Galois Cohomology

Lecture 1: Introduction

k field, e.g. $\mathbb{Q}$, $\mathbb{F}_p$

K/k field ext^n

- algebraic if $\forall x \in K$ $\underbrace{\dim_k k(x)}_{[k(x):k]} < \infty$ (smallest subfield of K containing k, x)

$\rightsquigarrow$ minimal poly $f_x(T) \in k[T]$ s.t. $f_x(x) = 0$.

- finite if $[K:k] < \infty$
- Galois if K/k algebraic + $\forall x \in K$ $\exists x_1, \dots, x_n \in K$ distinct s.t. $f_x(T) = \prod_i (T - x_i) \in K[T]$

Put $\mathrm{Gal}(K/k)$ = group of field automorphisms φ of K s.t. $\varphi|_k = \mathrm{id}_k$.

[$\varphi(0)=0$, $\varphi(1)=1$, $\varphi(a+b) = \varphi(a)+\varphi(b)$, $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.

group structure = comp^n]

Th^m (Galois theory) Let K/k be a finite Galois ext^n. Then

$$\{\text{subgroups of } \mathrm{Gal}(K/k)\} \longrightarrow \{\text{subfields of } K \text{ cf. } k\}$$
$$H \longmapsto K^H = \{x \in K \mid \varphi(x) = x \ \forall \varphi \in H\}$$

is a bijection.

Q1 What if K/k is infinite?

Ex $k = \mathbb{F}_p$ $\quad K = \overline{\mathbb{F}_p}$ $\quad G = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

$f : \overline{\mathbb{F}_p} \longrightarrow \overline{\mathbb{F}_p}$, $x \longmapsto x^p$

pf: $(x+y)^p = x^p + y^p$ in char p,

$\therefore f \in G$.

Note: $x \in \overline{\mathbb{F}_p}$ & $f(x) = x \Rightarrow x \in \mathbb{F}_p$

($X^p - X = 0$ has at most p sol^{ns})

If Galois theory works, then G must be gen. by f.

Only finitely many sol^{ns} to $X^{p^n} - X = 0$ but $\overline{\mathbb{F}_p}$ is infinite. $\therefore f^n \neq \mathrm{id}$ $\forall n > 0$

$\rightsquigarrow G \simeq \mathbb{Z}$ (if everything works)

Problem 1 There are many subfields of $\overline{\mathbb{F}_p}$ than subgps of $\mathbb{Z}$. Namely if $H \subset \mathbb{Z}$ is a subgp then $H = d\cdot\mathbb{Z}$ & then $\overline{\mathbb{F}_p}^H / \mathbb{F}_p$ is finite. (i.e. $x^{p^d} - x = 0$)

But $\overline{\mathbb{F}_p}$ admits proper infinite subext^{ns}.

Problem 2 There are more endomorphisms of $\overline{\mathbb{F}_p}$.

Let $a_1, a_2, \ldots \in \mathbb{Z}$. Put $e_n = \sum_{i=1}^{n} a_i \cdot i!$.

For $x \in \overline{\mathbb{F}_p}$, the seq. $f^{e_n}(x)$ is eventually stationary (b/c $\mathrm{Gal}(\mathbb{F}_p(x)/\mathbb{F}_p)$ is finite & hence for $i > |\mathrm{Gal}|$ get $f^{i!}_{\mathbb{F}_p(x)} = id$.)

$\therefore$ element "$\lim_n f^{e_n}$" $\in G = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$

$x \mapsto f^{e_n}(x)$ for $n \gg 0$ so that the sequence is already stationary.

If e.g. $a_i = 1$ $\forall i$ then "$\lim_n f^{e_n}$" $\in \mathbb{Z} \subset G$.

$\rightsquigarrow$ moral: want to think of a topology on G?
(so that limit makes more sense)

Resolution to both problems:

enter the "angel of topology"
(Hermann Weyl)

Let K/k be Galois. Call a (normal) subgroup $H \subset \mathrm{Gal}(K/k)$ open if there exist a finite Galois subext $k \subset k' \subset K$ s.t.

$$H = \ker(\mathrm{Gal}(K/k) \to \mathrm{Gal}(k'/k)).$$

FACT The "open" subgroups form a basis of open nbd. of $1 \in \mathrm{Gal}(K/k)$ for a (unique) topology on G

Th (infinite Galois theory) K/k Galois.

- $\mathrm{Gal}(K/k)$ is compact Hausdorff & tot. disconnected.
  ("profinite")
- $\{\text{closed subgroups}\} \xrightarrow{\sim} \{\text{subext's}\}$

  $\cup$ $\cup$

  $\{\text{open subgroups}\} \xrightarrow{\sim} \{\text{finite subext}\}$

Def^{n} k a field. $\mathrm{Gal}(k) := \mathrm{Gal}(k^s/k)$

↑ "separable closure" = biggest possible Galois ext^{n}.

Q2 How to study $\mathrm{Gal}(k)$?

Q2' How to study any profinite group?

Q2'' How to study any finite group?!

A2'' - Sylow theorem: any finite gp G admits a max. subgroup $P \subset G$ of order a power of p.

