Lecture 19: Separable and Inseparable Extensions

Let F be a field and $f(x) \in F[x]$ with leading coefficient a_n. Then $\exists$ a splitting field for which $\exists$ distinct elements $\alpha_1, \alpha_2, \dots, \alpha_k$ and

$$f(x) = a_n (x-\alpha_1)^{n_1} (x-\alpha_2)^{n_2} \cdots (x-\alpha_k)^{n_k}$$

where $n_i \geq 1$ for $i = 1, 2, \dots k$ and $n_1 + n_2 + \cdots + n_k = n$. Given this notation,

Def^n/ α_i is a <u>multiple root</u> of $f(x)$ if $n_i > 1$ and we call n_i the <u>multiplicity</u> of α_i. Furthermore, α_i is a <u>simple root</u> if α_i has $n_i = 1$.

When a polynomial has no multiple roots we have a name for that,

Def^n/ A polynomial over F is called <u>separable</u> if it has no multiple roots, in other words a polynomial is separable if all its roots are distinct. A polynomial which is not separable is called inseparable.

E1 $x^2 - 2 \in \mathbb{Q}[x]$ is $\boxed{\text{separable}}$ over $\mathbb{Q}$ since $\pm\sqrt{2}$ are roots of $x^2 - 2$ and $\sqrt{2} \neq -\sqrt{2}$.

E2 $x^2 - t \in \mathbb{F}_2(t)$ ← rational functions with coefficients from $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$.

Then $x^2 - t$ is irreducible yet

$$\begin{aligned}(x-\sqrt{t})(x+\sqrt{t}) &= (x+\sqrt{t})^2 \\ &= x^2 + 2\sqrt{t} + (\sqrt{t})^2 \\ &= x^2 + t \\ &= x^2 - t\end{aligned}$$

} mod 2 calculation is wild.

$\boxed{x^2 - t \text{ not separable}}$

As we discussed before, the derivative can be formally defined on $F[x]$ for any field F, no limits required!

Def^n/ $\frac{d}{dx}\left(a_n x^n + \cdots + a_1 x + a_0\right) = n a_n x^{n-1} + \cdots + a_1$

which we can denote by $D_x[f(x)] = \frac{df}{dx} = f'(x)$ as usual

Then $D_x : F[x] \longrightarrow F[x]$ is additive with $\mathrm{Ker}(D_x) = F$ and D is surjective, but

$$D_x[fg] = D_x[f]g + f D_x[g]$$

So D is not a ring homomorphism. That said, here is the theorem I was searching for a couple weeks ago when I introduced multiple roots,

Proposition (33) Let $f(x) \in F[x]$,

A polynomial $f(x)$ has multiple root α iff α is also a root of $D_x[f(x)]$, that is $f(x)$ and $D_x[f(x)]$ are both divisible by $m_{\alpha,F}(x)$. In particular, $f(x)$ is separable iff $f(x)$ is relatively prime to $D_x[f(x)]$; $(f(x), D_x[f(x)]) = 1$

Proof: Suppose α is multiple root of $f(x)$. Then

$$f(x) = (x-\alpha)^n g(x)$$

over some splitting field which contains α, $n \geq 2$.

Thus $\frac{df}{dx} = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n \frac{dg}{dx}$ $*$

Hence $f'(\alpha) = 0$ by evaluation of $*$ at α.

Proof continued

Conversely, suppose α is root of both $f(x)$ and $D_x[f(x)]$

Hence $f(x) = (x-\alpha)h(x)$ for some polynomial $h(x)$

Thus $f'(x) = h(x) + (x-\alpha)h'(x)$ and

by assumption $\therefore f'(\alpha) = 0 \Rightarrow 0 = h(\alpha) + 0$

thus $h(\alpha) = 0 \Rightarrow h(x) = (x-\alpha)h_2(x)$

$$\Rightarrow f(x) = (x-\alpha)^2 h_2(x)$$

Consequently, the multiplicity of α is at least two

$\therefore$ α is multiple root for $f(x)$.

