Continuing Galois theory:

Here's a basic fact we'll use over and over.

Prop (Extension Lemma)
Let $f(x) \in K[x]$ be irreducible, and let $K \subset L_1$, $K \subset L_2$ be two extensions s.t. some $\alpha_i \in L_i$ is a root of f. Then $\exists!$ K-linear isomorphism

$$K[\alpha_1] \xrightarrow{\cong} K[\alpha_2], \quad \alpha_1 \mapsto \alpha_2.$$

Pf: We have

$$\begin{tikzcd} K[x] \arrow[r, "x \mapsto \alpha_2"] \arrow[d, "x \mapsto \alpha_1"'] & L_2 \\ L_1 & \end{tikzcd}$$

hence, by 1^{st} $\cong$ thm,

$$\begin{tikzcd} K[x]/(f) \arrow[r, "\cong"] \arrow[d, "\cong"] & K[\alpha_2] \\ K[\alpha_1] & \end{tikzcd}$$

Uniqueness is by univ. prop. of quotients. //

Cor If $\{\alpha_1, \ldots, \alpha_n\} \subset \overline{K}$ are the roots of $f(x) \in K[x]$, f irreducible, $\exists$ exactly n K-linear embeddings
$$K[\alpha_1] \hookrightarrow \overline{K}.$$

Okay, so what's the deal w/ "separability?"

Last class I introduced inseparable extensions as a cautionary tale:

<u>Fact</u> For <u>some</u> K, $\exists$ irreducible polynomials $f \in K[x]$ such that
$$\#\text{roots}(f) < \deg(f).$$

Such an f is called <u>inseparable</u>.

<u>Defn</u> Fix a field K. An irreducible polynomial $f \in K[x]$ is <u>separable</u> (over K) if
$$\underset{\text{in } \overline{K}}{\#\text{roots}(f)} = \deg(f).$$

If f monic, $f = (x-a_1)\cdots(x-a_{\deg(f)})$ in $\overline{K}$, so this amounts to saying $a_i \neq a_j$ for $i \neq j$. That is, in $\overline{K}$ (hence in all algebraic extensions of K), no polyn of the form $(x-a)^2$ divides $f(x)$.

<u>Prop</u> An irreducible f is separable iff $\forall$ extensions $K \subset L$, and all $a \in L$,
$$(x-a)^2 \nmid f(x)$$
in $L[x]$.

Defn Let $K \subset L$ be algebraic.
L is called **separable** (over K)
iff $\forall\ \alpha \in L$, the irreducible
polynomial of α,

$$f(x) \in K[x],$$

is separable (over K).

If this holds for α, we also say α
is separable.

Here are some navigational tools:

Exer $f \in K[x]$ is separable iff
$\forall$ roots $\alpha \in \overline{K}$, $\exists$ exactly
$\deg f$ embeddings

$$K[\alpha] \hookrightarrow \overline{K}$$

that are K-linear.

Soln By corollary, $\{\Phi : K[\alpha] \hookrightarrow \overline{K}\} \cong \{\alpha_1, \ldots, \alpha_n \text{ roots of } f\}$.
Hence $\#\Phi = \deg(f) \iff \#\text{roots} = \deg(f)$. //

Let's try to discover when we might encounter inseparable polynomials.
[Below f is irreducible.]

Prop $f(x)$ is inseparable iff f and f' share a root in $\overline{K}$.

Pf We know f insep. $\iff \exists\, \alpha \in \overline{K}$ st $(x-\alpha)^2$ divides f.

Then

$$f' = \frac{d}{dx} f = \frac{d}{dx}\left((x-\alpha)^2 h(x)\right)$$
$$= 2(x-\alpha)h(x) + (x-\alpha)^2 h'(x).$$

Hence

$$f'(\alpha) = 2 \cdot 0 \cdot h(\alpha) + 0^2 \cdot h'(\alpha) = 0.$$

Conversely, if $f(\alpha) = 0 = f'(\alpha)$ for a common $\alpha \in \overline{K}$, we have that

$$f = (x-\alpha) g, \quad f' = (x-\alpha) g' + g.$$

Since $f'(\alpha) = 0$, $x - \alpha$ must divide g. Hence $f = (x-\alpha)^2 h$. //

Cor $f(x)$ is inseparable iff $\gcd(f, f') \neq \{\text{units}\}$ in $\overline{K}[x]$.

Cor f is inseparable iff $f' = 0 \in K[x]$.

Pf (of 2nd Corollary) Since f is irreducible, if $\alpha \in \overline{K}$ is a root, f is the minimal polynomial of α. But $\deg(f') < \deg(f)$; so if $f'(\alpha)$ is to equal zero, we must have that $f' = 0$. Conversely, if $f' = 0$, any root of f is a root of f'; hence f and f' share a root. //

Cor If $f \in K[x]$ is irreducible and inseparable, $\mathrm{char}(K) = 0$.

