"Field theory"

- algebraic extension fields, transcendental ext^n field
  algebraic element.
  separable / purely inseparable element / extension

$$\begin{tikzcd} & E \arrow[d, dash] \\ & F \\ k \arrow[uur, dash] & \end{tikzcd}$$

$\leftarrow$ ext^n fields i.e. $E \supseteq k$

k : base field

- Galois correspondence

(1) Finite Galois ext^n $\qquad [E : k] = n < \infty$

$$\underset{\text{dim}_k(E)}{\overset{\|}{}}$$

$$\begin{tikzcd} E \arrow[d, dash] \\ k \end{tikzcd}$$

Assume E/k is a Galois ext

$\Longleftrightarrow$ E is separable

E/k is normal [and E is the smallest field containing all roots of a suitable polynomial $f(x) \in k[x]$

$\Longleftrightarrow$ There are only a finite number of fields between E and k

Theorem 1 (finite Galois correspondence) E/k finite Galois

$$\begin{tikzcd} E \arrow[d, dash] \arrow[d, no head, bend right=60, "H"'] & \{1\} \arrow[d, dash] \\ F \arrow[d, dash] & H \arrow[d, dash] \\ k & G \end{tikzcd}$$

Let $G = \mathrm{Gal}(E/k) = \mathrm{Aut}_{\substack{\text{ring} \\ k\text{-linear}}}(E)$ = a finite group

$N \trianglelefteq G \Rightarrow$
$\mathrm{Gal}(E^N/k) \cong G/N$

1) There is an order reversing (by inclusions) bijection

$$F \longmapsto \mathrm{Gal}(E/F)$$

$$\left\{ \begin{matrix} \text{sub-extension fields} \\ F/k \subseteq E/k \end{matrix} \right\} \begin{matrix} \longrightarrow \\ \longleftarrow \end{matrix} \left\{ \begin{matrix} H \leq G = \mathrm{Gal}(E/k) \\ \text{subgroups} \end{matrix} \right\}$$

$$E^H = \left\{ x \in E \;\middle|\; \begin{matrix} \sigma(x) = x \\ \forall \sigma \in H \end{matrix} \right\} \longleftarrow\!\!\!\shortmid \quad H$$

2)

$$\left\{ \begin{matrix} \text{subext}^n \ F/k \\ \text{with } F/k \ \underline{\text{Galois}} \end{matrix} \right\} \begin{matrix} \longrightarrow \\ \longleftarrow \end{matrix} \left\{ \begin{matrix} \text{normal} \\ \text{subgroup } N \trianglelefteq G \end{matrix} \right\}$$

If <u>so</u>, have a natural isom

$$\mathrm{Gal}(F/k) \xrightarrow{\ \sim\ } G/N$$

Thm 2

$$\begin{tikzcd} E \arrow[d, dash] \\ k \end{tikzcd}$$

E : a (possible infinite) Galois ext^{n} field of k:

$$E = \bigcup_{i \in I} E_i$$

increasing union of finite Galois ext^{n} of k

I : a poset

$$\mathrm{Gal}(E/k) =: G$$

$$= \varprojlim_{I} \mathrm{Gal}(E_i/k)$$

$=$ a profinite group;

⇝ G is a locally compact totally disconnected topological group

The "same statement" hold

$$\left\{ \begin{array}{l} \text{sub-ext}^{n} \text{ fields } F/k \\ \text{of } E/k \end{array} \right\} \overset{\text{bijection}}{\rightleftarrows} \left\{ \begin{array}{l} \underline{\text{closed}} \text{ subgroups} \\ \text{of } G = \mathrm{Gal}(E/k) \end{array} \right\}$$

F is Galois $\Longleftrightarrow$ $N = \mathrm{Gal}(E/F)$ is normal

$$\mathrm{Gal}(F/k) \cong G/N$$

Better (?) picture:

$$\begin{tikzcd} E = k^{sep} = \text{a separable closure of } k \arrow[d, dash] \\ k \end{tikzcd}$$

$G = Gal(E/k)$

Reformulate Thm 2

$$\left\{ \begin{array}{l} \text{separable alg.} \\ \text{ext}^n \text{ of } k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{sets } \overset{\text{with discrete top.}}{S} \\ \text{with a transitive} \\ \text{continuous action} \\ \text{by } G \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{finite separable} \\ \text{alg. ext}^n \text{ of } k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{finite sets } S \\ \text{with transitive} \\ \text{continuous action by } G \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{finite dim}^l \text{ commutative} \\ \text{separable } k\text{-algebras} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{finite sets } S \\ \text{with continuous} \\ G\text{-action} \end{array} \right\}$$

Basic example

start with a separable polynomial $f(x) \in k[x]$ (all roots of $f(x)$ are distinct) adjoin all roots of $f(x)$ in a separable closure k^{sep} of k.

$\rightsquigarrow$ get a subfield $\underset{\substack{\cup \\ k}}{F} \subset k^{sep}$

$\underline{\underline{*}}$ $G = \mathrm{Gal}(k^{sep}/k)$ operates on the set $S := \{\lambda \in k^{sep} \mid f(\lambda) = 0\}$

$f(x)$ is irreducible over k

$\iff$ $\mathrm{Gal}(k^{sep}/k)$ operates transitively on S.

How to $\underline{\text{get}}$ abelian ext^n of k ?