$\boxed{E1}$ $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ has $f'(x) = p^n x^{p^n - 1} - 1 = -1 \mod p$

thus $f'(x)$ has no roots $\therefore$ $f(x)$ has no multiple roots.

$\therefore$ $f(x)$ is separable.

$\boxed{E2}$ $f(x) = x^n - 1$ then $f'(x) = nx^{n-1}$

then in any field in which $n \neq 0$ $(n \nmid \text{char}(F))$

we find the only zero of $f'(x)$ is just $x = 0$

and since $f(0) = -1 \neq 0$ we find $f(x)$ has

no multiple roots $\therefore$ $f(x)$ separable.

$\boxed{E3}$ in the other extreme, if $\text{char}(F) = p$ and

$p \mid n$ then $f(x) = x^n - 1$ has $f'(x) = nx^{n-1} \equiv 0$

Thus every root of $f(x)$ is multiple.

Corollary (34)

Every irreducible polynomial over a field of characteristic 0 is separable. A polynomial over such a field is separable iff it is the product of distinct irred. polys.

Proposition (35)

Let F be a field of characteristic p.
Then for any $a, b \in F$

$$(a+b)^p = a^p + b^p \quad \& \quad (ab)^p = a^p b^p$$

Def^n/ If F is a field of characteristic p then $\Phi(x) = x^p$ defines the **FROBENIUS ENDOMORPHISM** OF F

Corollary (36)

Suppose $\mathbb{F}$ is finite field of char $(\mathbb{F}) = p$. Then every element of $\mathbb{F}$ is a p^{th} power in $\mathbb{F}$

Propostion (37)

Every irreducible polynomial over a finite field $\mathbb{F}$ is separable. A polynomial in $\mathbb{F}[x]$ is separable iff it is product of distinct irreducible polynomials.

Def^n/ A field K of characteristic p is called **PERFECT** if every element of K is a p^{th} power of K; $K = K^p$. Any field of characteristic zero is also perfect.

Def^n/ The field K is said to be separable over F if every element of K is the root of a separable poly. over F. Otherwise the field is said to be inseparable

Corollary (39)/ Every finite extension of a perfect field is separable. Every finite extension of $\mathbb{Q}$ or finite field is separable.

So... what about $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$?

Let's begin by examining the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$ which we previously argued $(x^2-3)(x^2-2)$ is split by this field. I have asked if $\exists\, \alpha$ for which $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{3})$? If such α exists then $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is a <u>simple</u> extension over $\mathbb{Q}$. We found $[\mathbb{Q}(\sqrt{2},\sqrt{3}) ; \mathbb{Q}] = 4$ thus $\alpha = \sqrt{2}$ is ruled out since $\deg(\sqrt{6}) = 2$ as $m_{\sqrt{6},\mathbb{Q}}(x) = x^2 - 6$.

Let's study $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$,

$$(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2}) = (\sqrt{3})^2 - (\sqrt{2})^2 = 3-2 = 1$$

$$\therefore \boxed{(\sqrt{2}+\sqrt{3})^{-1} = \sqrt{3}-\sqrt{2}}$$

Then $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a field which includes both $\sqrt{2}+\sqrt{3}$ and $(\sqrt{2}+\sqrt{3})^{-1} = \sqrt{3}-\sqrt{2}$. Of course,

$$(\sqrt{2}+\sqrt{3}) + (\sqrt{3}-\sqrt{2}) = 2\sqrt{3} \Rightarrow \underline{\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})}.$$

$$(\sqrt{2}+\sqrt{3}) - (\sqrt{3}-\sqrt{2}) = 2\sqrt{2} \Rightarrow \sqrt{2} \in \underline{\mathbb{Q}(\sqrt{2}+\sqrt{3})}.$$

Consequently, we certainly have shown $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. It remains to demonstrate $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$.

<u>PROBLEM</u>: find the minimal polynomial of $\alpha = \sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$

$$\alpha^2 = (\sqrt{2}+\sqrt{3})^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$$

$$\left(\frac{\alpha^2-5}{2}\right) = \sqrt{6} \quad \therefore \quad (\alpha^2-5)^2 = 4\cdot 6 \Rightarrow \alpha^4 - 10\alpha^2 + 25 = 24$$
$$\Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0$$

This suggests $\underline{M_{\alpha,\mathbb{Q}}(x) = x^4 - 10x^2 + 1}$.