Pf: In the leading term $a_n x^n$ of f, $a_n \neq 0$. Hence $n \cdot a_n x^{n-1} \neq 0$, and $f' \neq 0$. //

Cor If $f \in K[x]$ is irreducible, inseparable, and $\mathrm{char}(K) = p > 0$, then

$$f(x) = h(x^p)$$

for some $h \in K[x]$. That is,

$$f(x) = a_n (x^p)^n + \cdots + a_1 (x^p) + a_0,$$

ie, every monomial in f has degree a multiple of p.

Pf: If $f = \sum a_i x^i$, $f'(x) = \sum i a_i \cdot x^{i-1}$. Since K a field, $a_i \neq 0 \implies i = (\underbrace{1 + \cdots + 1}_{i \text{ times}}) = 0 \in K$ $\forall i$. This means

i must be divisible by $\mathrm{char}(K)$. //

Here's a central tool in Galois theory in char $p>0$:

Prop. Let $\mathrm{char}(K)=p>0$.
Then

$$\begin{aligned} \varphi: K &\longrightarrow K \\ \alpha &\longmapsto \alpha^p \end{aligned}$$

is a ring homomorphism.

Defn: This is called the Frobenius map.

Pf $\cdot$ $1 \longmapsto 1^p = 1$

$\cdot$ $(xy) \longmapsto (xy)^p = x^p y^p$.

$\cdot$ $x+y \longmapsto (x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p$

$$= x^p + 0 + \cdots + 0 + y^p$$

$$= x^p + y^p. \quad //$$

Since K is a field, the Frobenius is always an injection.
It is NOT always a surjection.

Ex If K is finite, then φ is an injection $\Rightarrow$ φ is a bijection.
So φ is an automorphism.

Ex Let $K = \mathbb{F}_p(x) = \left\{ \frac{u(x)}{v(x)} \;\middle|\; u, v \in \mathbb{F}_p[x],\ v \neq 0 \right\}$

be the field of rational fractions. Then $x \notin \text{image}(\varphi)$.

Exer Prove $x \notin \text{image}(\varphi)$.

Sol'n If $\left(\frac{u}{v}\right)^p = x$, we have $u^p = x \cdot v^p$. This means

$$p \cdot \deg(u) = 1 + p \cdot \deg(v).$$

Violates divisibility. //

Defn K of char $p > 0$ is called perfect if φ is a surjection. (ie, if every $\alpha \in K$ admits a p^{th} root.)

Prop'n Let K have charac $p > 0$, and suppose $\exists$ $f \in K[x]$ irreducible, inseparable. Then K is NOT perfect.

Pf We know $f(x) = h(x^p) = \sum_{n=0}^{D} a_n (x^n)^p$. If K is perfect, $\forall$ a_n, $\exists$ b_n st $a_n = b_n^p$.
Hence $f(x) = \left(\sum b_n x^n\right)^p$, so f is NOT irreducible. //

The conclusion is that for K to admit an inseparable polynomial,

- K must have charac $p \neq 0$, and
- K must be <u>imperfect</u>. (Aren't we all?)

This rarely arises in a course like this — we usually talk about finite fields, or fields over $\mathbb{Q}$ (charac 0).
(which are perfect)

In fact,

Prop: Let $\mathrm{char}(K) = p > 0$.
Then

$$\exists \text{ irreducible, inseparable } f(x) \in K[x]$$
$$\Updownarrow$$
$$K \text{ is imperfect.}$$

Pf: $\Downarrow$ was done.

$\Uparrow$: Let $\alpha \in K$ st $\alpha \notin \mathrm{image}(\varphi)$. Then $x^p - \alpha$ has no root. In particular, even if $x^p - \alpha$ isn't irreducible in $K[x]$, its irreducible factors have $\deg \geq 2$. On the other hand, let $\beta \in \bar{K}$ be a root. Then $\alpha = \beta^p$, so

$$(x^p - \alpha) = x^p - \beta^p = (x - \beta)^p \in \bar{K}[x].$$

By unique factorization in $\bar{K}[x]$, any irreducible factor of $x^p - \alpha$ hence splits as $(x-\beta)^n$, exhibiting an inseparable polynomial in $K[x]$.

So lets fully see an example:

<u>Ex</u> Let $K = \mathbb{F}_p(x)$, and

$$f(t) = t^p - x \quad \in K[t].$$

We know x isn't in the image of the Frobenius, so $f(t)$ has no root. By Eisenstein (since $K = \mathrm{Quot}(\mathbb{F}_p[x])$ and $(x) \subset \mathbb{F}_p[x]$ is prime) $f(t)$ is irreducible. But in

$$L := K[t]/(f(t)), \qquad \ni \underline{t}$$

we know $\underline{t}^p = x$, so

$$f(y) = y^p - x = y^p - \underline{t}^p$$

$$= (y - \underline{t})^p \in L[y].$$

And, as promised, f is not separable.