1 Groups and Fields

Definition 1. *Group $(G, *)$ is a set G with a operation $*$ having the following properties*
1. $G \neq \emptyset$: non-empty
2. $* : G \times G \to G$ is a function. We write $*((a, b))$ as $a * b$ for $a, b \in G$.
3. $\forall a, b, c \in G; a * (b * c) = (a * b) * c$: associative
4. $\exists e \in G, \forall a \in G; e * a = a * e = a$: identity exists
5. $\forall a \in G, \exists \overline{a} \in G; a * \overline{a} = \overline{a} * a = e$: inverse exists

Definition 2. *Abelian Group $(G, *)$*
1-5. $(G, *)$ is a group
6. $\forall a, b \in G; a * b = b * a$: commutative

Example 1. *Check which of the following are groups*
1. $(\mathbb{R}, +)$
2. $(\mathbb{R} - \{1\}, +)$
3. $(\mathbb{R}, \cdot)$
4. $(\mathbb{R} - \{0\}, \cdot)$
5. $GL_2(\mathbb{R})$=General Linear group= all invertible 2×2 matrices with real entries, under matrix multiplication.
6. $\mathbb{B} = \{0, 1\}$ with boolean addition $+$
7. $\mathbb{B} = \{0, 1\}$ with boolean multiplication $\cdot$
8. $D_3 = \{R_0, R_1, R_2, R_3, L_1, L_2, L_3\}$=Dihedral group=set of symmetries of an equilateral triangle, under composition.
9. Elliptic Curve with point at infinity: $\mathbb{E} = \{(x, y) | y^2 = x^3 + Ax + B, 4A^3 + 27B^2 \neq 0\} \cup \mathcal{O}$ under elliptic curve addition $+$: If P, Q, R on a straight line in $\mathbb{E}$ then $P + Q + R = \mathcal{O}$.

Theorem 1. *If $(G, *)$ is a group and $a \in G$. Then*
1. e is unique
2. $\overline{a}$ is unique
3. $\overline{\overline{a}} = a$

Definition 3. *Field $(F, +, \cdot)$ is a set with two binary operations $+$ and $\cdot$ having the following properties*
1. $(F, +)$ is an abelian group. We write $e = 0$ and $\overline{a} = -a$
2. $(F - \{0\}, \cdot)$ is an abelian group. We write $e = 1$ and $\overline{a} = a^{-1}$
3. $\forall a, b \in F; a \cdot b \in F$
4. $\forall a, b, c \in F; a \cdot (b + c) = (a \cdot b) + (a \cdot c)$: distributive

Example 2. *Check which of the following are groups*
1. $(\mathbb{R}, +, \cdot)$
2. $(\mathbb{R}, \cdot, +)$
3. $(\mathbb{Q}, +, \cdot)$
4. $(\mathbb{Z}, +, \cdot)$
5. $\mathbb{B} = \{0, 1\}$ with boolean addition and multiplication

6. $\mathbb{B} = \{0, 1\}$ *with mod 2 addition and multiplication*
7. $\{0, 1, 2, 3\}$ *with mod 4 addition and multiplication*
8. $(GL_2(\mathbb{R}), +, \cdot)$

Theorem 2. *Finite Fields*
1. If p *is a prime, the set* $\mathbb{F}_p = \{0, 1, 2, 3, \cdots, p-1\}$ *under mod* p *addition and multiplication is a field.*
2. If F *is a finite field with* n *number of elements , then* $n = p^k$ *for some prime* p *and integer* k*.*

Theorem 3. *If* $(F, +, \cdot)$ *is a field and* $a \in F$
1. $a \cdot 0 = 0$
2. $1 \neq 0$
3. There must be at least two elements in a field.

Definition 4. *Vector space* $(V, *, \circ)$ *over the field* $(F, +, \cdot)$
1. $(V.*)$ *is an abelian group*
2. $(F, +, \cdot)$ *is a field*
3. $\circ : F \times V \to F$ *is a function. We write* $\circ((a, x))$ *as* $a \circ x$ *for* $a \in F$ *and* $x \in V$*.*
4. $\forall a \in F, \forall x, y \in V; a \circ (x * y) = (a \circ x) * (a \circ y)$
5. $\forall a, b \in F, \forall x \in V; (a + b) \circ x = (a \circ x) * (b \circ x)$
6. $\forall a, b \in F, \forall x \in V; (a \cdot b) \circ x = a \circ (b \circ x)$
7. $\forall x \in V; 1 \circ x = x$

Note 1. *Vector Space operations*
$+ : F \times F \to F$
$\cdot : F \times F \to F$
$* : V \times V \to V$
$\circ : F \times V \to V$

