The Structure of Finite Fields

**Definition:** The *characteristic* of a field (ring) $F$ is

$$\text{char}(F) := \min\{n \geq 1 : n1_F = 0\},$$

provided that this set is non-empty. (Here, $n\alpha = \underbrace{\alpha + \ldots + \alpha}_{n}$, for $n \geq 1$ and $\alpha \in F$.) Otherwise, put $\text{char}(F) = 0$.

**Proposition 1:** If $F$ is a field with $\text{char}(F) \neq 0$, then $\text{char}(F)$ is a prime.

**Corollary:** If $F$ is a finite field, then $\text{char}(F) = p$ is a prime.

**Definition:** Let $F$ be a field. A *subfield* of $F$ is a subset $K \subset F$ with $1_F \in K$ which is closed under the field operations.

The *prime subfield* is the intersection of all subfields of $F$:

$$P(F) = \bigcap_{K \subset F} K.$$  

**Proposition 2:** If $F$ is a field of $\text{char}(F) = p \neq 0$, then

$$P(F) \simeq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.$$
**Observation:** If $K \subset F$ is a subfield of a field $F$, then $F$ is a $K$-vector space. We call

$$[F : K] := \dim_K(F)$$

the *degree* of $F$ over $K$.

**Proposition 3:** Let $F$ be a finite field. Then

$$|F| = p^n,$$

where $p = \text{char}(F)$ and $n = [F : P(F)]$.

**Proposition 4:** Let $R$ be a commutative ring with $\text{char}(R) = p$, where $p$ is prime. Then

$$\text{(1)} \quad (x + y)^p = x^p + y^p,$$

for all $x, y \in R$.

Thus, the rule $\sigma_p(x) = x^p$ defines a ring homomorphism $\sigma_p : R \rightarrow R$, called the *Frobenius map*.

**Corollary:** If $F$ is a finite field of $\text{char}(F) = p$, then $\sigma_p$ is bijective and hence is an *automorphism* of $F$. Moreover,

$$P(F) = \text{Fix}(\sigma_p) := \{x \in F : \sigma_p(x) = x\}.$$ 

**Theorem 4:** Let $F$ be a finite field of $\text{char}(F) = p$. Then there exists an irreducible polynomial $f \in \mathbb{F}_p[X]$ such that $A_f := \mathbb{F}_p[X]/(f) \simeq F$. 