES 3.1.5.

(1) If V is a vector space over a field $\mathbb{F}$, then submodules are precisely vector subspaces.
(2) If ${}_ZM$ is an abelian group (i.e. a $\mathbb{Z}$–module), then the submodules of M are its subgroups.
(3) If ${}_RR$ is a ring considered as a module over itself, then the submodules of ${}_RR$ are the ideals of R.
(4) Let V be a module over the polynomial ring $\mathbb{F}[x]$, i.e. V a vector space endowed with a linear map $\alpha : V \to V$. Assume that $P \leq V$ is a sumodule of V. Then, as $\mathbb{F} \subseteq \mathbb{F}[x]$, for all $\lambda \in \mathbb{F}$ and for all $v \in P$ one has $\lambda v \in P$, thus P is a subspace of V. Also, for all $v \in P$ one must have $xp \in P$, but $xp = \alpha(p)$, thus P must satisfy $\alpha(P) \subseteq P$. In other words, P must be an α–invariant subspace of V. Conversely, if P is an α–invariant subspace of V is is easy to see that P is a submodule of V.

(5) For any R–module ${}_RM$ there are two distinguished submodules: the ***trivial submodule*** $0 := \{0\} \leq M$ and the ***total submodule*** $M \leq M$.

PROPOSITION 3.1.6. *If ${}_RM$ is an R–module, and $A, B \leq M$ are submodules of M, then the intersection $A \cap B$ is also a submodule of M. Moreover, $A \cap B$ is the* largest *(with respect to inclusion) sumbodule of M contained in both A and B. More generally, for any family $\{P_\alpha\}$ of sumbodules of M the intersection $\bigcap P_\alpha$ is also a submodule of M.*

PROOF. The proof is left as an exercise. □

PROPOSITION 3.1.7. *Let ${}_RM$ be an R–module, $A, B \leq M$ submodules. Define the sum of A and B as*

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

Then, $A+B$ is a submodule of M. Moreover, it is the smallest *submodule of M containing both A and B. More generally, for any* finite *collection $A_1, \ldots, A_n \leq M$ of submodules of M their sum*

$$\sum_{i=1}^{n} A_i = A_1 + \cdots + A_n = \{a_1 + \cdots + a_n \mid a_i \in A_i\} \leq M$$

is a submodule of M.

PROOF. The proof is left as an exercise. □

The inclusions of submodules given by the last two propositions can be encoded in the following diagram:

$$\begin{tikzcd}
 & A+B & \\
A \arrow[ur] & & B \arrow[ul] \\
 & A \cap B \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

3.1.2. Cyclic modules and finitely generated modules.

DEFINITION 3.1.8. Let ${}_RM$ be an R–module, $x \in M$. Define $Rx := \{rx \mid r \in R\}$. It is easy to check that $Rx \leq M$ is a submodule. The submodule Rx is called the ***cyclic submodule of*** M ***generated by*** x.

REMARK 3.1.9. Rx is the smallest submodule of M containing x.

DEFINITION 3.1.10. If ${}_RM$ is an R–module, and there exist some $x \in M$ such that $M = Rx$, we say that M is a ***cyclic module***.

DEFINITION 3.1.11. Let ${}_RM$ be an R–module, and let $x_1, \ldots, x_n \in M$; the set $Rx_1 + \cdots + Rx_n \leq M$ is the smallest sumbodules of M containing all the x_i. This submodule is called the ***submodule generated by*** $x_1, \ldots, x_n$**.** If $M = Rx_1 + \cdots + Rx_n$ we say that M is ***finitely generated***.

DEFINITION 3.1.12. Let $P \leq M$ be a submodule of the R–module ${}_RM$. Consider the abelian group

$$\frac{M}{P} = \{\overline{m} = m + P \mid m \in M\},$$

where addition is defined in the usual way as $\overline{m} + \overline{n} := \overline{m+n}$. For each $r \in R$ and each $\overline{m} \in M/P$, define $r\overline{m} := \overline{rm}$. This operation yields a well defined action of R on M/P, thus making M/P into an R–module. This module is called the ***quotient of*** M ***b y*** P.

