Lecture 27: Fixed field of a group

Tuesday, March 6, 2018 2:30 PM

<u>Proposition.</u> Let G be a subgp of $\mathrm{Aut}(E)$. Then

(1) $\mathrm{Fix}(G)$ is a subfield of E.

(2) If $|G|<\infty$, then $[E:\mathrm{Fix}(G)]\le |G|$.

<u>Pf.</u> (1) is easy.

(2) Let $G=\{\sigma_1,\ldots,\sigma_n\}$ and $F:=\mathrm{Fix}(G)$. It is enough to show any $n+1$ elements $\alpha_1,\ldots,\alpha_{n+1}$ of E are F-linearly dependent.

Let $V:=\{(c_1,\ldots,c_{n+1})\in E^{n+1} \mid \sum_{i=1}^{n+1} c_i\,(\sigma_1(\alpha_i),\ldots,\sigma_n(\alpha_i))=0\}$.

Then (1) V is an E-subspace of E^{n+1}; (it is the right kernel of

$$\begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_{n+1}) & \cdots & \sigma_n(\alpha_{n+1}) \end{bmatrix}_{(n+1)\times n} .\ )$$

(2) $V\neq 0$; (any $n+1$ vectors in E^n are E-linearly depend.)

(3) $\sigma\in G$, $(c_1,\ldots,c_{n+1})\in V \overset{?}{\Rightarrow} (\sigma(c_1),\ldots,\sigma(c_{n+1}))\in V$.

$0=\sum c_i\,(\sigma_1(\alpha_i),\ldots,\sigma_n(\alpha_i)) \Rightarrow 0=\sum \sigma(c_i)\left(\sigma\circ\sigma_1(\alpha_i),\ldots,\sigma\circ\sigma_n(\alpha_i)\right)$

Since $(\sigma\circ\sigma_1,\ldots,\sigma\circ\sigma_n)$ is a permutation of $\sigma_1,\ldots,\sigma_n$,

we deduce $0=\sum \sigma(c_i)\,(\sigma_1(\alpha_i),\ldots,\sigma_n(\alpha_i))$. Hence

$(\sigma(c_1), \ldots, \sigma(c_{n+1})) \in V$.

And so by the previous lemma $V^G \neq 0$; this means $\exists (c_1, \ldots, c_{n+1}) \in (F^{n+1} \cap V) \setminus \{0\}$, which implies $c_1\alpha_1 + \cdots + c_{n+1}\alpha_{n+1} = 0$; and α_i's are F-linearly dependent. ■

Theorem. Let G be a finite subgp of $\mathrm{Aut}(E)$, where E is a field. Let $F = \mathrm{Fix}(G)$. Then E/F is a Galois extension,

$[E:F] = |G|$, and $\mathrm{Aut}(E/F) = G$.

Pf. $\forall \alpha \in E$, consider $f(x) := \prod_{\sigma \in G} (x - \sigma(\alpha))$. Then $\forall \sigma \in G$, $\sigma(f) = f$. And so $f(x) \in F[x]$. Therefore $m_{\alpha,F}(x) \mid f(x)$; this implies all other zeros of $m_{\alpha,F}(x)$ are in E. Hence E/F is a normal extension. Therefore $|\mathrm{Aut}(E/F)| \leq [E:F]$.

Clearly $G \subseteq \mathrm{Aut}(E/F)$. Thus

$$|G| \leq |\mathrm{Aut}(E/F)| \leq [E:F] = [E:\mathrm{Fix}(G)] \underset{\text{previous proposition.}}{\leq} |G|$$

Hence (1) $G = \mathrm{Aut}(E/F)$

(2) $|\mathrm{Aut}(E/F)| = [E:F]$, which implies E/F is Galois. ■

Lecture 27: Fundamental theorem of Galois theory

Sunday, March 4, 2018 9:42 PM

Corollary Suppose E/F is a finite Galois extension. Then

$$\mathrm{Fix}(\mathrm{Aut}(E/F)) = F.$$

Pf. Let $F' := \mathrm{Fix}(\mathrm{Aut}(E/F))$. Then $F \subseteq F'$ and $[E:F'] = |\mathrm{Aut}(E/F)| = [E:F]$.

