

Math 491, Friday, April 17 Chapter 23 Galois Theory

Mon - Problem Session (22)

Sage 22
(Project Discussion)

23 ↓

Sun 11:59 AM
written project

[fields.ipynb]

Galois Theory

Field structure \longleftrightarrow group structure
(automorphisms)

roots of polynomials, equations for roots

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

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

$\text{Aut}(F) = \{ \sigma \mid \sigma: F \rightarrow F \text{ is a field isomorphism} \}$
↑ "auto" *↑ two operations* *↘ 1-1 onto*

$\sigma, \tau \in \text{Aut}(F) \Rightarrow \sigma\tau$ is a homomorphism
is 1-1 & onto
 $\tau^{-1}: F \rightarrow F$
exists (1-1, onto)
is homomorphism
1-1 & onto
 $i: F \rightarrow F \quad i(f) = f, f \in F$
 $\text{Aut}(F) \neq \emptyset$

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

Defn / Theorem Field Extension E/F

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

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

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 $\sigma(f(a))$.

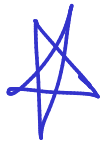
$$f(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

$b_i \in F$

① $\sigma(f(a)) = \underbrace{\sigma(0)}_{\text{isomorphism}} = 0$

②
$$\begin{aligned} \sigma(f(a)) &= \sigma(b_m a^m + b_{m-1} a^{m-1} + \dots + b_1 a^1 + b_0 a^0) \\ &= \sigma(b_m) \sigma(a^m) + \sigma(b_{m-1}) \sigma(a^{m-1}) + \dots + \sigma(b_1) \sigma(a^1) + \sigma(b_0) \sigma(a^0) \end{aligned}$$

σ operation-preserving



$$\begin{aligned}
 &= b_m \sigma(a^m) + b_{m-1} \sigma(a^{m-1}) + \dots + b_1 \sigma(a^1) + b_0 \sigma(a^0) \\
 &= b_m (\sigma(a))^m + b_{m-1} (\sigma(a))^{m-1} + \dots + b_1 (\sigma(a))^1 + b_0 (\sigma(a))^0 \\
 &= f(\sigma(a))
 \end{aligned}$$

σ fixes F element-wise
 σ σ -p

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

Let $R = \{r_1, r_2, \dots, r_k\}$ be k 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	\vdots
r_k	$\sigma(r_k) =$	r_{t_k}

$1 \rightarrow t_1$
$2 \rightarrow t_2$
\vdots
$k \rightarrow t_k$

bijection $R \rightarrow R$

Permutation

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

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

Defn E/F , $a, b \in E$, we say a & b are
conjugate if a & b have equal minimal polynomials. \mathbb{C} ?
(Specialize to \mathbb{C}/\mathbb{R})

