Finite fields

THEOREM. Let F be a finite field. Then $F^\times$ is cyclic.

Proposition. Let F be a finite field with q elements. Then $t^q - t$ splits in F.

pf. Let $\alpha \in F^\times$. Then $\langle \alpha \rangle \subseteq F^\times$ has order dividing $q-1$ by Lagrange's theorem. Then $\alpha^{q-1} = 1$ so $\alpha^q = \alpha$. This also holds for $\alpha = 0$, of course.

Now, $t^q - t$ has at most q roots in any given field, and we just found exactly q roots, so $t^q - t$ splits and F is precisely the set of roots of $t^q - t$. □

Rmk. Doesn't use cyclicity of the unit group, but does use its group theory.

Rmk. This shows F is the splitting field of $t^q - t$.

Cor. There exists a unique field of order $q = p^e$ for each prime power e.

pf. Let $F = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^q = \alpha\}$. One can check by the Children's Binomial Theorem that this is a field. As above, it is the splitting field of $t^q - t / \mathbb{F}_p$ and has q elements. Uniqueness is due to uniqueness of splitting fields. □

We denote $\mathbb{F}_q$ the field with q elements.

For convenience, we now work in a fixed algebraic closure $\overline{\mathbb{F}_p}$, so that $\mathbb{F}_q$ is the unique up to equality subfield with q elements.
Critically, $\mathbb{F}_q^\times = \mu_{q-1}(\overline{\mathbb{F}_q})$.

Prop. In $\overline{\mathbb{F}_p}$, $\mathbb{F}_{p^e} \subseteq \mathbb{F}_{p^d} \iff e \mid d$.

pf. ($\Leftarrow$). Let $ef = d$. Then fix $\alpha \in \mathbb{F}_{p^e}$. We know

$$\alpha^{p^e} = \alpha, \text{ so } \left(\alpha^{p^e}\right)^{p^e} = \alpha^{p^{2e}} = \alpha$$

$$\alpha^{p^e p^e} = \alpha^{p^{2e}}$$

Inductively, $\alpha^{p^{fe}} = \alpha$

$$\alpha^{p^d}$$

so $\alpha \in \mathbb{F}_{p^d}$

($\Rightarrow$) Let $\mathbb{F}_{p^e} \subseteq \mathbb{F}_{p^d}$. Then $\mathbb{F}_{p^d}$ is a vector space over $\mathbb{F}_{p^e}$,

so $|p^d| = |p^e|^{[\mathbb{F}_{p^d} : \mathbb{F}_{p^e}]}$

where $e[\mathbb{F}_{p^d} : \mathbb{F}_{p^e}] = d$ □

Galois Theory and Frobenius

Let q be a prime power, $q = p^e$.

Let $\varphi_q : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ the Frobenius automorphism.

$x \mapsto x^q$

Recall that $\mathbb{F}_q = \{ x \in \overline{\mathbb{F}_p} \mid x^q = x \}$

$= \overline{\mathbb{F}_p}^{\langle \varphi_q \rangle}$ the fixed field.

Thm. Let $\mathbb{F}_{q^e} / \mathbb{F}_q$ be an extension of finite fields. Then

$$G(\mathbb{F}_{q^e} / \mathbb{F}_q) = \langle \varphi_q \rangle \cong \mathbb{Z}/e\mathbb{Z}.$$

Pf. $\mathbb{F}_{q^e}^{\langle \varphi_q \rangle} = \{ \alpha \in \mathbb{F}_{q^e} \mid \alpha^q = \alpha \}$

$= \mathbb{F}_q$

Thus, $\mathbb{F}_q \subseteq \mathbb{F}_{q^e}^{\mathrm{Aut}(\mathbb{F}_{q^e}/\mathbb{F}_q)} \subseteq \mathbb{F}_{q^e}^{\langle \varphi_q \rangle} = \mathbb{F}_q$

so this is a Galois extension, and by counting degrees we know $G(\mathbb{F}_{q^e}/\mathbb{F}_q) = \langle \varphi_q \rangle$.

