Last week:

Field of size $p^n$ is splitting field of $x^{p^n}-x$ over $\mathbb{F}_p[x]$.

You will show there is a field of size $p^n$ $\Rightarrow$ unique one $\mathbb{F}_{p^n}$

Prop: $f \in \mathbb{F}_p[x]$ irred. $\alpha$ root of $f$ in $K/\mathbb{F}_p$ then other roots of $f$ are $\alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$ $d = \deg(f)$

So $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^d}$ is the s.f. of $f$.

Very different from char 0:
e.g. $\mathbb{Q}(\sqrt[3]{2})$ not s.f. of $x^3-2$ over $\mathbb{Q}$.

Ex: $x^3+x^2+1$ and $x^3+x+1$ irred. in $\mathbb{F}_2[x]$ b/c no root.

$\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3+x^2+1) \cong \mathbb{F}_2[x]/(x^3+x+1)$

How can we explicitly write down an iso?

$\alpha$ root of $x^3+x+1$ in $\mathbb{F}_8$

roots are $\alpha, \alpha^2, \alpha^4 = \alpha^2+\alpha$

Elements of $\mathbb{F}_8$: $\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+\alpha, \alpha^2+1, \alpha^2+\alpha+1\}$

Notice that $(\alpha+1)^3 + (\alpha+1)^2 + 1$

$$\alpha^3 + \cancel{\alpha^2} + \alpha + \cancel{1} + \cancel{\alpha^2} + \cancel{1} + 1 = 0.$$

$\alpha+1$ is a root of $x^3+x^2+1$.

$$\alpha+1, \underset{\substack{\| \\ \alpha^2+1}}{(\alpha+1)^2} = (\alpha+1)^4 = \underset{\substack{\| \\ \alpha^2+\alpha+1}}{\alpha^4+1}$$

So define a map

$$\mathbb{F}_2[x]/(x^3+x+1) \longrightarrow \mathbb{F}_2[x]/(x^3+x^2+1)$$

$$p(x) \bmod x^3+x+1 \longrightarrow p(x+1) \bmod x^3+x^2+1$$

is an iso.

---

Separability

$K/F$ is <u>Galois</u> if

$$|\mathrm{Aut}(K/F)| = [K:F].$$

$K = F(\alpha)$ last time we showed that

$$|\mathrm{Aut}(F(\alpha)/F)| \leq [F(\alpha):F]$$

bijection between

$$\left\{ \begin{array}{c} \text{extensions of } id_F \\ \text{to auto. of} \\ F(\alpha) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{roots of} \\ m_\alpha(x) \\ \in F(\alpha) \end{array} \right\}$$

What could make inequality strict?

1.) $F(\alpha)$ doesn't have all roots of $m_\alpha(x)$ $\leftarrow$ Normality

2.) If $m_\alpha$ has repeated roots in $F(\alpha)$, won't get enough automorphisms. $\leftarrow$ Separability

<u>Ex:</u> $F = \mathbb{F}_3(t)$

$x^3 - t \in F[x]$. This poly is irred. by same argument as problem 20.

$$\begin{array}{c} F(\sqrt[3]{t}) \\ \Big| \, 3 \\ F \end{array} \qquad \begin{array}{c} (x - \sqrt[3]{t})^3 \\ \parallel \\ x^3 - t \end{array} \text{ in } F(\sqrt[3]{t})[x]$$

$\sigma \in \mathrm{Aut}(F(\sqrt[3]{t})/F)$

$\sqrt[3]{t}$ has to map to another root of $x^3 - t$, i.e. there is only one choice!

__Def:__ $f(x) \in F[x]$

$f$ is called __separable__ if it has distinct roots in a splitting field.

__Def:__ $K/F$ alg. is called __separable__ if $m_\alpha(x) \in F[x]$ is separable for all $\alpha \in K$.

Prop: Let $\alpha$ be a root of $f(x) \in F[x]$ in some $K/F$.

$\alpha$ is a repeated root of $f(x) \iff f'(\alpha) = 0$.

Cor: $f(x) \in F[x]$ then $f$ is separable $\iff (f(x), f'(x)) = 1$ in $F[x]$.