Example 3. *Check which of the following are vector spaces*
1. $(\mathbb{R}^3, +, \cdot)$ *over* $(\mathbb{R}, +, \cdot)$
2. $(\mathbb{R}^3, +, \cdot)$ *over* $(\mathbb{C}, +, \cdot)$
3. $(\mathbb{C}^3, +, \cdot)$ *over* $(\mathbb{R}, +, \cdot)$
4. $(\mathbb{C}^3, +, \cdot)$ *over* $(\mathbb{C}, +, \cdot)$
5. $(\mathbb{Q}_n[x], +, \cdot)$ *over* $(\mathbb{Q}, +, \cdot)$ *where* $\mathbb{Q}_n[x]$ *is the set of polynomials of degree* n *or less in* x *with coefficients in* $\mathbb{Q}$*.*
6. $(\mathbb{R}^{m \times n}, +, \cdot)$ *over* $(\mathbb{R}, +, \cdot)$ *where* $\mathbb{R}^{m \times n}$ *is the set of* $m \times n$ *degree matrices with coefficients in* $\mathbb{R}$*.*
7. $(\mathbb{R}^+, *, \circ)$ *over* $(\mathbb{R}, +, \cdot)$ *where* $*$ *and* $\circ$ *operations are defined as*
$x * y = xy$ *and* $a \circ x = x^a$ *for* $x, y \in \mathbb{R}^+$ *and* $a \in \mathbb{R}$

Theorem 4. $(V, *, \circ)$ *over* $(F, +, \cdot)$ *is a vector space*
1. $\forall x \in V; 0 \circ x = e$
2. $\forall a \in F; a \circ e = e$
3. $\forall a \in F, \forall x \in V; a \circ x = e \Rightarrow a = 0$ *or* $x = e$
4. $\forall x \in V; (-1) \circ x = \overline{x}$

Note 2. *When there is no confusion, we will use the following notation and names*
1. $x * y = x + y$: *vector addition*
2. $a \circ x = a \cdot x = ax$: *scalar multiplication*
3. $e = \underline{0}$
4. $\overline{x} = -x$
5. $(V, *, \circ)$ *over* $(F, +, \cdot)$ *will be written as*
$(V, +, \cdot)$ *over* $(F, +, \cdot)$ *or* V *over* F *or just* V *when* F *is implied*

Note 3. *We will rewrite everything in the above notation for the vector space* V *over* F
1.1 $V \neq \emptyset$
1.2 $+ : V \times V \to V$ *is a function, i.e.* $+$ *is a binary operation on* V
1.3 $\forall x, y, z \in V; x + (y + z) = (x + y) + z$
1.4 $\exists \underline{0} \in V, \forall x \in V; x + \underline{0} = \underline{0} + x = x$
1.5 $\forall x \in V; \exists -x \in V; x + (-x) = (-x) + x = \underline{0}$
1.6 $\forall x, y \in V; x + y = y + x$
2. $(F, +, \cdot)$ *is a field*
3. $\cdot : F \times V \to V$ *is a function*
4. $\forall a \in F, \forall x, y \in V; a \cdot (x + y) = (a \cdot x) + (a \cdot y)$
5. $\forall a, b \in F, \forall x \in V; (a + b) \cdot x = (a \cdot x) + (b \cdot x)$
6. $\forall a, b \in F, \forall x \in V; (a \cdot b) \cdot x = a \cdot (b \cdot x)$
7. $\forall x \in V; 1 \cdot x = x$

Definition 5. *Subspace*
S is a subspace of the vector space V over F iff S is a non empty subset of V and S is a vector space over F.

Example 4. *Which of the following are subspaces of the given vector space*
1. $(\mathbb{R}^3, +, \cdot)$ *of* $(\mathbb{C}^3, +, \cdot)$ *over* $(\mathbb{R}, +, \cdot)$
2. $(\mathbb{R}_3[x], +, \cdot)$ *of* $(\mathbb{R}[x], +, \cdot)$ *over* $(\mathbb{R}, +, \cdot)$
3. $(GL_2(\mathbb{R}), +, \cdot)$ *of* $(\mathbb{R}^{2\times 2}, +, \cdot)$ *over* $(\mathbb{R}, +, \cdot)$
4. *Set of solutions to the ODE* $y'' - y - 6y = 0$ *of Continuous functions* $\mathcal{C}$ *over* $\mathbb{R}$.

Theorem 5. *Let S be a non empty subset of the vector space V over F. If S is closed under vector addition and scalar multiplication, then S is a subspace of V over F.*

Definition 6. *Linear Combination*
Let $B = \{x_1, x_2, \cdots, x_n\}$ be a non empty finite subset of a vector space V over F. Then an element of the form $\sum_{k=1}^{n} a_k x_k = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$ with $a_k \in F$ is called a Linear Combination of B.

Definition 7. *Span*
Let $B = \{x_1, x_2, \cdots, x_n\}$ be a non empty finite subset of the vector space V over F. Then the collection of all possible linear combinations is called the Span of B.
i.e. $SpanB = \{\sum_{k=1}^{n} a_k x_k | x_k \in B, a_k \in F\}$
If $SpanB = W$, we say that B spans W.