Linear Algebra 2 Notes

paraphrased by Tyler Wright

*An important note, these notes are absolutely **NOT** guaranteed to be correct, representative of the course, or rigorous. Any result of this is not the author's fault.*

1 Groups, Rings, and Fields

1.1 Definition of a Group

A group is a set G combined with a group operation $\circ : G \times G \to G$ such that:

- For all g, h, j in G, $g(hj) = (gh)j$ (associativity)
- There exists e in G such that $eg = ge = g$ for all g in G
- For all g in G, there exists g^{-1} in G such that $gg^{-1} = g^{-1}g = e$ where e is the identity of G.

1.2 Definition of a Homomorphism

A homomorphism between two groups G, H is a function $f : G \to H$ such that $f(gh) = f(g)f(h)$ for all g, h in G.

1.3 Properties of Homomorphisms

We can derive some properties of homomorphisms, for G, H groups, and $f : G \to H$ a homomorphism:

- The image of the identity in G is the identity in H
- The kernel of f is a subgroup of G
- The image of f is a subgroup of H
- Bijective homomorphisms are isomorphisms.

1.4 Definition of a Ring

A ring with unity is a set R along with an addition map $+$, and a multiplication map $\circ$ where $+, \circ : R \times R \to R$ such that:

- $(R, +)$ is an abelian group (of which the identity is called zero)
- The multiplication operation is associative
- The multiplication operation has a two-sided identity not equal to the zero identity (called one)
- For all a, b, c in R, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

A ring is commutative if the multiplication operation is commutative.

1.5 Definition of a Subring

For the ring $R = (R', +, \circ)$ and S a set, S is a subring of R if $S \subseteq R'$ and $(S, +, \circ)$ is a ring.

1.6 Definition of a Ring Homomorphism

For rings with unity R and S, $f : R \to S$ is a ring homomorphism if for all a, b in R:

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \\ f(1) &= 1 \end{aligned}$$

Essentially, this says that f is a homomorphism for the groups formed by R and S under addition and multiplication. It is also important to note that
$R \ni f(1) = 1 \in S$.

1.7 Definition of a Field

A field $\mathbb{F}$ is a ring with unity with the following properties:

- $(\mathbb{F} \setminus \{0\}, \circ)$ is an abelian group.

1.8 Definition of the Field Characteristic

For a field $\mathbb{F}$, the field characteristic char($\mathbb{F}$) is the smallest positive integer n such that:

$$\sum_{i=1}^{n} 1 = 1 + 1 + \ldots + 1 = 0,$$

or zero if no such value n exists.

1.9 Definition of the Algebraic Closure of Fields

A field $\mathbb{F}$ is called algebraically closed if all non-constant polynomials with coefficients in $\mathbb{F}$ also has a root in $\mathbb{F}$.

2 Vector Spaces

2.1 Definition of a Vector Space

A vector space over a field $\mathbb{F}$ is a set V with an addition operation $+ : V \times V \to V$ and a scalar multiplication operations $\circ : \mathbb{F} \times V \to V$ such that for all a, b in $\mathbb{F}$ and v, w in V:

- $(V, +)$ is an abelian group
- $1 \circ v = v$ where 1 is the multiplicative identity of $\mathbb{F}$
- $(ab) \circ v = a \circ (b \circ v)$
- $(a + b) \circ v = a \circ v + b \circ v$
- $a \circ (v + w) = a \circ v + a \circ w$.

2.2 Definition of a Subspace

For V a vector space over the field $\mathbb{F}$ and W a set, W is a subspace of V if it is a subset of V and is a vector space with respect to the addition and scalar multiplication defined by V.

It is sufficient to verify that for any a in $\mathbb{F}$ and v, w in W we have that $a(v + w)$ is in W.

2.3 Definition of a Linear Combination

For a set V with addition operation $+$, a field $\mathbb{F}$ and n in $\mathbb{N}$, a linear combination of $v_1, \ldots, v_n$ in V is:

$$\sum_{i=1}^{n} a_i v_i,$$

for $a_1, \ldots, a_n$ in $\mathbb{F}$.

2.4 Definition of the Span

For a set V with addition operation $+$ and a field $\mathbb{F}$, the span of $W \subseteq V$ is the set of all the linear combinations of the values in W. Denoted by $\mathrm{span}(W)$.

2.5 Definition of Linear Independence

For a vector space V and $W \subseteq V$, we say W is linearly dependent if there exists a non-trivial linear combination of all the vectors in W equal to zero (and linearly independent otherwise).

2.6 Properties of Linear Independence

For a vector space V with $W \subseteq V$:

- $0 \in W \Rightarrow W$ is linearly independent
- W linearly independent $\Rightarrow$ any $X \subseteq W$ is linearly independent
- If there's a linearly dependent subset of W, then W is linearly dependent.

2.7 Definition of a Basis

For a vector space V with $W \subseteq V$, if W is linearly independent and $\text{span}(W) = V$, we say that W is a basis of V.

Saying W is a basis is equivalent to saying that each vector in V can be **uniquely** written as a linear combination of vectors in W.

Additionally, for finite vector spaces, we have that all bases have the same amount of elements.

2.8 Definition of Dimension

For non-infinite bases, we say that the value of the basis is the dimension of the vector space it is a member of. Vector spaces with such bases are called finite-dimensional and all other vector spaces are infinite-dimensional.