Lecture 1: Motivation/Overview

1.1: Classical Galois theory

k field, $P(x) \in k[x]$ monic
polynomial of degree n

Roots of $P(x)$ may not all lie in k

Dfn 1.1: A splitting field for $P(x)$
is a field extension L/k, s.t.

(i) $P(x) = \prod_{i=1}^{n} (x - a_i) \in L[x]$

(ii) $L = k(a_1, \dots, a_n)$, i.e. L is gen. by the roots of $P(x)$

Splitting fields always exist and are unique (up to non-canonical isomorphism)

E.g.: $k = \mathbb{Q}$, $P(x) = x^2 - 2$

$L_1 := \mathbb{Q}(\sqrt{2}) \subset \mathbb{C}$

$$L_2 := \mathbb{Q}[x]/(x^2-2)$$

$$\varphi_1 : L_2 \longrightarrow L_1, \quad x \longmapsto \sqrt{2} \qquad , \qquad \varphi_2 : L_2 \longrightarrow L_1, \quad x \longmapsto -\sqrt{2}$$

No canonical isomorphism!

Equivalently: field extensions have nontrivial automorphisms

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$$

$$\mathrm{id}, \ \sqrt{2} \mapsto -\sqrt{2}$$

<u>**Dfn 12**</u>: L/K field extension,

$$\mathrm{Aut}(L/K) := \left\{ \varphi : L \longrightarrow L \ \middle|\ \begin{array}{l} \varphi(a) = a \\ \forall a \in K \end{array} \right\} \quad \text{field endo}$$

L/K splitting field for $P(X)$, then

$\mathrm{Aut}(L/K)$ acts on roots of $P(x)$

Want to study L/K by means of $\mathrm{Aut}(L/K)$.

Problem: $\mathrm{Aut}(L/k)$ might be too small! (could be trivial, even if L/k is not)

Dfn 1.3: L/k is (finite) Galois extension if it is the splitting field of some separable polyn. (automatic if $\mathrm{char}(k)=0$, or if k is finite)

Notation: If L/k is Galois, then we write $\mathrm{Gal}(L/k)$ for $\mathrm{Aut}(L/k)$.

Thm 1.3: Let L/k be a finite Galois extension, with $G=\mathrm{Gal}(L/k)$. The maps

$$M \mapsto \mathrm{Gal}(L/M), \quad H \mapsto L^H$$

fixed field of H

are order-reversing bijections

$$\left\{\begin{matrix}\text{intermediate fields}\\ L\supset M\supset k\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{subgroups}\\ H\subset G\end{matrix}\right\}$$

M/k is Galois if and only if $H \trianglelefteq G$ is normal, and we have

$$\mathrm{Gal}(M/k) \cong G/H$$

<u>Rmk 1.4:</u> A version of the theorem holds for infinite Galois extensions.

<u>1.2:</u> Differential Galois theory

Analogue of Galois theory for differential fields:

<u>Dfn 1.5:</u> A <u>differential field</u> is a pair (K, ∂), where K is a field ($\mathrm{char}(K)=0$!) and

$\partial: K \longrightarrow K$ derivation

i.e. an additive map s.t.

$$\partial(ab) = \partial(a)b + a\partial(b)$$

(Leibniz rule)

An <u>extension</u> $(L,\partial_2)/(K,\partial_1)$ of differential field s.t.

(i) L/K field extension

(ii) $\partial_2|_K = \partial_1$

(Usually write $\partial_1 = \partial_2 = \partial$ for such an extension)

<u>Exercise 1</u>: Verify that

$$k := \ker(\partial) \subset K$$

is a subfield of K.

(K,∂) differential field.

<u>Dfn 1.6.</u>: A <u>linear differential operator</u> $\mathcal{L}$ (of order n) is an element

$$\mathcal{L} = \partial^n + a_1 \partial^{n-1} + \dots + a_n \underbrace{\partial^0}_{= \mathrm{id}} \in k[\partial]$$

Given $\mathcal{L}$, we will denote by

$\mathcal{L}^{-1}(0) \subset k$ set of solutions

to $\mathcal{L}(u) = 0$

Warning: If $(L, \partial)/(k, \partial)$ is an extension, $\mathcal{L} \in k[\partial]$ as above, then $\mathcal{L}^{-1}(0)$ may, depending on context, either be taken inside, or inside L!

Exercise 2: Show that $\mathcal{L}^{-1}(0) \subset k$ is a k-sub vector space.

Prop 1.7: (k, ∂) is differential field, $\mathcal{L}$ linear diff. operator of order n, then

$$\dim_k \mathcal{L}^{-1}(0) \le n$$

What should be the analogue of a splitting field?

<u>Dfn 1.8</u>: A Picard–Vessiot extension $(L,\partial)/(K,\partial)$ for $\mathcal{L}$ is an extension, s.t.:

(i) $\dim_{k_L} \mathcal{L}^{-1}(0) = n = \operatorname{ord}(\mathcal{L})$

where $k_L \subset L$ field of constants

(ii) L is generated as a diff. field extension by $\mathcal{L}^{-1}(0)$

(iii) $k_L = k$

<u>Exmp 1.9</u>: $K = \mathbb{C}((x))$ formal Laurent series, $\partial = \frac{d}{dx}$

- $k = \mathbb{C}$ field of constants
- $\mathcal{L} = \partial - \mathrm{id}$

Let $k(Y)$ be rational functions in a new variable Y

$\partial(Y) = Y$

$k(Y)/k$ satisfies (i), (ii) above but <u>not</u> (iii)

<u>Exercise 3</u>: Show that field of constants of $k(Y)/k$ is

$\mathbb{C}(Ye^{-x}) \subset k(Y)$

Issue: $\partial(a) = a$ already had a solution in k, e^x

$\Rightarrow$ Want to keep constants under control!

<u>Exmp 1.10</u>: Differential fields in char. p are not well-behaved.

$(\mathbb{F}_p, \partial)$, $\partial = 0$

$\mathcal{L} = \partial$.

$\mathbb{F}_p(Y)/\mathbb{F}_p$, $\partial(Y) = 1$

not a Picard-Vessiot extension

for $\mathcal{L}$!

Constants of $(\mathbb{F}_p(Y), \partial)$ contain

$\mathbb{F}_p(Y^p)$ .... Problem

$\rightsquigarrow$ stick with $\mathrm{char}(k) = 0$:)