3/08/2021

Lemma 1 Let k be an infinite field, and let Ω/k be an extension field of k. Let $f(X_1,\dots,X_n)\in\Omega[X_1,\dots,X_n]$ be a polynomial with coeff. in Ω s.t. $f(a_1,\dots,a_n)=0$ $\forall a_1,\dots,a_n\in k$. Then $f(X_1,\dots,X_n)=0$ in $\Omega[X_1,\dots,X_n]$

Pf: Induction on n. $n=1$ obvious

Write

$$f(X_1,\dots,X_n)=\underbrace{g_d(X_1,\dots,X_{n-1})}_{\neq 0}X_n^d+\dots+g_1(X_1,\dots,X_{n-1})X_n+g_0(X_1,\dots,X_{n-1})$$

Assume $\neq 0$.

Induction: $\exists\, a_1,\dots,a_{n-1}\in k$ s.t. $g_d(a_1,\dots,a_{n-1})\neq 0$

$$\underset{\substack{\neq\\ 0}}{f(a_1,\dots,a_{n-1},X_n)}\in\Omega[X_n]$$

$\Rightarrow$ $\exists\, a_n\in k$ s.t. $f(a_1,\dots,a_{n-1},a_n)\neq 0$.

q.e.d.

Theorem 2 Let E/k be a separable algebraic extension of fields, let Ω be an extension field of k, $\#k=\infty$. Let $\sigma_1,\dots,\sigma_n: E\longrightarrow\Omega$ be n distinct k-linear field embeddings of E into Ω. Suppose $f(T_1,\dots,T_n)\in\Omega[T_1,\dots,T_n]$ and $f(\sigma_1(a),\dots,\sigma_n(a))=0$ $\forall a\in E$. Then $f(T_1,\dots,T_n)=0$ in $\Omega[T_1,\dots,T_n]$.

Pf. May and do assume $[E:k] < \infty$ and $n = [E:k]$.

Pick a k-basis $u_1, \dots, u_n$ of E/k (Exer!)

Our Assumption is:

$$0 = f\Big(\underbrace{\sigma_1\Big(\sum_{i=1}^n a_i u_i\Big)}_{= \sum_{i=1}^n a_i \sigma_1(u_i)}, \dots, \underbrace{\sigma_n\Big(\sum_{i=1}^n a_i u_i\Big)}_{= \sum_{i=1}^n a_i \sigma_n(u_i)}\Big) \qquad \forall a_1, \dots, a_n \in k$$

i.e. The polynomial

$$g(X_1, \dots, X_n) \overset{\text{def}}{=} f\Big(\sum_{i=1}^n X_i \sigma_1(u_i), \dots, \sum_{i=1}^n X_i \sigma_n(u_i)\Big)$$

when evaluated at k^n is identically 0.

$\xRightarrow{\text{Lemma 1}}$ $g(X_1, \dots, X_n) = 0$ in $\Omega[X_1, \dots, X_n]$

Note $g(X_1, \dots, X_n)$ is obtained from $f(X_1, \dots, X_n)$ by a linear change of variables, via the matrix

$$A = \big(\sigma_j(u_i)\big)_{1 \le i, j \le n} \in M_n(\Omega)$$
$$\in GL_n(\Omega)$$

This matrix is non-singular $\because$ the n embedding $\sigma_1, \dots, \sigma_n$ of E into Ω are linearly indep over Ω

if $b_1, \dots, b_n \in \Omega$

$b_1\sigma_1 + \dots + b_n\sigma_n = 0$ on E

$\Leftrightarrow \sum_j b_j \sigma_j(u_i) = 0 \quad \forall i = 1..n$

So: f is obtained from g by a linear change of variables via A^{-1}

$\Rightarrow f = 0$ in $\Omega[X_1, \dots, X_n]$.

QED.

