Definition 0.1. A field F is a set of with two operations $+$(addition) and $\cdot$ (multiplication) satisfiying the following conditions.

(i) $a + b,\ a \cdot b \in F\ \forall\ a,\ b \in F$.
(ii) $a + b = b + a, a \cdot b = b \cdot a\ \forall\ a,\ b \in F$. (commutative)
(iii) $(a + b) + c = a + (b + c), a \cdot (b \cdot c) = (a \cdot b) \cdot c$. (associative)
(iv) $a \cdot (b + c) = a \cdot b + a \cdot c\ \forall\ a,\ b,\ c \in F$. (distributive)
(v) $\exists 0, 1 \in F$ such that $a + 0 = a, a \cdot 1 = a\ \forall\ a \in F$. (identity elements)
(vi) $\exists c \in F$ such that $a + c = 0\ \forall\ a \in F$. (additive inverse of a)
(vii) $\exists c \in F$ such that $a \cdot c = 1\ \forall\ a \in F,\ a \neq 0$. (multiplicative inverse of a)

We will denote $a \cdot b$ simply by ab, additive inverse of a by $-a$ and multiplicative inverse of a by a^{-1}. For any field F, we can deduce the following from the axioms of definition:

1. The identity elements are unique.
2. $a0 = 0$.
3. $ab = 0 \implies a = 0$ or $b = 0$.
4. $-(-a) = a,\ (a^{-1})^{-1} = a$.
5. $(-1)a = -a$, also $(-a)(-a) = aa$ and we can continue.

0.1 Finite fields

Definition 0.2. A ***finite field*** is a field having a finite number of elements. The number of elements is called the ***order*** of the *field*.

Theorem 0.3. There exists a field of order q iff q is a *prime-power*. Also, if q is a prime, there is only one field, upto relabelling.

We will not go into proof as it requires some concepts of abstract algebra, which will be beyond the scope of this report. A field of order q is often called *Galois Field* of order q and is denoted by $GF(q)$.
Note: From now on in this report mentioning $GF(q)$ will imply that q is a prime power.

Theorem 0.4. $\mathbb{Z}_m$ is a field (addition and multiplication defined as *modulo* m) iff m is a *prime*.

Proof. The first six properties can be easily verified even if m is not a prime, as the addition and multiplication are *modular*.
Now for the multiplicative inverse property,
$\implies$: Suppose m is not prime, then $m = ab$ for some non-zero $a, b < m$, but then

$$ab \equiv 0 \pmod{m} \implies a = 0 \text{ or } b = 0$$

which is contradiction. Hence, m is prime.
$\impliedby$: We have to prove that for all a in $\mathbb{Z}_m$, there exists a multiplicative inverse, a^{-1}. Consider the elements $a, 2a, 3a, \ldots, (m-1)a$, each of these elements will have non-zero remainder with m. Further, these remainders will be distinct, for otherwise $(i-j)a \equiv 0 \pmod{m}$ for some $i, j \in \{1, 2, \ldots, m-1\}, i \neq j$, therefore $(i - j)a \equiv 0 \pmod{m}$, which is not possible as i, j are distinct and $|i - j|, a < m$ which is a prime. Therefore, there must exist an element with remainder 1 in the initial set . Hence, the multiplicative inverse exists. □

Theorem 0.5. Suppose F is a finite field, with $\alpha \in F$, then there exists a prime number p such that $p\alpha = \alpha + \alpha + \cdots + \alpha(\text{p terms}) = 0$. The prime number p is called ***characterstic*** of field F.

Proof. The term $n\alpha$ must have a same value for two different values of n as we iterate over n because F is a finite field. Let those n be $a,\ b$ such that $0 < a < b$, then $(b - a)\alpha = 0$. Let the minimum value of $b - a$ be p. So, $p\alpha = 0$. If p was co-prime, then $p = lm$, with $0 < l, m < p \implies (lm)\alpha = (l\alpha)(m\alpha) = 0 \implies l\alpha = 0$ or $m\alpha = 0$, which is contradiction. Hence, p is a prime. □

0.2 Vector spaces over finite fields

Definition 0.6. A set is V is called a ***vector-space*** over a field F, if $+$ and $\cdot$ are defined as $+ : V \times V \to V$ binary-operation on V, and $\cdot : F \times V \to V$ a function, and the following axioms are satisfied.

