Algebra

Vector Spaces over field $K$

**Def:** $\emptyset \neq W \subseteq V$ is a subspace of $V$ if

(i) $\overrightarrow{w_1}, \overrightarrow{w_2} \in W \Rightarrow \overrightarrow{w_1} + \overrightarrow{w_2} \in W$

(ii) $\overrightarrow{w} \in W, \lambda \in \mathbb{R} \Rightarrow \lambda \overrightarrow{w} \in W$

**Def:** $T : V \rightarrow W$ is a homomorphism if

(i) $T(\overrightarrow{v_1} + \overrightarrow{v_2}) = T(\overrightarrow{v_1}) + T(\overrightarrow{v_2})$

(ii) $T(\lambda \overrightarrow{v}) = \lambda T(\overrightarrow{v})$

$T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ in general $T(\overrightarrow{v}) = \mathbb{R}A$ with $A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$

"Homomorphisms of vector spaces have long been called linear transformations"

"Matrices represent linear transformations"

$\text{Ker}(T) = \{ \overrightarrow{v} : T(\overrightarrow{v}) = \overrightarrow{0} \}$

$\text{Im}(T) = \{ \overrightarrow{w} : \exists \overrightarrow{v} \text{ s.t. } T(\overrightarrow{v}) = \overrightarrow{w} \}$

1. $\overrightarrow{v_1}, \ldots, \overrightarrow{v_n}$ are linearly independent if $\sum_{i=1}^{n} a_i \overrightarrow{v_i} = \overrightarrow{0} \Rightarrow a_i = 0$

2. $\overrightarrow{v_1}, \ldots, \overrightarrow{v_n}$ span $V$ if $\forall \overrightarrow{w} \in V$ there exist $a_1, \ldots, a_n$ s.t. $\overrightarrow{w} = \sum_{i=1}^{n} a_i \overrightarrow{v_i}$

3. $\overrightarrow{v_1}, \ldots, \overrightarrow{v_n}$ is a basis for $V$ if both 1 & 2 hold.

**Big Fact:** If $V$ has a finite basis, then all basis have the same size called $\text{dim}(V)$.

**Example:** $Q(\overrightarrow{v}) = \{ a \overrightarrow{v} + b \overrightarrow{w} : a, b \in \mathbb{Q} \}$. Consider $Q(\overrightarrow{v})$ as a vector space over the $\mathbb{Q}$.

$\uparrow$ [Remember, we want to specify over what $\mathbb{Q}$]

**Claim:** $\overrightarrow{v_1}, \overrightarrow{v_2}$ basis. ["To prove this we need to show linear ind. & span"]

1. Span: All $x \in Q(\overrightarrow{v})$ here $x = a + b \overrightarrow{v}$

2. Linear Independence: Suppose $a + b \overrightarrow{v} = 0$

   $b = 0 \Rightarrow a = 0$

   $b \neq 0 \Rightarrow \overrightarrow{v} = -\frac{b}{a}$
More Facts:
- If \( v_1, \ldots, v_s \) is linearly independent then \( s \leq \dim(V) \)
- If \( v_1, \ldots, v_t \) span \( V \) then \( \dim(V) \leq t \)
- When \( \dim(V) = n \) ("when you know you are in \( n \) space")
  - \( v_1, \ldots, v_n \) linearly independent \( \Rightarrow \) basis
  - \( v_1, \ldots, v_n \) spans \( V \) \( \Rightarrow \) basis
- Extra fact: \( W \subset V \Rightarrow \dim(W) \leq \dim(V) \)

Example - \( V = \mathbb{F}[x]/(f(x)) \), where \( \deg(f(x)) = n \), is a vector space over \( \mathbb{F} \)
\( \dim(V) = n \) with basis \( 1, x, x^2, \ldots, x^{n-1} \)

\( \geq \) Def: Where \( F \subset K \)
\[ [K:F] = \text{dimension of } K \text{ as a vector space over } F \text{ (if no finite cases may be } \infty \) \]

Example - 1) \( [\mathbb{Q}(i) : \mathbb{Q}] = 2 \) where basis consists of \( 1, i \)
          2) \( [\mathbb{C} : \mathbb{R}] = 2 \) where basis consist of \( 1, i \)

Thm: Let \( F \subset K \), both fields \( [K:F] = 1 \iff K=F \)

Pf: (i) \( K=F \) then Basis \( \{1\} \)
(ii) Suppose \( F \subset K \). Pick \( x \in K \), \( x \notin F \) and claim \( x, 1 \) are linearly independent (over \( F \)).
    If \( a+bx = 0 \) with \( a, b \in F \)
    \( b=0 \Rightarrow a=0 \)
    \( b \neq 0 \Rightarrow x = -a/b \in F \)

\( \therefore [K:F] \geq 2 \)
**Tower Theorem**  Let \( F \subseteq K \subseteq L \) with \([K:F] < \infty\), \([L:K] < \infty\).

