Lecture 5: Galois Extensions

Aim Lecture: Intro. class of Galois ext$^{\underline{n}}$s where Galois group big enough to yield significant info.

Algebraic Differentiation

Let F = field

Prop$^{\underline{n}}$-Def$^{\underline{n}}$ 1: Let $R = \frac{F[x,\delta]}{\langle \delta^2 \rangle}$ & $f(x) = \sum a_i x^i \in F[x]$.

ⓐ There's a unique poly. $f'(x) \in F[x]$ s.t. $R \ni f(x+\delta) - f(x) = f'(x)\delta$ called the derivative of $f(x)$.

ⓑ $f'(x) = \sum i a_i x^{i-1}$.

Proof: same as $/\mathbb{R}$. $\square$

Eg.) If $\operatorname{char} F = p > 0$, $\alpha \in F$, $f(x) = x^p - \alpha$
$\implies f'(x) = px^{p-1} = 0$!

Facts: ⓐ $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$.
ⓑ α is a multiple root of $f(x) \in F[x]$ iff $0 = f(\alpha) = f'(\alpha)$

Proof: ex. Same as in case $F = \mathbb{R}$. $\square$

Separability

Propⁿ-Defⁿ 2: Let $f(x) \in F[x] - F$ be irred.
TFAE

ⓐ In the splitting field L for $f(x)/F$, $f(x)$ factorises into distinct linear factors.

ⓑ $f'(x) \neq 0$

ⓒ If α is a root of $f(x)$ then
$n := $ no. field hom $\sigma : F(\alpha) \to L$ over F
$= [F(\alpha):F] = \deg f(x)$.

In this case we say $f(x)$ & α are separable $/F$

Proof: Note σ determined by root $\sigma(\alpha) \in L$ of $f(x)$ so Lect. 4 Propⁿ 2 $\Rightarrow$ $n =$ no. roots of $f(x)$ in L &
ⓐ $\Leftrightarrow$ ⓒ
Fact ⓑ gives ⓐ $\Rightarrow$ ⓑ
Note ⓑ $\Rightarrow$ $\text{g.c.d.}(f(x), f'(x)) = 1$
so Fact ⓑ $\Rightarrow$ f has no multiple roots & ⓐ follows.

Defⁿ 1: A field extⁿ K/F is separable if it's gen. by separable elts $/F$. A poly. $f(x) \in F[x]$ is separable $/F$ if its irred. factors are.

Cor: If char $F = 0$ then all field extⁿs of F are separable.

Galois Extensions

Def^n 2: A field ext^n K/F is normal if K is the splitting field of some $f(x) \in F[x]$. It is Galois if furthermore we can choose $f(x)$ separable $/F$ (so K/F separable too).

E.g. 2. $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$ is Galois.

Thm: Let K be the splitting field of a sep. poly $f(x)/F$ & $\sigma : F \to F'$ a field isom. Let K' = splitting field of $(\sigma f)(x)$ $/F'$.
Then there are exactly $[K:F]$ field hom $\sigma_K : K \to K'$ extending σ.

Cor.: ($\sigma = id_F$ gives) $|Gal(K/F)| = [K:F]$

Proof THM: by induction on $[K:F]$
Let $\alpha \in K$ be a root of an irred. factor $f_1(x)$ of $f(x)$ & $\alpha' \in K'$ any root of $(\sigma f_1)(x)$.
Lect. 4 Prop^n 2 gives isom. σ_α below extending σ

$$\begin{tikzcd} F \arrow[r, "\sigma", "\sim"'] \arrow[d, hook] & F' \arrow[d, hook] \\ F(\alpha) \arrow[r, "\sigma_\alpha", "\sim"'] \arrow[d, hook] & F'(\alpha') \arrow[d, hook] \\ K \arrow[r, "\sigma_K", "\sim"'] & K' \end{tikzcd}$$

Now K (resp. K') is splitting field for $f(x)$ (resp $(\sigma f)(x)$) $/ F(\alpha)$ (resp. $F'(\alpha')$) so inductive hypothesis $\Rightarrow$ can extend σ_α to field isom. σ_K in $[K:F(\alpha)]$ no. ways.

no. choices for $\sigma_\alpha = [F(\alpha):F]$

so

total no. $\sigma_K = [K:F(\alpha)][F(\alpha):F]$

$= [K:F]$

$\square$

N.B. Cor. $\Rightarrow$

$$|\underbrace{\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})}_{K}/\mathbb{Q})| = 6$$

Since $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_3$ we immediately can conclude $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_3$.