Artin's Algebra Notes

Henry Lin

November 2025

1 Introduction

2 Vector Spaces

There are two operations on vectors:

1. vector addition
2. scalar multiplication

With only vector addition, this makes the vector spaces a commutative(Abelian) group, but it has more structure to it because of the scalar multiplication. These operations(addition and multiplication) make $\mathbb{R}^n$ into a vector space. A subset W of $\mathbb{R}^n$ is a subspace if it has these properties:

1. If w and w' in W, then $w + w'$ is in W. (Vector Addition)
2. If w is in W, c is in $\mathbb{R}$, then cw is in W. (Scalar Multiplication)
3. The zero vector is in W.

Here are the definition of vector space:

1. **Commutative Group** V under addition.
2. A field of scalars F.
3. $v \in V$ a vector, $f \in F$ a scalar $\to f \cdot v \in V$(scaled vector).
4. Distributive Property: $f \cdot (v_1 + v_2) = f \cdot v_1 + f \cdot v_2$.
5. Associative Property: $f_1 \cdot (f_2 \cdot v) = (f_1 \cdot f_2) \cdot v$.
6. Scaling by 1: $1 \cdot v = v$.

2.1 Fields

Here are some mathematical objects: **Group, Ring, Field.**
The operations allowed in each object is different. **Group** only allows addition and additive inverse (a + (-a)). **Ring** only allows addition, additive inverse, and multiplication. **Fields** only allows addition, additive inverse, multiplication, and multiplicative inverse($a \cdot \frac{1}{a}$).

A subfield of $\mathbb{C}$ is a subset that is closed under the four operations of addition, subtraction, multiplication, division, and contains 1. The properties are:

1. If a and b are in F, then a+b is in F.
2. If a is in F, then -a is in F.
3. If a and b are in F, then ab is in F.
4. If a is in F and $a \neq 0$, then a^{-1} is in F.
5. 1 is in F.

Prime fields and characteristic: Integer doesn't have multiplicative inverse, so it is not a field. However, rational numbers, $\mathbb{Q}$, and integer module 5, $\mathbb{Z}/5\mathbb{Z}$, are field. More generally, $\mathbb{Z}/p\mathbb{Z}$ will be a field, p is a prime. This is denoted as $\mathbb{F}_p$ and it is called prime field.

2.2 Vector Spaces

2.3 Direct Sum

Suppose we have subspaces $W_1, W_2, \dots, W_k$ of a vector space V, then the set of vectors v can be written as a sum:

$$v = w_1 + w_2 + \cdots + w_k$$

In other words,

$$W_1 + \cdots + W_k = \{v \in V | v = w_1 + w_2 + \cdots + w_k\}$$

Basically the whole vector spaces is spanned by the each subspace w_i. This idea is very similar with the idea of a vector that is spanned by the basis.
The subspaces $W_1, \dots, W_k$ are called independence if no sum $w_1 + \cdots + w_k$ with w_i in W_i is zero. Each subspace space W_i is spanned by some basis v_i.
Here are some properties:

1. If all the subspaces W_i are independent, then the sum $W_1 + \cdots + W_k$ is equal to V.
2. dim($W_1 + \cdots + W_k$)$\leq$ dim(W_1)$+ \dots +$dim(W_k) iff all the subspaces are independence.

If the first condition is met, then the vector space V is the direct sum of $W_1, \ldots, W_k$, and it is denoted as:

$$V = W_1 \oplus \cdots \oplus W_k$$

$W_1, \ldots, W_k$ are independent.

Let W_1 and W_2 be subspaces of finite-dimensional vector space V, then:

1. $\dim(W_1)+\dim(W_2) = \dim(W_1 \cap W_2)+\dim(W_1 + W_2)$.
2. W_1 and W_2 are independent iff $W_1 \cap W_2 = \{0\}$.
3. V is the direct sum $W_1 \oplus W_2$ iff $W_1 \cap W_2 = \{0\}$ and $W_1 + W_2 = V$.
4. If $W_1 + W_2 = V$, there is subspace W_2' of W_2 such that $W_1 \oplus W_2' = V$.

2.4 Infinite-Dimensional Vector Spaces

Vector spaces that are too big to be spanned by any finite set of vectors are called infinite dimensional. The span of an infinite set S is defined to be the set of the vectors v that are combinations of finitely many elements of S.

