

§ 48 Automorphisms of fields

How do we make sense of "symmetry of polynomial equation"?

If α, β satisfy the same eq.

$$f(\alpha) = 0, f(\beta) = 0 \quad \text{for } f(X) \text{ polynomial}$$

we should try to relate them.

Def. 48.1 $E \supset F$ field extension

$\alpha, \beta \in E$ algebraic over F (sol. to polynomial eq.)

α and β are conjugate over F if $\exists$ irred.

polynom. $f(X) \in F[X]$ st. $f(\alpha) = 0 = f(\beta)$

Ex. i and $-i$ in $\mathbb{C} \supset \mathbb{R}$ { i.e. min. poly of α
= min. poly. of β }
 $\sqrt{2}$ and $-\sqrt{2}$ in $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$

Thm 48.3 $\alpha, \beta \in E \supset F$ conjugate elements as above
 $F(\alpha), F(\beta) \subset E$ subfields generated by F and α or β .

$\leadsto$ We have an isomorphism $F(\alpha) \xrightarrow{\psi_{\alpha, \beta}} F(\beta)$

given by $\psi_{\alpha, \beta}(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1})$

$$= c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1}$$

for $n = \text{degree of } \alpha \text{ over } F$ (deg. of minimal polynomial.)

Proof $f(X) \in F[X]$ min. poly. of α over F (same for β)

Step 1 $\exists$ isom $F[X]/f(X) \xrightarrow{\psi_\alpha} F(\alpha)$
 image of $g(X) \mapsto g(\alpha)$.

Step 2 $\psi_{\alpha, \beta} = \psi_\beta \circ \psi_\alpha^{-1}$ will do $\square$

Sometimes we have $F(\alpha) = F(\beta)$

Ex. $-\sqrt{2} \in \mathbb{Q}(\sqrt{2}), \sqrt{2} \in \mathbb{Q}(-\sqrt{2}) \leadsto \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$

(But sometimes not: $\alpha = \sqrt[3]{2}$ and $\beta = e^{\frac{2\pi i}{3}} \sqrt[3]{2}$ are both roots of $X^3 - 2$, but $\mathbb{Q}(\alpha) \subset \mathbb{R}$, $\mathbb{Q}(\beta) \not\subset \mathbb{R}$)

Def. • if $E \xrightarrow{\sigma} E$ is an isomorphism from (a field) E to itself, we say σ is an automorphism of E (same for groups, rings, ...)

• if S is a collection of automorphisms of E ,
 $E_S = \{a \in E \mid \sigma(a) = a \text{ for all } \sigma \in S\}$
 is called the fixed field of S

Exercise (Thm 48.11) E_S is a subfield of E
 i.e. $a, b \in E_S \Rightarrow a+b, ab, a^{-1} \in E_S$
 if $a \neq 0$

Ex. $E = \mathbb{C}$, $S = \{\sigma\}$ with $\sigma(z) = \bar{z}$ (usual conj.)
 $\leadsto \mathbb{C}_S = \mathbb{R}$ from $z = \bar{z} \Leftrightarrow z \in \mathbb{R}$

Def. $E \supset F$ field extension

$G(E/F) = \{E \xrightarrow{\sigma} E \mid \text{field autom.}, \sigma(a) = a \text{ for } a \in F\}$

(also $\text{Aut}(E/F)$) is called the automorphism group of E over F

Exercise (Thm 48.15) $G(E/F)$ is a group by compos.

i.e. $\sigma, \tau \in G(E/F) \Rightarrow \sigma \circ \tau, \sigma^{-1}, e = \text{id}_E \in G(E/F)$

Ex. • $G(\mathbb{C}/\mathbb{R}) = \{\text{id}_{\mathbb{C}}, \sigma\}$ with $\sigma(z) = \bar{z}$

If $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ is an aut. s.t. $\varphi(t) = t$ for $t \in \mathbb{R}$

$$\begin{aligned} \varphi(s + ti) &= \varphi(s) + \varphi(ti) = s + \varphi(t)\varphi(i) \\ &= s + t\varphi(i) \end{aligned}$$

we also have $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$

• $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\text{id}, \sigma\}$ with $\sigma(a+b\sqrt{2}) = a-b\sqrt{2}$
 $a, b \in \mathbb{Q}$

- $G(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) = \{ \text{id} \}$

if φ is an autom. of $\mathbb{Q}(\sqrt[3]{2})$,

$\alpha = \varphi(\sqrt[3]{2})$ is a root of $X^3 - 2$

but $\sqrt[3]{2}$ is the only sol. in $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$

$$\mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mid a, b, c \in \mathbb{Q} \}$$

φ must fix $a, b, c, \sqrt[3]{2}, \sqrt[3]{2}^2$

- Suppose $E \supset \mathbb{Z}_p$ is a finite extension

i.e. E is a finite field

Then $\sigma_p(a) = a^p$ is an autom. of E .

In fact $G(E/\mathbb{Z}_p)$ is a cyclic group generated by σ_p ; If $E \cong \mathbb{GF}(p^n)$

we have $\sigma_p^n = \text{id}_E$ in $G(E/\mathbb{Z}_p)$

σ_p is called the Frobenius automorphism

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

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