

Lecture #10 (27/11/2024)

Galois cohomology continued

Let L/K be a cyclic Galois extension with $\text{Gal}(L/K) = \langle \sigma \rangle$.

Then (worksheet #8) $H^2(\langle \sigma \rangle, L^\times) \simeq K^\times / \text{im } N$

Theorem Let K be a field. If there exists L/K as above such that $N: L^\times \rightarrow K^\times$ is not surjective, then there exists a (finite dimensional) noncommutative division algebra $/K$.

Corollary If K is finite and L/K is finite ($\Rightarrow$ cyclic), then $N: L^\times \rightarrow K^\times$ is surjective.

Why? (Wedderburn) f.d. algebras in this case must be fields ($\Rightarrow$ commutative)

Corollary If $p \neq 2$ is a prime, then there exists a noncommutative division algebra over $K = \mathbb{F}_p(x)$.

proof We will construct a cyclic extension L/K such that $N: L^\times \rightarrow K^\times$ is not surjective.

Take $L = K(\sqrt{x})$. Then L is Galois of degree 2. Now, given $l \in L^\times$, we can write $l = \frac{a + b\sqrt{x}}{c}$ for some

$a, b, c \in \mathbb{F}_p[x]$. Thus, $N(l) = \frac{a^2 - b^2x}{c^2}$.

This characterizes $\text{im}(N)$. Note that, in particular, any $\alpha \in \mathbb{F}_p$ which is not a square does not lie in $\text{im}(N)$.

(Double check) If $p \not\equiv 1 \pmod{4}$ ($\Rightarrow -1$ is not a square) then $x^2 + x \notin \text{im}(N)$.

A brief introduction to the Inverse Galois Problem (IGP)

Q.: Given G a finite group, does there exist $L/\mathbb{Q}$ with $\text{Gal}(L/\mathbb{Q}) = G$?

Some Known cases:

Abelian, S_n , A_n , solvable groups

Hard

↳ Every finite abelian group is a quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$ for some n &

$$\text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

Today: S_n & A_n (Hilbert, 1892)

Theorem Every finite group G that can be realized as a Galois group over $\mathbb{Q}(t_1, \dots, t_n)$ can be realized as a Galois group over $\mathbb{Q}$.

Corollary Every symmetric group S_n ($n \geq 1$) can be realized as a Galois group over $\mathbb{Q}$

proof

$S_n \curvearrowright L = \mathbb{Q}(t_1, \dots, t_n)$. Let

$K = \mathbb{Q}(t_1, \dots, t_n)^{S_n}$. Then

$K = \mathbb{Q}(s_1, \dots, s_n)$, where s_i is the $t_1, \dots, t_n$ i -th elementary symmetric function on

Moreover, $\text{Gal}(L/K) = S_n$.

□

Rmk.: We can show that for any $n \geq 1$

$$\text{Gal}_{\mathbb{Q}}(x^n - x - 1) \simeq S_n.$$

The main ingredients in the proof of the theorem are:

① Hilbert's irreducibility theorem

If $f = f(t, x) \in \mathbb{Q}(t)[x]$ is irreducible. Then for almost all $b \in \mathbb{Q}$, $f_b = f(b, x) \in \mathbb{Q}[x]$ is irreducible.

② If $f(t, x) \in \mathbb{Q}(t)[x]$ is irreducible and $\mathbb{Q}(t)[x]/f$ is Galois over $\mathbb{Q}(t)$, then there exist infinitely many $b \in \mathbb{Q}$ such that $\mathbb{Q}[x]/f_b$ is Galois over $\mathbb{Q}$ with the same Galois group.

③ ① + ② are still true if we replace t by $t_1, \dots, t_n$.

proof of theorem

Let $L/\mathbb{Q}(t_1, \dots, t_n)$ be a Galois extension with Galois group G . By the primitive element theorem, $L \simeq \mathbb{Q}(t_1, \dots, t_n)[X]/f$ (for f the minimal polynomial of the primitive element)

Now, by HIT, we can specialize to some $f(b_1, \dots, b_n, x) \in \mathbb{Q}[x]$ irreducible. But then $\mathbb{Q}[x]/f_b$ is Galois w/ Galois group G . 