REMARK 3.1.13. For the previous definition to make sense, one needs to check that the action of R on M/P is well defined. This is the case as $\overline{m} = \overline{n}$ if and only if $m-n \in P$, and thus for all $r \in R$ one has $r(m-n) \in P$, yielding $\overline{rm} = \overline{rn}$.

EXAMPLES 3.1.14.

(1) For each R–module ${}_RM$, the submodule $0 = R0$ is a cyclic submodule.
(2) If V is a vector space over $\mathbb{F}$, $0 \neq x \in V$, then the cyclic submodule $\mathbb{F}x$ is the 1–dimensional subspace of V generated by x.
(3) Let M be a $\mathbb{Z}$–module (i.e. an abelian group), $x \in M$, then $\mathbb{Z}x$ is the cyclic subgroup of M generated by x.
(4) Let $x \in {}_RR$, then the cyclic submodule Rx is precisely the principal ideal (x) generated by x. In particular ${}_RR = R1$ is a cyclic R–module.
(5) The quotient of any R–module ${}_RM$ by the trivial submodule 0 is $M/0 = M$.
(6) The quotient of any R–module ${}_RM$ by the total submodule M is $M/M = 0$.
(7) The quotient of the $\mathbb{Z}$–module ${}_{\mathbb{Z}}\mathbb{Z}$ by the cyclic submodule $\mathbb{Z}n = (n)$ is the cyclic group of order n, $\mathbb{Z}_n = \mathbb{Z}/(n)$.

PROPOSITION 3.1.15. *Let ${}_RM$ be an R–module. If $P \leq M$ is a submodule and $\{x_1, \ldots, x_n\} \subseteq M$ generate M, then $\{\overline{x_1}, \ldots, \overline{x_n}\} \subseteq M/P$ generate the quotient module M/P.*

PROOF. Since $x_1, \ldots, x_n$ generate M, for each $m \in M$ there exist $r_1, \ldots, r_n \in R$ such that $m = \sum r_i x_i$, and hence

$$\overline{m} = \overline{\sum r_i x_i} = \sum r_i \overline{x_i},$$

therefore $\{\overline{x_1}, \ldots, \overline{x_n}\}$ generate M/P. □

COROLLARY 3.1.16. *If M is a cyclic R–module, then for any submodule $P \leq M$ the quotient M/P is also cyclic.*

PROOF. By the previous proposition, if $M = Rx$ then $M/P = R\overline{x}$. □

REMARK 3.1.17. Unlike it happens for groups, a submodule of a cyclic module doesn't need to be cyclic. For instance, one can take the R–module ${}_RR = R1$. Its submodules are the ideals of R, and in general ideals do not have to be principal, as long as we take R to be a ring which is not a principal ideal domain.

EXAMPLE 3.1.18. Let us consider the R–module ${}_RR = R1$, which is a cyclic module, and let $I \trianglelefteq R$ be an ideal of R, i.e. a submodule of ${}_RR$, then the quotient R/I is also a cyclic R–module. Indeed, it is generated by $\overline{1} = 1 + I$.

3.1.3. Module homomorphisms.

DEFINITION 3.1.19. Let R be a ring, ${}_RM$ and ${}_RN$ two R–modules; a map $\alpha : M \to N$ is said to be an ***R–module homomorphism*** (also called ***R–homomorphism*** or ***R–linear map***) if it satisfies the following conditions:

(1) α is an additive group homomorphism, i.e. $\alpha(0) = 0$ and $\alpha(m_1 + m_2) = \alpha(m_1) + \alpha(m_2)$ for all $m_1, m_2 \in M$.
(2) For all $r \in R$ and all $m \in M$ one has $\alpha(rm) = r\alpha(m)$

EXAMPLES 3.1.20.

