8.5. Cyclic groups

Lemma Let $G \cong \mathbb{Z}/n\mathbb{Z}$ be generated by σ. Then,

$$0 \leftarrow \mathbb{Z} \xleftarrow{\varepsilon} \mathbb{Z}[G] \xleftarrow{(\sigma-1)\cdot} \mathbb{Z}[G] \xleftarrow{N_G\cdot} \mathbb{Z}[G] \xleftarrow{(\sigma-1)\cdot} \cdots$$

$$\sum a_g \leftarrow\!\shortmid \sum_g a_g g$$

$$\left(N_G = \sum_g g \right)$$

is a free resolution of G-modules.

Pf HW. $\square$

$$\begin{tikzcd}
\rightsquigarrow 0 \arrow[r] & \mathrm{Hom}_G(\mathbb{Z}[G], A) \arrow[r, "(\sigma-1)\cdot"] \arrow[d, equal, "\text{as groups}"] & \mathrm{Hom}_G(\mathbb{Z}[G], A) \arrow[r, "N_G\cdot"] \arrow[d, equal] & \mathrm{Hom}_G(\mathbb{Z}[G], A) \arrow[r, "(\sigma-1)\cdot"] \arrow[d, equal] & \cdots \\
& A & A & A &
\end{tikzcd}$$

Cor $H^0(G, A) = \ker((\sigma-1)\cdot) = A^G$

$(\sigma-1)a = 0 \iff \sigma a = a$

$$H^1(G, A) = H^3(G, A) = \ldots = \ker(N_G\cdot)/\mathrm{im}((\sigma-1)\cdot) = \ker(N_G\cdot)/(\sigma-1)\cdot A$$

map $A \xrightarrow{N_G} A$

$$H^2(G, A) = H^4(G, A) = \ldots = \ker((\sigma-1)\cdot)/\mathrm{im}(N_G\cdot) = A^G/N_G\cdot A.$$

8.6. Examples

Ex Let $L|K$ be a Galois ext. with Galois group $G \cong \mathbb{Z}/n\mathbb{Z}$ gen. by σ.

a) $A = L^\times$

$\Rightarrow A^G = K^\times$

$\ker(N_G \cdot) = \{x \in L^\times : Nm_{L|K}(x) = 1\}$

$\mathrm{im}((\sigma - 1)\cdot) = \{\frac{\sigma(y)}{y} \mid y \in L^\times\}$

Hilbert 90

$\mathrm{im}(N_G \cdot) = Nm_{L|K}(L^\times)$.

$\Rightarrow H^0(G, L^\times) = K^\times$

$H^1(G, L^\times) = H^3(G, L^\times) = \dots = 1$

$H^2(G, L^\times) = H^4(G, L^\times) = \dots = \underbrace{K^\times / Nm_{L|K}(L^\times)}_{\text{We've encountered this in local CFT!}}$.

b) $A = L$

$\Rightarrow A^G = K$

$\ker(N_G \cdot) = \{x \in L \mid Tr_{L|K}(x) = 0\}$

$\mathrm{im}((\sigma - 1)\cdot) = \{\sigma(y) - y \mid y \in L\}$

Additive Hilbert 90

$\mathrm{im}(N_G \cdot) = Tr_{L|K}(L) = K$

$Tr_{L|K}(L) \neq 0$ by linear independence of the aut. of $L|K$

K-vector space contained in K

$\Rightarrow H^0(G, L) = K$

$H^1(G, L) = H^2(G, L) = \dots = 0$

Thm ("Hilbert 90", Noether)

Let $L|K$ be any finite Galois ext. with Galois group G. Then $H^1(G, L^\times) = 1$.

Pf Consider any 1-cocycle $(a_g)_{g\in G} \in Z^1(G, L^\times)$.

$\Rightarrow a_g \in L^\times \ \forall g\in G, \quad a_{gh} = a_g \cdot g(a_h) \ \forall g,h\in G$.

Let $t\in L$. Then, $b = \sum_{g\in G} a_g \, g(t) \in L$ satisfies

$$a_h h(b) = a_h \cdot \sum_g \underbrace{h(a_g\, g(t))}_{h(a_g)\cdot hg(t)} = \sum_g \underbrace{a_h h(a_g)}_{a_{hg}} \cdot hg(t)$$

$$= \sum_g a_{hg} \cdot hg(t) = \sum_g a_g \, g(t) = b \quad \forall h\in G.$$

Because the automorphisms $g\in G$ of $L|K$ are linearly independent, we can choose $t\in L$ so that $b\neq 0$, so $b\in L^\times$.

$$\Rightarrow a_g = \frac{g(b^{-1})}{b^{-1}} \quad \forall g\in G.$$

$\Rightarrow (a_g)_{g\in G}$ is a 1-coboundary ($\in B^1(G, L^\times)$).

$\Rightarrow Z^1(G, L^\times) = B^1(G, L^\times)$

$\Rightarrow H^1(G, L^\times) = 1$. $\square$

Normal basis theorem

Let $L|K$ be a fin. Gal. ext. with Galois group G.

Then, there is a <u>normal basis</u> of $L|K$: A basis of the form $(g(x))_{g\in G}$ for a fixed $x\in L$.

<u>Cor</u> $L \cong K[G]$ as left $K[G]$-modules.

(not as rings!!!)

~~$K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ splitting field of X^3-1~~

<u>Obs</u> If $(g(x))_{g\in G}$ is a basis, then $L=K(x)$.

