Linear Algebra & Matrix Theory

Review elementary linear algebra from a more advanced point of view, add topics, work over general fields.

Summary of algebraic structures covered in other algebra courses:

Def. A semigroup is a set G equipped with a binary operation $\cdot : G \times G \to G$ denoted $g_1 \cdot g_2 \in G$, $\forall g_1, g_2 \in G$, such that $\cdot$ is associative, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.

Note: We will use standard set theory concepts and notations.

Since a semigroup involves both G and $\cdot$ it is formally an ordered pair $(G, \cdot)$.

<u>Example</u>: Let $S = \{a_1, \ldots, a_n\}$ be a finite set (called letters) and let

$$G = \{w = a_{i_1} a_{i_2} \cdots a_{i_r} \mid a_{i_j} \in S\}$$

be the set of finite sequences from S.

Say $w \in G$ is "a word" from S.

Define binary operation "concatenation" on G by

$$(a_{i_1} \cdots a_{i_r}) \cdot (a_{j_1} \cdots a_{j_s}) = a_{i_1} \cdots a_{i_r} a_{j_1} \cdots a_{j_s}$$

Then $(G, \cdot)$ is a semigroup.

Def. A <u>monoid</u> is a semigroup $(G,\cdot)$ such that $\exists e \in G$ which is an <u>identity element</u>, that is, $\forall g \in G$, $g \cdot e = g = e \cdot g$. We denote the monoid by the triple $(G,\cdot,e)$.

Ex. In the previous example where G is the semigroup of words made from letters in S, if the empty word is included ($r=0$, no letters), then that is an identity element for concatenation.

Prop: In monoid $(G,\cdot,e)$ there can be only one identity element (uniqueness).

Pf. If $\forall g \in G$, $g \cdot e_1 = g = e_1 \cdot g$ and $g \cdot e_2 = g = e_2 \cdot g$ then $e_1 = e_1 \cdot e_2 = e_2$. $\square$

Def. A *group* is a monoid $(G, \cdot, e)$ such that every $g \in G$ has an "inverse", $\forall g \in G$, $\exists\, h \in G$ (depending on choice of g) s.t. $g \cdot h = e = h \cdot g$.

Prop. In a group G, each $g \in G$ has a unique inverse, which we denote by g^{-1}.

Pf. Fix $g \in G$ and suppose h_1 and h_2 are both inverses for g, so

$$g \cdot h_1 = e = h_1 \cdot g \quad \text{and} \quad g \cdot h_2 = e = h_2 \cdot g.$$

Then, since $\cdot$ is associative, we have

$$h_2 = e \cdot h_2 = (h_1 \cdot g) \cdot h_2 = h_1 \cdot (g \cdot h_2) = h_1 \cdot e = h_1.$$

$\square$

Def $(G, \cdot, e)$ is called *abelian* if $a \cdot b = b \cdot a$, $\forall a, b \in G$.

Prop. Let $(G, \cdot, e)$ be a group. Then $\forall a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

pf We have $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot (b^{-1} \cdot a^{-1}))$
$= a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e$
and $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot (a \cdot b)) =$
$b^{-1} \cdot ((a^{-1} \cdot a) \cdot b) = b^{-1} \cdot (e \cdot b) = b^{-1} \cdot b = e$.
So $x = b^{-1} \cdot a^{-1}$ satisfies $(a \cdot b) \cdot x = e = x \cdot (a \cdot b)$
and by uniqueness of inverses in a group,
$x = (a \cdot b)^{-1}$. $\square$

Prop. For $a_1, \cdots, a_r \in G$ any elements of group G we have $(a_1 \cdots a_r)^{-1} = a_r^{-1} \cdots a_1^{-1}$.

pf: By induction on $1 \le r \in \mathbb{Z}$. (Exercise)

Examples: You can devote your entire life to the study of groups and still not know it all. Most basic examples:

① Permutation groups: Let S be any set.

$$\mathrm{Perm}(S) = \{f : S \to S \mid f \text{ is bijective}\}$$

with composition of functions as the binary operation. For $|S| = n$ finite,

$$\mathrm{Perm}(S) = S_n = \left\{ f = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ f(1) & f(2) & \cdots & f(i) & \cdots & f(n) \end{pmatrix} \;\middle|\; \begin{matrix} f(1), \ldots f(n) \in S \\ \text{are distinct} \end{matrix} \right\}$$

$S = \{1, 2, \ldots, n\}$.

② Symmetries of an object (n-gon in plane, tetrahedren, cube, octahedron, icosahedron, tilings of plane, ...)

③ $(\mathbb{Z}, +, 0)$ integers under addition

④ $(\mathbb{Q}, +, 0)$ rationals " "

⑤ $(\mathbb{R}, +, 0)$ real numbers " "

⑥ $(\mathbb{C}, +, 0)$ complex numbers " "

⑦ $(\mathbb{Q}-\{0\}, \cdot, 1)$ non-zero rational numbers under multiplication

⑧ $(\mathbb{R}-\{0\}, \cdot, 1)$ non-zero real numbers under mult.

⑨ $(\mathbb{C}-\{0\}, \cdot, 1)$ non-zero complex numbers under mult.

⑩ $(\mathbb{R}_{>0}, \cdot, 1)$ positive reals under mult.

⑪ Matrix groups found in linear algebra:
$GL(n, \mathbb{F})$, $SL(n, \mathbb{F})$, ...

Def. Say group $(G, \cdot, e)$ acts on set S (left action) when have a map (function)

$\bullet : G \times S \to S$ s.t.