(1) For any two R–modules M and N, there is always a trivial module homomorphism from M to N, the ***zero homomorphism***, defined by $0(m) = 0_N$ for all $m \in M$. This homomorphism is simply denoted by 0.
(2) For any module M, the identity map $\mathrm{Id} : M \to M$ is a module homomorphism. Similarly, if $P \leq M$ is a submodule, the inclusion map $\imath : P \to M$ is also a module homomorphism.

(3) If V, W are vector spaces over a field $\mathbb{F}$, a map $\alpha : V \to W$ is an $\mathbb{F}$–module homomorphism if and only if it is a linear map.
(4) If M, N are $\mathbb{Z}$–modules, i.e. abelian groups, a map $\alpha : M \to N$ is a module homomorphism if and only if it is a group homomorphism.

DEFINITION 3.1.21. Let R be a ring, and let ${}_RM$ and ${}_RN$ be R–modules. We will denote by $\mathrm{Hom}_R(M, N)$ the set of all R–module homomorphisms from M to N, i.e.

$$\mathrm{Hom}_R(M, N) = \mathrm{Hom}(M, N) = \{\alpha : M \to N \mid \alpha \text{ is a module homomorphism}\}.$$

If $\alpha \in \mathrm{Hom}_R(M, N)$, it is easy to see that $-\alpha \in \mathrm{Hom}_R(M, N)$, and that for any $r \in R$ the map $r\alpha$ defined by $(r\alpha)(m) = r\alpha(m)$ is also a module homomorphism. Similarly it is immediate to prove that for any two module homomorphisms $\alpha, \beta \in \mathrm{Hom}_R(M, N)$ the sum map $\alpha + \beta$ is also a module homomorphism. As a consequence, we obtain that the set $\mathrm{Hom}_R(M, N)$ is also an R–module.

PROPOSITION 3.1.22. *Let M ,N and P be R–modules, $\alpha \in \mathrm{Hom}_R(M, N)$ and $\beta \in \mathrm{Hom}_R(N, P)$, then $\beta\alpha := \beta \circ \alpha \in \mathrm{Hom}_R(M, P)$.*

PROOF. The proof is completely straightforward, and thus left as an exercise. □

DEFINITION 3.1.23. Let $\alpha \in \mathrm{Hom}_R(M, N)$. If α is injective, we say that it is a ***monomorphism***, if α is surjective it is called an ***epimorphism***, and if it is bijective it is called an ***isomorphism***. If there exists an isomorphism $\alpha : M \to N$, we will say that M and N are ***isomorphic***, and write $M \cong N$.

DEFINITION 3.1.24. Let R be a ring, M and N two R–modules, $\alpha \in \mathrm{Hom}_R(M, N)$ a module homomorphism. The ***image*** of α is defined as

$$\mathrm{Im}(\alpha) := \{\alpha(m) \mid m \in M\} = \alpha(M),$$

the ***kernel*** of α is defined as

$$\mathrm{Ker}(\alpha) := \{m \in M \mid \alpha(m) = 0\} = \alpha^{-1}(\{0\}).$$

EXAMPLES 3.1.25.

(1) Let ${}_RM$ be an R–module, $P \leq M$ a submodule, and consider the canonical projection $\Pi_P : M \to M/P$ defined by $\pi_P(m) = \overline{m} = m + P$. The map π_P is a module homomorphism and we have $\mathrm{Ker}\,\pi_P = P$ and $\mathrm{Im}\,\pi_P = M/P$, i.e. π_P is an epimorphism.
(2) The zero map $0 : M \to N$, defined as $0(m) = 0_N$ for all $m \in M$, is a module homomorphism. One has $\mathrm{Ker}\,0 = M$, $\mathrm{Im}\,0 = 0$.
(3) $\alpha : M \to N$ is a monomorphism if and only if $\mathrm{Ker}\,\alpha = 0$

PROOF. One has $\alpha(m) = \alpha(n)$ if and only if $0 = \alpha(m) - \alpha(n) = \alpha(m - n)$, i.e. if and only if $m - n \in \mathrm{Ker}\,\alpha$. Thus if $\mathrm{Ker}\,\alpha = 0$ we have $\alpha(m) = \alpha(n)$ if and only if $m = n$, i.e. α is injective. Conversely, if α is injective, then if $0 = \alpha(m)$ we have $\alpha(m) = \alpha(0)$ and by injectivity we get $m = 0$, and hence $\mathrm{Ker}\,\alpha = 0$. □

(4) A module homomorphism $\alpha : M \to N$ is an isomorphism if and only if $\mathrm{Ker}\,\alpha = 0$ and $\mathrm{Im}\,\alpha = N$.

