Math 491, Friday, April 17 Chapter 23 Galois Theory

Mon- Problem Session (22)
Sage 22
(Project Discussion)

23 ↓

Sun 11:59 PM
written Project

[fields.ipynb]

Galois Theory

Field structure ⟷ group structure
(automorphisms)

roots of polynomials, equations for roots

$x^5+6x^4-8x^3+2x^2+5x+9=0$

Defn / Theorem F field, $\mathrm{Aut}(F)$ is a group.

$$\mathrm{Aut}(F) = \{\sigma \mid \sigma : F \to F \text{ is a field isomorphism}\}$$

"auto" — two operations — 1-1 onto

$\sigma, \tau \in \mathrm{Aut}(F) \Rightarrow \sigma\tau$ is a homomorphism

is 1-1 & onto

$: F \to F$

τ^{-1} exists (1-1, onto)

is homomorphism

1-1 & onto

$: F \to F$

$i : F \to F \quad i(f) = f, \ f \in F$

$\mathrm{Aut}(F) \neq \emptyset$

$\Rightarrow \mathrm{Aut}(F)$ group

Defn / Theorem Field extension E/F

Galois group (of the extension) $= G(E/F)$

$= \{ \sigma \mid \sigma \in \mathrm{Aut}(E),\ \underbrace{\sigma(f) = f \text{ for all } f \in F}_{\text{"fix } F \text{ element-wise"}} \}$ $\quad \sigma|_F = i$

Theorem E/F, $f(x) \in F[x]$

Any $\sigma \in G(E/F)$ defines ("gives rise to") a permutation of the roots of $f(x)$ that lie in E.

Proof Grab a, a root of $f(x)$ in E. Consider $\sigma(f(a))$.

$f(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$

$b_i \in F$

① $\sigma(f(a)) = \sigma(0) = 0$ (isomorphism)

② $\sigma(f(a)) = \sigma(b_m a^m + b_{m-1} a^{m-1} + \cdots + b_1 a^1 + b_0 a^0)$

$= \sigma(b_m)\sigma(a^m) + \sigma(b_{m-1})\sigma(a^{m-1}) + \cdots + \sigma(b_1)\sigma(a^1) + \sigma(b_0)\sigma(a^0)$

(σ operation-preserving)

$$= b_m \sigma(a^m) + b_{m-1}\sigma(a^{m-1}) + \cdots + b_1\sigma(a^1) + b_0\sigma(a^0)$$

$$= b_m (\sigma(a))^m + b_{m-1}(\sigma(a))^{m-1} + \cdots + b_1(\sigma(a))^1 + b_0(\sigma(a))^0$$

$$= f(\sigma(a))$$

σ fixes F element-wise

σ a $\mathbb{Q}$-hom

So ① + ② $\Rightarrow$ $f(\sigma(a)) = 0 \Rightarrow \sigma(a)$ root

Let $R = \{r_1, r_2, \ldots, r_k\}$ be distinct roots of f in E

Then

r_1	$\sigma(r_1)$	$= r_{t_1}$
r_2	$\sigma(r_2)$	$= r_{t_2}$
$\vdots$	$\vdots$	
r_k	$\sigma(r_k)$	$= r_{t_k}$

all different, else σ not 1-1, all roots, so R

$1 \to t_1$, $2 \to t_2$, $\ldots$, $k \to t_k$

bijection $R \to R$

permutation

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & k \\ t_1 & t_2 & t_3 & & t_k \end{pmatrix}$$

Defn E/F, $a, b \in E$, we say a & b are conjugate if a & b have equal minimal polynomials.

(Specialize to $\mathbb{C}/\mathbb{R}$)

$\mathbb{C}$?