Modern Classical Algebra

John C. Moore

Chapter 10

Notes by Peter May

Chapter 10: Homology of monoids and groups

This chapter will introduce the homology and cohomology theories of monoids and groups. We will first discuss the general theory and then study the simplest special case, that of free monoids and groups. Finally, we will treat the extension problem for modules and groups.

§1. Homology and cohomology theories.

In this section, we introduce the concepts of modules over monoids and groups and of monoid and group rings. Since the latter have natural structures as augmented rings, it will be convenient to define homology and cohomology as in section 3 of chapter 9. We will then derive an alternative characterization in terms of the functors A_G and A^G.

Throughout this chapter, the letter G will denote a monoid with unit 1.

<u>Definition 1.1</u>: Let A be an abelian group. A is said to be a G-module if there exists a map $\Phi: G \times A \to A$, denoted by $\Phi(\sigma, a) = \sigma a$, $\sigma \in G$, $a \in A$, such that:

i) $1a = a$

ii) $\sigma(a + a') = \sigma a + \sigma a'$

iii) $(\sigma\tau)a = \sigma(\tau a)$

<u>Definition 1.2</u>: Let K be a commutative ring. Let $K(G)$ denote the free K-module generated by the elements of G. If $\lambda = \sum_{\sigma \in G} k_\sigma \sigma$ and $\lambda' = \sum_{\tau \in G} k'_\tau \tau$ are elements of $K(G)$, define the product $\lambda\lambda'$ as $\lambda\lambda' = \sum_\sigma \sum_\tau k_\sigma k'_\tau (\sigma\tau)$. The resulting ring $K(G)$ is called the monoid

ring of G with coefficients in K.

If Z denotes the ring of integers, we observe that a G-module A may be given a structure of Z(G)-module by defining $\lambda a = \sum_{\sigma \in G} n_\sigma(\sigma a)$ if $\lambda = \sum_{\sigma \in G} n_\sigma \sigma \in Z(G)$. Conversely, a Z(G)-module has a unique induced structure as a G-module. In the following, if $\Lambda = Z(G)$, we will use the notations $A \otimes_G B$, $\mathrm{Hom}_G(A, B)$, $\mathrm{Tor}_n^G(A, B)$, and $\mathrm{Ext}_G^n(A, B)$ instead of $A \otimes_\Lambda B$, etc. Observe that the map $\epsilon: Z(G) \to Z$ defined by $\epsilon(\sum_{\sigma \in G} n_\sigma \sigma) = \sum_{\sigma \in G} n_\sigma$ is a ring epimorphism. ϵ is called the (unit) augmentation morphism.

<u>Definition 1.3</u>: The homology (resp., cohomology) groups of the augmented ring $(Z(G), \epsilon, Z)$ with coefficients in a right (resp., left) G-module A are called the homology (resp., cohomology) groups of G with coefficients in A.

<u>Remarks 1.4</u>: ϵ may be used to furnish Z with a structure as left and right G-module by defining $\sigma n = \epsilon(\sigma)n = n = n\epsilon(\sigma) = n\sigma$. In general, if A is an Abelian group, A may be given a structure of G-module in a similar manner. We then say that G acts trivially on A. If A is to be regarded as a left (resp., right) G-module with trivial action, we write ${}_\epsilon A$ (resp., A_ϵ). If A is a left G-module, we will use the notations $H_n(G, A) = \mathrm{Tor}_n^G(Z_\epsilon, A)$ and $H^n(G, A) = \mathrm{Ext}_G^n({}_\epsilon Z, A)$ and similarly for right g-modules. We recall that the homology and cohomology theories were axiomatized in chapter 9, section 3.

<u>Remarks 1.5</u>: If $I = \mathrm{Ker}(\epsilon)$, then I is a two-sided Z(G)-ideal, called the augmentation ideal of Z(G). $\sigma - 1 \in I$ for all $\sigma \in G$ and if $\sum n_\sigma \sigma \in I$, then $\sum_{\sigma \in G} n_\sigma \sigma = \sum_{\sigma \in G} n_\sigma(\sigma - 1)$ since $\sum_{\sigma \in G} n_\sigma = 0$. Thus

$\{\sigma - 1 \mid \sigma \in G\}$ is a set of generators for I over Z.

<u>Definition 1.6</u>: Let A be a (left) G-module. $A^G = \{a \mid a \in A, \sigma a = a$ for all $\sigma \in G\}$. If $\Phi: A \to B$ is a morphism of G-modules and $a \in A^G$, then $\Phi(a) = \Phi(\sigma a) = \sigma\Phi(a)$ for all $\sigma \in G$, and $\Phi(A^G) \subset B^G$. Thus A^G is an additive covariant functor of (left) G-modules with values as Z-modules.

<u>Proposition 1.7</u>: Let A be a (left) G-module. If $a \in A^G$, let $f_a \in \mathrm{Hom}_G({}_\epsilon Z, A)$ be given by $f_a(1) = a$. Then $\Phi(a) = f_a$ defines a Z-isomorphism $A^G \to \mathrm{Hom}_G({}_\epsilon Z, A)$, and Φ establishes a natural equivalence of functors of (left) G-modules A.

