

§ 53 Galois theory

Suppose $E \supset F$ is a Galois extension
(splitting & separable) $\nearrow$

We want to check that the correspondences

$$E \supset K \supset F \text{ subext.} \rightsquigarrow \overset{\lambda(K) \nearrow}{G(E/K)} = G(E/F) \text{ subgroup}$$

$$H \leq G(E/F) \text{ subgroup} \rightsquigarrow E \supset E_H \supset F \text{ subext.}$$

are inverse to each other.

$$\rightsquigarrow \text{we need } \lambda(E_H) = H, \quad E_{\lambda(K)} = K$$

Prop. (part 2 of Th'm 53.6) $E_{\lambda(K)} = K$

Proof $K \subset E_{\lambda(K)}$ is a formal conseq. of def.

To check $E_{\lambda(K)} \subset K$ we want: $\alpha \in E \setminus K$

$$\rightsquigarrow \exists \sigma \in \lambda(K) \text{ s.t. } \sigma(\alpha) \neq \alpha$$

Take $\beta \in E$ conj. to α over K

extend $\text{id}_{K, \beta} : K(\alpha) \rightarrow K(\beta)$ to an aut. σ

$$(\sigma \in G(E/K) = \lambda(K)) \rightsquigarrow \text{this will do}$$

Prop. (part 3 of Th'm 53.6) $\lambda(E_H) = H$

Suppose $E \supset F$ fin ext.

Proof we will use $[E : E_H] = \{E : E_H\} = |\lambda(E_H)|$
 $\uparrow_{\text{separable}} \quad \uparrow_{\text{split}}$

and: $E = E_H(\alpha)$ for some $\alpha \in E$ (Th'm 51.15; later)

Step 1 $f(X) = \prod_{\sigma \in H} (X - \sigma(\alpha))$ is in $E_H[X]$

$$\tau(f(X)) = \prod_{\sigma \in H} (X - \tau \sigma(\alpha)) = \prod_{\sigma' \in H} (X - \sigma'(\alpha))$$

Step 2 $|\lambda(E_H)| \leq |H| \quad (\rightsquigarrow \lambda(E_H) = H)$

$[E : E_H] = \text{deg. of min. polynom. of } \alpha \text{ over } E_H$

We know $f(\alpha) = 0$, $\text{deg } f(X) = |H|$ from Step 1

Thm 51.15 $E \supset F$ fin. sep. ext. $\leadsto E = F(\alpha)$
for some $\alpha \in E$

Proof for finite fields: take α s.t. $\langle \alpha \rangle = E^\times$
(use $E^\times$ cyclic)

Proof for infinite fields:

Step 1 $F(\beta, \gamma) = F(\alpha)$ for some α

S1-1 Find $a \in F$ s.t. $a(\gamma - \gamma') \neq \beta' - \beta$
whenever $\beta', \gamma' \in F$ are conj. to β, γ
(and diff. from)

$\uparrow$ this is possible by infiniteness assumption

Set $\alpha = \beta + a\gamma$; we want $\gamma \in F(\alpha)$
(then $\beta = \alpha - a\gamma \in F(\alpha)$)

S1-2 $f(X), g(X) \in F[X]$ min polynoms. of β, γ

$\leadsto h(X) = f(\alpha - aX) \in F(\alpha)[X]$

and $g(X)$ has γ as the only common root
in F

$$- h(\gamma) = f(\alpha - a\gamma) = f(\beta) = 0$$

- other roots of $g(X)$ are γ' , but

$$\alpha - a\gamma' \neq \beta' \quad (\text{this means } a(\gamma - \gamma') \neq \beta' - \beta)$$

S1-3 $\gamma \in F(\alpha)$

"greatest common divisor" of $h(X)$ and $g(X)$

in $F(\alpha)[X]$ must be $X - \gamma$ by Step 1-2

Step 2 General case $E = F(\alpha)$

Write $E = F(\beta_1, \dots, \beta_n)$ and use induction

$$F(\beta_1, \beta_2) = F(\alpha_1), \quad F(\alpha_1, \beta_3) = F(\alpha_2), \dots \quad \square$$

Rem. $E \supset F$ Galois (~~if~~ ~~ext~~)

$(E \supset K \supset F \text{ splitting ext}) \Leftrightarrow G(E/K) \subset G(E/F) \text{ normal}$

" $\Rightarrow$ " $\alpha \in K, \sigma \in G(E/F) \leadsto \sigma(\alpha)$ conj. to α , hence $\in K$

$$\leadsto \tau \sigma(\alpha) = \sigma(\alpha) \quad \text{for } \tau \in G(E/K)$$

" $\Leftarrow$ " $\sigma^{-1} \tau \sigma \in G(E/K)$ for $\sigma \in G(E/F)$

would allow reversing above argument

Ex. $E = \mathbb{Q}(\underbrace{\sqrt[3]{2}}_{\alpha}, \underbrace{e^{\frac{2\pi i}{3}} \sqrt[3]{2}}_{\beta}) \supset \mathbb{Q}$ gave $G(E/\mathbb{Q}) \cong S_3$

S_3 has nontriv. subgroups $\langle (1,2) \rangle, \langle (2,3) \rangle, \langle (1,3) \rangle$ and 2 non-normal

and $A_3 = \langle (1,2,3) \rangle$ and 3

corresp. subext. would be $\mathbb{Q}(\gamma)$ ($\gamma = e^{-\frac{2\pi i}{3}} \sqrt[3]{2}$)

$\mathbb{Q}(\alpha), \mathbb{Q}(\beta)$ deg 3, non-splitting ext.

and $\mathbb{Q}(e^{\frac{2\pi i}{3}})$ deg 2, splitting ext

with $G(\mathbb{Q}(e^{\frac{2\pi i}{3}}), \mathbb{Q}) \cong \mathbb{Z}_2$

1. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $F(x)$ defined by the equation

$$F(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $G(x)$ defined by the equation

$$G(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $H(x)$ defined by the equation

$$H(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $I(x)$ defined by the equation

$$I(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $J(x)$ defined by the equation

$$J(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $K(x)$ defined by the equation

$$K(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $L(x)$ defined by the equation

$$L(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $M(x)$ defined by the equation

$$M(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $N(x)$ defined by the equation

$$N(x) = \int_0^x \frac{1}{1+t^2} dt$$

and to the study of the function $O(x)$ defined by the equation

$$O(x) = \int_0^x \frac{1}{1+t^2} dt$$