3/12/2021

Today: Kummer theory (abelian extensions of fields. elementary)

Group cohomology
Galois cohomology] — Gallier–Shatz
(Serre: Galois cohomology)

Kummer theory:

Have seen (Hilbert 90): $Gal(E/k) = \sigma^{\mathbb{Z}/n\mathbb{Z}}$

If E/k is a finite cyclic extension with group $\mathbb{Z}/n\mathbb{Z}$,

$n \cdot 1_k \in k^\times$, and $a \in E^\times$ s.t. $Nm_{E/k}(a) = 1$,

then $\exists\ c \in E^\times$ s.t. $a = \sigma c \cdot c^{-1}$

Assume: $n \cdot 1 \in k^\times$, and $\# \mu_n(k) = n$.

i.e. k contains a primitive root of 1.

Then: $\forall d \in k^\times$, Consider $k(\sqrt[n]{d})/k$, where $\sqrt[n]{d}$ is an element of k^a whose n-th power is d,

then $k(\sqrt[n]{d})/k$ is Galois, and

$$Gal(k(\sqrt[n]{d})/k) = ?$$

and

$$Gal(k(\sqrt[n]{d})/k) \xhookrightarrow{\text{injection}} \mu_n(k)$$

$$\sigma \longmapsto \underbrace{\sigma(\sqrt[n]{d}) / \sqrt[n]{d}}$$

indep. of the choice of $\sqrt[n]{d}$

More generally, let $D \subseteq k^\times$ be a subset of $k^\times$, and let $E = k_D \overset{\text{def}}{=} k(\sqrt[n]{d})_{d \in D}$

Then: define a pairing

$$B : \underset{k_D}{\mathrm{Gal}(E/k)} \times \left((k^\times)^n \cdot D \big/ (k^\times)^n \right) \longrightarrow \mu_n(k)$$

with $(k^\times)^n \cdot D \subseteq k^\times$,

$$\left(\sigma \ , \ \underset{\substack{\cap \\ D}}{d} \cdot (k^\times)^n\right) \longmapsto \frac{\sigma \sqrt[n]{d}}{\sqrt[n]{d}}$$

Clearly, if $B(\sigma, d \cdot (k^\times)^n)) = 1 \ \forall \sigma$

then $\sqrt[n]{d} \in k$ i.e. $d \in (k^\times)^n$

Have shown: B is non-degen on the right

Similarly: if $\sigma \in \mathrm{Gal}(E/k)$ s.t.

$\sigma(\sqrt[n]{d}) = \sqrt[n]{d} \quad \forall d \in D$

then $\sigma = \mathrm{id}_{E = k_D}$ i.e. B is non-degen on the left

Conclusion: If $\# D < \infty$, then B defines a duality pairing between

$\mathrm{Gal}(k_D/k)$ and $D \cdot (k^\times)^n \big/ (k^\times)^n$

(Both groups are finite abelian, and are dual to each other.

B defines isoms

$$\mathrm{Gal}(k_D/k) \xrightarrow{\sim} \mathrm{Hom}_{grp}\left(D(k^\times)^n/(k^\times)^n, \mu_n\right)$$

$$\frac{D\cdot(k^\times)^n}{(k^\times)^n} \xrightarrow{\sim} \mathrm{Hom}_{grp}(\mathrm{Gal}(k_D/k), \mu_n).$$

Exercise: Formulate and prove an analog of the above when $\mathrm{char}(k) = p > 0$.

$\mathrm{Gal} \cong (\mathbb{Z}/p\mathbb{Z})^?$

Group cohomology:

Hilbert Thm 90 are special cases of the following more general statement. Let E/k be a finite Galois ext^n with grp G.

1) $H^1(\mathrm{Gal}(E/k), E^\times) = (0)$

"easy" $\Leftarrow$ normal basis theorem:

2) $H^i(\mathrm{Gal}(E/k), (E,+)) = 0 \quad \forall i \geq 1$

Remark
- multiplicative Hilbert 90 = the special case of 1) for cyclic extensions
- additive Hilbert 90 = the special case of 1) ~~for~~ cyclic extensions and $i = 1$

Meaning of these vanishing statement.

$E^\times$ = an abelian group with (left) action by $G = Gal(E/k)$

i.e. $E^\times$ is a left $\mathbb{Z}[G]$-module

$$H^1(Gal(E/k), E^\times) \overset{def}{=} Ext^1_{\mathbb{Z}[G]}(\mathbb{Z}, E^\times)$$

$\mathbb{Z}$ ← trivial $\mathbb{Z}[G]$-module

Recall: For any ring R and two left R-modules M, N have defined

$$Ext^i_R(M, N) \quad i \geq 0.$$

← an abelian group

Similarly,

$$H^i(Gal(E/k), (E,+)) = Ext^i_{\mathbb{Z}[G]}(\mathbb{Z}, (E,+))$$

$H^2(Gal(E/k), E^\times)$: Very interesting

$$\cong Br(k) = \text{the Brauer group of } k$$

$$= \left\{ \begin{array}{l} \text{isom. classes of finite} \\ \text{dimension central division} \\ \text{algebras over } k \end{array} \right\}$$

$$\ni [A]$$

A: division alg.

