

Lecture # 8 (08/11/2024)

Today: The Artin-Schreier theorem

Recall (Lecture #6)

Theorem (Artin-Schreier) Let K be a field of characteristic $p > 0$. Then we can consider the so-called Artin-Schreier operator

$$\begin{aligned} \varphi_p : K &\longrightarrow K & \text{and we have that:} \\ a &\longmapsto a^p - a \end{aligned}$$

Note: • $\varphi_p = \Phi_p - \text{id}$, where $\Phi_p : K \rightarrow K$ denotes

the Frobenius

$$\bullet \text{Ker}(\varphi_p) \cong \mathbb{F}_p$$

(i) If L/K is cyclic of degree p , then

$L = K(\alpha)$, where α is such that

$$\alpha^p - \alpha - a = 0 \text{ for some } a \in K$$

(ii) Conversely, given $a \in K$, the polynomial

$$f(x) = x^p - x - a$$

either

Ⓐ has a root in K , in which case all roots are in K

OR

Ⓑ it is irreducible. In this case, if α is a root, then $K(\alpha)/K$ is cyclic of degree p

► This happens precisely when $a \in K^\times \setminus \text{Im}(\varphi_p)$
Such polynomials are called Artin-Schreier polynomials.

► Eventhough $K(\alpha)/K$ is cyclic, hence $\text{Gal}(K(\alpha)/K) \simeq \mathbb{Z}/p\mathbb{Z}$ is solvable, such extensions may NOT be solvable (as we defined)

Lemma 1 Let K be a field of characteristic $p > 0$, $a \in K \setminus K^p$ and $n \in \mathbb{N}$. Then the polynomial $f(x) = x^{p^n} - a$ is irreducible.

proof By contradiction, assume that we can find $n \in \mathbb{N}$ such that $f(x) = x^{p^n} - a$ is reducible.

Write $f(x) = \underbrace{g(x)h(x)} \in K[x]$ and let L be an

here, we assume monic & $\deg > 0$

extension of K that contains a root β of f .

Then, in $L[x]$, $f(x) = x^{p^n} - \beta^{p^n} = (x - \beta)^{p^n}$.

Since $K[x] \subset L[x]$ and $L[x]$ is a UFD,

$g(x) = (x - \beta)^d$ for some $1 \leq d < p^n$ such that

$d = p^r$ for some $1 \leq \underbrace{r < n}$ and $\beta^d \in K$.

$\hookrightarrow \deg h \geq 1$

But then

$$a = \beta^{p^n} = \beta^{p^{n-r} p^r} = \left(\beta^{p^r} \right)^{p^{n-r}} \in K^{p^{n-r}} \subset K^p$$

Note: $L = K(\beta) / K$ is purely inseparable

□

Our goal today is to prove the following theorem:

↙ also due Artin-Schreier

Theorem Suppose that K is a field such that $1 < [K:K] < \infty$.

i.e. K is not algebraically closed & $\bar{K}/K$ is finite

Example: $K = \mathbb{R}$, $\bar{K} = \mathbb{C} = K(i)$

$K = \mathbb{A} \cap \mathbb{R}$, $\bar{K} = K(i)$

↖ real algebraic numbers

Then

- (i) $\bar{K} = K(i)$, where $i \in \bar{K}$ is such that $i^2 = -1$,
- (ii) Given $a \in K^\times$, exactly one of a and $-a$ is a square in K , and every finite non-empty sum of non-zero squares is again a non-zero square in K . In particular, $\text{char } K = 0$

{ $IP := \{a^2; a \in K^\times\}$ is closed under addition
& multiplication + does not contain 0
 $1 \in IP \Rightarrow n \cdot 1 = 1 + \dots + 1 \in IP \quad \forall n$
"
 $1^2 \Rightarrow n \cdot 1 \neq 0 \quad \forall n \Rightarrow \text{char } K = 0$

upshot: such extensions all look like $\mathbb{C}/\mathbb{R}$

Lemma 2 Suppose that K is as in the theorem and $\bar{K}/K$ is a finite extension of prime degree p . Then $p=2$, $\text{char } K \neq 2$ and $\bar{K} = K(i)$, where $i^2 = -1$.

proof By assumption, we have that $\bar{K}/K$ is cyclic **Galois** of degree p . ← see last page

If $\text{char } K = p$, by Artin-Schreier theory, $\bar{K} = K(\alpha)$, where α is a root of an irred. polynomial of the form $f(x) = x^p - x - a$ ($a \in K$)

Since $\bar{K}$ is algebraically closed, choose $b \in \bar{K}$ s.t. $b^p - b = a \alpha^{p-1}$. Write

$$b = b_0 + b_1 \alpha + \dots + b_{p-1} \alpha^{p-1}$$

(since $\{1, \alpha, \dots, \alpha^{p-1}\}$ is a K -basis for $\bar{K}$)

and observe that (since $\text{char } K = p$)

$$b^p - b = \left(b_{p-1}^p - b_{p-1} \right) \alpha^{p-1} + \text{lower degree terms in } \alpha$$

Thus, $b_{p-1} \in K$ is a root of f , which is an absurd since f is irred. / K .

Now, since $\bar{K}$ is alg. closed of char $\neq p$,
 $\exists$ a p -th root of unity in $\bar{K}$, say ζ .

Since there are no intermediate field extensions
 $K \subset L \subset \bar{K}$ (by assumption, $[\bar{K}:K] = p$ prime)
 $\& [K(\zeta):K] \leq p-1$, $\zeta \in K$.