3 Linear Operator

3.1 The Dimension Formula

let T be a linear transformation, $T : V \to W$, then:

$$\dim(\mathrm{ket}(T)) + \dim(\mathrm{Im}(T)) = \dim(\mathrm{V})$$

3.2 Jordan Form

Suppose we have a linear operator T, if all its eigenvalues are distinct, then it is diagonalizable. If its eigenvalues are not distinct, then there are two cases. The first case is that there are enough eigenvectors to diagonalize T. The second case is that there are not enough eigenvectors to diagonalize it, and this is when we need the generalized eigenvectors to diagonalize T). In this subsection, let's focused on the case when not all the eigenvalues are distinct and we don't have enough eigenvectors to diagonalize T.
When there are repeated eigenvalues, then the operator decomposes into Jordan blocks. Each block of size d corresponds to vector x satifying the following:

$$(T - \lambda I)^d x = 0, \quad \text{but } (T - \lambda I)^{d-1} x \neq 0$$

d is the smallest integer such that the left equation holds. The matrix $(T - \lambda I)^d = 0$ is called the Nilpotent matrix which matrix you raise a matrix to a power d it kills itself. This equation captures how many times you must apply

$(T-\lambda I)$ before the vector is killed. The length of the Jordan chain. The number of Jordan blocks is equal to the number of eigenvectors of the linear operator T. Let $u_j = (T-\lambda I)^j x$, then $B = (u_0, u_1, \ldots, u_{d-1})$. Jordan Chain is defined as:

$$\begin{aligned}
(T-\lambda I)u_0 &= 0 \\
(T-\lambda I)^2 u_1 &= 0 \\
(T-\lambda I)^3 u_2 &= 0 \\
&\vdots \\
(T-\lambda I)u_1 &= u_0 \\
(T-\lambda I)^2 u_2 &= u_0
\end{aligned}$$

4 Bilinear Forms

A function or matrix is said to be in bilinear form if the two vector spaces V and W satifies the following properties. A bilinear form of V is a real-valued function of two vector variables - a map $V \times V \to \mathbb{R}$. Given a pair v, w vectors, the form returns a real number that will usually denoted by $\langle v, w \rangle$. This means the bilinear form is required to be linear in each variable.

$$\langle rv_1, w_1 \rangle = r\langle v_1, w_1 \rangle$$

and

$$\begin{aligned}
\langle v_1 + v_2, w_1 \rangle &= \langle v_1, w_1 \rangle + \langle v_2, w_1 \rangle \\
\langle v_1, w_1 + w_2 \rangle &= \langle v_1, w_1 \rangle + \langle v_1, w_2 \rangle
\end{aligned}$$

5 Cayley-Hamilton Theorem

Every $n \times n$ square matrix satisfies its own characteristic equation which means:

$$\rho(A) = A + a$$

People can use this to express A^n as a finite sum of $A^0, ..., A^{n-1}$ terms weighted by some coefficients.

6 Group Representation

6.1 Definitions

A matrix representation of a group G is a homomorphism if:

$$R : G \to GL_n \tag{1}$$

General linear group of dimension n and over the field of complex number. R here is the matrix representation, that takes in an element from group G and maps it to an element in the general linear group.

A representation R is **faithful** if the homomorphism $R : G \to GL_n$ is injective, and therefore maps G isomorphically to its image, a subgroup of GL_n. This means every elements got mapped to some elements in the general linear group and also satisfy the homomorphism property.

6.1.1 Examples

Let's consider the **symmetric group** S_3 can be presented as generators and relations, $\langle x, y | x^3, y^2, xyxy \rangle$, so a representation of S_3 is denned by matrix R_x and R_y such that $R_x^3 = I, R_y^2 = I$, and $R_x R_y R_x R_y = I$. Since dihedral group D_3 is isomorphic to S_3, it has a two dimensional matrix representation that we denoted by A.

1. Standard Representations, A.
2. Sign Representations, Σ.
3. Trivial Representations, T.

All the representations can be built using the above 3 representations.
Representations are notationally complicated. The secret to understanding them is to throw out the most information that the matrices contain, and keeping only one essential part, its trace or character.
The character χ_R of a matrix representation R is the complex-valued function whose domain is the group G, defined by $\chi_R(g)$ =trace(R_g)

6.2 Irreducible Representations

Let ρ be a representation of a finite group G on the non-complex vector space V. A vector v is G-invariant if the operation of every group element fixes the vector:

$$\forall g \in G : gv = v \quad \text{or} \quad \rho_g(v) = v$$

If W is an invariant subspace of V, then $\forall g \in G : gW = W$

6.3 Unitary Representations

6.4 Characters