Galois theory: Pull-up the handout for weeks 11-12.

Roots of polynomials —— Field automorphisms

Recall If L/K and $f(x) \in K[x]$
then $Aut(L/K) \circlearrowright$ roots of $f \in L$

$\sigma(\alpha)$ is a root of f if α is.

$\parallel$

Field aut. of L that are the identity in K.

If $\sum a_n \alpha^n = 0$ $a_n \in K$

$$\sigma(\sum a_n \alpha^n) = \sigma(0)$$
$$\sum \sigma(a_n) \sigma(\alpha)^n = 0$$
$$\sum a_n \sigma(\alpha)^n = 0.$$

Observation If $L = K(\alpha_1, \dots, \alpha_n)$
$\sigma \in Aut(L/K)$ is determined by $\sigma(\alpha_1), \dots \sigma(\alpha_n)$.

If α_i are algebraic

m_{α_i} the minimal polynomial of α_i over K.

$\sigma(\alpha_i) \in$ Roots of m_{α_i} in L.

($\Rightarrow Aut(L/K)$ is finite if $[L:K]$ is finite).

Lemma: If L/K is the splitting field of an irreducible polynomial f then
$$|Aut(L/K)| \leq [L:K]$$

w/equality if and only if f is separable.

<u>Idea:</u> Let $\alpha_1, \dots, \alpha_n$ denote the roots.

$L = K(\alpha_1, \dots, \alpha_n)$

$\sigma \in \mathrm{Aut}(L/K)$ is determined by how it permutes these roots.

$$\left(\mathrm{Aut}(L/K) \hookrightarrow \mathrm{Aut}(\text{roots of } f \text{ in } L)\right)$$
$$\cong S_n.$$

To build σ: First, what does it do to α_1?

$\alpha_1 \longrightarrow \alpha_i \quad i = 1, \dots, n.$

$$\begin{array}{ccc} K(\alpha_1) & \longrightarrow & L \\ \cong & & \\ K[x]/f(x) & \longrightarrow & \\ x & \mapsto & \alpha_i, \quad i = 1, \dots, n \end{array}$$

$\leftarrow$ what are the possible maps? (that fix K)

So I get $\sigma_1 : K(\alpha_1) \to L$ s.t. $\sigma_1(\alpha) = i$ for any $i = 1, \dots, n$

$\sigma_2 : K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2) \to L$

Where can I send α_2? (extending σ_1)

$m(x) \leftarrow$ min polynomial of α_2 over $K(\alpha_1)$

$K(\alpha_1)(\alpha_2) \cong K(\alpha_1)[x]/m(x)$

Can send x to any root of

$\sigma_1(m)(x) \in L[x]$

There are $\deg m$ choices

$m(x) \mid f(x)$ $\quad$ $\sigma_1(m)(x) \mid \underset{\substack{\shortparallel \\ f(x),}}{\sigma_1(f)(x)}$

$\Rightarrow$ all roots in L

σ_2 extending σ_1 had m choices

$m = [K(\alpha_2, \alpha_1) : K(\alpha_1)]$

Repeat...

Deduce that $|Aut(L/K)| \underset{<\ \text{otherwise.}}{\overset{}{=}} [L:K]$. if f separable

$\mathbb{F}_p(t^{1/p}) / \mathbb{F}_p(t)$. $Aut(\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)) = \{1\}$

Definition / Theorem: L/K finite is Galois if any of the following equivalent conditions hold.

(1) $[L:K] = |Aut(L/K)|$.

(2) $K = L^{Aut(L/K)}$ $\left(:= \{ \ell \in L \mid \sigma(\ell) = \ell \ \ \forall \sigma \in Aut(L/K) \} \right)$

(3) L/K separable & normal | if $\alpha \in L$ then $m_\alpha(x) \in K[x]$ has $\deg m_\alpha(x)$ distinct roots in L

(4) L/K is a splitting field of a separable polynomial.

(4) $\Rightarrow$ (1) we basically just did

(2) $\Rightarrow$ (3) easy.

Proof if $\alpha \in L$

$$f(x) = \prod_{\beta \in Aut(L/K)\cdot\alpha} (x - \beta)$$ ← this is minimal polynomial

Point: To see this has coefficients in K.

$$\sigma(f) = \prod_{\beta \in Aut(L/K)\cdot\alpha} (x - \sigma(\beta)) \quad \text{for } \sigma \in Aut(L/K)$$

$$= \prod_{\beta \in Aut(L/K)\cdot\alpha} (x - \beta)$$

so all the coefficients are preserved by $Aut(L/K)$ ⟹ they are in K.

(3) ⟹ (4) easy. (Take product of minimal polynomials of a set of generators)

Lemma: If L is a field $G \leq Aut(L)$ a finite subgroup. then $[L : L^G] = |G|$

Proof: Uses independence of characters + descent.

$K \leq L^{Aut(L/K)}$

so $[L:K] = [L : L^{Aut(L/K)}][L^{Aut(L/K)} : K]$

$\overset{\text{By lemma}}{=} |Aut(L/K)| [L^{Aut(L/K)} : K]$

If these are equal then $[L^{Aut(L/K)} : K] = 1$ so $L^{Aut(L/K)} = K$.

Similar argument Shows $|Aut(L/K)| \leq [L:K]$.

(in fact divides it)
always

Lemma shows L/L^G is Galois w/ group G.
$\mathrm{Aut}(L/L^G) = G$.

Note: If L/K is Galois then the roots of minimal polynomial of $\alpha \in L$ are just the Galois orbits of α.

In particular: If $f \in K[x]$ is a separable polynomial and L/K is a splitting field then the irreducible factors of f in $K[x]$ are in bijection with the orbits of $\mathrm{Gal}(L/K)$ $(= \mathrm{Aut}(L/K))$ acting on the roots of f.

Fundamental theorem L/K Galois

Intermediate fields $\leftrightarrow$ Subgroups of $\mathrm{Aut}(L/K)$.

$M \to \mathrm{Fix}(M)$

$L^H \leftarrow H$

$K(\alpha_1, \alpha_2)$ $\quad \alpha_1^2 + 7\alpha_2 + 3\alpha_1\alpha_2 \ldots$