Abstract Algebra

Notes - Year 1, Semester 2

Angel Cervera Roldan
21319203

Contents

Fields

A field is a set F containing at least two elements, along with two operations:

- $+ : F \times F \to F$
- $\cdot : F \times F \to F$

that satisfies the following axioms:

1. $a + b = b + a, \text{ and } a \cdot b = b \cdot a \quad \forall a, b \in F$
2. $(a + b) + c = a + (b + c), \text{ and } (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b \in F$
3. $\exists 0 \in F$ such that $a + 0 = a \quad \forall a \in F$
4. $\exists 1 \in F$ such that $a \cdot 1 = a \quad \forall a \in F$, where $0 \neq 1$
5. $\forall a \in F, \ \exists(-a)$ such that $a + (-a) = 0$
6. $\forall a \in F - \{0\}, \ \exists(a^{-1})$ such that $a \cdot (-a) = 1$
7. $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in F$

Theorem

$\mathbb{Z}_p$ is the set of integers mod p, and it is a field iff p is a prime.

From the axioms, $\forall a, b, c \in F$ the following can be proven

1. $a + b = a + c \implies b = c$
2. $a \neq 0, \ ab = ac \implies b = c$
3. $-(-a) = a$
4. $a \cdot 0 = 0$

Vector Spaces

Let F be a field, a vector space over F is a non-empty set V along with two operations:

- $+ : V \times V \to V$
- $\cdot : F \times V \to V$

that satisfy the following axioms:

1. $u + (v + w) = (u + v) + w \quad \forall u, v, w \in V$
2. $u + v = v + u \quad \forall u, v \in V$
3. $\exists 0 \in V$ such that $0 + v = v \quad \forall v \in V$
4. $\forall u \in V,\ \exists - u \in V$ such that $u + (-u) = 0$
5. $\alpha(\beta u) = (\alpha\beta)u \quad \forall \alpha, \beta \in F, u \in V$
6. $\alpha(u + v) = \alpha u + \alpha v \quad \forall \alpha \in F, u, v \in V$
7. $\exists 1 \in V$ such that $\forall u \in V\ 1u = u$

Subspaces

If V is a vector space, and $B \subset V$ is also a vector space, then we say that B is a subspace of V.

Lemma

A non-empty subset $S \subseteq V$ is a vector space iff

- $u, s \in S \implies u + v \in S$
- $u \in S,\ \lambda \in F \implies \lambda u \in S$

To prove the last result, the key steps are to show that the zero vector $0 \in S$ and that for any $u \in S, (-1)u = -u \in S$. When S is a subset of a vector space, to verify that it is a subspace, we need to check that it is closed under the two operations on V.

Linear Independence and Span

Definition Linear Combination

Let $u \in V$, and $S = \{v_1, ..., v_m\}$ be a subset of V.
We say that u is a linear combination of the set S iff there exists $\lambda_1, ..., \lambda_m \in F$ such that:

$$u = \sum_{i=1}^{m} \lambda_i v_i$$

Definition Span

Let $M \subseteq V$, the span of M is the set of all linear combinations of finite sets of vectors from M, mathematically:

$$span(M) = \left\{ \sum_{i=1}^{m} \lambda_i u_i \mid m \in \mathbb{N},\ \lambda_i \in F,\ u_i \in M,\ i \leq i \leq m \right\}$$

For any subset M of V, $span(M)$ is a subspace.

If M is a finite set of vectors $u_1, ..., u_q$, we can denote $span(M)$ as $\langle u_1, ..., u_q \rangle$. If the $span(M) = V$, we say that M spans V. Lastly, we (by convention) say that $span(\emptyset) = 0$.

Lemma

If S is a subspace of the vector space V, and $v_1, ..., v_q \in S$, then $\langle v_1, ..., v_1 \rangle \subseteq S$.

The above is true since S is a vector space, therefore, it is closed under addition and under scalar multiplication.