1.6 Lecture 6. Möbuis transformations and algebraic number fields

1.6.1 Möbuis transformations

The ring $\mathbb{C}[\epsilon]$ of polynomials in a variable ϵ with coefficients in $\mathbb{C}$ has field of fractions

$$\mathbb{C}(\epsilon) = \left\{ \frac{f(\epsilon)}{g(\epsilon)} \mid f(\epsilon), g(\epsilon) \in \mathbb{C}(\epsilon) \text{ with } g(\epsilon) \right\} \qquad \text{with} \qquad \frac{a(\epsilon)}{b(\epsilon)} = \frac{c(\epsilon)}{d(\epsilon)} \quad \text{if} \quad a(\epsilon)d(\epsilon) = b(\epsilon)c(\epsilon),$$

The group of 2×2 invertible matrices with entries from $\mathbb{C}$ is

$$GL_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{C}) \mid ad - bc \neq 0 \right\}.$$

Proposition 1.13. *The map given by*

$$\begin{matrix} GL_2(\mathbb{C}) & \longrightarrow & \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(\epsilon)) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \sigma_{\substack{ab \\ cd}} \end{matrix} \qquad \textit{where} \qquad \begin{matrix} \sigma_{\substack{ab \\ cd}} : \mathbb{C}(\epsilon) & \longrightarrow & \mathbb{C}(\epsilon) \\ \frac{f(\epsilon)}{g(\epsilon)} & \longmapsto & \frac{f\left(\frac{a\epsilon+b}{c\epsilon+d}\right)}{g\left(\frac{a\epsilon+b}{c\epsilon+d}\right)} \end{matrix}$$

is a group homomorphism.

1.6.2 Examples of algebraic number fields

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$.

- An **algebraic number** is an element of $\overline{Q}$.
- An **algebraic number field** is a finite extension of $\mathbb{Q}$.

Let $f(x) \in \mathbb{Q}(x)$ and let where $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{Q}}$ are the roots of $f(x)$ so that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_k), \qquad \text{in } \overline{\mathbb{Q}}[x].$$

- The **discriminant of** $f(x)$ is D^2, where

$$D = \prod_{1 \le i < j \le k} (\alpha_i - \alpha_k),$$

Let $\mathbb{K}$ be the splitting field of $f(x) \in \mathbb{Q}[x]$. If $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$ then σ is a permutation of the roots of $f(x)$ and

$$\sigma \cdot D = (-1)^{\ell(\sigma)} D \qquad \text{so that} \qquad \sigma D^2 = D^2.$$

Thus D^2 is fixed by $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$ and $D^2 \in \mathbb{Q}$.

- If $D \notin \mathbb{Q}$ then the minimal polynomial of $x^2 - D^2$ is and $\mathbb{Q}(D)$ is a degree two extension of $\mathbb{Q}$.
- If $D \in \mathbb{Q}$ then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K}) \subseteq A_n$, where A_n is the alternating group.

Example 1. If $f(x) = x^2 + bx + c$ is an irreducible polynoimal in $\mathbb{Q}[x]$ and

$$f(x) = x^2 + bx + c = (x - \alpha_1)(x - \alpha_2) \in \overline{\mathbb{Q}}[x] \qquad \text{then} \qquad \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$$

since $\alpha_1 = b - \alpha_2$. If $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha_1))$ is the element given by

$$\sigma(\alpha_1) = \alpha_2, \qquad \text{then} \qquad \sigma(\alpha_2) = \alpha_1,$$

since $\alpha_2 + \sigma\alpha_2 = \sigma(\alpha_1 + \alpha_2) = \sigma(b) = b = \alpha_1 + \alpha_2$. So

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha_1)) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z} = S_2.$$

The discriminant

$$D^2 = b^2 - 4c \in \mathbb{Q} \qquad \text{and} \qquad D = \sqrt{b^2 - 4c} \qquad \text{and} \qquad D \in Q(\alpha_1).$$

So $\mathbb{Q}(\alpha_1) = \mathbb{Q}(D)$ and $\sigma D = -D$.

Example 2.. Let $f(x) = x^3 + a_2x^2 + a_2x + a_0$. Change variable $x = y - \frac{1}{3}a_2$. Then

$$f(x) = y^3 - a_2y^2 + \frac{3ya_2^2}{9} - \frac{a_2^3}{27} + a_2y^2 - \frac{2a_2}{3}y + \frac{a_2^3}{9} + a_1y - \frac{a_1a_2}{3} + a_0.$$

So assume that $f(x) = x^3 + bx + c$ and let $\mathbb{K}$ be the splitting field of $f(x)$. If $f(x)$ is separable and irreducible then

$$D^2 = -4b^3 - 27c^2 \qquad \text{and} \qquad \mathrm{Aut}_{\mathbb{Q}}(\mathbb{K}) = \begin{cases} S_3, & \text{if } D \notin \mathbb{Q}, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } D \in \mathbb{Q}. \end{cases}$$

