At the end last time:

Showed that if $|\mathbb{F}| = p^d$ then $\mathbb{F}/\mathbb{F}_p$ and $\mathbb{F}$ is a splitting field for $x^{p^d} - x$.

Remains to see that the splitting field of $x^{p^d} - x$ is a degree d extension of $\mathbb{F}_p$.

Before finishing: we'll introduce separability & the Frobenius map

Separability: If K is a field and $f \in K[x]$ then f is separable if it does not have any roots of multiplicity > 1 in a splitting field.

$i \neq j \Rightarrow$
$\alpha_i \neq \alpha_j$

$\hookrightarrow f(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2} \cdots (x-\alpha_m)^{k_m}$

α_i has multiplicity k_i.

Observation/Lemma: f is separable $\iff (f, f') = 1$

$f = a_0 + a_1 x + \cdots + a_n x^n$

$f' = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}$

(Apply chain rule in $L[x]$ for L/K a splitting field).

Examples: $(x-1)(x-2)$ is separable for any K

$(x-1)(x-2)^2$ is not separable for any K.

$(x-1)(x-2)(x-3)$ is separable for $\operatorname{char} K \neq 2$
inseparable if $\operatorname{char} K = 2$

$\parallel$

$(x-1)^2(x-2)$ if $\operatorname{char} K = 2$.

x^2+1 is separable over $\mathbb{R}$ (roots are i & $-i$ in $\mathbb{C}$).

$\rightsquigarrow$ $(x^2+1, 2x) = 1$

because $1(x^2+1) - \frac{1}{2}x(2x) = 1$.

$x^p - t$ over $\mathbb{F}_p(t)$ is inseparable.

irred. by Eisenstein.

in $\mathbb{F}_p(t^{1/p})$ $\quad (x^p - t) = (x - t^{1/p})^p$

Field w/ root

$$= x^p - \binom{p}{1}x^{p-1}t^{1/p} + \binom{p}{2}x^{p-2}t^{2/p} \dots + \binom{p}{p-1}x\,t^{p-1/p} - t$$

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$ is divisible by p

$1 \le i \le p-1$.

$$= x^p - t.$$

$f(x) = x^p - t$ ← constant term deriv = 0.

$f'(x) = px^{p-1} = 0$

because $p = 0$.

$(f, f') = (f)$.

Lemma: If f is irreducible then

f is separable $\iff$ $f' \neq 0$.

Pf: $f \in (f, f') = (g)$

$f' = hg$ for some h

If $f' \neq 0$ then

$\deg g \le \deg f' < \deg f$.

So $g \mid f \Rightarrow g$ is constant.

because f is irreducible

g nonzero constant $\Rightarrow (g) = (1)$.

Other direction easy.

$x = \sum^{\infty} a_n x^n \qquad a_n = 0$ for $n >> 0$.

$f'(x) = \sum_{n=0}^{\infty} n a_n x^{n-1} = 0 \iff n a_n = 0$ for

$n=1$

all $n \geq 1$

$\iff a_n = 0$ for $p \nmid n$, $p = \text{char } K$.

Theorem: • If $\text{char } K = 0$ then every irreducible polynomial in $K[x]$ is separable

• If $\text{char } K = p$ then if f is an irreducible polynomial in $K[x]$ then there exists a unique separable irreducible $g(x) \in K[x]$ and positive integer k s.t.

$$f(x) = g(x^{p^k}).$$

---

e.g. $x^p - t = g(x^p)$ for $g(x) = x - t$.

Warning: If $g(x)$ is irreducible $g(x^p)$ may not be — e.g. $g(x) = x - 1$ in $\mathbb{F}_p[x]$

$$f(x) = g(x^p) = x^p - 1 = (x-1)^p$$ not irreducible.

Motto: Separability of irreducibles ~ taking pth roots in characteristic p.

Why are pth roots / powers special in characteristic p?.

Theorem If K has characteristic p then

$K \longrightarrow K$

Frob_p:

$$\alpha \longmapsto \alpha^p$$

is a ring homomorphism.

($\mathbb{Q} \to \mathbb{Q}$
$\alpha \to \alpha^2$
does not satisfy
$(\alpha+\beta)^2 \cancel{=} \alpha^2+\beta^2$.
$= \alpha^2+2\alpha\beta+\beta^2$).

Proof: $(ab)^p = a^p b^p \qquad 1^p = 1 \quad 0^p = 0$

$$(a+b)^p = a^p + b^p$$

$$\| $$

$$a^p + \underbrace{\cancel{\binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \dots + \binom{p}{p-1}ab^{p-1}}}_{\text{divisible by } p \,=\, 0} + b^p.$$

Corollary: 1 is the only pth root of unity in any field of characteristic p.

PF: Field maps are injective. $(x^p - 1) = (x-1)^p$

Corollary: Any $\alpha \in K$ has at most one pth root.

If $\alpha^{1/p}$ is such a root,

$$(x - \alpha^{1/p})^p = x^p - \alpha.$$

Definition/Theorem: A field K is perfect if every irreducible polynomial in $K[x]$ is separable.

$$\iff$$

K has characteristic zero

or $\operatorname{char} K = p$ and Frob_p is surjective (=bijective)

Example If $\mathbb{F}$ is a finite field, $\mathbb{F}$ is perfect.

Proof: An injective map from a finite set to itself is bijective.

Let $\mathbb{F}/\mathbb{F}_p$ a splitting field of $x^{p^d} - x \in \mathbb{F}_p[x]$

will show $[\mathbb{F}:\mathbb{F}_p]=d$ ($\Leftrightarrow |\mathbb{F}|=p^d$).

Step 1: $(x^{p^d}-x)' = -1$ so

it has p^d distinct roots.

$(x^{p^d}-x, -1) = (1)$

so it's separable

all roots of $x^{p^d}-x$

Step 2: $\{\alpha\in\mathbb{F} \mid \alpha^{p^d}=\alpha\}$ ← has size p^d

is a subfield

$$\alpha^{p^d} = \underbrace{\mathrm{Frob}_p\circ\mathrm{Frob}_p\circ\mathrm{Frob}_p\circ\cdots\circ\mathrm{Frob}_p}_{d}(\alpha).$$

$$\mathrm{Frob}_{p^d} := \mathrm{Frob}_p\circ\cdots\circ\mathrm{Frob}_p(\alpha) = ((\alpha^p)^p)^{p\cdots}$$
$$= \alpha^{p^d}$$

is a an automorphism of $\mathbb{F}$.

$\alpha^{p^d}=\alpha \iff \mathrm{Frob}_{p^d}(\alpha)=\alpha$.

i.e. α is fixed by Frob_{p^d}.

Easy check: If K is any field and $\sigma: K\to K$ is any automorphism then $\{x\in K \mid \sigma(x)=x\}$ is a subfield.

$\overline{K}/K$ algebraic closure $\Rightarrow$ $\overline{K}$ algebraically closed.

Let $f\in\overline{K}[x]$ be non-constant.

$f = a_0 + a_1x + \cdots + a_nx^n$.

$$L = K(a_0, \ldots, a_1) \subseteq \overline{K}$$

L/K finite because f.g + alg.

Take g irreducible factor of f in $L[x]$

$$L[t]/_{g(t)} \underbrace{/\ L\ /\ K}_{\text{finite extension.}}$$

$\overline{t}$ is algebraic$/K$ so it is the root of some irreducible $h(x) \in K[x]$.

$h(x)$ splits completely in $\overline{L}$.

g splits completely in $\overline{L}$ so has a root in $\overline{L}$.