LEMMA 3.1.26. *Let M, N be R–modules, $\alpha \in \mathrm{Hom}_R(M, N)$, then we have:*

(1) $\mathrm{Ker}(\alpha) \leq M$ *is a submodule of* M.
(2) $\mathrm{Im}\,\alpha \leq N$ *is a submodule of* N.

PROOF.

(1) Let $m_1, m_2 \in \operatorname{Ker}\alpha$, $r_1, r_2 \in R$, then, using the fact that α is a homomorphism, we have

$$\alpha(r_1m_1 + r_2m_2) = r_1\alpha(m_1) + r_2\alpha(m_2) = r_10 + r_20 = 0,$$

thus $r_1m_1 + r_2m_2 \in \operatorname{Ker}\alpha$, and hence $\operatorname{Ker}\alpha$ is a submodule of M.

(2) Let $r_1, r_2 \in R$, and let $n_1, n_2 \in \operatorname{Im}\alpha$,.then $n_1 = \alpha(m_1)$ and $n_2 = \alpha(m_2)$ for some $m_1, m_2 \in M$. Thus, we have

$$r_1n_1 + r_2n_2 = r_1\alpha(m_1) + r_2\alpha(m_2) = \alpha(r_1m_1 + r_2m_2),$$

hence $r_1n_1 + r_2n_2 \in \operatorname{Im}\alpha$ and thus $\operatorname{Im}\alpha$ is a submodule of N.

□

THEOREM 3.1.27 (First Isomorphism Theorem for Modules). *Let M, N be R–modules, and $\alpha \in Hom_R(M, N)$ a module homomorphism, then*

$$\frac{M}{\operatorname{Ker}\alpha} \cong \operatorname{Im}\alpha.$$

PROOF. The isomorphism is given by $m + \operatorname{Ker}\alpha \leftrightarrow \alpha(m)$. The proof is almost identical, *mutatis mutandi*, to the one made for ring homomorphisms or for group homomorphisms. □

EXAMPLES 3.1.28.

(1) $0 : M \to M$ the zero homomorphism, $\operatorname{Ker} 0 = M$, $\operatorname{Im} 0 = 0$, so the first isomorphism theorem tells us that $M/M \cong 0$.
(2) $\operatorname{Id} : M \to M$, the identity map, $\operatorname{Ker}\operatorname{Id} = 0$, $\operatorname{Im}\operatorname{Id} = M$, thus $M/0 \cong M$.
(3) Let ${}_RM$ be an R–module, $P \leq M$ a submodule, $\pi_P : M \to M/P$ the canonical projection, so $\operatorname{Ker}\pi_P = P$, $\operatorname{Im}\pi_P = M/P$, and the first isomorphism theorem tells us that $M/P \cong M/P$.

THEOREM 3.1.29 (Classification of cyclic modules). *Let ${}_RM$ be an R–module, then M is cyclic if and only if $M \cong R/I$ for some ideal $I \trianglelefteq R$. Moreover, the ideal I is **unique**.*

REMARK. This result only holds for commutative rings.