Thus, Kummer theory now applies, and

$$\bar{K} = K(\alpha^{1/p}) = K(\beta), \quad \beta^p = \alpha \in K$$

Now (since $\bar{K}$ is alg. closed) choose $\gamma \in \bar{K}$
 s.t. $\gamma^p = \beta$. Then for any $\sigma \in \text{Gal}(\bar{K}/K)$
 non-trivial, $\sigma(\gamma) = \omega \gamma$ for some primitive
 p^2 root of 1.

Note:

$$\triangleright \sigma(\gamma^{p^2}) = \sigma(\beta^p) = \beta^p = \gamma^{p^2}$$

$$\begin{array}{c} \parallel \\ \Rightarrow (\sigma(\gamma))^{p^2} = \gamma^{p^2} = (\omega \gamma)^{p^2} \end{array} \quad \begin{array}{c} \uparrow \\ \alpha = \beta^p \in K \end{array}$$

$$\triangleright \text{if } \omega^p = 1, \text{ then } \sigma(\gamma^p) = \gamma^p = \beta$$
$$\parallel$$
$$\sigma(\beta)$$

$$\Rightarrow \beta \in K \quad \downarrow$$

$$\text{But then } \frac{\sigma(\omega)}{\omega} \in \mu_p \quad \text{since } \omega^p \in \mu_p \subset K$$

$$\text{Thus } \sigma(\omega) = \omega \omega^{p^k} \text{ for some } k \in \mathbb{Z}$$
$$= \omega^{1+p^k}$$

Using $\sigma(\gamma) = \omega \gamma$ one deduces that

$$p=2 \text{ \& } k \text{ is odd} \Rightarrow \sigma(\omega) = \omega^3$$

$\parallel$

$$\Rightarrow \omega \notin K \text{ \& } \bar{K} = K(\omega)$$

ω has order 4

Note:

$$\begin{aligned}\sigma^P(r) &= \sigma^{P-1}(\overset{\sigma(r)}{\omega r}) \\ &= \sigma^{P-2}(\sigma(\omega) \sigma(r)) \\ &= \sigma^{P-2}(\sigma(\omega) \omega r) \\ &= \sigma^{P-3}(\sigma^2(\omega) \sigma(\omega) \omega r) \\ &\vdots \\ &= \sigma^{P-1}(\omega) \cdot \dots \cdot \sigma(\omega) \omega r \\ &= \omega^N r\end{aligned}$$

But $\sigma^P = \text{id}$ (by assumption, $\text{Gal}(\bar{K}/K) \simeq C_p$)

$$\text{Thus, } \underbrace{1 + (1+pK) + \dots + (1+pK)^{P-1}}_{=N} \equiv 0 \pmod{p^2}$$

$$\Rightarrow p + \frac{P(P-1)}{2} pK \equiv 0 \pmod{p^2}$$

& this equation implies

$$\frac{P(P-1)}{2} K \equiv -1 \pmod{p}$$

Back to the theorem (page 4)

proof of theorem (i)

Take K a field s.t. $1 < [\bar{K}:K] < \infty$.

and write $G = \text{Gal}(\bar{K}/K)$. If p is a prime that divides $|G|$, $\exists \sigma \in G$ of order p .

Let $L = \bar{K}^{\langle \sigma \rangle}$. Lemma 2 applied to

$\bar{K}/L$ implies that $p=2$. So, $|G| = 2^m$

for some $m \in \mathbb{N}$. It now suffices to

show that G contains no subgroup of order 4.

G must have a subgroup of order $p^k \forall 0 \leq k \leq m$

By contradiction, assume such a subgroup H exists. Then, applying Lemma 2 again,

$\exists K < F_2 < \bar{K}$ s.t. $\bar{K} = F_2(i)$

($F_2 =$ fixed field of an element of order 2)

But then we look at $F_4 = \bar{K}^H$ and the degree 2 extension $\bar{K}/F_4(i)$

Applying Lemma 2 once more,

$\bar{K} = F_4(i)(j)$ for some $j^2 = -1$, $j \notin F_4(i)$
which is absurd, since $j = i$ or $j = -i$
both of which are in $F_4(i)$.

Thus, $|G| = 2$ & Lemma 2 $\Rightarrow \bar{K} = K(i)$.

Remarks (about part (ii))

① -1 is not a square in $K \Rightarrow$ for any $a \in K^\times$
exactly one of a and $-a$ is a square

$$a = b^2 \text{ and } -a = c^2 \Rightarrow -1 = (b/c)^2$$

$$\text{both not a square} \Rightarrow \left(\sqrt{-a} / \sqrt{a} \right)^2 = -1$$

$\uparrow$
 K

$$\text{Note: } \bar{K} = K(\sqrt{-a}) = K(\sqrt{a})$$

$$\sqrt{-a} = x + y\sqrt{a} \Rightarrow -a = x^2 + y^2a + 2xy\sqrt{a}$$

$\sqrt{a} \notin K$, $\text{char } K \neq 2$ & $-a$ not a square

$$\Rightarrow x = 0 \text{ \& } y = \frac{\sqrt{-a}}{\sqrt{a}} \in F \text{ is such that}$$
$$y^2 = -1$$

② The second part follows from the fact that every element of $K(i)$ is a square in $K(i)$ since $K(i) = \overline{K}$.

Take $a, b \in K^\times$.

$$\text{Write } a+bi = (c+di)^2 \quad (K(i) = \overline{K})$$

$$\begin{aligned} \text{Then } a^2 + b^2 &= (c^2 - d^2)^2 + (2cd)^2 \\ &= (c^2 + d^2)^2 \end{aligned}$$

Remark (about Lemma 1) For $0 < [K:K] < \infty$,

$\overline{K}/K$ is Galois: if $\text{char } K = 0$ this is clear. If $\text{char } K = p$, then Lemma 1 implies $K = K^p$ ($\Rightarrow K$ is perfect) & the extension is separable.