$\dim_k(A) < \infty$

$Z(A) = k$

$[A], [B] = [C]$

$[C]$ is determined by $A \otimes_k B \cong M_m(C)$

C is a central division alg. $/k$

This multiplication is associative

$[A] = [A^{opp}]^{\circ\,\circ}_{\circ}$

$A \otimes_k A^{opp} \cong M_{\underbrace{N}_{\dim_k(A)}}(k)$

$Br(k)$ is known if $k =$ a number field or a finite ext^n field of $\mathbb{F}_p(T)$

(part of class field theory)

finite ext^{ns} of $\mathbb{Q}(x, y)$

Normal basis theorem:

E/k finite Galois $\quad G = Gal(E/k)$

$\Longrightarrow (E, +) \cong k[G]$

as left $k[G]$-modules

$\rightsquigarrow$ $k[G]$ is extended from $\{1\} \hookrightarrow G$ (corestriction)

Explain two things

(i) standard complex; i.e. a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module.

(ii) the usual/standard way of representing elements of $H^i(G, ?)$ by cocycles.

Def. Standard homogeneous chain complex of a group G. i.e. left $\mathbb{Z}[G]$-modules

Homogeneous version

$$
\begin{array}{ccccccccc}
0 \leftarrow \mathbb{Z} & \xleftarrow{\text{"augmentation"}} & \mathbb{Z}[G] & \longleftarrow & \mathbb{Z}[G\times G] & \longleftarrow & \mathbb{Z}[G\times G\times G] \\
 & & & & \| & & \| \\
 & & & & C_1(G) & & C_2(G) \\
 & & \text{degree } 0 & & \text{degree } 1 & & \text{degree } 2 \\
\Psi & & \Psi & & \Psi & & \\
[\;] & & [\sigma_0] & & [\sigma_0, \sigma_1] & & [\sigma_0, \sigma_1, \sigma_2] & \sigma_i \in G \ \forall i
\end{array}
$$

$$C_n(G) = \mathbb{Z}[G^{n+1}] \longrightarrow \mathbb{Z}[G^n] = C_{n-1}(G)$$

$$[\sigma_0, \sigma_1, \dots, \sigma_n] \longmapsto \sum_{j=0}^{n} (-1)^j [\sigma_0, \dots, \hat{\sigma_j}, \dots \sigma_n]$$

$$= [\sigma_1, \sigma_2, \dots, \sigma_n] - [\sigma_0, \sigma_2, \dots, \sigma_n] + (-1)^n [\sigma_0, \dots, \sigma_{n-1}]$$

action of G on $C_n(G)$:

$$\tau \cdot [\sigma_0, \dots, \sigma_n] = [\tau\sigma_0, \tau\sigma_1, \dots, \tau\sigma_n]$$

$\forall \tau \in G$, $\forall \sigma_0, \sigma_1, \dots, \sigma_n \in G$

Exer: This is a resolution of $\mathbb{Z}[G]$-modules.

$\forall$ left G-module M, define
$\mathbb{Z}[G]$

$$C^n(G,M) := \operatorname{Hom}_{\mathbb{Z}[G]}\big(\underset{\mathbb{Z}[G^{n+1}]}{C_n(G)}, M\big)$$

$\Downarrow$

$f \leftarrow$ a homogeneous n-cochain.

$$f : [\sigma_0, \sigma_1, \dots, \sigma_n] \longrightarrow f(\sigma_0, \sigma_1, \dots, \sigma_n)$$

such a cochain is completely determined by a corresponding map $\varphi : G^n \longrightarrow M$

$$\varphi(s_1, s_2, \dots, s_n) = f(1, s_1, s_1 s_2, s_1 s_2 s_3, \dots, s_1 \cdots s_n)$$

This establishes a bijection

$$\underset{\overset{\Downarrow}{f}}{C^n_{homog}(G,M)} \quad \text{and} \quad \underset{\overset{\Downarrow}{\varphi}}{\operatorname{Maps}(G^n, M)}$$

Question

What happens when you take the coboundary?

Recall:
$$\delta f(\sigma_0, \sigma_1, \dots, \sigma_{n+1}) = \sum_{i=0}^{n+1} (-1)^j f(\sigma_0, \dots, \hat{\sigma}_j, \dots, \sigma_{n+1})$$

$C^n_{homog}(G)$

$$f \longleftrightarrow \varphi \qquad \varphi(s_1 s_2, s_3)$$

$$\delta f \longleftrightarrow \delta\varphi$$

Example: $n=2$

Have $f(\sigma_0, \sigma_1, \sigma_2)$

$\rightsquigarrow \delta f(\sigma_0, \sigma_1, \sigma_2, \sigma_3)$

$s_1 f(1, s_2, s_2 s_3) = s \cdot \varphi(s_2, s_3)$

$$\begin{aligned}
&\delta\varphi(s_1, s_2, s_3) \\
&= \delta f(1, s_1, s_1 s_2, s_1 s_2 s_3) \\
&= f(s_1, s_1 s_2, s_1 s_2 s_3) - f(1, s_1 s_2, s_1 s_2 s_3) \\
&+ \underbrace{f(1, s_1, s_1 s_2 s_3)}_{= \varphi(s_1, s_2 s_3)} - \underbrace{f(1, s_1, s_1 s_2)}_{= \varphi(s_1, s_2)}
\end{aligned}$$

Ans.: For $n=2$ $\quad \delta\varphi(s_1, s_2, s_3)$

$$= {}^{s_1}\varphi(s_2, s_3) - \varphi(s_1 s_2, s_3) + \varphi(s_1, s_2 s_3) - \varphi(s_1, s_2)$$

formula for nonhomog cochain.