Lecture 18 Feb 22, 2021

Separability

Def. $f \in F[x]$ is *separable* if given a splitting field $F \subseteq K$ for f, then $f = c(x-\alpha_1)\cdots(x-\alpha_n)$ in $K[x]$ where $\alpha_1, \ldots, \alpha_n$ are distinct.

Otherwise we say f is *inseparable*.

Rmk. This is independent of choice of splitting field.

Ex. $(x^2-2)^2 \in \mathbb{Q}[x]$ is inseparable since in a splitting field in $\mathbb{C}$ it factors as

$$(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{2}).$$

More interesting: if $f \in F[x]$ is irreducible, can it be inseparable?

<u>Def.</u> Let $f \in F[x]$ F a field. Let $f = a_0 + a_1 x + \dots + a_n x^n$. The derivative is

$$f' = a_1 + \underline{2} a_2 x + \dots + \underline{(n-1)} a_{n-1} x^{n-2} + \underline{n} a_n x^{n-1}.$$

$\in F[x]$.

Here $i a_i$ means the ith multiple of a_i, or i means the image of $i \in \mathbb{Z}$ under $\mathbb{Z} \to F$

So if $\operatorname{char} F = p > 0$ then some coefficients become 0.

e.g. char $F = p$, $(X^p)' = pX^{p-1} = 0$

Rmk if $f, g \in F[x]$

$(f+g)' = f' + g'$

$(fg)' = f'g + fg'$

$(f^d)' = d f^{d-1} f'$.

Thm. $f \in F[x]$ is separable iff $\gcd_{F[x]}(f, f') = 1$.

Pf. in a splitting field K we have

$f = c(x-\alpha_1)^{e_1} \cdots (x-\alpha_n)^{e_n}$

where $\alpha_1, \dots, \alpha_n$ are distinct $e_i \geq 1$.

f is separable iff $e_i = 1$ for all i.

Now note

$(f_1 f_2 \cdots f_k)' = f_1' f_2 \cdots f_k + f_1 f_2' \cdots f_k + \cdots + f_1 f_2 \cdots f_k'$.

So
$$f' = \sum_{i=1}^{n} c(x-\alpha_1)^{e_1} \cdots e_i(x-\alpha_i)^{e_i-1} \cdots (x-\alpha_n)^{e_n}.$$

Suppose $e_i \geq 2$ for some i. Then $(x-\alpha_i) \mid f'$. Also $(x-\alpha_i) \mid f$ in $K[x]$ so $\gcd_{K[x]}(f, f') \neq 1$.

Conversely if $e_i = 1$ then $(x-\alpha_i)$ does not divide f' for all i, while $(x-\alpha_i)$ are the only irreducible factors of f in $K[x]$, so $\gcd_{K[x]}(f, f') = 1$.

Last, $\gcd_{K[x]}(f, f') = \gcd_{F[x]}(f, f')$.

(e.g. since you can calculate gcd using the Euclidean algorithm) $\square$.

<u>**Prop.**</u> Suppose $f \in F(x)$ is irreducible over F. Then f is inseparable iff char $F = p > 0$ and $f = \sum_{i=0}^{n} b_i x^{pi}$ $b_i \in F$.

Pf. Suppose f is inseparable.

Then $\gcd_{F[x]}(f, f') \neq 1$.

but f is irreducible. This forces $\gcd(f, f') = f$.

So $f \mid f'$ even though $\deg f' < \deg f$.

This forces $f' = 0$.

Then char $F = p > 0$.

if $f = \sum_{i=1}^{m} a_i x^i$

$$f' = \sum_{i=1}^{m} i a_i x^{i-1}$$

So for all i, $i a_i = 0$ so either $a_i = 0$ or $0 = \bar{i} \in F$

where $\mathbb{Z} \longrightarrow F$

$i \longmapsto \bar{i}$.

either $a_i = 0$ or $p \mid i$.

So $f = \sum_{i=1}^{n} b_i x^{ip}$ some $b_i \in F$.

The converse is clear, since f of that form has $f' = 0$.

<u>Cor.</u> if char $F = 0$ then all irreducible polys $f \in F[x]$ are separable.

<u>Def.</u> Let F be a field with char $F = p$. Then the Frobenius homomorphism is

$$\phi : F \longrightarrow F$$
$$a \longmapsto a^p.$$

this <u>is</u> a homomorphism since

$$\phi(a+b) = (a+b)^p = a^p + b^p.$$

<u>Def.</u> A field F is <u>perfect</u> if char $F = 0$ or char $F = p > 0$ and the Frobenius is surjective, i.e.

$F^p = \{a^p \mid a \in F\} = F.$

Thm. If F is perfect, then every irreducible $f \in F[x]$ is separable.

Pf. if $\operatorname{char} F = 0$, we saw this.

Now let $\operatorname{char} F = p > 0$. Suppose f is inseparable.

So $f = \sum_{i=0}^{n} b_i x^{ip}$ $b_i \in F$.

Since F is perfect $b_i = (a_i)^p$ $a_i \in F$.

$$f = \sum_{i=0}^{n} a_i^p x^{ip} = \sum_{i=0}^{n} (a_i x^i)^p$$

$$= \left(\sum_{i=0}^{n} a_i x^i\right)^p$$ which is not irreducible in $F[x]$.

This is a contradiction.

Cor. if F is finite, then F is perfect.

Pf. $\operatorname{char} F = p > 0$.

The Frobenius $\phi: F \to F$
$a \mapsto a^p$

is injective since F is a field
then since $|F| < \infty$, it is also
surjective.

Ex. let $F = \overline{\mathbb{F}_p(y)}$ be a rational
function field. Then F is not perfect.

Claim: y has no pth root in F.

If it did, $y = (f/g)^p$ $f, g \in \mathbb{F}_p[y]$.

Then $y g^p = f^p$ in $\mathbb{F}_p[y]$.

So $\deg(y g^p) = p \deg g + 1 = p \deg f$
$= \deg(f^p)$; which doesn't happen.

Also $F[x]$ has an irreducible
inseparable polynomial $f = x^p - y$

- irreducible by Eisenstein with the
prime $y \in \mathbb{F}_p[y]$. (F = field of fractions
of $\mathbb{F}_p[y]$).

- inseparable. In a splitting field K for f, there is a root $\alpha \in K$, $f(\alpha)=0$, or $\alpha^p - y = 0$ or $\alpha^p = y$.

Then $(x-\alpha)^p = x^p - \alpha^p = x^p - y$ $= f$. So f is inseparable.

<u>Thm.</u> If F is <u>not</u> perfect then $F[x]$ does have irreducible inseparable polynomials.