(5) The Differential Galois Group

Goal: Understand the "structure" of a PV-field, in particular: identify (interesting) subfields.

Recall: algebraic Galois theory

Given a sqf $p \in K[x]$.

Consider the splitting field E of p over K.

Ex: $p = (x^2-2)(x^2-6) \in \mathbb{Q}[x]$

$E = \mathbb{Q}(\sqrt{2}, \sqrt{6})$
$= \mathbb{Q}[x_1, x_2, x_3, x_4] / \langle x_1^2 - 2,\ x_1 + x_2,\ x_3^2 - 6,\ x_3 + x_4 \rangle$.

Let $\sigma : E \to E$ be a field automorphism which keeps every element of K fixed.

Then σ is a permutation of the roots of p which preserves the algebraic relations among them.

e.g. $\sigma : x_1 \mapsto x_2,\ x_2 \mapsto x_1,\ x_3 \mapsto x_3,\ x_4 \mapsto x_4$ ✓

$\sigma : x_1 \mapsto x_3$ not OK because $x_1^2 - 2 = 0$ while $x_3^2 - 2 \neq 0$.

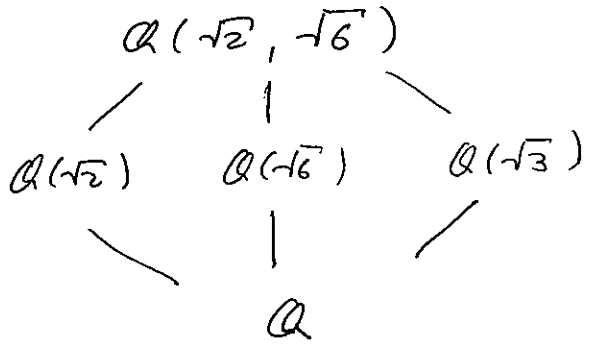
The group $G \subseteq S_n$ of all these automorphisms is called the Galois group of E over K, $\mathrm{Gal}(E, K) := G$.

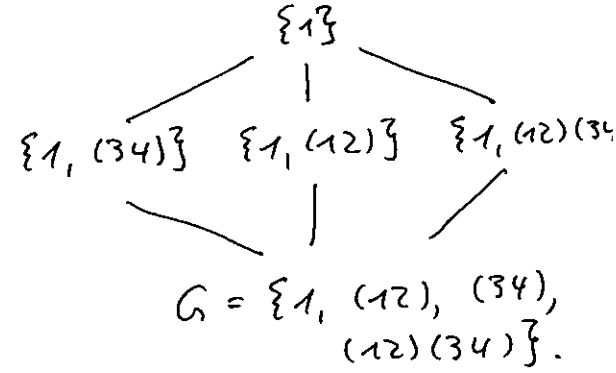
$\mathrm{Gal}(E, \mathbb{Q})$
$= \{1, (12), (34), (12)(34)\} \subseteq S_4$

For each subgroup H of $G := \mathrm{Gal}(E, K)$, define

$$E^H := \{ e \in E \mid \forall h \in H : he = e \}.$$

Then the map $H \mapsto E^H$ is a bijection between the subgroups of G and the subfields of E containing K.





We have:

(1) $H = \mathrm{Gal}(E, E^H)$

(2) $H_1 \subseteq H_2 \iff E^{H_1} \supseteq E^{H_2}$

Key feature:

The roots of p can be expressed "in closed form"

$\iff$ E is a tower of radical extensions

(i.e. $E = K(\sqrt[a]{\square})(\sqrt[b]{\square}) \dots (\sqrt[c]{\square})$)

$\iff$ $\mathrm{Gal}(E, K)$ is a solvable group

(i.e. $\exists$ $H_1, \dots, H_n$ subgroups of $G = \mathrm{Gal}(E, K)$

with $\{1\} = H_1 \lhd H_2 \lhd \dots \lhd H_n = G$

and H_{i+1} / H_i is abelian for each i)

$\forall a \in H_i \, \forall b \in H_{i+1} : a^{-1} b a \in H_{i+1}$

Recall also: If K is a differential field and $A \in K^{n \times n}$, then the PV-field of KA over K is defined (up to isomorphism) as

$$E = \mathrm{Quot}(R/m)$$

where $R = K[y_{11} \cdots y_{1n} \; \vdots \; \ddots \; \vdots \; y_{n1} \cdots y_{nn}, \frac{1}{\det(\|y_{ij}\|)}]$

is made a differential ring by setting

$$\begin{pmatrix} y'_{11} & \cdots & y'_{1n} \\ \vdots & \ddots & \vdots \\ y'_{n1} & \cdots & y'_{nn} \end{pmatrix} := A \cdot \begin{pmatrix} y_{11} & \cdots & y_{1n} \\ \vdots & \ddots & \vdots \\ y_{n1} & \cdots & y_{nn} \end{pmatrix}$$

and m is a maximal differential ideal of R.

