5.5 Finite fields

Recall: The characteristic of a field F is the smallest positive integer n s.t. $n \cdot 1 = 1 + 1 + ... + 1 = 0$. If no such n, we say F has characteristic 0
Note:
(1) $Char(F) = 0$ or a prime p
(2) $Char(F) = p \Rightarrow \mathbb{Z}_p \subseteq F$, where $\mathbb{Z}_p = \{0, 1, 2, ..., p-1\}$
(3) $Char(F) = 0 \Rightarrow \mathbb{Q} \subseteq F$

Recall:
$Char(F) = 0 \Rightarrow \mathbb{Q} \subseteq F$
$Char(F) = p \Rightarrow \mathbb{Z}_p \subseteq F$
In particular if $|F| < \infty$ then $|F| = p^n$ where n is the dimension of F over $\mathbb{Z}_p$

Theorem. *Let F be a field and $G \subseteq F - \{0\}$ be finite multiplication subgroup. Then G is cyclic.*

Proof. Suppose G not cyclic. Then $G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{m_k}$, where $(m_1, m_2) \neq 1$ set $n = lcm(m_1, m_2)$.
Then $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times < e > \times < e > \times ... \subseteq \{\alpha \in G | \alpha^n = 1\}$.
But the LHS has size $m_1 m_2$, the RHS has size at most $n = lcm(m_1, m_2)$, a contradiction. $\square$

ex. $F = \mathbb{C}, G = \{\alpha \in \mathbb{C} | \alpha^8 = 1\} = \{e^{\frac{2\pi}{8}ki} | k = 0, 1, ...7\} \cong (\mathbb{Z}_8, +)$ *is cyclic.*

ex. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} = \{0, 2, 2^2 = 4, 2^3 = 3, 2^4 = 1\} = \{0, 3, 3^2 = 4, 3^3 = 2, 3^4 = 1\} \neq \{0, 4, 4^2 = 1, 4^3 = 4, 4^4 = 1\}$

ex. $\mathbb{Z}_7 \neq \{0, 2, 2^2 = 4, 2^3 = 1, 2^4 = 2\} = \{0, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\}$

Theorem. *Let F be a field, then $|F| = p^n \Leftrightarrow$ F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$*

Proof. $\Leftarrow$)
Claim 1: $\mathbb{Z}_p(x^{p^n} - x) = \{\alpha | \alpha^{p^n} - \alpha = 0\}$

Proof. ($\supseteq$) Clear.
($\subseteq$) It suffices to show $\{\alpha | \alpha^{p^n} - \alpha = 0\}$ is a field. For $\alpha, \beta \in F', \beta \neq 0$, $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$ and $(\frac{\alpha}{\beta})^{p^n} = \frac{\alpha^{p^n}}{\beta^{p^n}} = \frac{\alpha}{\beta}$ Hence F' is a field. $\square$

Claim 2. $|F| = p^n$
Since $\frac{dx^{p^n} - x}{dx} = p^n x^{p^n - 1} - 1 = 0 - 1 = -1$ is relative prime to $x^{p^n} - x$, $x^{p^n} - x$ has not repeated roots. Hence $F = \{\alpha | \alpha^{p^n} - \alpha = 0\}$ has p^n elements.

$\square$

ex. *(Wilson's Theorem) Show* $(p-1)! \equiv -1(modp)$, *where* p *is a prime.*

Proof. In $\mathbb{Z}_p$,$(p-1)! = \prod_{a \neq 0} a = \alpha^1 \alpha^2 ... \alpha^{p-1} = \alpha^{\frac{p(p-1)}{2}} = \alpha^{\frac{p-1}{2}} \neq -1$
where α is a multiplication generator of $U_p = \mathbb{Z}_p - \{0\}$. Note $(\alpha^{\frac{p-1}{2}})^2 = 1$
Hence $\alpha^{\frac{p-1}{2}} \equiv -1(modp)$ $\square$

ex. *Suppose* $p = 4n + 1$ *is a prime. Then* $x^2 \equiv -1 mod p$ *has a solution.*

Proof. In $\mathbb{Z}_p$, $-1 = 1 \times 2 \times 3 \times ... \times \frac{p-1}{2} \times \frac{p+1}{2} \times ... \times (p-1) = 1 \times 2 \times ... \times \frac{p-1}{2} \times (-1)\frac{p+1}{2} \times ... \times (-1) = (1 \times 2 \times ... \times \frac{p-1}{2})^2$
Hence $(\frac{p-1}{2})!$ is a solution of $x^2 \equiv -1(modp)$ $\square$