Lecture 31: Hilbert's theorem 90

Tuesday, March 13, 2018 4:00 PM

(For the easy direction look at the end of today's note!)

In the previous lecture we proved $\chi_1,\ldots,\chi_m \in \mathrm{Hom}(G, E^\times)$ are E-linearly independent if $\chi_1,\ldots,\chi_m$ are distinct.

<u>Theorem</u>. (Hilbert's theorem 90)

Suppose E/F is a finite Galois extension; and $\mathrm{Gal}(E/F)=\langle\sigma\rangle$ is cyclic. Then $N_{E/F}(\alpha)=1 \iff \alpha=\sigma(\beta)/\beta$ for some $\beta\in E^\times$ where $N_{E/F}(\alpha)=\prod_{i=0}^{m-1}\sigma^i(\alpha)$ and $[E:F]=m$.

<u>Pf</u>. Let $\tau_\alpha: E\to E$, $\tau_\alpha(e):=\alpha\,\sigma(e)$. So τ_α is an F-linear map. Then $\tau_\alpha^2(e)=\tau_\alpha(\alpha\,\sigma(e))=\alpha\,\sigma(\alpha)\,\sigma^2(e)$

And by induction $\tau_\alpha^i(e)=\alpha\,\sigma(\alpha)\ldots\sigma^{i-1}(\alpha)\,\sigma^i(e)$; and so

$$\tau_\alpha^m=(\alpha\,\sigma(\alpha)\ldots\sigma^{m-1}(\alpha))\underbrace{\sigma^m}_{\mathrm{id}}=\alpha\,\sigma(\alpha)\ldots\sigma^{m-1}(\alpha)\,I_E=N_{E/F}(\alpha)\,I_E=I_E$$

And so the minimal polynomial of the F-linear transformation τ_α divides x^m-1. On the other hand, $1,\sigma,\ldots,\sigma^{m-1}: E^\times\to E^\times$ are distinct characters and so they are E-linearly independent.

Hence $I,\tau_\alpha,\ldots,\tau_\alpha^{m-1}$ are F-linearly indep. And so $\min_{\tau_\alpha}(x)=x^m-1$.

In particular, 1 is an eigenvalue of τ_α. So $\exists\,\beta'\in E$, $\tau_\alpha(\beta')=\beta'$.

Lecture 31: Towards sol. of Galois gp implies sol. in rad

Tuesday, March 13, 2018 12:24 AM

$\Rightarrow \alpha\,\sigma(\beta') = \beta' \Rightarrow \alpha = \dfrac{\sigma(\beta'^{-1})}{\beta'^{-1}}$. ■

Corollary. Suppose $\mathrm{char}(F) \nmid n$, F contains n^{th} roots of unity, E/F is a finite Galois extension, $\mathrm{Gal}(E/F) = \langle\sigma\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Then $\exists\, \alpha \in E$ s.t. $E = F[\alpha]$ and $\alpha^n \in F$.

Pf. Let $\mu_n := \{\zeta \in F \mid \zeta^n = 1\}$. Then by one of your homework assignments μ_n is a cyclic group; and by assumption it has n elements. ($x^n - 1$ is separable as $\mathrm{char}(F) \nmid n$.) Suppose $\mu_n = \langle \zeta_n \rangle$. Then

$N_{E/F}(\zeta_n) = \prod_{i=0}^{n-1} \sigma^i(\zeta_n) = \zeta_n^n = 1$. Hence, by Hilbert's theorem 90, $\exists\, \alpha \in E$, $\zeta_n = \sigma(\alpha)/\alpha$. And so $\sigma(\alpha) = \zeta_n \alpha$. Therefore

$$N_{E/F}(\alpha) = \prod_{i=0}^{n-1} \sigma^i(\zeta_n \alpha) = \prod_{i=0}^{n-1} \zeta_n^i \alpha = \alpha^n \cdot \zeta_n^{\frac{n(n-1)}{2}} \in F$$

$$\left(\zeta_n^{\frac{n(n-1)}{2}}\right)^2 = 1 \Rightarrow \zeta_n^{\frac{n(n-1)}{2}} = \pm 1 \qquad \Rightarrow \alpha^n \in F.$$

Let $E' := F[\alpha] \subseteq E$. Since $\mathrm{Gal}(E/F)$ is abelian, all of its subgps are normal. And so E'/F is a Galois extension, and

$\mathrm{Gal}(E/F) \to \mathrm{Gal}(E'/F)$, $\sigma^i \longmapsto \sigma^i|_{E'}$ is onto. Since $\sigma^i(\alpha) = \zeta_n^i \alpha$, we have $\left|\{\sigma^i|_{E'} \mid 0 \le i < n\}\right| = n$. And so $E = E'$. ■

Lecture 31: Galois's theorem on solvability in rad

Tuesday, March 13, 2018 12:49 AM

__Theorem__. Suppose $\mathrm{char}(F)=0$, $f(x)\in F[x]$, E is a splitting field of $f(x)$ over F. Suppose $\mathrm{Gal}(E/F)$ is solvable. Then $f(x)$ is solvable in radicals.

