3. Modules

Definition: Let R be a commutative ring with identity. A (left) R-module [dt. R-Modul] is an abelian group $(M,+)$ with a function $R\times M\to M$, $(x,m)\mapsto x\cdot m$ such that

(i) $(x+y)m = xm+ym \quad \forall x,y\in R \ \forall m\in M$,

(ii) $x(m+n) = xm+xn \quad \forall x\in R \ \forall m,n\in M$,

(iii) $x(ym) = (xy)m \quad \forall x,y\in R \ \forall m\in M$,

(iv) $1_R\cdot m = m \quad \forall m\in M$.

Remark. There are other, more general definitions of a module.

Examples: 1) If R is a field an R-module is the same as an R-vector space.

2) An abelian group is the same as a $\mathbb{Z}$-module. Each ($\mathbb{Z}$-)module is an abelian group by definition. If $(G,+)$ is an abelian group then the equations

$$(m+n)a = ma+na \quad \forall m,n\in\mathbb{Z} \ \forall a\in G,$$
$$m(a+b) = ma+mb \quad \forall m\in\mathbb{Z} \ \forall a,b\in G,$$
$$m(na) = (mn)a \quad \forall m,n\in\mathbb{Z} \ \forall a\in G$$
$$1\cdot a = a \quad \forall a\in G$$

(which are checked in algebra) shows that G is a $\mathbb{Z}$-module.

3) If R is a commutative ring with identity and S a subring of R with $1_S=1_R$ then R is an S-module (where $x\cdot y$ with $x\in S$ and $y\in R$ is the product of elements of R).

4) If R is a commutative ring with identity the polynomial ring $R[x_1,\dots,x_n]$ is an R-module. (This is a special case of 3).)

5) If R is a commutative ring with identity and I an ideal of R then I is an R-module.

6) If R is a commutative ring with identity and $n\in\mathbb{N}$ then R^n can be made into an R-module by setting $(x_1,\dots,x_n)+(y_1,\dots,y_n):=(x_1+y_1,\dots,x_n+y_n)$ and $a(x_1,\dots,x_n)=(ax_1,\dots,ax_n)$ for $a,x_1,\dots,x_n,y_1,\dots,y_n\in R$.

Remark: The examples above shows that it can be very misleading to imagine that an R-module is "just a vector space over a ring R." The structure of modules is much more complicated than that of vector spaces.

Lemma 36 Let R be a commutative ring with identity and M an R-module.

(i) $0_R \cdot m = 0_M \quad \forall m \in M$,

(ii) $\alpha \cdot 0_M = 0_M \quad \forall \alpha \in R$,

(iii) $(-1)\cdot m = -m \quad \forall m \in M$.

Proof: (i) $0\cdot m = (0+0)\cdot m = 0\cdot m + 0\cdot m \Rightarrow 0 = 0\cdot m + (-0\cdot m) = 0\cdot m + 0\cdot m + (-0\cdot m) = 0\cdot m$

(ii) $\alpha\cdot 0 = \alpha\cdot(0+0) = \alpha\cdot 0 + \alpha\cdot 0 \Rightarrow 0 = \alpha\cdot 0 + (-\alpha\cdot 0) = \alpha\cdot 0 + \alpha\cdot 0 + (-\alpha\cdot 0) = \alpha\cdot 0$

(iii) $(-1)\cdot m + m = (-1)\cdot m + 1\cdot m = ((-1)+1)\cdot m = 0\cdot m \overset{(i)}{=} 0$ (and $m + (-1)\cdot m = 0$)

imply $(-1)\cdot m = -m$.

Definition Let R be a commutative ring with identity, M an R-module and $(N,+)$ a subgroup of $(M,+)$ such that $\alpha m \in N \ \forall \alpha \in R \ \forall m \in N$. Then N is called a submodule of M [dt. Untermodul von M].

Remarks: 1) Clearly, a submodule of an R-module is also an R-module.

2) To check that $N \subseteq M$ is a submodule, it suffices to prove that $m+n \in N \ \forall m,n \in N$ and that $\alpha m \in N \ \forall \alpha \in R \ \forall m \in N$. (If $m \in N$ then $-m = (-1)m \in N$ by Lemma 36(iii). Therefore, $m - n = m + (-n) \in N \ \forall m,n \in N$ and $(N,+)$ is a subgroup of $(M,+)$.)

Examples: 1) Every R-module M has the submodules $\{0\}$ and M.

2) If R is a field, an R-module V is an R-vector space and each subspace of V is an R-submodule of V.

3) If G is an abelian group, G is a $\mathbb{Z}$-module and each subgroup of G is a $\mathbb{Z}$-submodule of G.

4) If R is a commutative ring with identity and I an ideal of R then I is an R-submodule of R.

