Lecture # 8 (06/11/2025)

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

$$\begin{aligned} \varphi_p : K &\longrightarrow K \\ a &\longmapsto a^p - a \end{aligned}$$

and we have that:

Note: • $\varphi_p = \Phi_p - id$, where $\Phi_p : K \longrightarrow K$ denotes the Frobenius

• $\ker(\varphi_p) \simeq \mathbb{F}_p$

(i) If L/K is cyclic of degree p, then $L = K(\alpha)$, where α is such that

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

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

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

either

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

OR

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

- This happens precisely when $a \in K^\times \setminus \mathrm{Im}(\varphi_p)$

  Such polynomials are called Artin-Schreier polynomials.

- Eventhough $K(\alpha)/K$ is cyclic, hence $\mathrm{Gal}(K(\alpha)/K) \simeq \mathbb{Z}/p\mathbb{Z}$ 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 $f(x) = g(x)\,h(x) \in K[x]$ 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 $1 \le d < p^n$ such that

$d = p^r$ for some $1 \le r < n$ and $\beta^d \in K$.

↳ deg $h \ge 1$

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

∎

Remark For $0 < [\bar{K} : K] < \infty$, if char $K = p$

Lemma 1 implies $K = K^p$ ($\Rightarrow K$ is perfect)

& the extension is separable.

Lemma 2 Suppose that K is a field such that $1 < [\overline{K} : K] < \infty$.

K not alg. closed
$\overline{K}/K$ finite

with $\overline{K}/K$ a finite extension of prime degree p. Then $p = 2$, $\operatorname{char} K \neq 2$ and $\overline{K} = K(i)$, where $i^2 = -1$.

proof By assumption, we have that $\overline{K}/K$ is cyclic Galois of degree p. If $\operatorname{char} K = p$, by Artin-Schreier theory, $\overline{K} = K(\alpha)$, where α is a root of an irred. polynomial of the form $f(X) = X^p - X - a$ $(a \in K)$

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

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

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

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

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

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

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

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

Thus, Kummer theory now applies, and

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

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

Note:

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

  $\alpha = \beta^p \in K$

  $\Rightarrow (\sigma(\gamma))^{p^2} = \gamma^{p^2} = (\omega\gamma)^{p^2}$

- if $\omega^p = 1$, then $\sigma(\gamma^p) = \gamma^p = \beta$

  $\sigma(\beta)$

  $\Rightarrow \beta \in K$ ↯

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

Thus $\sigma(\omega) = \omega\,\omega^{pK}$ for some $K \in \mathbb{Z}$

$= \omega^{1+pK}$

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

$p = 2$ & K is odd $\Rightarrow \sigma(\omega) = \omega^3$

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

ω has order 4

Note:

$$\sigma^p(\gamma) = \sigma^{p-1}\Big(\underbrace{\sigma(\gamma)}_{\| \; \omega\gamma}\Big)$$

$$= \sigma^{p-2}\Big(\sigma(\omega)\,\sigma(\gamma)\Big)$$

$$= \sigma^{p-2}\Big(\sigma(\omega)\,\omega\gamma\Big)$$

$$= \sigma^{p-3}\Big(\sigma^2(\omega)\,\sigma(\omega)\,\omega\gamma\Big)$$

$$\vdots$$

$$= \sigma^{p-1}(\omega)\cdot\ldots\cdot\sigma(\omega)\,\omega\gamma$$

$$= \omega^N\gamma$$

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

Thus, $\underbrace{1 + (1+pK) + \cdots + (1+pK)^{p-1}}_{= N} \equiv 0 \bmod p^2$

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

& this equation implies

$$\frac{p(p-1)}{2}K = -1 \bmod p$$

also due Artin-Schreier

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

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

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

$K = \overline{\mathbb{Q}} \cap \mathbb{R}$, $\overline{K} = K(i)$

↖ real algebraic numbers

Then

(i) $\overline{K} = K(i)$, where $i \in \overline{K}$ 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, $\operatorname{char} K = 0$

$\mathbb{P} := \{a^2 ; a \in K^\times\}$ is closed under addition & multiplication + does not contain 0

$1 \in \mathbb{P} \Rightarrow n \cdot 1 = 1 + \cdots + 1 \in \mathbb{P} \quad \forall n$

$1 = 1^2 \Rightarrow n \cdot 1 \neq 0 \quad \forall n \Rightarrow \operatorname{char} K = 0$

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

proof of theorem (i)

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

and write $G = Gal(\bar{K}/K)$. 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 $\forall\, 0 \le k \le m$

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

$\exists \quad K \subset F_2 \subset \bar{K} \quad$ 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

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

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

$\sqrt{a} \in K$

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

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

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

$\Rightarrow x = 0$ & $y = \dfrac{\sqrt{-a}}{\sqrt{a}} \in F$ 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 $a, b \in K^{\times}$.

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

Then $a^2 + b^2 = (c^2 - d^2)^2 + (2cd)^2$

$= (c^2 + d^2)^2$