<u>Pf</u> Since $g(x)\neq x$ for all $g\neq id$, the number x doesn't lie in any proper subfield of L (which would be fixed by all elements of a nontrivial subgroup of G). □

<u>Cor</u> L is a (co-)induced G-module.

<u>Cor of Cor</u> $H^i(G,L)=0 \quad \forall i\geq 1.$

("Additive Hilbert 90")

<u>Cor</u> $L_G \xrightarrow[\mathrm{Tr}_{L|K}]{\sim} K$

<u>Pf</u>

$$L_G = L/\langle gx-x \mid g\in G, x\in L\rangle_{\mathbb{Z}}$$

$$\cong K[G]/\langle gx-x \mid g\in G, x\in K[G]\rangle_{\mathbb{Z}} \cong K$$

$$\sum_g a_g g \mapsto \sum a_g$$

□

Proof of the normal basis theorem assuming $|K|=\infty$.

Fix a basis $\omega_1, \ldots, \omega_n$ of $L|K$. Let $G = \{g_1, \ldots, g_n\}$.

Write $x = a_1\omega_1 + \ldots + a_n\omega_n$ with $a_1, \ldots, a_n \in K$.

Let M be the $n\times n$-matrix sending the basis $(\omega_1, \ldots, \omega_n)$ to $(g_1(x), \ldots, g_n(x))$. $\left(g_j(x) = \sum_i a_i\, g_j(\omega_i) \right)$

Then, $(g(x))_{g\in G}$ is a basis of $L|K$ if and only if $f(a_1, \ldots, a_n) := \det(M) \neq 0$.

Note that $f(X_1, \ldots, X_n)$ is a polynomial (homogeneous of degree n).

Since $|K|=\infty$, if $f(a_1, \ldots, a_n) = 0$ $\forall a_1, \ldots, a_n \in K$, then $f(X_1, \ldots, X_n) = 0$.

Since the automorphisms $g_1, \ldots, g_n$ of $L|K$ are linearly independent, there exists $b_1, \ldots, b_n \in L$ s.t.

$$\sum_{i=1}^{n} b_i\, g_j(\omega_i) = \omega_j \quad \forall j = 1, \ldots, n.$$

$$\Rightarrow f(b_1, \ldots, b_n) = \det(I_n) = 1 \neq 0. \qquad \square$$

8.7. Functoriality

"$H^n(G,A)$ is covariant in A and contravariant in G"

<u>Def</u> Let A be a G-module and A' be a G'-module. Homomorphisms $\mu: G' \to G$ and $f: A \to A'$ of groups are <u>compatible</u> (for cohomology) if

$$f(\mu(g')a) = g' f(a) \quad \forall g' \in G, a \in A.$$

We then obtain a homomorphism

$$\tilde{C}^n(G,A) \longrightarrow \tilde{C}^n(G',A')$$

$$(\underbrace{a_{g_0,\dots,g_n}}_{A})_{g_0,\dots,g_n \in G} \longmapsto (\underbrace{f(a_{\mu(g_0'),\dots,\mu(g_n')})}_{A'})_{g_0',\dots,g_n' \in G'}$$

which induces a homomorphism

$$H^n(G,A) \longrightarrow H^n(G',A').$$

<u>Ex</u> If $G=G'$, $\mu = id$, we get the usual hom.

$$H^n(G,A) \longrightarrow H^n(G,A').$$

<u>Def</u> For $H \subseteq G$ and any G-module A, the maps

$H \overset{\mu}{\hookrightarrow} G$, $A \xrightarrow{id} A$ induce the <u>restriction</u> hom.

$$\mathrm{Res}: H^n(G,A) \longrightarrow H^n(H,A).$$

<u>Ex</u> $(n=0)$: $\underset{H^0(G,A)}{\overset{\|}{A^G}} \hookrightarrow \underset{H^0(H,A)}{\overset{\|}{A^H}}$

Rmk A resolution $0 \leftarrow \mathbb{Z} \leftarrow P_0 \leftarrow P_1 \leftarrow \dots$ of $\mathbb{Z}$ by free G-mod. is a resolution by free H-mod. The inclusion $\mathrm{Hom}_G(P_n, A) \longrightarrow \mathrm{Hom}_H(P_n, A)$ induces the restriction hom. $H^n(G, A) \to H^n(H, A)$.

Def For $H \trianglelefteq G$ a normal subgroup and any G-module A, the maps $G \xrightarrow{\mu} G/H$, $\underset{G/H\text{-mod.}}{A^H} \longrightarrow \underset{G\text{-mod.}}{A}$

induce the inflation hom.

$$\mathrm{Inf}: H^n(G/H, A^H) \longrightarrow H^n(G, A).$$

Def For $H \leq G$ (of finite index) and any H-mod. A, then induced G-module is

$$\mathrm{Ind}_H^G A := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A. \qquad (g(x \otimes a) = (gx) \otimes a)$$

(Note: $h(1 \otimes a) = h \otimes a = 1 \otimes ha$)

Rmk $\mathrm{Ind}_H^G A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A \cong \{\phi : G \to A \text{ map (not nec. hom.)} \mid \phi(hg) = h\phi(g) \ \forall h \in H, g \in G\}$,

$$\sum_{g \in H \backslash G} \underbrace{g^{-1} \otimes \phi(g)}_{=(hg)^{-1} \otimes \phi(hg) \ \forall h \in H} \longleftarrow\!\shortmid \phi$$

Ex $\mathrm{Ind}_1^G A \cong \{\phi : G \longrightarrow A \text{ map}\}$ (not nec. hom.) (an induced G-module!)