If $M_{\alpha,\mathbb{Q}}(\sqrt{2}+\sqrt{3}) = 0$ then $[\mathbb{Q}(\alpha);\mathbb{Q}] \leq 4$.

Minimal Polynomial for $\alpha = \sqrt{2}+\sqrt{3}$ continued,
we suspect $m_{\alpha,\mathbb{Q}}(x) = x^4 - 10x^2 + 1$ is irreducible and has $\alpha = \sqrt{2}+\sqrt{3}$ as a root (otherwise calling it $m_{\alpha,\mathbb{Q}}(x)$ would be very bad tact.)

$$(\sqrt{2}+\sqrt{3})^2 = (\sqrt{2}+\sqrt{3})(\sqrt{2}+\sqrt{3}) = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$$

$$(\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})(5+2\sqrt{6}) = 25 + 20\sqrt{6} + 24 = 49 + 20\sqrt{6}$$

$$\begin{aligned}(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 &= 49 + 20\sqrt{6} - 10(5+2\sqrt{6}) + 1 \\ &= 49 + 20\sqrt{6} - 50 - 20\sqrt{6} + 1 \\ &= 0.\end{aligned}$$

Remark: this is not surprising, our construction of $x^4 - 10x^2 + 1$ made the above inevitable.

Irreducibility? Sadly Eisenstein doesn't seem to help directly,

$$f(x) = x^4 - 10x^2 + 1$$

$\mathbb{Z}_2$: $\overline{f(x)} = x^4 + 1$ in $\mathbb{Z}_2$ $\therefore$ $\overline{f(0)} = 1$ & $\underbrace{\overline{f(1)} = 1+1 = 0}_{\text{aww man.}}$

$\mathbb{Z}_3$: $\overline{f(x)} = x^4 - x^2 + 1$ $\therefore$

$$\begin{aligned}\overline{f(0)} &= 1 \\ \overline{f(1)} &= 1 - 1 + 1 = 1 \\ \overline{f(2)} &= 16 - 4 + 1 = 12 + 1 = 1\end{aligned}$$

Thus $\overline{f(x)}$ is possibly irreducible over $\mathbb{Z}_3$. We must investigate if it factors into product of irreducible quadratics over $\mathbb{Z}_3$. We know $\exists$ 3 such irred. quadratics:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2$$

$$\begin{array}{r} x^2+1 \\ x^2+1 \overline{\big) x^4 - 10x^2 + 1} \\ \underline{x^4 + x^2} \\ -11x^2 + 1 \\ \underline{-(x^2+1)} \\ 12x^2 + 0 = 0 \end{array}$$

rats, $x^4-10x^2+1 = (x^2+1)^2$ in $\mathbb{Z}_3[x]$ $\therefore$ no help.

Of course, $x^4-10x^2+1 = x^4+2x^2+1 = (x^2+1)^2$ over $\mathbb{Z}_3$.

Well, on to $\mathbb{Z}_5$ ... or, perhaps we should use the theory of field extensions.

1.) $\alpha = \sqrt{2}+\sqrt{3}$ solves $m_{\alpha,\mathbb{Q}}(x) = x^4-10x^2+1 = 0$

Thus $\deg(\alpha) \leq 4$ or $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] \leq 4$

2.) $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and we previously proved $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$

$$\therefore \quad [\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4$$

since $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ contains a 4-dim'l subspace over $\mathbb{Q}$ and is at most 4-dim'l over $\mathbb{Q}$.

Then why is $m_{\alpha,\mathbb{Q}}(x) = x^4-10x^2+1$ irreducible over $\mathbb{Q}$? If it was reducible then $\exists\, f(x)$ of lower degree, irreducible with $f(\alpha) = 0$ and then $\mathbb{Q}(\alpha) \cong \dfrac{\mathbb{Q}[x]}{(f(x))}$