Then \([L:F] < \infty\) and \([L:F] = [L:K][K:F]\).

\[
\begin{bmatrix}
\text{dim}(5) \\
\text{dim}(15)
\end{bmatrix}
\]

\[
\begin{bmatrix}
\text{dim}(4) \\
(1, \sqrt{2}, \sqrt{3}, \sqrt{6})
\end{bmatrix}
\]

**Example:** \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{ \alpha + \beta \sqrt{3} : \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \} \)

\[
\begin{align*}
\text{dim}(1) & \quad (1, \sqrt{2}, \sqrt{3}, \sqrt{6}) \\
\text{dim}(2) & \quad \mathbb{Q}(\sqrt{2}) \\
\text{dim}(5) & \quad \mathbb{Q}(\sqrt{2}) \\
\text{dim}(15) & \quad \mathbb{Q}(\sqrt{2}, \sqrt{3})
\end{align*}
\]

**Proof:** Let \( \lambda_1, \ldots, \lambda_n \) be the basis for \( L \) over \( K \). Let \( \mu_1, \ldots, \mu_m \) be the basis for \( K \) over \( F \).

**Claim:** \( \lambda_i \mu_j : 1 \leq i \leq N, 1 \leq j \leq M \) is a basis for \( L \) over \( F \).

(i) span. Let \( \alpha \in L \), write \( \alpha = \sum_{j=1}^{m} B_j \mu_j \) with \( B_j \in K \).

\[ \alpha = \sum_{j=1}^{m} \sum_{i=1}^{n} \alpha_{ij} \lambda_i \mu_j \]

(ii) linearly independent. Suppose \( 0 = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} \lambda_i \mu_j \) (\( a_{ij} \in F \))

\[ = \sum_{j=1}^{m} B_j \mu_j \] where \( B_j = \sum_{i=1}^{n} a_{ij} \lambda_i \)

Since \( \mu_1, \ldots, \mu_m \) forms a basis \( \Rightarrow \) all \( B_j = 0 \).

\[ 0 = \sum_{i=1}^{n} a_{ij} \lambda_i \] \( \Rightarrow \) all \( a_{ij} = 0 \)

This proof is also in the book.

**Corollary:** Let \( F \subseteq K \subseteq L \) with \([L:F] < \infty\). Then \([K:F], [L:K]\) is finite and so is \([L:F] = [L:K][K:F]\).

**Pf:** (1) Let \( \alpha_1, \ldots, \alpha_s \) be basis for \( L \) over \( F \).

**Claim:** \( \alpha_1, \ldots, \alpha_s \) span \( L \) over \( K \)

**Claim:** \( \exists \) finite basis of \( L \) over \( K \)
2. $K$ is a subspace of $L$. (as vector spaces over $F$)

$s [K:F] \leq [L:F]$. [Note we use the extra fact $I$]

Example -

\[
\begin{array}{c}
\text{Big} \\
\text{Small}
\end{array}
\]

with a prime dimension, then there do not exist
intermediate fields (unless they are trivial).

Example -

\[
\begin{array}{c}
\text{Big} \\
\text{Small}
\end{array}
\]

where the dimension is a power of two. Then the
dimension from intermediate field to small field
would also be a power of 2. (This example will
come up a lot.)

Let $F = \Omega, \alpha \in F$.

Def. We say that $\alpha$ is algebraic over $F$ if \exists $a_0, \ldots, a_n \in F$ where not all
equal 0, then $a_0 + a_1 \alpha + \ldots + a_n \alpha^n = 0$.

Default. $F = \mathbb{Q}, \Omega = \mathbb{C}$ and $\alpha$ is algebraic. (Complex number
that satisfies some polynomial.)

[Ex. Algebraic over $K$, then coefficients are $K$. The algebraic default]

is complex numbers.

[Ex. $\pi$ is not algebraic, it is transcendental.

Every $\alpha \in \Omega$ is algebraic over $F$, written as $\alpha = x + iy$.

$(x - x)^2 = (iy)^2 = -y^2$ where $x, y$ are constants.

$\alpha^2 - 2\alpha x + (x^2 + y^2) = 0.$]