<u>Theorem 3</u> Let E/k be a finite Galois extension with Galois group G. Then $\exists\ \xi \in E$ s.t. $\{\sigma(\xi) \mid \sigma \in G\}$ is a k-basis of E.

equivalently.
$$\begin{array}{ccc} k[G] & \longrightarrow & E \\ \Downarrow & & \Downarrow \\ \sum_{\sigma\in G} a_\sigma \cdot [\sigma] & \longmapsto & \sum_{\sigma\in G} a_\sigma \cdot \sigma_\xi \end{array}$$
is an isom. of $k[G]$-modules

Pf: Suppose k is infinite
$G = \{\underset{\substack{\| \\ id}}{\sigma_1}, \ldots, \sigma_n\}$ $\quad n = \# G$

<u>Need</u>: $\xi \in E$ s.t. $\sigma_1(\xi), \ldots, \sigma_n(\xi)$ is k-linearly indep

$\Updownarrow$ linear indep. of embeddings

$$\left(\sigma_i(\sigma_j(\xi))\right)_{1\le i,j\le n} \in GL_n(E)$$

Define $c : \{1,\ldots,n\} \times \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$

by $\sigma_{c(i,j)} = \sigma_i \cdot \sigma_j \quad \forall\, i,j \in \{1,\ldots,n\}$

Consider $\underset{0\neq}{\det}\left(T_{c(i,j)}\right)_{1\le i,j\le n} = f(T_1, \ldots, T_n) \in E[T_1, \ldots, T_n]$

<u>Note</u>: For any n elements $a_1, \ldots, a_n \in E$

$a_1, \ldots, a_n$ is k-linearly indep $\Longleftrightarrow \left(\sigma_i(a_j)\right)_{1\le i,j\le n} \in GL_n(E)$

$\xLeftarrow{\text{obvious}}$

$\xRightarrow{\text{(exer.)}}$

$\leadsto \exists\ \underset{E}{\xi}$ s.t. $f(\sigma_1(\xi), \ldots, \sigma_n(\xi)) \neq 0$

$$\| $$
$$\det\left(\left(\sigma_i \cdot \sigma_j(\xi)\right)_{1\le i,j\le n}\right)$$

q.e.d.

Case $\#k < \infty$ (exercise!)

Note If $k = \mathbb{F}_q$ and $E = \mathbb{F}_{q^n}$

$\rightsquigarrow \mathrm{Gal}(E/k) =$ cyclic, generated by

$$\underset{E}{\sigma_q}\; x \mapsto x^q$$

$$= \sigma_q^{\mathbb{Z}/n\mathbb{Z}}$$

"Hilbert Theorem 90" for cyclic extensions.

Thm 4 (Hilbert Satz 90, multiplicative form)

E / k cyclic Galois extension. $n = [E:k]$

$\mathrm{Gal}(E/k) = \sigma^{\mathbb{Z}/n\mathbb{Z}}$

Given $\xi \in E^\times$ $\quad \mathrm{Nm}_{E/k}(\xi) = 1 \iff \exists\, \eta \in E^\times$ s.t. $\xi = \eta \cdot {}^{\sigma}\eta^{-1}$

$\Leftarrow$:

$$\because \mathrm{Nm}_{E/k}(\eta \cdot {}^{\sigma}\eta^{-1}) = (\eta \cdot {}^{\sigma}\eta^{-1}) \cdot {}^{\sigma}(\eta \cdot {}^{\sigma}\eta^{-1}) \cdots {}^{\sigma^{n-1}}(\eta \cdot {}^{\sigma}\eta^{-1})$$

$$= \eta \cdot {}^{\sigma^n}\eta^{-1} = 1$$

Pf:

Consider elements of the form

$$\eta = \theta + \xi \cdot {}^{\sigma}\theta + \underline{\xi \cdot {}^{\sigma}\xi} \cdot {}^{\sigma^2}\theta + \cdots + \underline{\xi \cdot {}^{\sigma}\xi \cdots {}^{\sigma^{n-2}}\xi} \cdot {}^{\sigma^{n-1}}\theta$$

