

4/15/07

Recall Let $f(x)$ be an irred poly in $F[x]$. Suppose α, β are roots in a splitting field. Then

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\cong} & F(\beta) \\ \downarrow & & \downarrow \\ F & \xrightarrow{id} & F \end{array}$$

This is "next" choices where to map α .

Key Theorem

Let $f(x) \in F[x]$ w/ splitting field E . Any

$\cong \varphi: F \rightarrow F'$ extends to an $\cong \varphi: E \rightarrow E'$
where E' is a splitting field of $\varphi(f(x))$

Moreover the # of such extensions φ is $\leq [E:F]$
with equality iff $f(x)$ is separable

Proof Induction, use above, etc...

Remark In applications almost always
 $\varphi = id: F \rightarrow F'$, $E = E'$, i.e. we are actually
counting $Aut(E/F)$. However the induction
needs more generality, i.e.

$$\varphi: F(\alpha) \rightarrow F(\beta)$$

COR. Let E/F be a splitting field of $f(x)$. Then

$$|Aut(E/F)| \leq [E:F]$$

w/ equality iff $f(x)$ is separable

Example $f(x) = x^3 - 2 \in \mathbb{Q}$ $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$
 $\omega = e^{2\pi i/3}$

$E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ Degree is 6! Thus

all 6 perms of the roots extend to Auto.

Example $\sigma: \sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega$
 $\sqrt[3]{2}\omega \rightarrow \sqrt[3]{2}\omega^2$
 $\sqrt[3]{2}\omega^2 \rightarrow \sqrt[3]{2}$ plus fix \mathbb{Q}

$\sqrt{-3} = 2\omega + 1 = 2 \cdot \frac{\sqrt[3]{2}\omega}{\sqrt{2}} + 1$

Thus $\sigma(\sqrt{-3}) = 2 \cdot \frac{\sqrt[3]{2}\omega^2}{\sqrt{2}} + 1 = 2\omega + 1 = \sqrt{-3}$

etc. —

$\langle \text{id}, \sigma, \sigma^2 \rangle$ is a subgroup of order 3,
 index is 2. Fixed field is $\mathbb{Q}(\sqrt{-3})$.

Def. Let K/F be a finite extension. Say K is Galois / F ,
 and K/F is a Galois extension if $|\text{Aut}(K/F)| = [K:F]$

In this case $\text{Gal}(K/F) := \text{Aut}(K/F)$ is the Galois group of the extension.

Examples

- 1. Any S.F. of a separable poly is Galois, by prev. cor.
2. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois
3. S.F. of any poly / \mathbb{Q} (just remove mult factors)

ONLY
 Example

Def Let $f(x)$ be separable $/F$ w/ splitting field E .
The Galois group of $f(x)$ is $\text{Gal}(E/F)$.

Examples

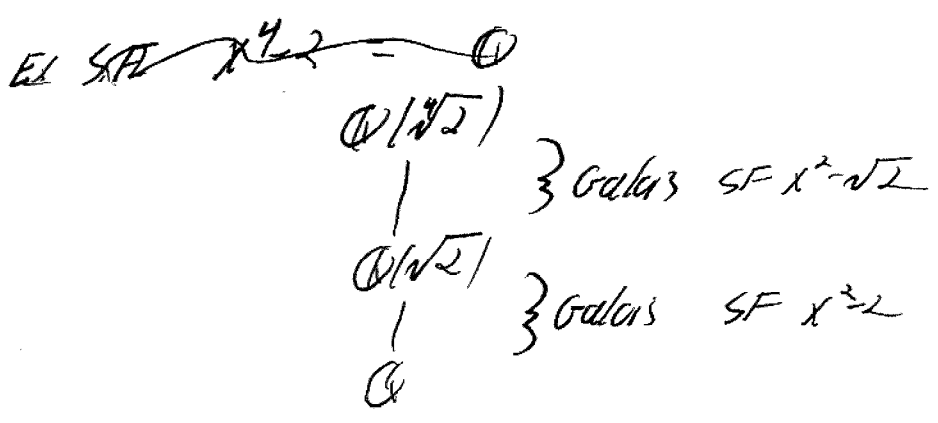
$f(x) = x^2 - 2 / \mathbb{Q} \quad \text{Gal} \cong \mathbb{Z}_2$

$f(x) = (x^2 - 2)(x^2 - 3) \quad \text{Gal} \cong V$

$f(x) \cong x^3 - 2 \quad \text{Gal} \cong S_3$

Prop $\deg f(x) = n \Rightarrow \text{Gal} \leq S_n$

Prop Galois ext of Galois ext not nec Galois



Ex $\mathbb{F}_{p^n} / \mathbb{F}_p$ is Galois, SF of $x^{p^n} - x$ separable

Lemma Galois group of $x^{p^n} - x / \mathbb{F}_p$ is cyclic of order n generated by Frobenius.

EX SPL FIELD \Rightarrow Galois extension.

Base field $\mathbb{F}_2(t)$ poly $x^2 - t = 0$

splitting field is $\mathbb{F}_2(t)(\sqrt{t})$ only root.

Thus $\text{Aut}(\mathbb{F}_2(t)(\sqrt{t})/\mathbb{F}_2(t)) = \text{id}$.

need SF of separable poly

FTOGT

Preliminaries

Def A linear character χ of G is a group homomorphism

$$\chi: G \rightarrow L^\times$$

Ex $\chi(g) = 1 \quad \forall g$ This may be the only such.

Then suppose $\chi_0, \chi_1, \dots, \chi_n$ distinct linear characters Then they are linearly independent.

Proof straight forward.

COR Suppose $\sigma_1, \sigma_2, \dots, \sigma_n$ are distinct embeddings of $K \hookrightarrow L$.

Then they are lin. ind. Thus distinct elements of $\text{Aut } K$ are lin. ind.

Thm Let $G = \{\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_n\} \leq \text{Aut } K$.
 Let $F = K^G$ Then $[K:F] = n = |G|$.

Proof

Suppose $[K:F] < n$, choose basis w_1, w_2, \dots, w_m of K/F .

Consider the system:

$$\sigma_1(w_1)x_1 + \sigma_2(w_1)x_2 + \dots + \sigma_n(w_1)x_n = 0$$

$$\sigma_1(w_m)x_1 + \dots + \sigma_n(w_m)x_n = 0 \quad \text{mess, } n \text{ unknowns}$$

Has nontrivial solution B_1, B_2, \dots, B_n .

Choose $a_1, a_2, \dots, a_m \in F$ arbitrary. Then

~~$$\sigma_1(a_1 w_1) B_1 + \dots + \sigma_n(a_1 w_1) B_n = 0$$~~

$$\sigma_1(a_1 w_1) B_1 + \dots + \sigma_n(a_1 w_1) B_n = 0$$

$$\sigma_1(a_m w_m) B_1 + \dots + \sigma_n(a_m w_m) B_n = 0.$$

Now add!

$$\sigma_1(a_1 w_1 + \dots + a_m w_m) B_1 + \dots + \sigma_n(a_1 w_1 + \dots + a_m w_m) B_n = 0.$$

$\forall a_1, \dots, a_m$.

Thus $\sigma_1, \sigma_2, \dots, \sigma_n$ lin dep. \neq

Thus $n \leq [K:F]$

Other way similar but uses group struct.

COR Let K/F be finite. Then

$$|\text{Aut}(K/F)| \leq [K:F]$$

w/ equality iff $F = K^{\text{Aut}(K/F)}$.

Proof

$$F \subseteq K^{\text{Aut}(K/F)} \subseteq K$$

\uparrow
 $= |\text{Aut}(K/F)|$