Recall finally: $\sigma : K \to K$ is a differential homomorphism [isomorphism] if σ is a ring homomorphism [isomorphism] with $D \circ \sigma = \sigma \circ D$.

Def: Let E be the PV-field for $A \in K^{n\times n}$ over K. Then

$$Gal(E,K) := \{ \sigma : E \to E \text{ diff iso} \mid \sigma|_K = id \}$$

is called the differential Galois group of E over K.

$\sigma \in Gal(E,K)$ is uniquely determined by its action on the generators y_{ij}.

Furthermore, it must map fundamental matrices to fundamental matrices because

$$Y' = AY \iff \begin{array}{ccc} \sigma(Y') & = & \sigma(AY) \\ \| & & \| \\ \sigma(Y)' & & \sigma(A)\,\sigma(Y) \\ & & \| \\ & & A \end{array}.$$

Since any two fundamental systems for A in E are related by a matrix $M \in GL_n(C)$, it follows that

$$\boxed{Gal(E,K) \text{ is a subgroup of } GL_n(C)}$$

More precisely, if $E = \mathrm{Quot}(R/m)$, then $\mathrm{Gal}(E,K)$ consists precisely of those $M \in GL_n(C)$ [or rather: the corresponding isomorphisms] for which $M \cdot m \subseteq m$.

Ex: $K = \mathbb{Q}(x)$, $D = \frac{d}{dx}$.

$A = \begin{pmatrix} 0 & 1 \\ \frac{1-x}{x} & \frac{2x-1}{x} \end{pmatrix}$, the companion matrix of

$$x y'' - (2x-1) y' - (1-x) y = 0.$$

Direct calculation confirms that

$$Y = \begin{pmatrix} e^x & e^x \log x \\ e^x & e^x \log x + \frac{1}{x} e^x \end{pmatrix}$$

is a fundamental matrix. ($Y' = AY$, $\det Y = \frac{1}{x}(e^x)^2 \neq 0$)

Let $E = \mathrm{Quot}(K[y_{11}, y_{12}, y_{21}, y_{22}, \frac{1}{\det(y_{ij})}] / m)$

with $m = \langle y_{11} - y_{21},\ y_{22} - y_{12} - \frac{1}{x} y_{21},$ ~~$\ldots$~~ $\rangle$.

(so $y_{11} \hat{=} e^x$ $\quad y_{12} \hat{=} e^x \log x$

$y_{21} \hat{=} e^x$ $\quad y_{22} \hat{=} e^x \log x + \frac{1}{x} e^x$)

Then E is the PV-field of A over K.

Suppose $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gal(\bar{E}, K) \leq GL_2(\mathbb{Q})$.

$$\bar{Y} = YM = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a y_{11} + c y_{12} & b y_{11} + d y_{12} \\ a y_{21} + c y_{22} & b y_{21} + d y_{22} \end{pmatrix}$$

$$\bar{y}_{11} - \bar{y}_{21}$$

$$= (a y_{11} + c y_{12}) - (a y_{21} + c y_{22})$$

$$= a y_{21} + c y_{12} - a y_{21} - c\left(y_{12} + \tfrac{1}{x} y_{21}\right)$$

$$= -c \tfrac{1}{x} y_{21} \overset{!}{=} 0 \Rightarrow \boxed{c = 0}$$

$$\bar{y}_{22} - \bar{y}_{12} - \tfrac{1}{x}\bar{y}_{21}$$

$$= (b y_{21} + d y_{22}) - (b y_{11} + d y_{12}) - \tfrac{1}{x}(a y_{21} + c y_{22})$$

$$= b y_{21} + d\left(y_{12} + \tfrac{1}{x} y_{21}\right) - b y_{21} - d y_{12} - \tfrac{1}{x} a y_{21}$$

$$= (d - a) \tfrac{1}{x} y_{21} \overset{!}{=} 0 \Rightarrow \boxed{a = d}$$

$$\Rightarrow Gal(\bar{E}, K) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^\times,\ b \in \mathbb{Q} \right\}. \quad \square$$

In general, $Gal(\bar{E}, K)$ is always an algebraic group, i.e. there exists an ideal $\mathfrak{R} \subseteq \mathbb{C}[x_{11} \dots x_{nn}, z]$ such that

$$Gal(\bar{E}, K) = \left\{ (m_{ij})_{i,j=1}^{n} \in GL_n(\mathbb{C}) \;\middle|\; \forall p \in \mathfrak{R}: p\left(m_{11} \dots m_{nn}, \frac{1}{\det M}\right) = 0 \right\}.$$

Ex: For $G = \{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^\times, b \in \mathbb{Q} \}$ we can take $\theta_2 = \langle x_{11}^2 z - 1,\ x_{11} - x_{22},\ x_{21} \rangle$.

