University of Southern California

EE 510: Discussion 3

September 11, 2020

Exercise 1 *: Let V_1 and V_2 be two vector sub-spaces of a vector space V over a field $\mathbb{F}$.*

1) *Prove that $V_1 \cap V_2$ is a vector sub-space of the vector space V.*

2) *Prove that $V_1 \cup V_2$ is a vector sub-space of the vector space V if and only if $V_1 \subset V_2$ or $V_2 \subset V_1$.*

Solution:

1) Let $x, y \in V_1 \cap V_2$ and $\alpha \in \mathbb{F}$,
We have, $x \in V_1 \cap V_2 \subset V_1$ and $y \in V_1 \cap V_2 \subset V_1$. Then, $\alpha x + y \in V_1$ since V_1 is a vector sub-space of V.
Similarly, $x \in V_1 \cap V_2 \subset V_2$ and $y \in V_1 \cap V_2 \subset V_2$. Then, $\alpha x + y \in V_2$ since V_2 is a vector sub-space of V.
Therefore, $\alpha x + y \in V_1 \cap V_2$, then $V_1 \cap V_2$ is a vector sub-space of V.

2)

- If $V_1 \subset V_2$ or $V_2 \subset V_1$, then $V_1 \cup V_2 = V_2$ or $V_1 \cup V_2 = V_1$, respectively. So, $V_1 \cup V_2$ is a vector sub-space of V.

- If $V_1 \cup V_2$ is a vector sub-space of V. Next, we will prove by contradiction that $V_1 \subset V_2$ or $V_2 \subset V_1$.
  We assume that $V_1 \not\subset V_2$ and $V_2 \not\subset V_1$. So, $\exists x \in V_1$ and $x \notin V_2$. Similarly, $\exists y \in V_2$ and $y \notin V_1$.
  So, $x \in V_1 \subset V_1 \cup V_2$ and $y \in V_2 \subset V_1 \cup V_2$. Given $V_1 \cup V_2$ is a vector sub-space, then $z = x + y \in V_1 \cup V_2$.
  Thus, $z \in V_1$ or $z \in V_2$.
  1^{st} case $z \in V_1$: Since V_1 is a vector sub-space of V, then $y = z - x$ is a vector of V_1 which is impossible from the definition of y (i.e., $y \notin V_1$).
  2^{nd} case $z \in V_2$: Since V_2 is a vector sub-space of V, then $x = z - y$ is a vector of V_2 which is impossible from the definition of x (i.e., $x \notin V_2$).
  Therefore, the assumption $V_1 \not\subset V_2$ and $V_2 \not\subset V_1$ is not possible, assuming we have $V_1 \cup V_2$ is a vector sub-space of V. Consequently, we have $V_1 \subset V_2$ or $V_2 \subset V_1$.

---

1 Finite fields

Let $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ is a field if and only if p is a prime number.
Example: $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ is a finite field where $2^{-1} = 4; 3^{-1} = 5$ and $6^{-1} = 6$.
An irreducible polynomial over $\mathbb{K}$ means that the polynomial cannot be factored over $\mathbb{K}$.
Example: $P(X) = X^2 + 1$

- $\mathbb{K} = \mathbb{R}$: P cannot be factored $\Rightarrow P(X)$ is irreducible.
- $\mathbb{K} = \mathbb{C}$: $P(X) = (X - i)(X + i) \Rightarrow P(X)$ is reducible.
- $\mathbb{K} = \mathbb{F}_2$: $P(X) = (X + 1)^2 \Rightarrow P(X)$ is reducible.

Theorem 1 If $P(X)$ is irreducible over a finite field $\mathbb{F}_p$ and has a degree m. Then, the set $\mathbb{F}_{p^m}$ of all polynomials of degree $\leq m - 1$ where the coefficients over $\mathbb{F}_p$ with the operations modulus $P(X)$ is a finite field with p^m elements.

Example: $P(X) = X^3 + X^2 + 1$ is an irreducible polynomial over $\mathbb{F}_2$. Hence, the set $\{0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1\}$ is a finite field modulus $P(X) = X^3 + X^2 + 1$. Also, we have

$$X^3 = X^2 + 1 \mod (X^3 + X^2 + 1)$$

$$X^4 = X^2 + X + 1 \mod (X^3 + X^2 + 1)$$

The corresponding table of multiplication is as follows

	0	1	X	$X+1$	X^2	X^2+1	X^2+X	X^2+X+1
0	0	0	0	0	0	0	0	0
1	0	1	X	$X+1$	X^2	X^2+1	X^2+X	X^2+X+1
X	0	X	X^2	X^2+X	X^2+1	X^2+X+1	1	$X+1$
$X+1$	0	$X+1$	X^2+X	X^2+1	1	X	X^2+X+1	X^2
X^2	0	X^2	X^2+1	1	X^2+X+1	$X+1$	X	X^2+X
X^2+1	0	X^2+1	X^2+X+1	X	$X+1$	X^2+X	X^2	1
X^2+X	0	X^2+X	1	X^2+X+1	X	X^2	$X+1$	X^2+1
X^2+X+1	0	X^2+X+1	$X+1$	X^2	X^2+X	1	X^2+1	X