Beginning of Aug. 22, 2022

Some Preliminaries

Groups and Rings

Definition: Group

A **group** is a set G with a binary operation $\cdot$ on G satisfying:

(1) (identity) there exists (unique) $e \in G$ with $eg = ge = g$ for all $g \in G$,

(2) (inverse) for $g \in G$, there exists $h \in G$ satisfying $gh = hg = e$ (in which case we write h as g^{-1}), and

(3) (associativity) for all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

We say G is **Abelian** if we in addition have commutativity.

Examples of groups:

- $(\mathbb{Z}, +), (\mathbb{C}, +), (\mathbb{R}[x], +)$ where $\mathbb{R}[x]$ denotes the set of real coefficient polynomials.
- For X nonempty, $\text{Sym}(X) := \{f : X \to X : f \text{ is bijective}\}$ under composition is called the symmetric group. In particular if $|X| = n$ then $|\text{Sym}(X)| = n!$.
- $\text{GL}_n(\mathbb{C})$ or $\text{GL}_n(\mathbb{R})$, the general linear group (of real/complex invertible matrices). More generally, $\text{GL}(V)$, the group of all invertible linear transformations of vector space V (finite- or infinite- dimensional).

Definition: Subgroup

A **subgroup** H of G is a subset $H \subset G$ which is a group itself under the same operation.

Example: given an arbitrary vector space V, $\text{GL}(V)$ is a subgroup of $\text{Sym}(V)$.

Definition: Ring (assumed to have unit)

A **ring** is a set R with two binary operations, $+$ and $\cdot$, such that:

(1) $(R, +)$ is Abelian with 0 being the additive identity,

(2) $(R, \cdot)$ is a *monoid* (associative, has identity, but not ncessarily satisfies the inverse property),

(3) $0 \neq 1$, and

(4) $(R, +, \cdot)$ is (left and right) distributive: $(r + s)t = rt + st$ and $r(s + t) = rs + rt$.

A **subring** is a subset $S \subset R$ which is itself a ring under the same two operations.

Examples of rings: $(\mathbb{Z}, +, \cdot), (\mathbb{R}[x], +, \cdot)$, $\underline{M_{n\times n}(\mathbb{R})}$, and ring of continuous functions on $[0, 1]$ with pointwise addition and multiplication.

Different types of rings:

(1) R is called a **commutative ring** if $rs = sr$ for all $r, s \in R$. (E.g. $M_{n\times n}(\mathbb{R})$ is NOT commutative.)

(2) R is called a **domain** if $rs = 0$ implies either $r = 0$ or $s = 0$.

(3) R is called an **integral domain** if R is a commutative domain. (E.g. $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{R}[x], +, \cdot)$.)

(4) R is called a **division ring** or (skew field) if $R^* = R\backslash\{0\}$ is a group (namely, every nonzero element has a two-sided inverse).

† An example of division ring but not a field: the quaternion algebra or Hamiltonians $\mathbb{H}$. Let i, j, k be elements satisfying $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i$, and $ki = j$. Define

$$D := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

with component-wise addition and multiplication based on distributive law. Then

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2,$$

so every (nonzero) element has a multiplication inverse. To visualize i, j, k, consider

$$i := \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix} \qquad j := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad k := ij.$$

(5) R is called a **field** if it is a commutative division ring. (E.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition and multiplication; $\mathbb{R}(x) :=$ set of rational functions, i.e., $f(x)/g(x)$ where $f, g \in \mathbb{R}[x]$ and $g \not\equiv 0$.)

Definition: Left *R*-module

Let R be a ring. A **left *R*-module** is an Abelian group $(M, +)$ with identity 0 such that there exists a function $R \times M \to M$, $(r, m) \to rm$, scalar multiplication, satisfying

(1) $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$,

(2) $r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$ and $m_1, m_2 \in M$, and

(3) $r(sm) = (rs)m$, and

(4) $1m = m$ for all $m \in M$.

If R is a field, then M is a vector space.

Examples:

- R itself is a left R-module (left multiplication).
- $\mathbb{R}^n$ with coordinate-wise addition and

$$r \cdot (r_1, ..., r_n) := (rr_1, ..., rr_n).$$

Linear Independence, Spam, and Basis

Definition: Linear Independence

Let M be a R-module. We say $m_1, \ldots, m_n$ are **linearly independent** if whenever $r_i \in R$,

$$\sum_{i=1}^{n} r_i m_i = 0 \implies r_1 = \ldots = r_n = 0.$$

For an infinite collection, we say they are linearly independent if any finite subcollection satisfies the above implication.
We say $m_1, \ldots, m_n$ **span** M if every element of M can be written as a linear combination of the m_i's, i.e., of form $r_1 m_1 + r_2 m_2 + \ldots$ for $r_i \in R$. If $\{m_1, \ldots, m_n\}$ both spam M and are linearly independent, we say they are a **basis** of M. (Here we assume a finite basis exists.) If the basis is finite we say M is **finite-dimensional**. Also, such M is called a **free *R*-module** if it has a basis.

Example:

- $\mathbb{Q}$ is not a free $\mathbb{Z}$-module. If it had a basis it must only consist of one element, but the $\mathbb{Z}$-multiples of that rational number cannot possibly span $\mathbb{Q}$.
- Conversely, $\mathbb{Q}$ is a free $\mathbb{Q}$-module for obvious reasons, for any rational can be represented as a rational times another rational.

Proposition

Every finite spanning set contains a basis.

Proof. Let S be a spanning set $\{v_1, \ldots, v_m\}$. If it is linearly independent then we are done. If not, then there exist nonzero coefficients $a_1, \ldots, a_m$ with $\sum_{i=1}^{m} a_i v_i = 0$. By relabelling and assusming $a_m \neq 0$, we have

$$a_m v_m = -a_1 v_1 - \ldots - a_{m-1} v_{m-1},$$

and by multiplying a_m^{-1},

$$v_m = \sum_{n=1}^{m-1} -\frac{a_n}{a_m} \cdot v_{m-1},$$

so any linear combination of S can be re-written as a linear combination of $\{v_1, \ldots, v_{m-1}\}$. By induction, if S does not contain a basis, eventually S reduces to $\varnothing$ whose span is $\{0\}$ by convention, contradiction, unless the space is itself $\{0\}$, but in that case $\{0\}$, the only possible finite spanning set, is still a basis. □

Remark. Similarly, if V is finite-dimensional, then any linearly independent subset is contained in a basis.