And so $F = F'$. ■

So far we have proved:

Theorem. Suppose E/F is a finite extension. Then the following are equivalent: (1) E is a splitting field of a separable polynomial over F

(2) E/F is a normal and separable extension.

(3) $|\mathrm{Aut}(E/F)| = [E:F]$.

(4) $\mathrm{Fix}(\mathrm{Aut}(E/F)) = F$.

Proposition. Suppose E/F is Galois, and $F \subseteq K \subseteq E$ is a subfield.

Then E/K is Galois.

Pf. • Since $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$ and E/F is separable, $m_{\alpha,K}$ does not multiple zeros. So E/K is separable.

• Since E/F is normal, all the zeros of $m_{\alpha,F}$ are in E;

Lecture 27: Fundamental theorem of Galois theory

Sunday, March 4, 2018 10:51 PM

Hence all the zeros of $m_{\alpha,K}$ are in E. So E/K is normal. ■

Theorem 1. Suppose E/F is a finite Galois extension. Then

$$\begin{array}{ccc} \{K \mid \underset{\text{subfield}}{F \subseteq K \subseteq E}\} & & \{H \mid H \leq \mathrm{Gal}(E/F)\} \\ K & \xmapsto{\Psi} & \mathrm{Gal}(E/K) \\ \mathrm{Fix}(H) & \xleftarrow{\Phi} & H \end{array}$$

are inverse of each other.

Pf. Since E/F is Galois, by the previous Proposition E/K is Galois.

And so $\mathrm{Fix}(\mathrm{Aut}(E/K)) = K$.

- For any $H \leq \mathrm{Aut}(E/F)$, $F \subset \mathrm{Fix}(H) \subseteq E$ and $E/\mathrm{Fix}(H)$ is Galois.

So $\mathrm{Aut}(E/\mathrm{Fix}(H)) = H$. ■

Theorem 2. Suppose E/F is a finite Galois extension.

$$\begin{array}{ccc} \{K \mid F \subseteq K \subseteq E,\ K/F \text{ normal}\} & & \{N \mid N \trianglelefteq \mathrm{Aut}(E/F)\} \\ K & \longmapsto & \mathrm{Gal}(E/K) \\ \mathrm{Fix}(N) & \longleftarrow & N \end{array}$$

Moreover, if K/F is normal, then K/F is Galois and

$$\mathrm{Gal}(K/F) \simeq \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K).$$

Pf. Suppose K/F is normal. Since E/F is separable, K/F is clearly separable. Hence K/F is Galois.

Lecture 27: Fundamental theorem of Galois theory

Sunday, March 4, 2018 11:13 PM

. As K/F and E/F are normal, restriction gives us an onto group homomorphism

$$\mathrm{Aut}(E/F) \twoheadrightarrow \mathrm{Aut}(K/F)$$
$$\sigma \longmapsto \sigma|_K \; ;$$

and clearly kernel of this map is $\mathrm{Aut}(E/K)$. Hence $\mathrm{Aut}(E/K) \triangleleft \mathrm{Aut}(E/F)$ and $\mathrm{Aut}(K/F) \simeq \mathrm{Aut}(E/F)/\mathrm{Aut}(E/K)$.

Now suppose $N \triangleleft \mathrm{Aut}(E/F)$; and let $K := \mathrm{Fix}(N)$. To show K/F is normal, it is enough to show for any $\sigma \in \mathrm{Aut}(E/F)$ $\sigma(K) \subseteq K$. So for $\alpha \in K$ and $\tau \in N$ we have to show

$$\tau(\sigma(\alpha)) \overset{?}{=} \sigma(\alpha)$$

$$\tau(\sigma(\alpha)) = \sigma(\underbrace{\sigma^{-1}\tau\sigma}_{\text{in } N}(\overset{\text{in Fix}(N)}{\alpha})) = \sigma(\alpha). \quad \blacksquare$$

as $N \triangleleft \mathrm{Aut}(E/F)$