Lecture # 9 (13/11/2024)

① G - modules

Definition Let G be a group. A G-module is an abelian group M ($=\mathbb{Z}$-module) that is a left module over the group ring $\mathbb{Z}[G]$ ($=$ abelian grp. of formal finite sums of elements of G).

This means that we have a left G-action on M: A map
$$\begin{aligned} G \times M &\longrightarrow M \\ (g, m) &\longmapsto g \cdot m \end{aligned}$$
satisfying
$$\begin{cases} 1_G \cdot m = m \\ (\sigma \tau) \cdot m = \sigma \cdot (\tau \cdot m) \\ \sigma \cdot (m + n) = \sigma \cdot m + \sigma \cdot n \end{cases}$$

Or, alternatively, a ring homomorphism:
$$\begin{aligned} \mathbb{Z}[G] &\longrightarrow \mathrm{End}_{\mathbb{Z}}(M) \\ \left(\sum a_\sigma \sigma\right) &\longmapsto \left(m \mapsto \sum a_\sigma \, \sigma \cdot m\right) \end{aligned}$$

$\in M$

$\mathbb{Z} \circlearrowleft M$

Facts (A) The collection of all G-modules form an abelian category $\underset{\sim}{\mathrm{Mod}}_G$.

(B) The map

$$M \mapsto M^G := \{ m \in M ;\ g \cdot m = m \ \forall g \in G \}$$

is a left exact functor from Mod_G to the category of abelian groups $\underset{\sim}{\mathrm{Ab}}$

(C) We will define functors

$$H^p(G, \_) : \underset{\sim}{\mathrm{Mod}}_G \to \underset{\sim}{\mathrm{Ab}}$$

which are right derived functors of the functor in (B)

The idea Consider G a group, M a G-module & N a submodule.

Then $$0 \to N \overset{i}{\hookrightarrow} M \overset{\pi}{\twoheadrightarrow} M/N \to 0$$

is exact. So,

$$\begin{array}{ccccccc} 0 \to & N^G & \to & M^G & \to & (M/N)^G & \text{is exact} \\ & \| & & \| & & \| & \\ & H^0(G,N) & & H^0(G,M) & & H^0(G,M/N) & \end{array}$$

and we want a l.e.s.

$$0 \to H^0(G,N) \to H^0(G,M) \to H^0(G,M/N) \to H^1(G,N) \to H^1(G,M) \to H^1(G,M/N) \to \cdots$$

Slogan: $H^1(G,N)$ should measure the failure of extending fixed points in M/N to fixed points in M.

If we choose $[a] \in (M/N)^G$, $ga - a \in N \ \forall g \in G$ and $ga - a = 0 \ \forall g \in G \iff a \in M^G$.

Now, observe that the map $f: G \longrightarrow N$, $g \mapsto ga - a$ satisfies

$$f(g\tilde{g}) = (g\tilde{g})\cdot a - a = g\cdot(\tilde{g}\cdot a) - a = g\cdot(f(\tilde{g}) + a) - a$$
$$= g\cdot f(\tilde{g}) + \underbrace{g\cdot a - a}_{= f(g)}$$

2 Group cohomology

Given a group G and a G-module M, define the n-cochains by

- $C^0(G,M) := M$
- $C^n(G,M) := \mathrm{Hom}(\underbrace{G\times\cdots\times G}_{n}, M)$, $n \geq 1$

and the boundary maps δ_n by

- $\delta_0 : C^0(G,M) = M \longrightarrow C^1(G,M)$

$$m \mapsto \left(g \mapsto g \cdot m - m \right)$$

- $\delta_n : C^n(G,M) \longrightarrow C^{n+1}(G,M)$

$$f \mapsto \delta_n f : \underbrace{G \times \cdots \times G}_{n+1} \longrightarrow M$$

where
$$\delta_n f \left(g_1, \dots, g_{n+1} \right) := g_1 f(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f\left(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1} \right) + (-1)^{n+1} f\left(g_1, \dots, g_n \right)$$

Then $\delta_{n+1} \circ \delta_n$ is the zero map & we can introduce the corresponding cohomology groups...