__Pf__. Let L be a splitting field of x^n-1 over E where $n=[E:F]$. Then $\mathrm{Gal}(L/E)\hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. And so

$$1\to \underbrace{\mathrm{Gal}(L/E)}_{\text{abelian}} \to \mathrm{Gal}(L/F)\to \underbrace{\mathrm{Gal}(E/F)}_{\text{solvable}}\to 1 \quad \text{is a S.E.S.}$$

Hence $\mathrm{Gal}(L/F)$ is solvable. Notice that $\mathrm{char}(F)=0$ implies L/F is separable; and L/F is splitting field of a family of poly. as E/F is normal and L/E is splitting field of x^n-1. Hence L/F is Galois. Let $F':=F[\zeta_n]$ where $\mu_n=\{\zeta\in L \mid \zeta^n=1\}=\langle\zeta_n\rangle$.

And consider $\mathrm{Gal}(L/F')$. Since $\mathrm{Gal}(L/F')\subseteq \mathrm{Gal}(L/F)$, $\mathrm{Gal}(L/F')$ is solvable. Hence $\exists$ a series of subgps

$$1=N_0\lhd N_1\lhd\cdots\lhd N_m=\mathrm{Gal}(L/F') \text{ s.t. } N_i/N_{i+1}\simeq \mathbb{Z}/k_i\mathbb{Z}$$

Let $E_i:=\mathrm{Fix}(N_i)$. So $F'\subseteq E_{m-1}\subseteq\cdots\subseteq E_1\subseteq E_0=L$,

Lecture 31: Galois's theorem on solvability in rad

Wednesday, March 14, 2018 10:37 AM

L/E_i is Galois and $Gal(L/E_i) = N_i$. Since $Gal(L/E_i) \lhd Gal(L/E_{i+1})$,

E_i/E_{i+1} is a Galois extension. And $Gal(E_i/E_{i+1}) \simeq Gal(L/E_{i+1})/Gal(L/E_i)$

$$= N_{i+1}/N_i \simeq \mathbb{Z}/k_i\mathbb{Z}$$

<u>Claim</u>. $k_i \mid n$

<u>Pf of claim</u>. $k_i = [E_i : E_{i+1}] \mid [L:F']$; $L = E[\zeta_n]$ and $F' = F[\zeta_n]$.

Then
$$Gal(L/F') = Gal(E[\zeta_n]/F[\zeta_n]) \longrightarrow Gal(E/F)$$
$$\sigma \longmapsto \sigma|_E$$

is a well-defined injective group homomorphism.

<u>Well-defined</u>. E/F is a Galois extension and $F \subseteq F[\zeta_n]$.

<u>Group homomorphism</u>. Is clear.

<u>Injective</u>. $\left.\begin{array}{l} \sigma|_E = id_E \\ \sigma|_{F[\zeta_n]} = id_{F[\zeta_n]} \end{array}\right\} \Rightarrow \sigma|_{E[\zeta_n]} = id \Rightarrow \sigma = I$.

Therefore $|Gal(L/F')| \mid |Gal(E/F)|$; and so $[L:F'] \mid [E:F]$,

and claim follows.

Since $\mu_n \subseteq F' \subseteq E_{i+1}$ and $k_i \mid n$, $\mu_{k_i} \subseteq E_{i+1}$. Thus the previous

corollary implies $\exists \alpha_i \in E_i$ such that $E_i = E_{i+1}[\alpha_i]$ and $\alpha_i^{k_i} \in E_{i+1}$;

As $F' = F[\zeta_n]$ claim follows. ■

Lecture 31: Summary of solvability

Tuesday, March 13, 2018 1:20 AM

<u>Theorem</u> (Galois) Let F be a char. 0 field, $f(x) \in F[x]$, and E is a splitting field of $f(x)$ over F. Then f is solvable in radicals if and only if $\mathrm{Gal}(E/F)$ is solvable.

- E/F : finite, Galois. $\Rightarrow$ $N_{E/F}(\sigma(\beta)/\beta) = 1$ $\forall\, \sigma \in \mathrm{Gal}(E/F)$ and $\beta \in E^\times$.

<u>Pf.</u> $N_{E/F}(\sigma(\beta)/\beta) = \prod_{\tau \in \mathrm{Gal}(E/F)} \tau(\sigma(\beta)/\beta)$

$$= \prod_{\tau \in \mathrm{Gal}(E/F)} (\tau \circ \sigma)(\beta) \Big/ \prod_{\tau \in \mathrm{Gal}(E/F)} \tau(\beta)$$

$$= N_{E/F}(\beta) / N_{E/F}(\beta) = 1. \quad \blacksquare$$