PROOF.
$\boxed{\Leftarrow}$ The module $R = R1$ is cyclic, so for any ideal $I \trianglelefteq R$ the quotient R/I is also cyclic (cf. corollary 3.1.16).
$\boxed{\Leftarrow}$ Let M be a cyclic R–module, then there is some $x \in M$ such that $M = Rx$. Define $\alpha : R \to Rx = M$ by $\alpha(r) := rx$. For any $a, b \in {}_RR$, $r, s \in R$ we have

$$\alpha(ra + sb) = (ra + sb)x = rax + sbx = r(ax) + s(bx) = r\alpha(a) + s\alpha(b),$$

thus $\alpha \in \operatorname{Hom}_R({}_RR, Rx)$ is a module homomorphism. As M is cyclic, we get $\operatorname{Im}\alpha = M$, i.e. α is surjective. By the first isomorphism theorem for modules, we get $M \cong R/\operatorname{Ker}\alpha$, where $\operatorname{Ker}\alpha \leq {}_RR$ is a submodule of R. But we know that submodules of R are precisely ideals, thus $\operatorname{Ker}\alpha = I \trianglelefteq R$, and thus $M \cong R/I$.

It remains to prove the uniqueness of the ideal I. Suppose $M \cong R/I \cong R/J$ for two ideals $I, J \trianglelefteq R$. Then there is some R–module isomorphism $\beta : R/I \xrightarrow{\sim} R/J$ (note that β does **not** need to be a ring homomorphism). As β is surjective, there must exist some $\overline{r} = r + I$ such that $\beta(r + I) = 1 + J \in R/J$. For any $i \in I$, on ehas $i\overline{r} = \overline{ir} = \overline{0}$, as $ir \in I$, thus

$$0 + J = \overline{0} = \beta(0 + I) = \beta(i\overline{r}) = i\beta(\overline{r}) = i(1 + J) = i + J,$$

and hence $i \in J$, so we obtain $I \subseteq J$. Doing the same reasoning with the inverse isomorphism $\beta^{-1} : R/J \to R/I$ one gets $J \subseteq I$, and therefore $I = J$. □

DEFINITION 3.1.30. Let ${}_RM$ be an R–module, $X \subseteq M$ a nonempty subset of M. The ***annihilator*** of X is defined by

$$\operatorname{ann}(X) := \{r \in R \mid rx = 0 \ \forall x \in X\}.$$

PROPOSITION 3.1.31. *For ${}_RM$ R–module and $X \subseteq M$, the annihilator $\operatorname{ann}(X)$ is an ideal of R.*

PROOF. Proof is straightforward and left as an exercise. □

REMARK 3.1.32. If $Rx \subseteq M$ is a cyclic submodule of an R–module M, and we define the map $\alpha : R \to Rx$ by $\alpha(r) := rx$, as in the proof of the previous theorem, then $\operatorname{Ker}\alpha$ is precisely the annihilator $\operatorname{ann}(x)$. In other words, we have

$$Rx \cong \frac{R}{\operatorname{ann}(x)}.$$

PROPOSITION 3.1.33. *For any subset $X \subseteq M$, one has $\operatorname{ann}(X) = \bigcap_{x \in X} \operatorname{ann}(x)$.*

PROOF. Exercise. □

EXAMPLES 3.1.34.

(1) Let $(M, +)$ be an abelian group, $0 \neq x \in M$ an element of order n, i.e. n is the smallest positive integer such that $nx = 0$. Then $\operatorname{ann}(x) = (n) \trianglelefteq \mathbb{Z}$, and $\mathbb{Z}x = \mathbb{Z}/(n) = \mathbb{Z}_n$.
(2) Let ${}_{\mathbb{F}}M$ be a module over a field $\mathbb{F}$ (i.e. M is a vector space over $\mathbb{F}$), and let $0 \neq x \in M$ be a nonzero vector. Suppose that there is some scalar $\lambda \in F$ such that $\lambda \in \operatorname{ann}(x)$, i.e. $\lambda x = 0$. As x is a nonzero vector, the set $\{x\}$ is linearly independent, so if $\lambda x = 0$ it must be $\lambda = 0$, hence $\operatorname{ann}(x) = 0$, and $\mathbb{F}x \cong \mathbb{F}/0 \cong \mathbb{F}$ as a vector space.
(3) Let R be an **ID**, $0 \neq x \in R$, then $\operatorname{ann}(x) = 0$ (prove it as an exercise!), and hence $(x) = Rx \cong R/ =\cong R$ as R–modules.

