

$$(M1) \quad \alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v);$$

$$(M2) \quad (\alpha + \beta) \cdot u = (\alpha \cdot u) + (\beta \cdot u);$$

$$(M3) \quad (\alpha * \beta) \cdot u = \alpha \cdot (\beta \cdot u);$$

$$(M4) \quad 1 \cdot u = u.$$

Given $\alpha \in A$ and $v \in M$, the element $\alpha \cdot v$ is also denoted by αv . The ring A is often called the ring of scalars.

Unless specified otherwise or unless we are dealing with several different rings, in the rest of this chapter, we assume that all A -modules are defined with respect to a fixed ring A . Thus, we will refer to a A -module simply as a module.

From (M0), a module always contains the null vector 0, and thus is nonempty. From (M1), we get $\alpha \cdot 0 = 0$, and $\alpha \cdot (-v) = -(\alpha \cdot v)$. From (M2), we get $0 \cdot v = 0$, and $(-\alpha) \cdot v = -(\alpha \cdot v)$. The ring A itself can be viewed as a module over itself, addition of vectors being addition in the ring, and multiplication by a scalar being multiplication in the ring.

When the ring A is a field, an A -module is a vector space. When $A = \mathbb{Z}$, a \mathbb{Z} -module is just an abelian group, with the action given by

$$\begin{aligned} 0 \cdot u &= 0, \\ n \cdot u &= \underbrace{u + \cdots + u}_n, & n > 0 \\ n \cdot u &= -(-n) \cdot u, & n < 0. \end{aligned}$$

All definitions from Section 3.4, linear combinations, linear independence and linear dependence, subspaces renamed as *submodules*, apply unchanged to modules. Proposition 3.5 also holds for the module spanned by a set of vectors. The definition of a basis (Definition 3.6) also applies to modules, but the only result from Section 3.5 that holds for modules is Proposition 3.12. Unfortunately, it is longer true that every module has a basis. For example, for any nonzero integer $n \in \mathbb{Z}$, the \mathbb{Z} -module $\mathbb{Z}/n\mathbb{Z}$ has no basis since $n \cdot \bar{x} = 0$ for all $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$. Similarly, \mathbb{Q} , as a \mathbb{Z} -module, has no basis. Any two distinct nonzero elements p_1/q_1 and p_2/q_2 are linearly dependent, since

$$(p_2 q_1) \left(\frac{p_1}{q_1} \right) - (p_1 q_2) \left(\frac{p_2}{q_2} \right) = 0.$$

Furthermore, the \mathbb{Z} -module \mathbb{Q} is not finitely generated. For if $\{p_1/q_1, \dots, p_n/q_n\} \subset \mathbb{Q}$ generated \mathbb{Q} , then for any $x = r/s \in \mathbb{Q}$, we have

$$c_1 \frac{p_1}{q_1} + \cdots + c_n \frac{p_n}{q_n} = \frac{r}{s},$$