$\theta \in E$ $\quad$ Suppose $\eta \neq 0$

$$\xi\, {}^{\sigma}\eta = \xi\, {}^{\sigma}\theta + \xi\, {}^{\sigma}\xi\, {}^{\sigma^2}\theta + \cdots + \underbrace{\xi\, {}^{\sigma}\xi \cdots {}^{\sigma^{n-1}}\xi}_{\mathrm{Nm}_{E/k}(\xi) = 1}\, \theta$$

$$\xi \cdot {}^{\sigma}\eta = \eta \underset{\text{if } \eta \neq 0}{\Longrightarrow} \xi = \eta \cdot {}^{\sigma}\eta^{-1}$$

It suffices to show: $\exists\theta$ s.t.

$$\underline{1}\cdot\theta+\underline{\xi}\,{}^{\sigma}\theta+\cdots\cdots+\underline{\xi\cdot{}^{\sigma}\xi\cdots\cdot{}^{\sigma^{n-2}}\xi}\cdot{}^{\sigma^{n-1}}\theta\neq 0.$$

This follows from: the linear independence of

$id,\ \sigma,\ \cdots\cdots,\ \sigma^{n-1}$

QED.

Thm 5 (Hilbert Satz 90, additive form for cyclic extensions)

E/k cyclic $Gal(E/k)=\sigma^{\mathbb{Z}/n\mathbb{Z}}$ (Replace Nm by Tr.)

Suppose $\alpha\in E$. Then $Tr_{E/k}(\alpha)=0$

$\Updownarrow$ $\Uparrow$ obvious

$\exists\beta$ s.t $\alpha=\beta-{}^{\sigma}\beta$

Pf of $\Downarrow$

Consider elements of the form

$$\gamma=\cancel{\theta+}\ \alpha\,{}^{\sigma}\theta+(\alpha+{}^{\sigma}\alpha)\,{}^{\sigma^2}\theta+\cdots+(\alpha+{}^{\sigma}\alpha+\cdots+{}^{\sigma^{n-2}}\alpha)\cdot{}^{\sigma^{n-1}}\theta$$

$${}^{\sigma}\gamma=\quad{}^{\sigma}\theta+\quad{}^{\sigma}\alpha\ {}^{\sigma^2}\theta+\cdots+\ {}^{\sigma}\alpha+\cdots+{}^{\sigma^{n-2}}\alpha\cdot{}^{\sigma^{n-1}}\theta$$

$$+\underbrace{({}^{\sigma}\alpha+{}^{\sigma^2}\alpha+\cdots+{}^{\sigma^{n-1}}\alpha)}_{=-\alpha}\theta$$

$$\gamma-{}^{\sigma}\gamma=\alpha\cdot\underbrace{({}^{\sigma}\theta+\cdots+{}^{\sigma^{n-1}}\theta+\theta)}_{=Tr_{E/k}(\theta)\in}$$

If $Tr_{E/k}(\theta)\in k^{\times}$, then $\beta=\dfrac{\gamma}{Tr_{E/k}(\theta)}$ satisfies: $\beta-{}^{\sigma}\beta=\alpha$

The existence of an element $\theta \in E$ with

$$\underbrace{\theta + \sigma\theta + \dots + \sigma^{n-1}\theta}_{\mathrm{Tr}_{E/k}(\theta)} \in k^{\times}$$

again follows from linear indep. of embeddings.!

QED.

Cor E/k is cyclic Galois, $\mathrm{Gal}(E/k) \cong \mathbb{Z}/n\mathbb{Z} = \sigma^{\mathbb{Z}/n\mathbb{Z}}$ and $\mu_n(k) = \zeta^{\mathbb{Z}/n\mathbb{Z}}$, $n^{-1} \in k^{\times}$

Then $\exists\ \xi \in E \setminus k$ s.t. $\xi^n \in k$, $\xi^n = b$.

and $\sigma\xi = \zeta \cdot \xi$ $\Rightarrow E = k(\sqrt[n]{b})$

$\therefore\ \mathrm{Nm}_{E/k}(\zeta) = \zeta^n = 1$

and $\gamma \mapsto \gamma\xi \cdot \xi^{-1}$, $\mathrm{Gal}(E/k) \xrightarrow{\sim} \mu_n(k)$