If $f(x) = x^3 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ then

$$\begin{aligned} -c &= e_3 = \alpha_1\alpha_2\alpha_3 = -c, \\ b &= e_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \\ 0 &= e_1 = \alpha_1 + \alpha_2 + \alpha_3, \end{aligned}$$

and the Hasse diagrams of the posets in the Galois correspondence are

$$\begin{array}{ccccc} & & \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) & & \\ \mathbb{Q}(\alpha_1) & \mathbb{Q}(\alpha_2) & \mathbb{Q}(\alpha_3) & & \\ & & & \mathbb{Q}(D) & \\ & \mathbb{Q} & & & \end{array} \qquad \begin{array}{cccc} & \{1\} & & \\ \{1, s_{12}\} & \{1, s_{13}\} & \{1, s_{23}\} & \\ & & & A_3 \\ & S_3 & & \end{array}$$

A concrete example is $f(x) = x^3 - 2$ which has roots $2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2$, where $\omega = e^{2\pi i/3}$ is a primitive cube root of unity and

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K}) = S_3 \qquad \text{and} \qquad D = \sqrt{-27 \cdot 4} = 6\sqrt{3}\, i.$$

Examples of the two cases are

$$\begin{aligned} f(x) &= x^3 - 3x + 1, \qquad \text{which has } D = \sqrt{81} = 9, \quad \text{and} \\ f(x) &= x^3 + 3x + 1, \qquad \text{which has } D = \sqrt{-135} = 3\sqrt{15}i. \end{aligned}$$

Example 4.. Let $f(x) = x^4 + 1$ which has roots $\omega, \omega^3, \omega^5, \omega^7$, where $\omega = e^{2\pi i/8}$. Let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{Q}$. Then

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \text{the Klein four group.}$$

Let $a, b \in \mathbb{Q}$ and let $\mathbb{K} = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, which is the splitting field of

$$f(x) = (x^2 - a)(x^2 - b) = x^4 - (a+b)x^2 + ab.$$

Then

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{a}, \sqrt{b})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

generated by $\sigma \colon \mathbb{K} \to \mathbb{K}$ and $\tau \colon \mathbb{K} \to \mathbb{K}$ where

$$\begin{array}{l} \sigma(\sqrt{a}) = -\sqrt{a}, \\ \sigma(\sqrt{b}) = \sqrt{b}, \end{array} \qquad \text{and} \qquad \begin{array}{l} \tau(\sqrt{a}) = \sqrt{a}, \\ \tau(\sqrt{b}) = -\sqrt{b}, \end{array}$$

The Hasse diagrams of the posets in the Galois correspondence are

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt{a}, \sqrt{b}) & \\ \mathbb{Q}(\sqrt{b}) & \mathbb{Q}(\sqrt{a}) & \mathbb{Q}(\sqrt{ab}) \\ & \mathbb{Q} & \end{array} \qquad \text{and} \qquad \begin{array}{ccc} & \{1\} & \\ \{1, \sigma\tau\} & \{1, \sigma\} & \{1, \tau\} \\ & \{1, \sigma, \tau, \sigma\tau\} & \end{array}$$

Here, $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$ since $(\sqrt{a} + \sqrt{b})^2 = a + 2\sqrt{a}\sqrt{b} + b \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$ and so $(\sqrt{ab})(\sqrt{a} + \sqrt{b}) = (a\sqrt{b} + b\sqrt{a}) \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. So $(b-a)\sqrt{a} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

Example 5. Let $f(x) = x^n - 1$. The polynomial $f(x)$ has roots $1, \omega, \omega^1, \ldots, \omega^{n-1}$, where $\omega = e^{2\pi i/n}$. Let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{Q}$. Then

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong (\mathbb{Z}/n\mathbb{Z})^\times \qquad \text{and} \qquad \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\times) = \phi(n),$$

where $\phi(n)$ is Euler's phi function.

Example 6. Assume $\mathbb{F}$ contains a primitive nth root of unity and let $\mathbb{K}$ be a finite Galois extension of $\mathbb{F}$. Then

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \cong \mathbb{Z}/n\mathbb{Z} \qquad \text{if and only if} \qquad \begin{array}{c} \text{there exists } b \in \mathbb{F} \text{ such that} \\ x^n - b \in \mathbb{F}[x] \text{ is irreducible and} \\ \mathbb{K} \text{ is the splitting field of } x^n - b \end{array}$$

Example 7. Assume $\mathbb{F} = \mathbb{E}(x_1, \ldots, x_n)$ and $\mathbb{K} = \mathbb{E}(e_1, \ldots, e_n)$, where $e_1, \ldots, e_n$ are the elementary symmetric functions in $x_1, \ldots, x_n$. Then

$$\mathbb{K} \text{ is the splitting field of} \qquad f(x) = (x - x_1)(x - x_2) \cdots (x - x_n) \in \mathbb{F}[x],$$

and

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \cong S_n.$$