Last time: # Construction of $\mathbb{F}_{p^k}$

Fermat's little theorem: Let $m \in \mathbb{Z} \setminus p\mathbb{Z}$ be an integer not divisible by a given prime p. Then $m^{p-1} \equiv 1 \mod p$.

In the language of our class: The Frobenius automorphism $F : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ is equal to the identity map.

What about the Frobenius automorphisms

$$F : \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_{p^k}$$

for $1 < k < \infty$?

Assume we are given a field K with p^k elements. Then the multiplicative group $K^\times$ has order p^k-1 and hence

$$a \in K^\times \implies a^{p^k-1} = 1$$

or

$$a \in K \implies a^{p^k} = a.$$

Corollary: If K is a field with p^k elements, then K is a splitting field of the polynomial $X^{p^k} - X$ over $\mathbb{F}_p$.

Proof: Since each of the p^k elements of K is a root of $X^{p^k} - X$, we have the equality in $K[X]$

$$X^{p^k} - X = \prod_{a \in K} (X - a).$$

Further, K is obviously generated by all of its elements (over $\mathbb{F}_p$), so $K = K(a \mid a \text{ is a root of } X^{p^k} - X)$. $\square$

It turns out that the converse is also true.
For this we need two lemmas.

<u>Lemma 1</u>: Let K be a field, $p(x) \in K[X]$ a polynomial over K. If $a \in K$ is a root of p with multiplicity greater or equal to 2, then a is also a root of the derivative

$$p'(x) = n a_n X^{n-1} + \dots + 2a_2 X + a_1$$

(where $p(x) = a_n X^n + \dots + a_1 X + a_0$).

<u>proof</u>: Exercise.

<u>Lemma 2</u>: Let K be a field and let $f: K \longrightarrow K$ be a field automorphism of K. Then the elements of K fixed by f form a subfield

$$K^f = \{ a \in K \mid f(a) = a \}.$$

<u>proof</u>: Exercise.

<u>Corollary</u>: Let K be a field of characteristic p, let $k \geq 1$. Then the roots of the polynomial $X^{p^k} - X$ form a subfield of K.

<u>proof</u>: These roots are exactly the elements fixed by the k^{th} power of the Frobenius automorphism

$$F^k = \underbrace{F \circ \dots \circ F}_{k \text{ times}} : K \longrightarrow K.$$

<u>Theorem</u>: Let K be a splitting field of the polynomial $X^{p^k} - X$ over $\mathbb{F}_p$. Then $|K| = p^k$.

<u>proof</u>: The derivative of $X^{p^k} - X$ is equal to -1.
So, $X^{p^k} - X$ has p^k distinct roots in K.

Further, $a \in K$ is a root of $X^{p^k} - X$ if and only if a is fixed by the kth power of the Frobenius homomorphism

$$F^k = \underbrace{F \circ \dots \circ F}_{k \text{ times}} : K \longrightarrow K.$$

So, $K^{F^k} \subset K$ is a subfield consisting of all the roots in K. Since we assumed K to be a splitting field, we assumed K to be generated (over $\mathbb{F}_p$) by the roots of $X^{p^k} - X$. Hence $K^{F^k} = K$. $\square$

<u>Theorem:</u> Let k be a field, $p(x) \in k[x]$ a polynomial over k. Then there exists a splitting field E of $p(x)$ over k whose degree over k is at most $n!$, where $n = \deg(p)$.

<u>Proof:</u> ~~Strong~~ <u>induction:</u> $n = 1$, take $E = k$.
Assume the statement holds for polynomials of degree $\le n$.
~~Case the p is irreducible Then $E = k[x]/p(x)$~~
Let $q(x)$ be an irreducible factor of $p(x)$.
Set $K := k[x]/(q(x))$, and let a be the coset of x. Then $a \in K$ is a root of p.

$$p(x) = (x-a)\,q(x) \quad \text{over } K.$$

Apply the induction hypothesis with K in the role of k and q in the role of p.

This gives a splitting field E of q over K.

So

$$k \subset \underset{a \in}{K} \subset \underset{\uparrow \text{ splitting field of } q}{E}$$

We claim that E is also a splitting field of p over k. Indeed, q factors into linear factors

$$q(x) = \prod_{\substack{\alpha \text{ root of } q \\ \text{in } E}} (x-\alpha)^{\overset{\text{multiplicity}}{n(\alpha)}}$$

over E. We need to show that the roots of p generate E as field extension of k. Let $k \subseteq K' \subseteq E$ be an intermediate extension containing all roots of p. Then K' contains a and hence

$$k \subseteq K = k[a] \subseteq K'.$$

Since K' contains all the roots of $q(x)$ and K and E is a splitting field of q over K, it follows that $K' = E$. $\square$

Reminder

Def of splitting field of
$p(x) \in k[X]$.

$k \subset E$ field extension s.t.

- $p(X) = \prod (X-\alpha)^{n(\alpha)}$ over E
- E is generated by the roots of p (as extension of k).