12 Local class field theory

$$0 \to I_G \to R[G] \to R \to 0$$
$$\sum a_g g \mapsto \sum a_g$$
$$\Rightarrow R[G]_G \xrightarrow{\sim} R$$

12.1 Cohomology of cyclic groups

Let G be a finite cyclic group of order n with a generator g. For a commutative ring R we are interested in the ideal $\underbrace{I_G}_{\text{augmentation ideal}} := (g-1)$ of the group ring $R[G]$ and the element

$$\boxed{N_G := \sum_{g' \in G} g'} \in R[G].$$

$R[G]^G = R \cdot N_G.$

$\Rightarrow \boxed{N_G M \subset M^G}$

Definition 12.1.1: For any $R[G]$-module M we define the *Tate cohomology* groups:

$$\hat{H}^0(G,M) := M^G/N_G M,$$
$$\hat{H}^{-1}(G,M) := \ker(N_G|M)/I_G M.$$

$I_G M = (g-1)M$

$\downarrow N_G$

$N_G(g-1)M = 0$

$\Rightarrow \boxed{I_G M \subset \ker(N_G|M).}$

Definition 12.1.2: If these are both finite, the *Herbrand quotient* of M is defined as

$$\boxed{h(G,M) := \frac{|\hat{H}^0(G,M)|}{|\hat{H}^{-1}(G,M)|}.}$$

$H^0(G,M) = M^G$

Proposition 12.1.3: If M is a free $R[G]$-module, then $\hat{H}^i(G, M) = 0$ for all i and $h(G, M) = 1$.

Proof: $M = R[G] \Rightarrow N_G M = N_G \cdot R = R[G]^G = M^G \Rightarrow \hat{H}^0 = 0$

$I_G M = (g-1)R[G] = \ker(N_G : R[G] \to R[G]) \Rightarrow \hat{H}^{-1} = 0.$

$\sum a_{g'} g' \mapsto (\underbrace{\sum a_{g'}}) N_G.$

$M = \bigoplus_{i \in I} R[G]$ same.

qed.

Proposition 12.1.4: If M is finite, then $h(G, M)$ is defined and equal to 1.

Proof: $0 \to M^G \to M \xrightarrow{g-1} I_G M \to 0$ exact.

$0 \to \ker(N_G|M) \to M \to N_G M \to 0$ exact.

$\Rightarrow h(G, M) = \frac{|\hat{H}^0|}{|\hat{H}^{-1}|} = \frac{|M^G| / |N_G M|}{|\ker(N_G|M)| / |I_G M|} = \frac{|M^G| \cdot |I_G M|}{|\ker(N_G|M)| \cdot |N_G M|} = \frac{|M|}{|M|} = 1.$

qed

Now consider a short exact sequence of $R[G]$-modules $0 \to M_1 \to M_2 \to M_3 \to 0$.

Proposition 12.1.5: There exists a natural exact hexagon

$$\begin{tikzcd}
 & \hat{H}^0(G, M_1) \arrow[r, "f_1"] & \hat{H}^0(G, M_2) \arrow[dr, "f_2"] & \\
\hat{H}^{-1}(G, M_3) \arrow[ur, "{f_6\ [N_G]}"] & & & \hat{H}^0(G, M_3) \arrow[dl, "{f_3\ [g-1]}"] \\
 & \hat{H}^{-1}(G, M_2) \arrow[ul, "f_5"] & \hat{H}^{-1}(G, M_1) \arrow[l, "f_4"] &
\end{tikzcd}$$

Proof:

$$\left(\cdots \xrightarrow{N_G} M \xrightarrow{g-1} \underset{\uparrow \atop \hat{H}^{-1}}{M} \xrightarrow{N_G} \underset{\uparrow \atop \hat{H}^{0}}{M} \xrightarrow{g-1} M \xrightarrow{N_G} M \xrightarrow{g-1} \cdots \right) =: C^\bullet_M$$

Short exact exact sequence $0 \to C^\bullet_{M_1} \to C^\bullet_{M_2} \to C^\bullet_{M_3} \to 0$

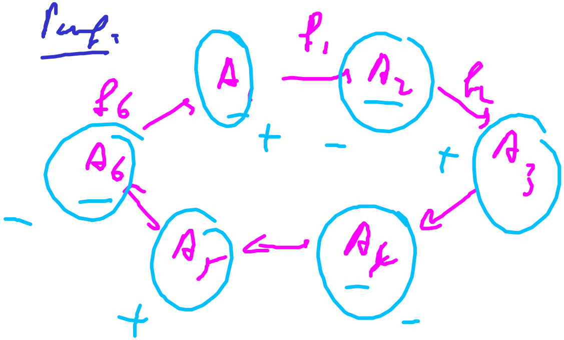
Use Homological Algebra.

qed.

Proposition 12.1.6: If two of the numbers $h(G, M_i)$ are defined, so is the third and we have

$$h(G, M_2) = h(G, M_1) \cdot h(G, M_3).$$

Proof:



$i \bmod (6)$

$$|A_i| = |\mathrm{im}(f_i)| \cdot |\ker(f_i)|$$
$$= |\mathrm{im}(f_i)| \cdot |\mathrm{im}(f_{i-1})|$$

$$\Rightarrow \prod_{i \bmod (6)} |A_i|^{(-1)^i} = 1.$$

qed.

12.2 Some Galois cohomology

Consider a finite cyclic field extension L/K with Galois group Γ. For any representation M of Γ we write

$$\hat{H}^i(L/K, M) \;:=\; \hat{H}^i(\Gamma, M).$$

Proposition 12.2.1: *(Normal basis theorem)* There exists $b \in L$ such that the elements ${}^{\gamma}b$ for $\gamma \in \Gamma$ form a basis of L over K.

Proof: Pick a generator $\gamma \in \Gamma$ of order n $\Rightarrow$ $K[\Gamma] \cong K[X]/(X^n - 1)$, $\gamma \longleftarrow X$

and view L as a $K[X]$-module.

Recall: The γ^i for $i \bmod (n)$ are L-linearly independent in $\mathrm{End}_K(L)$ a vector space

$\Rightarrow$ K- " "

So $K[\Gamma] \hookrightarrow \mathrm{End}_K(L)$ $\Rightarrow$ γ has min. polynomial $X^n - 1$.

Write $L \cong \bigoplus_{i=1}^{r} K[X]/(f_i)$ with $f_1 | f_2 | \ldots | f_r$ as $K[X]$-module

$\Rightarrow f_r = X^n - 1$. Then $\underbrace{\dim_K(L)}_{n} = \sum_i \deg(f_i) = \sum_{i<r} \deg(f_i) + \underbrace{\deg(f_r)}_{n}$

$\Rightarrow \forall\, i<r : \deg(f_i) = 0$ $\Rightarrow$ $L \cong K[X]/(f_r) = K[X]/(X^n - 1) \cong K[\Gamma]$.

qed

Proposition 12.2.2: We have $\hat{H}^i(L/K, L) = 0$ for each i.

Proof: L is a free $K[\Gamma]$-module. $\Rightarrow$ thm 12.1.3. qed.

i.e. $\exists\, b \in L$: $\{\gamma b \mid \gamma \in \Gamma\}$ is a basis of L over K.

Proposition 12.2.3: We have $\hat{H}^{-1}(L/K, L^\times) = 1$. *(Hilbert theorem 90)*

Proposition 12.2.4: We have $\hat{H}^i(L/K, L^\times) = 1$ for each i if K is finite.