5) If $I \neq \emptyset$ is an index set and N_i is a submodule of the R-module M $\forall i \in I$ then $\bigcap_{i\in I} N_i$ is a submodule of M. (We know from algebra that $(\bigcap_{i\in I} N_i, +)$ is a subgroup of $(M,+)$. If $\alpha \in R$ and $m \in \bigcap_{i\in I} N_i$ then $m \in N_i \ \forall i \in I \Rightarrow \alpha m \in N_i \ \forall i \in I \Rightarrow \alpha m \in \bigcap_{i\in I} N_i$.)

Definition: Let R be a commutative ring with identity, M an R-module and $X \subseteq M$. Then $\langle X \rangle_R = \bigcap_{\substack{X \subseteq N \\ N \text{ is submodule}}} N$ is called the submodule generated by X (or spanned by X) [dt. der von X erzeugte Untermodul].

Definition: Let R be a commutative ring with identity and M an R-module. If there is a finite $X \subseteq M$ such that $\langle X \rangle_R = M$ then M is said to be finitely generated.

Theorem 37 Let R be a commutative ring with identity, M an R-module and $X \subseteq M$.
Then $\langle X \rangle_R = \left\{ \sum_{i=1}^{k} \alpha_i m_i \;\middle|\; \alpha_i \in R \text{ and } m_i \in X \text{ for } 1 \le i \le k \right\}$.

Proof: Let $N_0 := \left\{ \sum_{i=1}^{k} \alpha_i m_i \;\middle|\; \alpha_i \in R \text{ and } m_i \in X \text{ for } 1 \le i \le k \right\}$. Then $X \subseteq N_0$ (as $m = 1 \cdot m \in N_0 \ \forall m \in X$) and N_0 is a submodule of M (as $\sum_{i=1}^{k} \alpha_i m_i + \sum_{i=k+1}^{k+l} \alpha_i m_i = \sum_{i=1}^{k+l} \alpha_i m_i \in N_0$ and $\beta \sum_{i=1}^{k} \alpha_i m_i = \sum_{i=1}^{k} (\beta \alpha_i) m_i \in N_0$ if $\alpha_i \in R$ and $m_i \in X$ for $1 \le i \le k+l$ and $\beta \in R$).

This proves $\langle X \rangle_R \subseteq N_0$.

If N is a submodule with $X \subseteq N$ then $\sum_{i=1}^{k} \alpha_i m_i \in N$ if $\alpha_i \in R$ and $m_i \in X$ for $1 \le i \le k$.

I.e., $N_0 \subseteq N$ and therefore $N_0 \subseteq \bigcap_{\substack{X \subseteq N \\ N \text{ submodule}}} N = \langle X \rangle_R$.

Definition: Let R be a commutative ring with identity and M and N two R-modules. A map $\varphi : M \to N$ which satisfies

1) $\varphi(m+n) = \varphi(m) + \varphi(n) \ \forall m, n \in M$,
2) $\varphi(\alpha m) = \alpha \varphi(m) \ \forall \alpha \in R \ \forall m \in M$

is called an R-module homomorphism [dt R-Modul Homomorphismus].

An R-module homomorphism φ is called an R-module monomorphism (resp. epimorphism resp. isomorphism) if φ is injective (resp. surjective resp. bijective).

Examples: 1) If V and W are two K-vector spaces any K-linear map $\varphi : V \to W$ is a K-module homomorphism.

2) If $(G,+)$ and $(H,+)$ are two abelian groups any group homomorphism $\varphi : G \to H$ is a $\mathbb{Z}$-module homomorphism.

3) If R is a commutative ring with identity and M and N are two R-modules the map $\varphi : M \to N$, $\varphi(m) = 0_N \ \forall m \in M$ is an R-module homomorphism

4) If R is a commutative ring with identity the map $\varphi : R[X] \to R[X]$, $p(X) \mapsto X \cdot p(X)$ is an R-module homomorphism (as $X \cdot (p(X) + q(X)) = X \cdot p(X) + X \cdot q(X) \ \forall p, q \in R[X]$ and $X \cdot (\alpha p(X)) = \alpha \cdot (X p(X)) \ \forall \alpha \in R \ \forall p \in R[X]$) but not a ring homomorphism (as $\varphi(X^2) = X \cdot X^2 = X^3$ but $\varphi(X)\varphi(X) = (X \cdot X) \cdot (X \cdot X) = X^4$).

Definition: Two R-modules M and N are called isomorphic (i.e., $M \cong N$) if there is an R-module isomorphism $\varphi : M \to N$.

If $\varphi : M \to N$ is an R-module homomorphism then $\ker \varphi := \{ m \in M \mid \varphi(m) = 0 \} = \varphi^{-1}(\{0\})$ is called the kernel of φ and $\operatorname{Im} \varphi = \{ \varphi(m) \mid m \in M \} = \{ n \in N \mid \exists m \in M : \varphi(m) = n \} = \varphi(M)$ is called the image of φ.