THEOREM 3.1.35 (Second Isomorphism Theorem for modules). *Let ${}_RM$ be an R–module, $A, B \leq M$ submodules, then*

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}.$$

PROOF. The proof is similar to the one for rings. □

THEOREM 3.1.36 (Third Isomorphism Theorem for modules). *Let ${}_RM$ be an R–module, $P \leq M$ a submodule. There is a bijection between the set $\{Q \leq M \mid P \subseteq Q\}$ of submodules of M containing P, and the set of submodules of M/P, given by $Q \mapsto Q/P$. Moreover, one has*

$$\frac{M/P}{Q/P} \cong M/Q.$$

3.1.4. Direct sum of modules. We have already classified cyclic modules, which will be our basic "building blocks". Now, we shall study the construction that will allow us to glue these building block together.

DEFINITION 3.1.37. Let $M_1, \ldots, M_n$ be R–modules. Let M be the set

$$M = \{(m_1, \ldots, m_n) \mid m_i \in M_i\}$$

of ordered n–tuples in $M_1 \times \cdots \times M_n$. In the set M, define

$$\begin{gathered}(m_1, \ldots, m_n) + (m'_1, \ldots, m'_n) := (m_1 + m'_1, \ldots, m_n + m'_n),\\ 0 = (0_{M_1}, \ldots, 0_{M_n}),\\ -(m_1, \ldots, m_n) := (-m_1, \ldots, -m_n),\\ r(m_1, \ldots, m_n) := (rm_1, \ldots, rm_n).\end{gathered}$$

Endowed with these operations, M becomes an R–module, called the ***external direct sum*** of the modules M_i. We will represent this as

$$M = M_1 \oplus \cdots \oplus M_n = \bigoplus_{i=1}^{n} M_i.$$

Given an external direct sum $M = \bigoplus M_i$, we will denote by

$$M_i' := \{(0, \ldots, m_i, 0, \ldots, 0) \mid m_i \in M_i\},$$

where the only possibly nonzero coordinate is in position i. Obviously M_i' is a submodule of M, and the maps $m_i \longleftrightarrow (0, \ldots, m_i, 0, \ldots, 0)$ provide a module isomorphism $M_i \cong M_i'$. Henceforth, we can identify the modules M_i with the M_i' and thus think of M_i as submodules of M.

Question: Given an R–module ${}_RM$ and submodules $M_i \leq M$, when can we ensure that $M \cong M_1 \oplus \cdots \oplus M_n$? What properties must the submodules M_i satisfy?

If it is the case that we can rewrite a module M as a direct sum of certain submodules $M_i \leq M$, we say that M is an ***internal direct sum*** of the M_i's.

Firstly, let $m \in M = \bigoplus M_i$, then

$$m = (m_1, \ldots, m_n) = (m_1, 0, \ldots, 0) + \cdots + (0, \ldots, 0, m_n),$$

and hence we get $M = M_1 + \cdots + M_n = \sum M_i$. Secondly, if $m_i \in M_i$ then $m_i = (0, \ldots, 0, m_i, 0, \ldots, 0)$, and $m_1 + \cdots + m_n = 0$ if and only if $(m_1, \ldots, m_n) = (0, \ldots, 0)$, i.e if and only if $m_i = 0$ for all i. This condition leads us to the following notion:

DEFINITION 3.1.38. Let ${}_RM$ be an R–module, $M_1, \ldots, M_n \leq M$ submodules of M. We say that $\{M_i\}_{i=1}^n$ is an ***independent set of submodules*** if whenever $m_1 + \cdots + m_n = 0$ for some $m_i \in M_i$, then one must have $m_i = 0$ for all $i = 1, \ldots, n$.

REMARK 3.1.39. From what we have stated above, if $M = \bigoplus M_i$, then $\{M_i\}$ is always an independent set of submodules. This also means that "being independent" is not an intrinsic property of the submodules, but rather of the way they are included inside M.

