10 Introduction to Module Theory

10.1 Definitions and examples.

Definition. A *semigroup* $(S, \cdot)$ is a nonempty set S with an associative binary operation $\cdot$

Example.

$(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$

Set of functions $\{f : X \to X\}$ under composition.

A group $(G, \cdot)$ is a semigroup such that

1) $\exists 1 \in G \ \forall a \in G: \quad 1 \cdot a = a$

2) $\forall a \in G \ \exists a^{-1} \in G: \quad a^{-1} \cdot a = 1$

Definition. A *ring* $(R, +, \cdot)$ is a nonempty set R with binary operations $+, \cdot$ such that

(1) $(R, +)$ is an abelian group,
(2) $(R, \cdot)$ is a semigroup,
(3) For all $a, b, c \in R$

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc$$

left & right distributive

Example.

$\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
polynomial ring $\mathbb{Z}[x]$ } commutative rings } rings with 1
$n \times n$ matrix ring $M_n(\mathbb{Z})$
$2\mathbb{Z}$ ring without 1

Definition. A ring $(R, +, \cdot)$ is *commutative* if $\cdot$ is commutative.
$(R, +, \cdot)$ is a *ring with* 1 if $\exists 1 \in R \ \forall a \in R$

$$1 \cdot a = a \cdot 1 = a$$

Matrices act on vectors by multiplication. We formalize this idea:

Definition. Let R be a ring. A *left R-module* M is an abelian group $(M, +)$ with a map

$$R \times M \to M, \ (r, m) \mapsto rm$$

such that $\forall r, s \in R, m, n \in M$

(1) $(r + s)m = rm + sm$,
(2) $r(sm) = (r \cdot s)m$,
(3) $r(m + n) = rm + rn$.

cf. group actions
R acts linearly on M

If R has a 1, then also

(4) $1 \cdot m = m$.

Remark.

- Modules over fields are called vector spaces
- *Right modules* are defined similarly.
- Modules satisfying (4) are called *unital* or *unitary*.
- $(R, +)$ is not a group action on $(M, +)$ since (1) implies $0 \cdot m = 0 \ \forall m \in M$, (4) yields $(-1)m = -m$.

Convention. All our rings have 1. All modules are left, unital modules.

Example. Let R be a ring.

1) R is an R-module (regular R-module) where
$R \times R \to R$, $(r, s) \mapsto rs$ ring multiplication.

2) $M_n(R)$ is an R-module via
$(rA)_{ij} := (rA_{ij})$

3) R^n is an R-module (the free R-module of rank n).

4) R^n is a $M_n(R)$-module via

$$A \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} := \begin{bmatrix} \sum A_{1i} \cdot x_i \\ \vdots \\ \sum A_{ni} \cdot x_i \end{bmatrix}$$