Cohomology 2: Hilbert's Theorem 90

Aim Lecture: Prove Hilbert's thm 90 & complete solvability criterion.

Linear Independence of Automorphisms

Let K = field. Below view $\sigma \in \mathrm{Aut}\,K$ as a "vector" in K-space of K-valued fns on K with pointwise add$^{\underline{n}}$ & scalar mult$^{\underline{n}}$.

Lemma (Dedekind): The set $\mathrm{Aut}\,K$ of field automorphisms is linearly independent $/K$.

Proof: by contradiction. Let $\sigma_1, \dots, \sigma_n \in \mathrm{Aut}\,K$ be the smallest lin. dependent set so

$$\alpha_1\sigma_1 + \dots + \alpha_n\sigma_n = 0 \quad \dots\dots (1)$$

$\alpha_i \neq 0$ for all i. Note $n > 1$.

For $\alpha, \beta \in K$ we have

$$0 = \alpha_1\sigma_1(\alpha\beta) + \dots + \alpha_n\sigma_n(\alpha\beta)$$
$$= \alpha_1\sigma_1(\alpha)\sigma_1(\beta) + \dots + \alpha_n\sigma_n(\alpha)\sigma_n(\beta)$$
$$\Rightarrow \quad 0 = \alpha_1\sigma_1(\beta)\sigma_1 + \dots + \alpha_n\sigma_n(\beta)\sigma_n \dots\dots (2)$$

Get rel$^{\underline{n}}$ $\sigma_1(\beta)$ eq$^{\underline{n}}$ (1) $-$ eq$^{\underline{n}}$ (2)

$$0 = [\underbrace{\alpha_2\sigma_1(\beta) - \alpha_2\sigma_2(\beta)}_{\neq 0}]\sigma_2 + \dots + [\alpha_n\sigma_1(\beta) - \alpha_n\sigma_n(\beta)]\sigma_n$$

Picking β so $\sigma_1(\beta) \neq \sigma_2(\beta)$ we see $\sigma_2, \dots, \sigma_n$ lin. depend. contradicting minimality of n.

Hilbert's Theorem 90

Thm 90 (Hilbert): Let G be a finite subgroup of $\mathrm{Aut}\, K$. Then
$$H^1(G, GL_n(K)) = 1$$

Proof: in case $n=1$ only. Let $\alpha_* : G \to GL_1 = K^*$ be a 1-cocycle. Dedekind's lemma $\Rightarrow$ we can find $\alpha \in K$ s.t.
$$\beta := \sum_{\tau \in G} \alpha_\tau \tau(\alpha) \neq 0$$

Suffice show $\alpha_\sigma = \beta \sigma(\beta)^{-1} \; \forall \sigma \in G$.

$$\sigma(\beta) = \sum_\tau \sigma(\alpha_\tau)(\sigma\tau)(\alpha) = \sum \alpha_\sigma^{-1} \alpha_{\sigma\tau} (\sigma\tau)(\alpha)$$
$$= \alpha_\sigma^{-1} \beta$$

ex. Extend argument to $n > 1$. $\square$

Cor: Let K/F = Galois field ext$^{\underline{n}}$ with cyclic Galois group $G = \langle \sigma \rangle$. If $\alpha \in K$ has norm 1 then $\alpha = \beta \sigma(\beta^{-1})$ for some $\beta \in K$.

Proof: Lecture: Cohomology 1 $\Rightarrow \exists$ 1-cocycle α_* with $\alpha = \alpha_\sigma$ so Thm 90 $\Rightarrow$ Cor.

Criterion for Solvability

Can finally show our nec. criterion for solvability is sufficient in char. 0.

Lemma: Let K/F = Galois ext$^{\underline{n}}$ with cyclic Galois group $G = \langle \sigma \rangle \simeq \mathbb{Z}/n$. Suppose F contains n distinct roots of 1. Then $K = F(\sqrt[n]{\alpha})$ for some $\alpha \in F$.

Proof: Let $\zeta \in F$ be primitive n-th root of 1.

$N_{K/F}\,\zeta = \zeta^n = 1$ so cor. $\Rightarrow$ $\exists\, \beta \in K$ with $\zeta = \beta\sigma(\beta)^{-1}$ i.e. $\sigma(\beta) = \zeta\beta$. Thm lect. 2 $\Rightarrow$ the min. poly. of β/F is

$$p(x) = \prod_{i=0}^{n-1} (x - \sigma^i(\beta)) = \prod (x - \zeta^i\beta) = x^n - \beta^n$$

$\therefore$ If $\alpha = \beta^n$ we see $K = F(\sqrt[n]{\alpha})$. $\square$

Thm: Let F = field char 0 & K/F = solvable extension i.e. a Galois ext$^{\underline{n}}$ with solvable Galois group G. Then K/F embeds in a radical ext$^{\underline{n}}$.

Proof: by induction on $[K:F]$.

G solvable $\Rightarrow$ can find $H \trianglelefteq G$ with G/H cyclic say order n.

Claim: We can assume F contains all n-th roots of 1.

Why?
$$\begin{tikzcd} & K_1 & \\ K \arrow[ur, dash] & & F_1 \arrow[ul, dash] \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$
Else let K_1 = splitting field of $x^n - 1 / K$ & F_1 = subfield gen. by F & roots of $x^n - 1$.

Then $\mathrm{Gal}(K_1/F_1)$ isom. to subgroup of G

so is solvable & K_1/F_1 embeds in a radical ext$^{\underline{n}}$ $\Rightarrow$ so does K/F.

$\therefore$ Can replace K/F with K_1/F_1 $\square$

Now H solvable $\overset{\text{ind.}}{\Longrightarrow}$ K/K^H embeds in a radical ext$^{\underline{n}}$.

Also K^H/F Galois, cyclic Galois group G/H $\overset{\text{lemma}}{\Longrightarrow}$ $K^H = F(\sqrt[n]{\alpha})$, some $\alpha \in F$.

$\square$

$\boxed{\text{Solving cubics}}$

Cor. + proof Lemma tell us which roots need to be extracted to solve cubics, quartics etc.

Let F = field char $\neq 2$ or 3 with prim. $\sqrt[3]{1} = \zeta$.
Let $f(x) = x^3 + px + q \in F[x]$ have roots $\alpha_1, \alpha_2, \alpha_3$ say & suppose $Gal(f(x)/F) = S_3 = G$

$$1 < H = \langle \sigma = (1\,2\,3) \rangle < G.$$

$$\rightsquigarrow \quad K = F(\alpha_1, \alpha_2, \alpha_3) \supset K^H = F(\sqrt{D}) \supset F.$$

$$\sqrt{D} = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3).$$

$\gamma = \alpha_1 + \zeta^{-1}\alpha_2 + \zeta^{-2}\alpha_3$ is a ζ-e-vector for σ $\because$ $\sigma(\gamma) = \alpha_2 + \zeta^{-1}\alpha_3 + \zeta^{-2}\alpha_1 = \zeta\gamma$.

Cor + lemma $\Rightarrow$ $\gamma^3 \in K^H = F \oplus F\sqrt{D}$

Expanding γ^3 gives formula in terms of $\sqrt{D}$, p & q.

Can sim. find ζ^2-e-vector $\gamma' = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$. Since $\alpha_1 + \alpha_2 + \alpha_3 = 0$, roots $\alpha_1, \alpha_2, \alpha_3$ obtainable from γ & γ'.