Lecture # 10 (20/11/2025)

Galois cohomology continued

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

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 $N: L^\times \to K^\times$ is not surjective, the there exists a (finite dimensional) noncommutative division algebra $/K$.

Corollary If K is finite and L/K is finite ($\Rightarrow$ cyclic), then $N: L^\times \to K^\times$ 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 $N: L^\times \to K^\times$ is not surjective.

Take $L = K(\sqrt{x})$. Then L is Galois of degree 2. Now, given $\ell \in L^\times$, we can write $\ell = \frac{a + b\sqrt{x}}{c}$ for some $a, b, c \in \mathbb{F}_p[x]$. Thus, $N(\ell) = \frac{a^2 - b^2 x}{c^2}$.

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

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

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

proof

$S_n \curvearrowright L = \mathbb{Q}(t_1, \cdots, t_n)$. Let $K = \mathbb{Q}(t_1, \cdots, t_n)^{S_n}$. Then $K = \mathbb{Q}(s_1, \cdots, s_n)$, where s_i is the i-th elementary symmetric function on $t_1, \cdots, t_n$

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

RmK.: We can show that for any $n \geq 1$ $\mathrm{Gal}_{\mathbb{Q}}(x^n - x - 1) \simeq S_n$.

$$s_i(t_1, \cdots, t_n) = \sum t_{j_1} t_{j_2} \cdots t_{j_i}$$

w/ $1 \leq j_1 < j_2 < \cdots < j_i \leq n$

A brief introduction to the Inverse Galois Problem (IGP)

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

Some Known cases: (Hard)

Abelian, S_n, A_n, solvable groups

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

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

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 $\mathbb{Q}$.

The main ingredients in the proof of the theorem are:

① Hibert'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 $t_1, \ldots, t_n$.

proof of theorem

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

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

∎

- We now now 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!

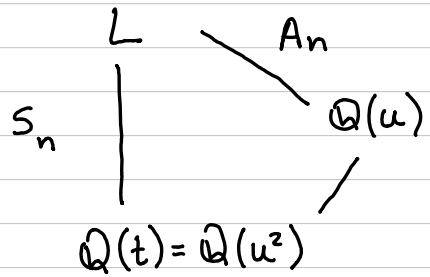
Proposition With $f \in \mathbb{Q}[x]$ as above, let $L = SF_{\mathbb{Q}}(f)$. Write $f(x) = \prod (x - \alpha_i) \in L[x]$ and let $\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in \mathbb{Q}$.

discriminant

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

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

Then:



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

Cubic and quartic polynomia

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

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

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

idea: $G \subset A_n \iff$ any $\sigma \in G$ is even

$\iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta}$

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

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

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

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

The case of degree 4

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

$\rightsquigarrow$ Write $f(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$ in $L[X]$ $\left(L = SF_K(f)\right)$.

Let $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$,
$\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$,
$\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$.

Define $r(X) := (X-\beta_1)(X-\beta_2)(X-\beta_3)$

$:= F$

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

(i) $G = S_4 \iff n = 6$

$\iff$ r is irred. $/K$ & $\Delta(f) \notin K^2$

(ii) $G = A_4 \iff n = 3$

$\iff$ r is irred. $/K$ & $\Delta(f) \in K^2$

note: r irred. $\iff n = 3$ or $6 \iff 3 \mid |G|$

(iii) $G \simeq C_4 \iff n = 2$ & f is reducible $/F$

(iv) $G \simeq D_4 \iff n = 2$ & f is irred. $/F$

(v) $G \simeq V$ (Klein) $\iff n = 1$

Examples

① $f = x^3 - 3x + 1$ has discriminant $81 = 9^2$

& it is irred. / $\mathbb{Q}$.

$\Rightarrow \quad Gal_{\mathbb{Q}}(f) = A_3$

② $f = x^3 - 4x + 2$ has discriminant

$148 = 2^2 \cdot 37$ & it is irred. / $\mathbb{Q}$

$\Rightarrow \quad Gal_{\mathbb{Q}}(f) = S_3$

③ p a prime, $f(x) = x^4 + px + p$

$\Rightarrow r(x) = x^3 - 4px - p^2$

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

$\rightsquigarrow Gal_{\mathbb{Q}}(f) = S_4$ if $p \neq 3, 5$

$= D_4$ if $p = 3$ $\quad F = \mathbb{Q}(\sqrt{21})$

$= C_4$ if $p = 5$ $\quad F = \mathbb{Q}(\sqrt{5})$