(i) $u + v = v + u \; \forall \, u, v \in V$.
(ii) $u + (v + w) = (u + v) + w \; \forall \, u, v, w \in V$.
(iii) There exists $0 \in V$ such that $\forall \, u \in V : v + 0 = v$.
(iv) For every $u \in V$, $\exists w \in V$ such that $v + w = 0$.
(v) $a \cdot (v + w) = a \cdot u + a \cdot v \; \forall \, u, v \in V, \; a \in F$.
(vi) $(a + b) \cdot (u) = a \cdot u + b \cdot u \; \forall \, u \in V, \; a, b \in F$.
(vii) $(ab) \cdot (u) = a \cdot (b \cdot u) \; \forall \, u \in V, \; a, b \in F$.
(viii) $1 \cdot u = u \; \forall \, u \in V$ (1 is multiplicative identitiy of F).

Elements of V are called *vectors* and of F are called *scalars*.

The set $GF(q)^n$ of all the n-tuples over $GF(q)$ will be denoted as $V(n, q)$.
It can be seen that $V(n, q)$ is a vector-space over $GF(q)$ if we define addition and scalar multiplication as follows for $\mathbf{x} = \{x_1, x_2, \ldots, x_n\}, \mathbf{y} = \{y_1, y_2, \ldots, y_n\} \in V(n, q)$ and $a \in F$.

- $\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$
- $a\mathbf{x} = (ax_1, ax_2, \ldots, ax_n)$

Definition 0.7. A subset of $V(n, q)$ is called a ***subspace*** of $V(n, q)$ if itself is vector space under same addition and scalar multiplication.

Theorem 0.8. A subset C of $V(n, q)$ is a subspace if and only if
(i) If $\mathbf{x}, \mathbf{y} \in C$, then $\mathbf{x} + \mathbf{y} \in C$.
(ii) If $a \in GF(q)$ and $\mathbf{x} \in C$, then $a\mathbf{x} \in C$.

Proof. One can easily see that if these conditions are true, then all the axioms of vector space are satisfied. Therefore, C is a subspace. □

A ***linear combination*** of r vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ is a vector of the form $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r$, where a_i are scalars. **Note:** Set of all linear combinations of a set of given vectors is a subspace of$V(n, q)$.
A set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ is called ***linearly independent*** if

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r = 0 \implies a_1 = a_2 = \cdots = a_r = 0.$$

If C is a subspace of $V(n, q)$. Then a subset $\{textbfv_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ of C is called ***generating set*** if every vector of C can be expressed as the linear combination of these vectors.
A *generating set* of C which is also linearly independent is called ***basis*** of C.

Theorem 0.9. If C is a non-trivial subspace of $V(n, q)$. Then any generating set of C contians a basis of C.

Proof. We equate linear combination of generating matrix elements with $\mathbf{0}$, then the vectors with non-zero coefficients are removed from the generating matrix and we get a basis of C. □

Theorem 0.10. Suppose $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be the basis of a subspace C of $V(n, q)$. Then
(i) every vector of C can be expressed *uniquely* as a linear combination of the basis vectors.
(ii) C contains exactly q^k vectors.

The order of basis of C is called the ***dimension*** of the subspace C, denoted by $\dim C$.

Proof. Let the basis of C be the set $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$.

(i) If $\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$, and $\mathbf{x} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_k\mathbf{v}_k$, then $\mathbf{x} = (a_1 - b_1)\mathbf{v}_1 + (a_2 - b_2)\mathbf{v}_2 + \cdots + (a_k - b_k)\mathbf{v}_k = 0$, but as basis is linearly independent, $a_i - b_i = 0$ for all $0 < i < k$.

(ii) q choices for coefficient of each the basis element, therefore q^k elements in the subspace.

□