Chapter 22 Finite Fields

Theorem 22.1 For each prime number p and positive integer n, there is a unique finite field of order p^n up to isomorphism.
Every finite field has order p^n.

Proof. Let $\mathbb{F}$ be a finite field with characteristic field p, which must be a prime.
Then $\mathbb{Z}_p = \{1, 2, \ldots, p\}$ is a subfield, and $\mathbb{F}$ is a finite dimensional vector space of $\mathbb{Z}_p$, say, of dimension n, so that it has p^n elements.
Next, consider the splitting field $\mathbb{F}$ of $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Note that $f(x)$ and $f'(x)$ has no common factor. So, $f(x)$ has p^n distinct zeros.
The set of distinct zeros form a field. So, $\mathbb{F}$ equals the set of zeros. □

Theorem 22.2 The set of nonzero elements form a cyclic group under multiplication.

proof. By the Fundamental theorem of finitely generated Abelian group, the set of nonzero elements of $\mathbb{F}$ is isomorphic to $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ under addition. □

Corollary A finite field $\mathbb{F} = GF(p^n)$ with p^n elements over the ground field has degree n.

Any generator a of $\mathbb{F}^*$ under multiplication has degree n.

Example 1 $GF(16) = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$.

Example 2 $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$ and F^* is generated by $a =$ ..., and $f(x) = (x + a)(x + a^2)(x + a^4)$.

Theorem 22.3 Suppose $GF(p^n)$ is given. For every positive integer $m < n$, there is a unique subfield $GF(p^m)$ in $GF(p^n)$. These are the only subfields of $GF(p^n)$.

Proof. Suppose $m|n$. Consider the zeros of $x^{p^m} - x$ in $GF(p^n)$. They are the elements of order $x^{p^m-1} = 1$ and 0.
In fact, the nonzero elements are generated by a^ℓ so that a^ℓ has order $p^m - 1$, where $\langle a \rangle = GF(p^n)^*$ and

$$\ell = (p^n - 1)/(p^m - 1) = p^{n-m} + p^{n-2m} + \cdots + p^m + 1.$$

Now, if $\mathbb{F}$ is a subfield of $GL(p^n)$ with r elements. Then $[GL(p^n) : \mathbb{F}] = k$ implies that $r^k = p^n$ so that $r = p^m$ and $m|n$. $\square$

Examples

Example 3 Subfield with 4 elements in $GF(16) = \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$ is $\{0, 1, x^5, x^{10}\}$.

Example 4 Proper subfields of $GF(3^6)$ with $\langle a \rangle = GF(3^6)^*$ are:

$$GF(3) = \{0\} \cup \langle a^{364} \rangle, \quad GF(9) = \{0\} \cup \langle a^{91} \rangle, \quad GF(27) = \{0\} \cup \langle a^{28} \rangle.$$

Example 5 Subfieds of $GF(2^{24})$. See p. 394.