Proof: If $f$ is not separable, then there is $\alpha$ s.t. $f(\alpha) = f'(\alpha) = 0$, so $m_\alpha(x) \mid f(x)$ and $f'(x)$

$\Rightarrow (f(x), f'(x)) \neq 1$.

If $d = (f(x), f'(x))$ then

any root of $d$ is s.f. of $f$

is a root of $f$ and $f'$ $\Longrightarrow$

repeated root.

<u>Cor:</u> $f(x) \in F[x]$ is <u>irred.</u>

If $\operatorname{char}(F) = 0$, then

$f(x)$ is Separable.

If $\operatorname{char}(F) = p$ and $f(x) \notin$

$F[x^p]$ then $f(x)$ is Separable.

<u>Proof:</u> Let $\deg(f) = n$. Then

as long as $f'(x) \neq 0$,

$1 \le \deg(f') < n$. The only divisors of $f(x)$ (up to constant multiple) are $1$ and $f(x)$, so clearly $(f(x), f'(x)) = 1$ if this holds.

If $\mathrm{Char}(F) = 0$, $f'(x)$ is never $0$ for $f$ non-constant.

If $\mathrm{Char}(F) = p$, $f'(x) = 0 \Leftrightarrow f(x) \in F[x^p]$ (HW).

Ex:

- $f(x) = x^3 - 4x^2 + 5x - 2 \in \mathbb{Q}[x]$.

$f'(x) = 3x^2 - 8x + 5$

$f(1) = f'(1) = 0$. So $f$ is not separable.

In fact $f(x) = (x-1)^2(x-2)$.

- $x^3-2 \in \mathbb{Q}[x]$ is separable b/c it's irreducible. but over $\mathbb{F}_3[x]$ $x^3-2 = (x-2)^3$.

- $x^n-1 \in F[x]$. $f'(x) = nx^{n-1}$
  $\overset{\shortparallel}{f(x)}$

if $\text{char}(F) \nmid n$, then only root of $f'(x)$ is $0$ which clearly isn't a root of $x^n-1$.

$\Longrightarrow$ $x^n-1$ is separable so s.f. containing a full set of $n^{th}$ roots of unity.

if $\mathrm{Char}(F) = p \mid n$  $n = pk$

$$x^n - 1 = x^{pk} - 1 = (x^k - 1)^p$$

this is not separable (all roots are repeated!)

e.g. $x^6 - 1 \in \mathbb{F}_3[x]$

$$\shortparallel$$

$$(x-1)^3 (x+1)^3$$

So this only 2 $6^{th}$ roots of unity.

Rmk: $K/F$ finite and $\mathrm{char}(F)=0$

$\Longrightarrow$ $K/F$ is separable.

So separability is a purely characteristic $p$ phenomenon.

Def: $F$ is called perfect if all irred. in $F[x]$ are separable.

Alternatively: every $K/F$ algebraic is separable.

**Ex:** · Any field of char 0
· Finite fields (HW)

**Non example:** $\mathbb{F}_p(t)$ is not perfect by first example.

**Prop:**

$$\left.\begin{array}{c} L \\ | \\ K \\ | \\ F \end{array}\right) \text{ separable} \implies \begin{array}{c} L \\ | \\ K \end{array} \text{ sep} \qquad \begin{array}{c} K \\ | \\ F \end{array} \text{ sep}$$

**Proof:** $\alpha \in K \subseteq L$ $\quad m_{\alpha,F}(x)$ is sep. b/c $L/F$ sep. this doesn't change if $\alpha$ is viewed as living in $K$ or $F$.

$m_{a,F}(x) \in K[x] \Longrightarrow$

$m_{a,K}(x) \mid m_{\alpha,F}(x).$

b/c $m_{\alpha,F}(x)$ has distinct roots $\Longrightarrow$ $m_{\alpha,K}(x)$ has distinct roots.

Goal:

$K|F$ is s.f. of separable $f(x) \in F[x] \Longrightarrow K|F$ Galois.

Rmk: by what we've done so far, if $F(\alpha)|F$ splits $m_\alpha(x)$ then $F(\alpha)|F$ is Galois.