Cohomology I: $H^1(G, A)$

Aim Lecture: Intro. Galois cohomology.

Today G = finite group

G-actions Let A = group &
$\mathrm{Aut}\, A$ = group of group automorphisms of A.

Defn 1: A *G-action on the group A* is a group hom $\varphi: G \to \mathrm{Aut}\, A$. Since $\mathrm{Aut}\, A \leq \mathrm{Hom}(A, A)$, G acts on the set A & we also write

$$g.a := [\varphi(g)](a).$$
$$\uparrow_G \quad \uparrow_A$$

Eg. 1. Let K/F = finite Galois ext^n, $G = \mathrm{Gal}(K/F)$
Then G acts on $GL_n(K)$ = group of invertible matrices / K by $g.(\alpha_{ij}) = (g(\alpha_{ij}))$
Why? Check corresp. $\varphi(g) \in \mathrm{Aut}\, GL_n(K)$

$$g.[(\alpha_{ij})(\beta_{rs})]_{is} \overset{??}{=} [g.(\alpha_{ij})]_{ir}[g.(\beta_{rs})]$$

$$g.\left[\left(\sum_j \alpha_{ij}\beta_{js}\right)\right] \quad \left(\sum_j g(\alpha_{ij})g(\beta_{js})\right)_{is}$$

1-cocycles Let G act on group A

Defn 2: A *1-cocycle of G with values in A* is a fn $\alpha_\bullet: G \to A: g \mapsto \alpha_g$ satisfying

$$\alpha_{gh} = \alpha_g(g.\alpha_h), \quad \forall g, h \in G.$$

The set of these is denoted $Z^1(G,A)$.

N.B. $\alpha_* \in Z^1(G,A) \Rightarrow \alpha_1 = 1$.

Lemma 1: (a) Constant map $1_*: G \to 1$ is a 1-cocycle called the trivial 1-cocycle.

(b) If A is abelian, then $Z^1(G,A)$ is an abelian group under pointwise multⁿ.

Proof: (a) easy. (b) $Z^1(G,A) \leq$ abelian group of fns $G \to A$ so just check closure axioms

e.g. $\alpha_*, \beta_* \in Z^1(G,A) \Rightarrow$

$$(\alpha\beta)_{gh} = \alpha_{gh}\beta_{gh} = \alpha_g(g.\alpha_h)\,\beta_g(g.\beta_h)$$
$$= (\alpha\beta)_g\,(g.(\alpha\beta)_h)$$

Lemma 2: (a) For any $a \in A$, $\alpha_* \in Z^1(G,A)$

$a.\alpha_*: G \to A$ defined by

$$(a.\alpha)_g = a\,\alpha_g\,(g.a^{-1})$$

is a 1-cocycle.

(b) This defines an A-action on set $Z^1(G,A)$

(c) If A is abelian,

$$\varphi: A \to Z^1(G,A): a \mapsto a(g.a^{-1})$$

is a group hom. & $a \in A$ acts on $Z^1(G,A)$ by multⁿ by $\varphi(a)$. Write

$B^1(G,A) = \operatorname{im}\varphi \leq Z^1(G,A)$.

Proof: easy computations e.g. $a.\alpha_* \in Z^1(G,A)$

$$\because\ (a.\alpha)_{gh} = a\,\alpha_{gh}((gh).a^{-1})$$
$$= a\,\alpha_g(g.\alpha_h)\,g.(h.a^{-1})$$

$$= a\,\alpha_g (g.a^{-1})(g.a)(g.\alpha_h)\, g.(h.a^{-1})$$
$$= (a.\alpha)_g\; g.(a.\alpha)_h$$

1-cohomology set G acts on group A

Defn 3: $\alpha_*, \beta_* \in Z^1(G,A)$ are 1-cohomologous if $\beta_* = a.\alpha_*$ for some $a \in A$. The 1-cohomology set of G with values in A is $H^1(G,A)$ = set of A-orbits in $Z^1(G,A)$. It comes with distinguished elt, the orbit of 1_*.

N.B. A abelian $\Rightarrow$ $H^1(G,A)$ = group $\dfrac{Z^1(G,A)}{B^1(G,A)}$

Propⁿ: Suppose $G = \langle g \rangle \simeq \mathbb{Z}/n$. Then

(a) $\alpha_* \in Z^1(G,A)$ is uniquely determined by $\alpha_g \in A$.

(b) α_g satisfies

(t) $\quad \alpha_g (g.\alpha_g)(g^2.\alpha_g) \cdots (g^{n-1}.\alpha_g) = 1$

(c) Any $\alpha_g \in A$ satisfying (t) determines a 1-cocycle.

Proof: ex e.g. for (b)

$1 = \alpha_1 = \alpha_{g^n} = \alpha_{g^{n-1}}(g^{n-1}.\alpha_g) = \ldots = LHS(t)$

Norms Let K/F = finite Galois extⁿ, Galois group G so

G acts on abelian group $GL_1(F) = K^*$.

Prop^n-Def^n: The norm of $\alpha \in K$ over F is $N_{K/F}(\alpha) := \prod_{g \in G} g(\alpha)$.

Note $N_{K/F}(\alpha) \in K^G = F$. The norm map $N_{K/F}: K^* \to F^*$ is a group hom

Rem ①: If G cyclic, Prop^n ⑥ $\Rightarrow$ 1-coycles in $Z^1(G, K^*)$ correspond to norm 1 elts of K.

② $\alpha \in F \Rightarrow N_{K/F}(\alpha) = \alpha^{[K:F]}$.

Eg. 2 def, char $\neq 2$; non-square $K = F(\sqrt{d})$.

$G = Gal(K/F) = \{1, g\}$

$N_{K/F}: K^* \longrightarrow F^*$:

$a, b \in \mathbb{Q}$, $a + b\sqrt{d} \longmapsto (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2$.

sub e.g. $d = -1$, $F = \mathbb{R} \Rightarrow Z^1(G, \mathbb{C}^*) = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$

$B^1(G, A) = \{\frac{z}{\bar{z}} \mid z \in \mathbb{C}^*\} = Z^1(G, \mathbb{C}^*)$

$\Rightarrow H^1(G, \mathbb{C}^*) = 1$.

sub e.g. 2: $K = \mathbb{Q}$ Number theorists ask $\mathbb{Q}$ like "For which $c \in \mathbb{Q}^*$ can you solve for a, b in $a^2 - db^2 = c$?" i.e. what's im $N_{K/\mathbb{Q}}$?

This viewpoint immediately $\Rightarrow$ im $N_{K/\mathbb{Q}}$ is a subgroup of $\mathbb{Q}^*$.

Thm: $p/q \in \mathbb{Q}^*$ w th g.c.d. $(p, q) = 1$ is of form $a^2 + b^2$, $a, b \in \mathbb{Q}$ iff the prime

factors of p & q $\equiv 3 \pmod 4$
occur an even number of times.