- $|G:P|$ coprime to p
- any two such P are conjugate

--

- in general: p-groups (i.e. order a power of p) are particularly nice
- less well-known: p-completion of G = maximal quotient which is a p-group. $\rightsquigarrow G_p^\wedge$
- describe G by gens & rel^{n}s.

A2' - pro-p-group = profinite gp s.t. every

finite quotient is a p-group

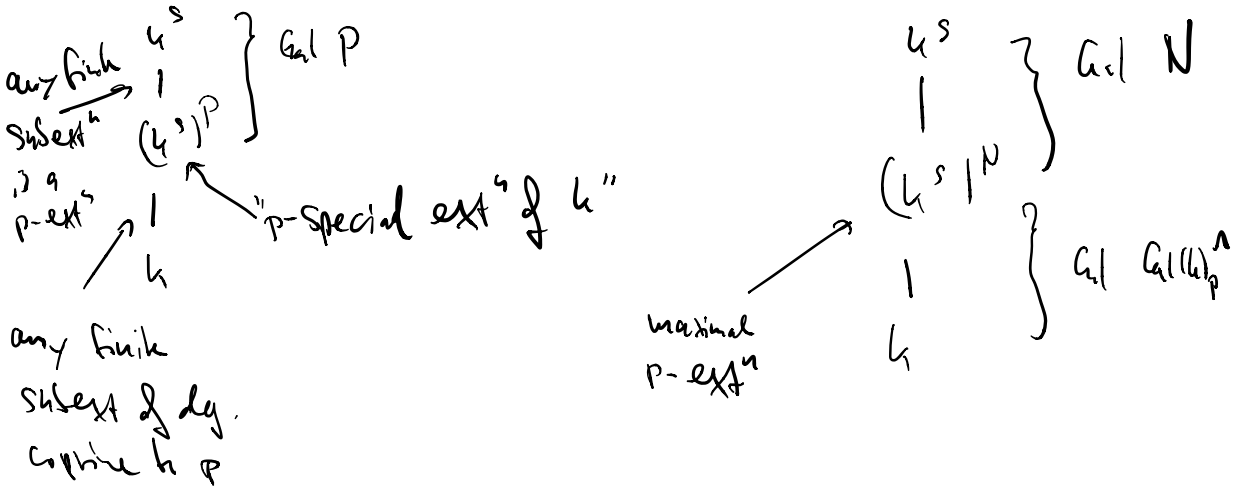
- profinite Sylow theorem
- pro-p- completion

(can also make sense of genus of $\mathcal{X}(k)$)

A2 interpretation of pro-sylow & pro-p-comp^{n} for $Gal(k)$.

$P \subset Gal(k)$ $\qquad$ $Gal(k) \twoheadrightarrow Gal(k)_p^{\wedge}$

N = kernel.



Enter the angel again

If G is a finite gp, $\exists!$ top space BG

s.t. $\pi_0 BG = *$

$\pi_1 BG = G$

$\pi_i BG = 0 \quad \forall\, i > 1.$

Same as gp.

Def^n $H^*(G, A) := H^*_{sing}(BG, A)$

"group cohomology of G"

Useful invariant. Great invariant for pro-p groups.

Def^n G a profinite group.

$$H^*(G, A) = \varinjlim_{N \trianglelefteq G \text{ open, normal}} H^*(G/N, A)$$

usual gp. coh. ; finite gp

Th^m Let G be a pro-p-group.

$$d = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$$
$$e = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$$

Then d is the minimal # of gens
e is the min. # of relations

is a pres^n of G by gens & rel^{n}s.

Ex $G = C_2$

$BG = \mathbb{RP}^\infty$

$H^*(\mathbb{RP}^\infty, \mathbb{Z}/2) = \mathbb{F}_2[t] \qquad |t| = 1$

$\rightsquigarrow d = 1 \quad e = 1$

$G_2 = \langle x \mid x^2 = 1 \rangle$

1 gen 1 rel ✓

Hence plan: ① Pick a field k & a p-ext^n K/k.

Put $G = Gal(K/k)$.

② Compute $\dim H^2(G, \mathbb{F}_p)$, $\dim H^2(G, \mathbb{F}_p)$ & hope to get small #.

③ Work out a presentation ?!?

Ex $k = \mathbb{Q}$

K = maximal 2-ext^n "unramified outside of 2"

(i.e. discriminant $\pm 2^n$)

Will find $d = 2 \quad e = 1$.

In fact $\mathrm{Gal}(k/\mathbb{Q}) = \langle \sigma, \tau \mid \tau^2 = 1 \rangle_2$

What is going on? · τ = cx. conj.

· cyclotomic field $\mathbb{Q}(\zeta_{2^n}) \subset k$

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_{2^n})) & \xrightarrow{\sim} & (\mathbb{Z}/2^n)^\times \\ \uparrow & & \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{n-2} \\ \mathrm{Gal}(k/\mathbb{Q}) & & \uparrow \quad \uparrow \\ & & \tau \quad \sigma \end{array}$$

There must be bigger ext^n where σ & τ do not commute. (Ex: adjoin $2^{1/2^n}$ to $\mathbb{Q}(\zeta_{2^n})$)