Thm: Let E be a PV-field over K, $C = \mathrm{Const}\, K = \bar{C}$. $G = \mathrm{Gal}(E,K) \subseteq GL_n(C)$. For an algebraic subgroup H of G define

$$E^H := \{ e \in E \mid \forall h \in H : he = e \}.$$

Then the map $H \mapsto E^H$ is a bijection between the algebraic subgroups of G and the differential subfields of $\bar{E}$ containing K. We have:

(1) $H = \mathrm{Gal}(\bar{E}, E^H)$

(2) $H_1 \subseteq H_2 \iff E^{H_1} \supseteq E^{H_2}$.

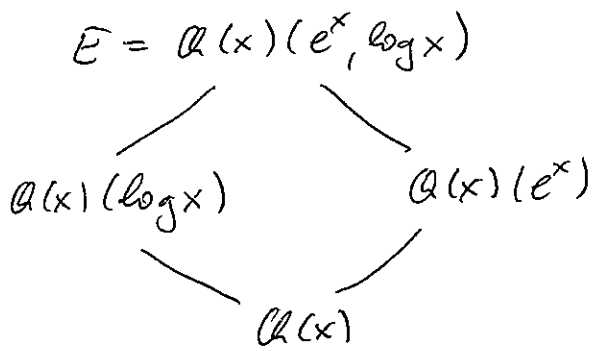
Ex: $G = \{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^\times, b \in \mathbb{Q} \}$ has two non-trivial subgroups:

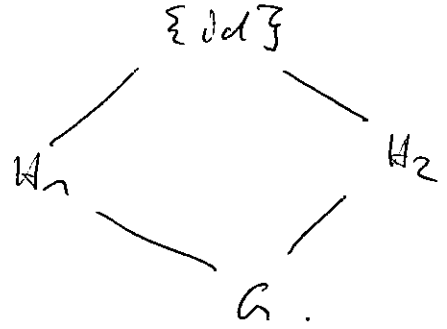
$$H_1 = \{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^\times \} \quad \text{and} \quad H_2 = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Q} \}$$

They correspond to the fields

$$E^{H_1} = \mathbb{Q}(x)(\log x) \quad \text{and} \quad E^{H_2} = \mathbb{Q}(x)(e^x)$$

respectively.





$(e^x \mapsto a \cdot e^x, \quad \log x \mapsto \log x + b)$ □

The ideal $\mathfrak{R}$ of relations among the entries of $M \in \mathrm{Gal}(E, K)$ can always be assumed to be radical (i.e. $p^m \in \mathfrak{R} \Rightarrow p \in \mathfrak{R}$), but it may not be prime (i.e. $pq \in \mathfrak{R} \not\Rightarrow p, q \in \mathfrak{R}$). If it is not prime, consider the prime decomposition

$$\mathfrak{R} = \mathfrak{P}_1 \cap \dots \cap \mathfrak{P}_m$$

of $\mathfrak{R}$. Then precisely one $\mathfrak{P}_i$ is such that $p(1,0\dots0, 0,1,0\dots0, \dots, 0\dots0,1,1) = 0$ for all $p \in \mathfrak{P}_i$. Then

$$G^0 := \left\{ \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \dots & m_{nn} \end{pmatrix} \;\middle|\; \forall\, p \in \mathfrak{P}_i : p\left(m_{11}, \dots, m_{nn}, \frac{1}{\det}\right) = 0 \right\}$$

is a subgroup of G, called the identity component.

Key feature:

The solutions of an ODE have a "closed form"

$\Leftarrow$) E is a tower of Liouvillean extensions

(i.e. $E = K(y_1 \dots y_m)$ st each y_i is alg or exp or log over $K(y_1 \dots y_{i-1})$)

$\Rightarrow$) $Gal(E,K)^\circ$ is a solvable group

(i.e. $\exists$ $H_1 \dots H_n$ algebraic subgroups of G with $\{id\} = H_1 \lhd H_2 \lhd \dots \lhd H_n = G$ and H_{i+1}/H_i is abelian for all i)