Rmk. All finite extensions of finite fields are Galois

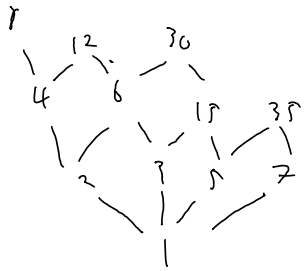
Cor. Let $f \in \mathbb{F}_q[t]$ be irreducible of degree d. Then $f \mid t^{q^e} - t \iff d \mid e$.

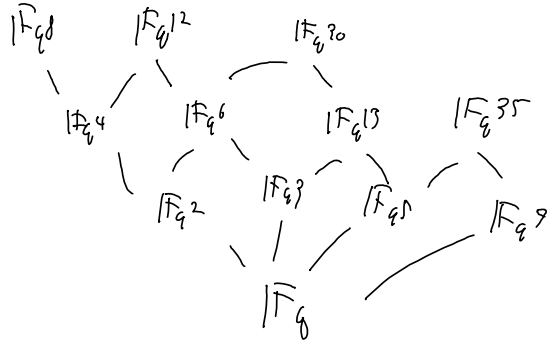
Pf. $f \mid t^{q^e} - t \iff f$ splits in $\mathbb{F}_{q^e} \iff f$ has a root in $\mathbb{F}_{q^e}$

$\iff \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^e}$, for $f(\alpha) = 0$

$\mathbb{F}_{q^d}$

$\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^e} \iff d \mid e$. $\square$





Cor. $t^{p^n} - t = \prod_{f \text{ irreducible monic in } \mathbb{F}_q[t] \text{ of degree } d \mid n} f$

Rmk. What is "$G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$"?

Is it $\langle \varphi_q \rangle$?

Not quite, but this is dense in here.

e.g. Consider $\mathbb{F}_{q^{5^\infty}} := \bigcup_{n \geq 1} \mathbb{F}_{q^{5^n}}$

$= \{ \alpha \in \overline{\mathbb{F}_q} \mid \varphi_q^{5^n}(\alpha) = \alpha \text{ for some } n \geq 1 \}$

$\frac{1}{4} = \frac{1}{5-1} = -\sum_{n \geq 0} 5^n$ converges in $\mathbb{Z}_5$

We "let" $\varphi_q^{1/4} := \varphi_q^{-\sum_{n \geq 0} 5^n} = \varphi_q^{-1} \circ \varphi_q^{-5} \circ \varphi_q^{-5^2} \circ \varphi_q^{-5^3} \circ \cdots$

For $\alpha \in \mathbb{F}_{q^{5^n}}$, $\varphi_q^{-5^N}(\alpha) = \alpha$ $\forall N \geq n$, so $\varphi_q^{1/4}(\alpha)$ makes sense for all $\alpha \in \mathbb{F}_{q^{5^\infty}}$.

Example

$t^{15} - 2$ over $\mathbb{F}_7$

$\langle 2 \rangle \subseteq \mathbb{F}_7^\times \cong \mathbb{Z}/6\mathbb{Z}$

$2^3 \equiv 1 \bmod 7$, so $o(2) = 3$.

If $\alpha^{15} = 2$, then $o(\alpha) = 45$

Suppose we had $\mathbb{F}_{7^e}$ with a primitive 45^{th} root of unity,

Thus, by cyclicity, there is some primitive 45^{th} root of unity

whose 15^{th} power is 2

$15\,\mathbb{Z}/45\mathbb{Z} = \{$ elts of order $|3\}$

$\exists$ a primitive 45^{th} root of unity in $\mathbb{F}_{7^e}$ $\iff 45 \mid 7^e - 1$ (as cyclic)

$\iff 15 \mid 7^e - 1$ as $\mathbb{F}_7$ has 3^{rd} roots of unity

We compute powers of 7 mod 15.

7, $7^2 \equiv 49 \equiv 4 \bmod 15$, $7^3 \equiv 28 \equiv -2 \bmod 15$, $7^4 \equiv -14 \bmod 15$

$\equiv 1 \bmod 15$

So $\mathbb{F}_{7^4}$ is the splitting field of $t^{15} - 2 / \mathbb{F}_7$.