PROPOSITION 3.1.40. *Let ${}_RM$ be an R–module, $M_i \leq M$ for $i = 1, \ldots, n$ submodules. The following are equivalent:*

(1) $\{M_1, \ldots, M_n\}$ is an independent set of modules.
*(2) Any $m \in M_1 + \cdots + M_n$ can be written as $m = m_1 + \cdots + m_n$ for **unique** $m_i \in M_i$.*
(3) For each $i = 1, \ldots, n$ one has $M_i \cap \widehat{M_i} = 0$, where $\widehat{M_i} = \sum i \neq j M_i$.

PROOF.
1 ⇒ 2 If $m = m_1 + \cdots + m_n = m_1' + \cdots + m_n'$m then $0 = (m_1 - m_1') + \cdots + (m_n - m_n')$, where $m - i - m_i' \in M_i$, thus $m_i - m_i' = 0$ and thus $m_i = m_i'$ for all $i = 1, \ldots, m_n$, i.e. the m_i are unique.
2 ⇒ 3 Let $m \in M_i \cap \widehat{M_i}$, then $m = m_i = m_1 + \cdots + m_{i-1} + m_{i+1} + \cdots + m_n$, thus $m_1 + \cdots + m_{i-1} - m_i + m_{i+1} + \cdots + m_n = 0$, and hence $m_1 = \cdots = m_n = 0$, implying $m = 0$.
3 ⇒ 1 □

EXAMPLE 3.1.41. Let ${}_RM$ be an R–module, $A, B \leq M$ submodules, then $\{A, B\}$ is an independent set of modules if and only if $A \cap B = 0$.

PROPOSITION 3.1.42. *Let ${}_RM$ be an R–module, $M_1, \ldots, M_n \leq M$ submodule. The following are equivalent:*

(1) $M = \bigoplus_{i=1}^n M_i$.
(2) $M = \sum_{i=1}^n M_i$ and $\{M_i\}$ is an independent set of modules.

PROOF.
1 $\Rightarrow$ **2** Already shown above.
1 $\Rightarrow$ **1** Define $\alpha : M \to \bigoplus M_i$ by $m \mapsto (m_1, \dots, m_n)$, where $m_1, \dots, m_n$ are the unique elements with $m_i \in M_i$ such that $m = m_1 + \cdots + m_n$. Clearly, α is a surjective module homomorphism. Let $m \in \operatorname{Ker}\alpha$, then $\alpha(m) = 0 = (0, \dots, 0)$ and thus $m = 0 + 0 + \cdots + 0 = 0$, hence α is injective and therefore an isomorphism.

□

EXAMPLE 3.1.43. Let ${}_RM$ be an R–module, A, B submodules, then $M = A \oplus B$ if and only if $M = A + B$ and $A \cap B = 0$. In this case, A and B are called ***direct summands*** of M and B is called a ***complement*** of B in M.

REMARK 3.1.44. If $M = A \oplus B$, then using the second isomorphism theorem we have

$$\frac{M}{A} = \frac{A \oplus B}{A} = \frac{A + B}{A} \cong \frac{B}{A \cap B} = \frac{B}{0} \cong B.$$

Similarly, we obtain $(A \oplus B)/B \cong A$.

DEFINITION 3.1.45. If $M_1 = M_2 = \cdots = M_n = M$, we will represent the external direct sum $M_1 \oplus \cdots \oplus M_n = M \oplus \cdots \oplus M$ simply by M^n.

3.1.5. Free modules.

DEFINITION 3.1.46. Let R be a ring. A module of the form ${}_RR^n = {}_RR \oplus \overset{(n)}{\cdots} \oplus {}_RR$ is called a ***free module*** over R.

DEFINITION 3.1.47. Let $\{e_1, \dots, e_n\} \subseteq M$ be a subset of an R–module M. We say that the set $\{e_1, \dots, e_n\}$ is a ***basis*** for M if for all $m \in M$ there exist **unique** $r_i \in R$ such that $m = r_1e_1 + \cdots + r_ne_n$.

PROPOSITION 3.1.48. *Let ${}_RM$ be an R–module, the following are equivalent:*

(1) M is a free module.
(2) M has a basis.