Definition / Proposition Given G and M as before, the elements of $Z^n(G,M) := \operatorname{Ker}(\delta_n)$ are called n-cocycles. Since $\operatorname{im}(\delta_{n-1}) \subset \operatorname{Ker}(\delta_n)$ the elements of the subset $B^n(G,M) : \operatorname{im}(\delta_{n-1})$ are called n-coboundaries, where $B^0(G,M) = \{0\}$.

We can thus define the n-th cohomology group $H^n(G,M)$ of G with coefficients in M as the quotient

$$H^n(G,M) := Z^n(G,M)/B^n(G,M)$$

In particular,

$$H^0(G,M) = \mathrm{Ker}(\delta_0) = M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$$

morphisms of G-modules

Question: How is this related to Galois theory?

We want to look at $G = \mathrm{Gal}(L/K)$ and $M = L^\times$ or L and the action

$$\begin{aligned} \mathrm{Gal}(L/K) \times M &\to M \\ (\sigma, a) &\mapsto \sigma \cdot a := \sigma(a) \end{aligned}$$

③ Hilbert's theorem 90

Proposition 1 Let L/K be a Galois extension with Galois group G. Then $H^1(G, L^\times) = \{0\}$ and $H^1(G, L) = \{0\}$.

In other words, letting $M = L^\times$ or L, we have that every 1-cocycle $f : G \to M$ is cohomologous to a 1-coboundary $g : G \to M$.

- f is a 1-cocycle $\Leftrightarrow \delta_1(f) = 0$

  $\Leftrightarrow f(\sigma\tau) = \sigma \cdot f(\tau) + f(\sigma)$ if $M = L$ OR

  $f(\sigma\tau) = (\sigma \cdot f(\tau)) f(\sigma)$ if $M = L^\times$ The abelian operation + in $L^\times$ is the product!

- g is a 1-coboundary $\Leftrightarrow \exists\, a \in M$ s.t.

  $g(\sigma) = \sigma \cdot a - a \quad \forall \sigma \in G$ if $M = L$

  OR $g(\sigma) = \sigma(a)/a$ if $M = L^\times$

Thus, an equivalent statement is:

Given a cocycle $f : G \to M$, $\exists\, a \in M$ s.t.

$f(\sigma) = \sigma \cdot a - a \quad \forall \sigma \in G.$ (if $M = L$)

(OR $\sigma \cdot a / a$ if $M = L^\times$)

Theorem (Hilbert 90) Let L/K be a cyclic extension and let $Gal(L/K) = \langle \sigma \rangle$. Pick $\alpha \in L$. Then

(i) $N_{L/K}(\alpha) = 1 \iff \alpha = \dfrac{\sigma(a)}{a}$ for some $a \in L$

(ii) $Tr_{L/K}(\alpha) = 0 \iff \alpha = \sigma(a) - a$

Proof for both (i) & (ii), the implication ($\Leftarrow$) is "easy".

(i) Assume that $\alpha \in L$ is s.t. $N(\alpha) = 1$.

Then $f: G \longrightarrow L^\times$ is a 1-cocycle

$$\begin{aligned} id &\mapsto 1 \\ \sigma &\mapsto \alpha \\ \sigma^i &\mapsto \alpha\,\sigma(\alpha) \cdots \sigma^{i-1}(\alpha) \end{aligned}$$

But $H^1(G, L^\times) = \{0\}$. So, $\exists\ a \in L^\times \subset L$ s.t. $f(\sigma^i) = \dfrac{\sigma^i(a)}{a}\ \forall i$. Thus, $\alpha = f(\sigma) = \dfrac{\sigma(a)}{a}$.

(ii) Pick $\alpha \in L$ w/ $\mathrm{Tr}(\alpha) = 0$. Then the map

$$
\begin{aligned}
g: G &\longrightarrow L \\
\mathrm{id} &\longmapsto 0 \\
\sigma &\longmapsto \alpha \\
\sigma^i &\mapsto \alpha + \sigma(\alpha) + \cdots + \sigma^{i-1}(\alpha)
\end{aligned}
$$

is a 1-cocycle and since $H^1(G, L) = \{0\}$, $\exists\, a \in L$ s.t. $g(\sigma^i) = \sigma^i(a) - a \quad \forall i$

Thus, $\alpha = g(\sigma) = \sigma(a) - a$ as claimed.

