1 Galois Fields II

Theorem 1.1. *Let p be a prime, and let $q = p^n$ for some $n \in \mathbb{N}$. Then:*

(a) There exists a field $\mathbb{F}_q$ of order q, and this field is unique up to isomorphism.

(b) All elements of $\mathbb{F}_q$ satisfy the equation $t^q = t$, and hence $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension for $t^q - t$.

(c) There is a unique copy of $\mathbb{F}_q$ inside any algebraically closed field containing $\mathbb{F}_p$.

Theorem 1.2. *Let p be a prime, and suppose that $q = p^n$ for some $n \in \mathbb{N}$. Then:*

(a) $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$;

(b) The field $\mathbb{F}_q$ contains a subfield of order p^d if and only if $d \,\big|\, n$. When $d \,\big|\, n$, moreover, there is a unique subfield of $\mathbb{F}_q$ of order p^d.

Definition 1 (Norm, Trace)**.** *Let p be a prime and let $\alpha \in F_q$ where $q = p^n$ for some $n \in \mathbb{N}$. Then we define*

$$\begin{aligned}\mathrm{Tr}(\alpha) &= \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}} \\ &= \alpha + \varphi(\alpha) + \cdots + \varphi^{n-1}(\alpha)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Norm}(\alpha) &= \alpha \cdot \alpha^p \cdots \alpha^{p^{n-1}} = \alpha^{\frac{p^n-1}{p-1}} \\ &= \alpha \cdot \varphi(\alpha) \cdots \varphi^{n-1}(\alpha)\end{aligned}$$

Lemma 1.3. *Let p be a prime and let $\alpha \in F_q$ where $q = p^n$ for some $n \in \mathbb{N}$.*

1. *For all $\alpha \in \mathbb{F}_q$, one has $\mathrm{Tr}(\alpha), \mathrm{Norm}(\alpha) \in \mathbb{F}_p$;*
2. *If $p \neq 2$, then $\exists \alpha_1$ such that $\mathrm{Tr}(\alpha_1) \neq 0$ and $\exists \alpha_2 (\neq 0)$ such that $\mathrm{Norm}(\alpha_2) \neq 1$.*