Field Automorphisms

F field

Def: A field automorphism σ of F is a bijective ring homomorphism $\sigma : F \to F$.

Ex: $id_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}$, $id_{\mathbb{C}}(a+ib) = a+ib$ identity

Ex: $\sigma : \mathbb{C} \to \mathbb{C}$, $\sigma(a+ib) = a-ib$ complex conjugation

$$\begin{aligned}
\sigma((a+ib)(c+id)) &= \sigma(ac-bd+i(bc+ad)) \\
&= ac-bd-i(bc+ad) \\
&= (a-ib)(c-id) \\
&= \sigma(a+ib)\sigma(c+id)
\end{aligned}$$

Ex: Automorphisms of $\mathbb{Q}$?

$$\sigma(1) = 1, \quad \sigma(k) = \sigma(\overbrace{1+\dots+1}^{k\text{-times}})$$
$$= \sigma(1)+\dots+\sigma(1) = k$$

$$\sigma(l^{-1})l = \sigma(l l^{-1}) = \sigma(1) = 1 \Rightarrow \sigma(l^{-1}) = l^{-1}$$

$$\sigma(k/l) = \sigma(k)\sigma(l^{-1}) = k/l. \qquad \therefore \sigma = id_{\mathbb{Q}}$$

Ex: Automorphisms of $\mathbb{Q}(\sqrt{2})$?

$$\mathbb{Q}(\sqrt{2}) = \{a+\sqrt{2}b \mid a,b \in \mathbb{Q}\}$$

$$\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$

By similar argument,

$$\sigma(a) = a \quad \text{for all } a \in \mathbb{Q}$$

and therefore

$$\sigma(a+\sqrt{2}\,b) = a+\sigma(\sqrt{2})b.$$

What can $\sigma(\sqrt{2})$ be?

$$2 = \sigma(2) = \sigma((\sqrt{2})^2)$$
$$= \sigma(\sqrt{2})^2$$

and therefore $\sigma(\sqrt{2}) = \pm\sqrt{2}$.

Two automorphisms:

- $\sigma_+ : a+\sqrt{2}\,b \mapsto a+\sqrt{2}\,b$ identity
- $\sigma_- : a+\sqrt{2}\,b \mapsto a-\sqrt{2}\,b$ conjugation

$\sigma_+ = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$

<u>Def</u>: The set of all automorphisms of F is called the <u>automorphism group of F</u>.

<u>Notation</u>: $\mathrm{Aut}(F) = \{\sigma : F \to F \mid \sigma \text{ is an automorphism}\}$

<u>Prop</u>: $\mathrm{Aut}(F)$ is a group with binary operation defined by composition

Def: An element $\alpha \in F$ is *fixed* by $\sigma \in \mathrm{Aut}(F)$ if $\sigma(\alpha) = \alpha$. A subset $S \subseteq F$ is fixed by σ if each element of S is fixed by σ.

Notation: $F^{\sigma} = \{ \alpha \in F \mid \alpha \text{ fixed by } \sigma \}$
$= \{ \alpha \in F \mid \sigma(\alpha) = \alpha \}$

Ex: $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{ id, \ \sigma : a + \sqrt{2}b \mapsto a - \sqrt{2}b \}$

$$\mathbb{Q}(\sqrt{2})^{id} = \mathbb{Q}(\sqrt{2}), \qquad \mathbb{Q}(\sqrt{2})^{\sigma} = \mathbb{Q}$$

Theorem: Let $H \subseteq \mathrm{Aut}(F)$ and let

$$F^H = \{ \alpha \in F \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H \}$$

Then F^H is a subfield of F and

Likewise, given a field extension E of F, we can consider the automorphisms of E which fix F.

$$\mathrm{Aut}_F(E) = \{ \sigma \in \mathrm{Aut}(E) \mid \sigma \text{ fixes } F \}$$

Theorem: Let $F \subseteq E$ be a field extension. Then $\mathrm{Aut}_F(E)$ is a subgroup of $\mathrm{Aut}(E)$.

Def: Two elements $\alpha, \beta \in E$ are *conjugate over F* if $\mathrm{irr}(\alpha, F) = \mathrm{irr}(\beta, F)$

Theorem: If α, β are conjugate over F then the map

$$\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$$

defined by

$$\psi_{\alpha,\beta}(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{d-1}\alpha^{d-1}) = a_0 + a_1\beta + a_2\beta^2 + \dots + a_{d-1}\beta^{d-1}$$

is an isomorphism of fields

Def: $\psi_{\alpha,\beta}$ is called the <u>conjugation isomorphism</u> of α, β.

<u>Ex</u>: Let $\zeta_n = \exp(2\pi i/n)$. The elements

$$\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1} \qquad (p\text{-prime})$$

all have the same minimal polynomial $1 + x + \dots + x^{p-1}$ and therefore are all conjugate. Also

$$\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p^2) = \dots = \mathbb{Q}(\zeta_p^{p-1})$$

so we have automorphisms

$$\psi_{\zeta^j, \zeta^k} \in \mathrm{Aut}(\mathbb{Q}(\zeta_p)) \qquad \forall\, j,k.$$