# Algebra

11.6,11.13

## 4.1 Modules and Homomorphism

**Definition.** *Let $R$ be a ring. $M$ is a $R$-module if there exists a binary operation $+$ on $M$,and a map $R \times M \to M$ (denoted by $(r, m) = rm$) such that for any $a, b, c \in M$,$r, s \in R$,we have*
*(1a)* $a + b = b + a$
*(1b)* $(a + b) + c = a + (b + c)$
*(1c)* $a + 0 = a$
*(1d) there exists* $-a \in M$ *s.t* $a + (-a) = 0$
*(2)* $r(a + b) = ra + rb$
*(3)* $(r + s)a = ra + rb$
*(4)* $(rs)a = r(sa)$
*(5) If* $1 \in R$ *then* $1a = a$

Note:
1. Right R-module can be defined similarly,
2. we always assume a module is a left module.

We always assume M is a R-module.

**ex.** *$M = \mathbb{R}^n$,$R = \mathbb{R}$ with $+$ on $M$, and $R \times M \to M$ defined as in high school. Hence $\mathbb{R}^n$ is $\mathbb{R} - module$*

**ex.** *Let $R \subseteq M$ be two rings. Then $M$ is $R$-module.*

**ex.** *Fix an* $n \times n$ *matrix* $A$ *over* $\mathbb{R}$*. Set* $R = \mathbb{R}[x]$ *and* $M = \mathbb{R}^n$*. Then* $+$ *on* $M$ *is natural. For* $f(x) \in \mathbb{R}[x]$ *and* $u \in \mathbb{R}^n$ *define* $f(x)u = f(A)u$*. Then* $\mathbb{R}^n$ *is a* $\mathbb{R}[x]$*-module.*

*proof.* Check (4)
$(f(x)g(x))u = f(x)(g(x)u)$ for $f(x), g(x) \in \mathbb{R}[x]$ and $u \in \mathbb{R}^n$;
$(f(x)g(x))u = (f(A)g(A))u = f(A)(g(A)u) = f(x)g(A)u = f(x)(g(x)u)$ □

Note: In previous example, we can set $R = \{f(A)|f(x) \in \mathbb{R}[x]\}$ and then $\mathbb{R}^n$ is a R-module, but we do not prefer to this setting.

**Lemma.** *(1)* $r0_M = 0_M$*,*
*(2)* $0_R = 0_M$*,*
*(3) (-r)a=r(-a)=-(ra)*
*for all* $r \in R$*,* $a \in M$

*proof.* (1) $r0_M + r0_M = r(0_M + 0_M) = r0_M$, we have $r0_M = 0$.
(2),(3) can be done similarly. □

**Definition.** $N \subseteq M$ *is a R-submodule of M if N is a R-module with the same* $+, \cdot$ *inherited from M.*

**ex.** $M = \{(a_1, a_2, a_3)|a_i \in \mathbb{R}\}$
$N = \{(a_1, a_2, 0)|a_i \in \mathbb{R}\}$
$\Rightarrow$ *N is a* $\mathbb{R}$*-submodule of M.*
*(Check closed* $a_1 + a_2 \in N$ *and* $ra_1 \in N$*)*

**Definition.** *Let N be a R-submodule of M. Set* $M/N := \{a + N|a \in M\}$ *and* $(a+N)+(b+N) = (a+b)+N$ *and* $r(a+N) = (ra)+N$*. Then* $M/N$ *is a R-module called the quotient module of M by N.*

**ex.** $M = \mathbb{Q}$*,*$N = \mathbb{Z}$*,*$R = \mathbb{Z}$*,*$\Rightarrow$ $\mathbb{Q}/\mathbb{Z}$ *is a* $\mathbb{Z}$*-module.*
*Note:*$\mathbb{Q}/\mathbb{Z} = \{a + \mathbb{Z}|a \in [0, 1) \cap \mathbb{Q}\}$

**Definition.** *For $S \subseteq M$, let $(s)$ denote the intersection of all R-submodules containing S.*
*(The intersection of R-submodules is a R-submodule.)*

Note: 1. If H,K are R-submodules of M, then $(H \cup K) = H + K$.
2. (S) is finite generated if $|S| < \infty$
3. (S) is cyclic if $|S| = 1$.

**Definition.** *Let M,N be R-module. A map $f : M \mapsto N$ is a R-module homomorphism if*
*(1) $f(a+b) = f(a) + f(b)$*
*(2) $f(ra) = rf(a)$*
*Note:*
*(1) If R is a field, a R-module homomorphism is also called a linear transformation.*
*(2) A R-module isomorphism is a bijective R-module homomorphism.*

Three theorem for homomorphisms.

**Theorem.** *Let $f : M \mapsto N$ be R-module homomorphism and $kerf := \{a \in M | f(a) = 0\}$. Then $kerf$ is a R-submodule of M and $M/kerf$ is isomorphic to $f(M)$*

**Theorem.** *Let K,N be R-submodule of M. Then $(K+N)/N$ is isomorphic to $K/K \cap N$.*

**Theorem.** *Let $K \subseteq N$ be R-submodules of M. Then $N/K$ is a R-submodule of $M/K$ and $(M/K)/(N/K)$ is isomorphic to $M/N$.*

*proof.* "mutatis mutandis"="with those things having been changed which need to be changed." $\square$

**Definition.** *For $m \in M$, $0_m := \{r \in R | rm = 0\}$ is called the order ideal of m, or the amihilator of m.*
*Note: $0_m$ is an ideal of R.*

**Prop.** *For $m \in M$, the R-submodule $(m)$ is isomorphic to the R-module $R/O_m$.*

*proof.* Let $f := R \mapsto (m)$ by $f(r) = rm$. Hence f is surjective R-module homomorphism with $kerf = 0_m$.
By homomorphism theorem, $R/0_m \cong rangf = (m)$ □

**ex.** *$R = \mathbb{Z}$,$(M = \mathbb{Z} \times \mathbb{Z})/((2,2) \times (4,-2))$. Find $0_{\overline{(1,1)}}$ and $0_{\overline{(1,0)}}$*

Sol: $0_{\overline{(1,1)}} = 2\mathbb{Z}$,$0_{\overline{(1,0)}} = 6\mathbb{Z}$

**Definition.** *$M_t := \{m \in M | 0_m \neq 0\}$ is called the torsion R-submodule of M, where R is commutative.*
*If $M_t = M$, then M is called a torsion module.*
*If $M_t = 0$, then M is called torsion-free.*