↑ construct

Will show some examples

- Kummer theory
- Artin-Schreier theory

k : a number field

understand

an alg. closure

$$\mathrm{Gal}(\bar{k}/k)^{ab} = \mathrm{Gal}\left(\begin{array}{l}\text{the maximal abelian} \\ \text{subextension field of } k\end{array}\right)$$

Ans. Given by class field theory

Very Weak structural result on finitely generated extension fields.

<u>Computing</u> Galois groups $\mathrm{Gal}(\overset{\text{given } f(x)}{E}/k)$

is not easy

e.g. $\underset{\text{monic}}{f(x)} \in \mathbb{Q}(x)$ $\qquad \underset{\text{irred}}{\deg f(x) = 20}$.

computing the Galois group of

$$\mathrm{Gal}\left(\mathbb{Q}(\lambda : f(\lambda)=0)/\mathbb{Q}\right)$$

$$\subseteq \text{ a subgroup of } S_{20}$$

Basics

$$\begin{tikzcd} E \ni \alpha \arrow[d, dash, "\text{an extension field}"] \\ k \end{tikzcd}$$

1) An element $\alpha \in E$ is algebraic over k

$\underset{\text{def}}{\Longleftrightarrow}$ $\exists$ a non-zero polynomial $f(x) \in k[X]$ s.t. $f(\alpha)=0$

$\underset{\text{easy}}{\Longleftrightarrow}$ $k(\alpha) :=$ the smallest subfield of E containing k and α is a finite dim v. subspace of E/k

$\left(k(\alpha) = \mathrm{Im}\left(\begin{array}{ccc} k[X] & \longrightarrow & E \\ x & \mapsto & \alpha \end{array} \right) \right)$

Notation $[F : k] = \dim_k (F/k)$

$\nearrow$ a "subext" of E/k

2) If $\alpha \in E/k$ is algebraic over k

then $\{ f(x) \in k[x] \mid f(\alpha) = 0 \}$

$= $ a non-zero ideal of $k[x]$

$= f_{min,\alpha}(x) \cdot k[x]$

$\nearrow$ monic polynomial, uniquely determined by α.

irreducible in $k[x]$

$$\left(\because \; \underset{\text{a field}}{k(\alpha)} = k[\alpha] \xleftarrow{\sim} k[x] / \left(f_{min,\alpha}(x)\right) \right)$$

3) If $\alpha \in E/k$ is not algebraic over k,

then say: α is transcendental over k

and

$$\begin{tikzcd}
k[X] \arrow[r, "ev_\alpha", "\sim"'] \arrow[d, hook] & k[\alpha] \arrow[d, hook] & \subseteq & E \arrow[d, equal] \\
k(X) \arrow[r, "ev_\alpha", "\sim"'] & k(\alpha) & \subseteq & E
\end{tikzcd}$$

4) $E \supseteq F$ a subfield containing k

$$\begin{tikzcd} E \arrow[d, dash] \\ k \end{tikzcd}$$

If F is algebraic$/k$
(*i.e* every element is alg. over k)

and F is finitely generated as an extension field of k

then $[F:k] < \infty$

Conversely: If $[F:k] < \infty$, then F/k is algebraic (*Obvious* *Exer.*)

5) $\underset{\neq 0}{f(x)} \in k[X]$, *irreducible*.

then $\exists$ an ext^n field F/k

and an element $\alpha \in F$

s.t. $f(\alpha) = 0$ *and* $k[X]/f(x)\cdot k[X]$

$$\xrightarrow{\sim} k(\alpha)$$

This easy fact + transfinite induction

$\Updownarrow$

Zorn's Lemma

(existence of algebraic closure)

$\Rightarrow$ (1) $\exists$ Field k, there exists an algebraic extension field E/k such that every non-zero poly $f(x) \in \underset{\in E[x]}{k[x]}$ has a root in E

($\underline{\text{i.e}}$ E/k is algebraically closed)

(2) Suppose E_1 and E_2 are algebraic closures of k. There exists a k-linear ring isomorphism

$$\phi : E_1 \xrightarrow{\sim} E_2$$

(Consider the poset

$$\left\{ (F, \psi) \;\middle|\; \begin{array}{l} F/k \subseteq E/k \text{ is a subext}^n \text{ field} \\ \psi : F/k \to E/k \text{ is a } k\text{-linear ring homom} \end{array} \right\}$$

$\underline{\text{and}}$ apply Zorn's lemma)

$\underline{\text{An example}}$: suppose that $k \subseteq \mathbb{C}$ $\leftarrow$ or any alg. closed field

$\underline{\text{Then}}$ $\left\{ \alpha \in \mathbb{C} \;\middle|\; \begin{array}{l} \alpha \text{ is algebraic} \\ \text{over } k \end{array} \right\}$ is an algebraic closure of k.

6. transcendence degree:

E/k is a field ext^n.

trans. deg (E/k)

$= \text{Card}(I)$

I is a set

$\exists$ a map $\beta : I \longrightarrow E$

s.t. (a)

$$\begin{tikzcd} k[\beta(i_1),\dots,\beta(i_n)] \\ k[Y_1,\dots,Y_n] \arrow[u, "\cong"] \end{tikzcd}$$

$i_1,\dots,i_n$ distinct elements in I

(b) $E/k(\beta(i))_{i\in I}$ is algebraic

and $\{\beta(i)_{i\in I}\}$ is a trans. basis of E/k

is uniquely determined by E/k

Next time

- separable, insep.
- normal ext^n.