Remarks: 1) Being isomorphic is an equivalence relation of R-modules. If M is an R-module then $M \cong M$ (as $id_M : M \to M$ is an isomorphism), if $M \cong N$ then $N \cong M$ (as $\varphi^{-1} : N \to M$ is an isomorphism if $\varphi : M \to N$ is an isomorphism) and $M \cong N$ and $N \cong L$ imply $M \cong L$ (if $\varphi : M \to N$ and $\psi : N \to L$ are isomorphisms then $\psi \circ \varphi : M \to L$ is an isomorphism).

2) An R-module homomorphism $\varphi : M \to N$ is an isomorphism if and only if there is an R-module homomorphism $\psi : N \to M$ such that $\psi \circ \varphi = id_M$ and $\varphi \circ \psi = id_N$.

7.11.2022

Lemma 38 Let R be a commutative ring with identity, M and N two R-modules and $\varphi : M \to N$ an R-module homomorphism.

(i) If M' is a submodule of M then $\varphi(M')$ is a submodule of N,

(ii) If N' is a submodule of N then $\varphi^{-1}(N')$ is a submodule of M.

Proof: (i) If $m_1, m_2 \in M'$ ($\Rightarrow \varphi(m_1), \varphi(m_2) \in \varphi(M')$) then $\varphi(m_1) + \varphi(m_2) = \varphi(\underbrace{m_1+m_2}_{\in M'}) \in \varphi(M')$

If $\alpha \in R$ and $m \in M'$ ($\Rightarrow \varphi(m) \in \varphi(M')$) then $\alpha\varphi(m) = \varphi(\underbrace{\alpha m}_{\in M'}) \in \varphi(M')$.

(ii) If $m_1, m_2 \in M$ with $\varphi(m_1), \varphi(m_2) \in N'$ (i.e., $m_1, m_2 \in \varphi^{-1}(N')$) then $\varphi(m_1+m_2) = \varphi(m_1) + \varphi(m_2) \in N'$, i.e., $m_1 + m_2 \in \varphi^{-1}(N')$. If $\alpha \in R$ and $m \in M$ with $\varphi(m) \in N'$ (i.e., $m \in \varphi^{-1}(N')$) then $\varphi(\alpha m) = \alpha\varphi(m) \in N'$, i.e., $\alpha m \in \varphi^{-1}(N')$.

Corollary 39 Let R be a commutative ring with identity, M and N two R-modules and $\varphi : M \to N$ an R-module homomorphism.

(i) $\ker\varphi$ is a submodule of M,

(ii) $\operatorname{Im}\varphi$ is a submodule of N.

Proof: (i) Follows from Lemma 38 (ii) as $\ker\varphi = \varphi^{-1}(\{0\})$ and $\{0\}$ is a submodule of N.

(ii) Follows from Lemma 38 (i) as $\operatorname{Im}\varphi = \varphi(M)$ and M is a submodule of M.

Theorem 40 Let R be a commutative ring with identity, M an R-module and N a submodule of M.

(i) The factor group $(M/N, +)$ (with addition $(m+N) + (n+N) := (m+n) + N \ \forall m,n \in M$) can be made into an R-module by setting $\alpha \cdot (m+N) := (\alpha m) + N \ \forall \alpha \in R \ \forall m \in M$.

(ii) The map $\varphi : M \to M/N$, $\varphi(m) = m + N$ is an R-module epimorphism with $\ker\varphi = N$.

Proof: (i) We already know (from algebra) that $(M/N, +)$ is an abelian group. If $m + N = n + N$ for some $m, n \in M$ then $m - n \in N \Rightarrow \alpha m - \alpha n = \alpha(m-n) \in N$ $\Rightarrow \alpha m + N = \alpha n + N$, i.e., this is well defined. For all $\alpha, \beta \in R$ and $m, n \in M$ we have

- $(\alpha+\beta)(m+N) = ((\alpha+\beta)m)+N = (\alpha m+\beta m)+N = (\alpha m+N)+(\beta m+N) = \alpha(m+N)+\beta(m+N)$
- $\alpha((m+N)+(n+N)) = \alpha((m+n)+N) = (\alpha(m+n))+N = (\alpha m+\alpha n)+N = (\alpha m+N)+(\alpha n+N)$
  $= \alpha(m+N)+\alpha(n+N)$
- $\alpha(\beta(m+N)) = \alpha((\beta m)+N) = (\alpha(\beta m))+N = ((\alpha\beta)m)+N = (\alpha\beta)(m+N)$
- $1\cdot(m+N) = (1\cdot m)+N = m+N$

(ii) We already know (from algebra) that $M \to M/N$, $\varphi(m) = m+N$ is a group epimorphism with $\ker\varphi = N$. As $\varphi(\alpha m) = (\alpha m)+N = \alpha(m+N) = \alpha\varphi(m)$ $\forall \alpha\in R$ $\forall m\in M$ it is also an R-module homomorphism.