$\boxtimes$

Applications (recall from Lecture # 6)

1) Let K be a field, assume that $\mu_n \subset K$ (n prime to char K)

If L/K is cyclic of degree n, then $L = K(\alpha)$, where $\alpha^n = a \in K$

Why? Write $G = \langle \sigma \rangle$ and take $\zeta \in \mu_n$ primitive. Then $N(\zeta) = 1$. Thus, $\exists\, \alpha \in L$ s.t. $\sigma(\alpha) = \zeta\alpha$. Then $\zeta^i \alpha$ (for $i = 1, \ldots, n$) are

n distinct conjugates of α $\Rightarrow$ $L = K(\alpha)$.

Moreover, $\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n$

$\Rightarrow$ $\alpha^n = a$ for some $a \in K$.

2) K a field of char $= p$, L/K cyclic of degree p.

Then $L = K(\alpha)$, where $\alpha^p - \alpha - a = 0$ for some $a \in K$.

Why? $Tr(1) = p \cdot 1 = 0 \Rightarrow 1 = \sigma(\alpha) - \alpha$ for some $\alpha \in L$ and such α does the job.

Back to Proposition 1

- L/K Galois, $G = Gal(L/K)$.

Pick $f \in Z^1(G, L^\times)$. We want to show that $f \in B^1(G, L^\times)$.

Let $n = |G|$ and write $G = \{\sigma_1, \dots, \sigma_n\}$

Then $\chi := \sum_{i=1}^{n} f(\sigma_i)\sigma_i$ is a non-trivial character $L \to L^\times$ since $f(\sigma_i) \neq 0 \ \forall i$ (Dedekind).

This means that there exists some $c \in L$ such that $\sum_{i=1}^{n} f(\sigma_i)\, \sigma_i(c) \neq 0$

Let $b \in L^\times$ be this non-zero element. Then, given any $\tau \in G$ we have that

$$\tau(b) = \sum_{i=1}^{n} \tau\big(f(\sigma_i)\big)(\tau\sigma_i)(c) \Rightarrow$$

$$f(\tau)\,\tau(b) = \sum_{i=1}^{n} f(\tau)\,\tau\big(f(\sigma_i)\big)(\tau\sigma_i)(c)$$

$$= \sum_{i=1}^{n} f(\tau\sigma_i)(\tau\sigma_i)(c) = b$$

$$\Rightarrow f(\tau) = \frac{b}{\tau(b)}$$

Thus, letting $a = b^{-1}$, we have shown that $\forall\, \tau \in G$, $f(\tau) = \frac{\tau(a)}{a}$

So, f is a 1-coboundary.

Back to theorem (Hilbert 90, multiplicative)

- For a finite cyclic group G and a G-module M, $H^1(G,M) \simeq \mathrm{Ker}(N_M) / I_G(M)$, where

$$N_M : M \longrightarrow M^G, \quad m \longmapsto \sum_{g \in G} g \cdot m$$

and $I_G(M)$ is the submodule of M obtained by restricting to the augmentation ideal of $\mathbb{Z}[G]$

i.e. $I_G(M) = \{ g \cdot m - m = (g-1)\cdot m \ ; \ m \in M \ \& \ g \in G \}$.

- Proposition 1 $\Rightarrow$ L/K cyclic Galois, $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ then $H^1(G, L^\times) = 0$. So, $\mathrm{Ker}(N_{L/K}) = \mathrm{Im}\left(a \mapsto \frac{\sigma(a)}{a} \right)$

i.e. $N_{L/K}(\alpha) = 1 \iff \alpha = \frac{\sigma(a)}{a}$ for some $a \in L$

Consequence (rational points on S^1)

Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $G = \mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z}$.

A point $\alpha = a + bi \in L$ has norm $1 \iff \underbrace{a^2 + b^2}_{\alpha\bar{\alpha}} = 1$

($\leftrightarrow (a,b) \in S^1$ w/ rational coordinates)

But then, by Hilbert 90, $\exists\, \beta = c + di \in \mathbb{Q}(i)$ such that

$$a + bi = \frac{c+di}{c-di} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2+d^2}\, i$$

So, we obtain a parametrization of the rational points in S^1.