① $a \bullet (b \bullet s) = (a \cdot b) \bullet s$ $\forall a, b \in G, \forall s \in S,$

② $e \bullet s = s$, $\forall s \in S.$

Def. A ring $(R, +, \cdot, 0)$ is a set R with two binary operations $+$ (addition) and $\cdot$ (mult) such that

① $(R, +, 0)$ is an abelian group,

② $(R, \cdot)$ is a semigroup,

③ Distributive Laws hold:

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

R is commutative if $a \cdot b = b \cdot a$ $\forall a, b \in R$

R may have an id. elt. for mult.

Def. An R-module is an abelian group $(M,+,0)$ such that ring R acts on M:

① $r\circ(m_1+m_2)=(r\circ m_1)+(r\circ m_2)$

② $(r_1+r_2)\circ m=(r_1\circ m)+(r_2\circ m)$

③ $(r_1\cdot r_2)\circ m=r_1\circ(r_2\circ m)$

$\boxed{\circ : R\times M\to M \text{ satisfies ①-③.}}$

Ex: $(\mathbb{Z},+,\cdot,0,1)$ is a comm. ring with unity elt. 1 under usual $+$ and $\cdot$ of integers.

$(\mathbb{Q},+,\cdot,0,1)$ "same" for rationals

$(\mathbb{R},+,\cdot,0,1)$ " " reals

$(\mathbb{C},+,\cdot,0,1)$ " " complex numbers.

$(\mathbb{Q},+,0)$, $(\mathbb{R},+,0)$, $(\mathbb{C},+,0)$ are each $\mathbb{Z}$-modules

Def. $(\mathbb{F}, +, \cdot, 0, 1)$ is a <u>field</u> if
1. It is a commutative ring with unity elt. 1
2. $(\mathbb{F}-\{0\}, \cdot, 1)$ is an abelian group.

<u>Examples:</u> $\mathbb{F} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$.
For p prime in $\mathbb{Z}$, $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, integers modulo p, is a <u>finite</u> field.

The theories of rings (and their modules) and fields (extensions, Galois theory) are very rich, covered in other courses in the algebra sequence.

Def. Let $(\mathbb{F}, +, \cdot, 0, 1)$ be a field. A <u>vector space</u> over $\mathbb{F}$, $(V, +, \theta)$ is an abelian group, whose operation $+$ has "zero vector" θ to distinguish it from the $0 \in \mathbb{F}$, and with an action of $\mathbb{F}$ on V, so V is an $\mathbb{F}$-module. The action of $\mathbb{F}$ on V is called "scalar multiplication". In detail:

1. $+ : V \times V \to V$ closure of V under vector $+$
2. $\cdot : \mathbb{F} \times V \to V$ closure of V under scalar mult. $\cdot$
3. $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$ assoc of vector $+$
4. $v_1 + v_2 = v_2 + v_1$ $+$ is abelian (comm.)
5. $\exists\, \theta \in V,\ \forall v \in V,\ v + \theta = v$ [$= \theta + v$ by 4] θ is unique
6. $\forall v \in V,\ \exists -v \in V$ s.t. $v + (-v) = \theta$ additive inverse
7. $\forall \alpha \in \mathbb{F},\ \forall v_1, v_2 \in V,\ \alpha \cdot (v_1 + v_2) = (\alpha \cdot v_1) + (\alpha \cdot v_2)$
8. $\forall \alpha_1, \alpha_2 \in F\ \forall v \in V,\ (\alpha_1 + \alpha_2) \cdot v = (\alpha_1 \cdot v) + (\alpha_2 \cdot v_2)$
9. $\alpha_1 \cdot (\alpha_2 \cdot v) = (\alpha_1 \cdot \alpha_2) \cdot v$
10. $1 \cdot v = v$

Ex: $m \times n$ matrices with entries from $\mathbb{F}$.

Def. Let $1 \le m, n \in \mathbb{Z}$. Let

$$\mathbb{F}_n^m = \{A = [a_{ij}] \mid 1 \le i \le m,\ 1 \le j \le n,\ a_{ij} \in \mathbb{F}\}$$

be the set of all $m \times n$ matrices over $\mathbb{F}$, so

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

is a rectangular array of elements (entries) from $\mathbb{F}$ where a_{ij} is the entry in row i and column j.

For $A = [a_{ij}]$, $B = [b_{ij}] \in \mathbb{F}_n^m$ define

$A + B = C = [c_{ij}] \in \mathbb{F}_n^m$ by $c_{ij} = a_{ij} + b_{ij}$

and for $\alpha \in \mathbb{F}$ define

$\alpha \cdot A = [\alpha \cdot a_{ij}] \in \mathbb{F}_n^m$, and let $O_n^m = [0] \in \mathbb{F}_n^m$ be the $m \times n$ matrix with all entries 0.

Th: $(\mathbb{F}_n^m, +, 0_n^m)$ is a vector space over $\mathbb{F}$.

pf. Exercise.

Notation: We write $\mathbb{F}_1^m = \mathbb{F}^m$ and $\mathbb{F}_n^1 = \mathbb{F}_n$

so $\mathbb{F}^m = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} \middle| \, a_i \in \mathbb{F}, 1 \le i \le m \right\}$ "column vectors"

and

$\mathbb{F}_n = \{ [a_1 \; a_2 \cdots a_n] \mid a_j \in \mathbb{F}, \; 1 \le j \le n \}$ "row vectors."

since double subscripts are not needed.

In our textbook almost all examples use

$\mathbb{F} = \mathbb{R}$ (real vector spaces) or

$\mathbb{F} = \mathbb{C}$ (complex vector spaces).

Most theorems are true for vector spaces over any field.