PROOF.
1 $\Rightarrow$ **2**: Suppose $M = R^n$ is a free module, let $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, where the 1 is in the i–th position. If $m \in M = R^n$, then $m = (r_1, \dots, r_n)$ with $r_i \in R$, and hence $m = r_1e_1 + \cdots + r_ne_n$ for unique $r_i \in R$.
2 $\Rightarrow$ **1**: Let $\{e_1, \dots, e_n\}$ be a basis of M, then for each $m \in M$ there exist unique $r_i \in R$ such that $m = r_1e_1 + \cdots + r_ne_n$. Define the map $\alpha : M \to R^n$ by $\alpha(m) := (r_1, \dots, r_n)$. It is easy to check that this is an R–module isomorphism, showing that $M \cong R^n$. □

REMARK 3.1.49. If $\{e_i\}$ is a basis of M and $r \in R$ is such that $re_i = 0$, then $0 = 0e_1 + \cdots + 0e_{i-1} + re_i + 0e_{n+1} + \cdots + 0e_n$, and hence $r = 0$, thus $\operatorname{ann}(e_i) = 0$ and $Re_i \cong R/(0) = R$. Henceforth, for any module with a basis we have $M \cong Re_1 \oplus \cdots \oplus Re_n \cong R \oplus \overset{(n)}{\cdots} \oplus R = R^n$.

PROPOSITION 3.1.50. *Let $F = R^n$ be a free module with basis $\{e_1, \dots, e_n\}$. Let ${}_RM$ be a module over R, and let $m_1, \dots, m_n \in M$. Then, there is a **unique** R–module homomorphism $\alpha : F \to M$ such that $\alpha(e_i) = m_i$.*

REMARK. In other words, the proposition states that any module homomorphism having as a source a free module is completely determined by its effect on the elements of a basis.

PROOF. Let $u = r_1e_1 + \cdots + r_ne_n$. Assume that α is a module homomorphism such that $\alpha(e_i) = m_i$; then, necessarily we must have

$$\alpha(u) = \alpha(r_1e_1 + \cdots + r_ne_n) = r_1\alpha(e_1) + \cdots + r_n\alpha(e_n) = r_1m_1 + \cdots + r_nm_n,$$

and hence α is uniquely defined. Thus, define $\alpha : F \to M$ by $\alpha(r_1e_1 + \cdots + r_ne_n) := r_1m_1 + \cdots + r_nm_n$; we only need to show that α is a module homomorphism.

Let $r, s \in R$, $u = u_1e_1 + \cdots + u_ne_n, v = v_1e_1 + \cdots + v_ne_n \in F$, then

$$\begin{aligned}
\alpha(ru + sv) &= \alpha\left(\sum(ru_i + sv_i)e_i\right) \\
&= \sum(ru_i + sv_i)m_i \\
&= \sum ru_im_i + \sum sv_im_i \\
&= r\sum u_im_i + s\sum v_im_i \\
&= r\alpha(u) + s\alpha(v),
\end{aligned}$$

therefor α is an R–module homomorphism, and clearly it verifies $\alpha(e_i) = m_i$. □

PROPOSITION 3.1.51. *Let ${}_RM$ be a finitely generated R–module, so that $M = Rm_1 + \cdots Rm_n$ for some $m_i \in M$; then, there exists a free module F and a submodule $P \leq F$ such that $M \cong F/P$.*

PROOF. Leet $F = R^n$, consider the unique module homomorphism $\alpha : F \to M$ satisfying $\alpha(e_i) = m_i$. If $m \in M$, then there exist $r_i \in R$ such that $m = r_1m_1 + \cdots + r_nm_n$, and hence

$$\alpha(r_1e_1 + \cdots r_ne_n) = \sum r_i\alpha(e_i) = \sum r_im_i = m,$$

thus α is surjective, i.e. $\operatorname{Im}\alpha = M$. Applying the first isomorphism theorem for modules, we conclude that $M \cong F/\operatorname{Ker}\alpha$, where $\operatorname{Ker}\alpha$ is a submodule of F. □