- We now show that for infinitely many $t \in \mathbb{Q}$,

$$f(x) = x^n - ntX - (n-1)t \in \mathbb{Q}[x]$$

has Galois group over $\mathbb{Q}$ equal to S_n . The same is true for A_n !

Proposition With $f \in \mathbb{Q}[X]$ as above,

let $L = \text{SF}_{\mathbb{Q}}(f)$. Write $f(x) = \prod (x - \alpha_i) \in \mathbb{Q}[x]$

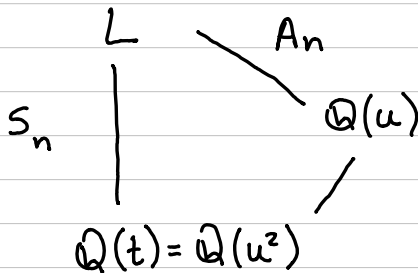
and let $\Delta(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in \mathbb{Q}$.

← discriminant

Write $t = 1 - (-1)^{\frac{n(n-1)}{2}} n u^2$.

$\Rightarrow \mathbb{Q}(u^2) = \mathbb{Q}(t) \quad \& \quad \mathbb{Q}(u) = \mathbb{Q}(u^2, \sqrt{\Delta(f)})$.

Then:



Corollary We can realize A_n as a Galois group over $\mathbb{Q}$.

Cubic and quartic polynomials

Proposition Let K be a field w/ $\text{char } K \neq 2$ and let $f \in K[x]$ be irred. & separable.

Let $L = SF_K(f)$ & $G = \text{Gal}(L/K)$.

Then $G \subset A_n \iff \Delta(f) \in K^2$.

(As before, $\Delta(f)$ = discriminant of f)

Corollary (L, K & f as above) Assume that $\deg(f) = 3$. Then

$$(i) \text{ Gal}(L/K) = S_3 \iff \Delta(f) \notin K^2$$

$$(ii) \text{ Gal}(L/K) = A_3 \iff \Delta(f) \in K^2$$

The case of degree 4

Take $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$
irred. & sep.

$\leadsto$ Write $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$
in $L[x]$ ($L = SF_K(f)$).

$$\begin{aligned}\text{Let } \beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4, \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4, \\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3.\end{aligned}$$

$$\text{Define } r(x) := (x - \beta_1)(x - \beta_2)(x - \beta_3)$$

Proposition Let $n = [K(\beta_1, \beta_2, \beta_3) : K]$:= F
and $G = \text{Gal}(L/K)$ as before.

$$(i) \quad G = S_4 \Leftrightarrow n = 6$$

$$\Leftrightarrow r \text{ is irred. / } K \text{ \& } \Delta(f) \notin K^2$$

$$(ii) \quad G = A_4 \Leftrightarrow n = 3$$

$$\Leftrightarrow r \text{ is irred. / } K \text{ \& } \Delta(f) \in K^2$$

$$(iii) \quad G \simeq C_4 \Leftrightarrow n = 2 \text{ \& } f \text{ is reducible / } F$$

$$(iv) \quad G \simeq D_4 \Leftrightarrow n = 2 \text{ \& } f \text{ is irred. / } F$$

$$(v) \quad G \simeq V \text{ (Klein)} \Leftrightarrow n = 1$$

Examples

① $f = x^3 - 3x + 1$ has discriminant $81 = 9^2$
& it is irred. / $\mathbb{Q}$.

$$\Rightarrow \text{Gal}_{\mathbb{Q}}(f) = A_3$$

② $f = x^3 - 4x + 2$ has discriminant
 $148 = 2^2 \cdot 37$ & it is irred. / $\mathbb{Q}$

$$\Rightarrow \text{Gal}_{\mathbb{Q}}(f) = S_3$$

③ p a prime, $f(x) = x^4 + px + p$
 $\Rightarrow r(x) = x^3 - 4px - p^2$

$$\Delta(f) = p^3(256 - 27p) \notin \mathbb{Q}^2$$

$$\begin{aligned} \leadsto \text{Gal}_{\mathbb{Q}}(f) &= S_4 \quad \text{if } p \neq 3, 5 \\ &= D_4 \quad \text{if } p = 3 \quad F = \mathbb{Q}(\sqrt{21}) \\ &= C_4 \quad \text{if } p = 5 \quad F = \mathbb{Q}(\sqrt{5}) \end{aligned}$$