<u>Proof</u>: Φ is clearly a monomorphism, and if $f \in \mathrm{Hom}_G({}_\epsilon Z, A)$, $f(1) = f(\sigma 1) = \sigma f(1)$ for all $\sigma \in G$, so that $f(1) \in A^G$. The rest is clear.

<u>Corollary 1.8</u>: A^G is a left exact functor of A; the right derived functors of A^G provide a cohomology theory for G.

Definition 1.6′: Let A be a (left) G-module. $A_G = A/IA$, where I is the augmentation ideal. If $\Phi: A \to B$ is a morphism of G-modules, then $\Phi(IA) \subset IB$ and Φ induces a morphism $A_G \to B_G$. Thus A_G is an additive covariant functor of (left) G-modules with values as Z-modules.

<u>Proposition 1.7′</u>: Let A be a (left) G-module. The morphism $\Phi: Z_\epsilon \otimes_G A \to A_G$ defined by $\Phi(n \otimes a) = n\bar{a}$, where $\bar{a}$ is the natural image of a in A_G, is a Z-isomorphism and establishes a natural equivalence of functors of (left) G-modules A.

<u>Proof</u>: Φ is clearly an epimorphism. Let $x \epsilon \ker \Phi$, and write $x = 1 \otimes a$. $\bar{a} = 0$, so $a = \sum_i \lambda_i a_i$, $\lambda_i \epsilon I$, $a_i \epsilon A$. $x = \sum_i 1 \otimes \lambda_i a_i = \sum_i 1\lambda_i \otimes a_i = 0$, since $Z_\epsilon I$ is clearly zero. The rest is obvious.

<u>Corollary 1.8'</u>: A_G is a right exact functor of A; the left derived functors of A_G provide a homology theory for G.

§2. Standard resolutions of Z

It is usually most convenient to calculate homology and cohomology theories of monoids and groups by means of resolutions of Z. In this section we will obtain certain standard resolutions of Z for arbitrary monoids and groups.

Let G be a monoid. For $n \geq 0$, let $X_n(G)$ be the free G-module generated by all ordered sets $[\sigma_1, \ldots, \sigma_n]$, $\sigma_i \varepsilon G$, where $X_o(G) \cong Z(G)$ is generated by the symbol $[\ ]$. Define a differentiation by

$$d_n[\sigma_1, \ldots, \sigma_n] = \sigma_1[\sigma_2, \ldots, \sigma_n] + \sum_{r=1}^{n-1} (-1)^r[\sigma_1, \ldots, \sigma_r\sigma_{r+1}, \ldots, \sigma_n] + $$
$$+ (-1)^n[\sigma_1, \ldots, \sigma_{n-1}],\ n \geq 1,$$

where $d_1[\sigma_1] = \sigma_1[\ ] - [\ ]$. Define an augmentation $e\colon X_o(G) \to Z$ by $e[\ ] = 1$. Simple calculations give that $d_{n-1}d_n = 0$, $n > 1$, and $ed_1 = 0$. To show that the resulting complex $X(G)$ is actually a resolution of Z, define the Z-morphisms (not G-morphisms)

$s_{-1}\colon Z \to X_o(G)$, $s_n\colon X_n(G) \to X_{n-1}(G)$, $n \geq 0$, by

$s_{-1}(1) = [\ ]$, $s_n(\sigma[\sigma_1, \ldots, \sigma_n]) = [\sigma, \sigma_1, \ldots, \sigma_n]$. Then

$es_{-1} = i_Z$, $s_{-1}e + d_1s_o = i_{X_o(G)}$, $d_{n+1}s_n + s_{n-1}d_n = i_{X_n(G)}$ so that the complex $\ldots \to X_n(G) \to \ldots \to X_o(G) \to Z \to 0 \to \ldots$ is null homotopic:

$$H_n(X(G)) = 0,\ n > 0,\ H_o(X(G)) = Z.$$

<u>Definition 2.1</u>: The resolution of Z obtained above is called the standard non-homogeneous free resolution of Z.

Now let A be a right G-module. $H_n(G, A) = H_n(A \otimes_G X(G))$. An element of $A \otimes X_n(G)$ is called a (standard) n-chain.

$$d_n(a \otimes [\sigma_1, \dots, \sigma_n]) = a\sigma_1 \otimes [\sigma_2, \dots, \sigma_n] + \sum_{r=1}^{n-1} (-1)^r a \otimes$$

$$\otimes [\sigma_1, \dots, \sigma_r\sigma_{r+1}, \dots, \sigma_n] + (-1)^n a \otimes [\sigma_1, \dots, \sigma_{n-1}].$$

Observe that if G acts trivially on A, $a\sigma_1 = a$, then the homology groups are the same when G operates on the left as when G operates on the right.

If C is a left G-module, the elements of $\mathrm{Hom}_G(X_n(G), C)$ are called (standard) n-cochains. Since a typical n-cochain f is determined by an arbitrary mapping of the base elements $[\sigma_1, \dots, \sigma_n]$ into C, we write $f(\sigma_1, \dots, \sigma_n)$ for the image of $[\sigma_1, \dots, \sigma_n]$. The differentiation d_n on $\mathrm{Hom}_G(X_n(G), C)$ is given by

$$(d_n f)(\sigma_1, \dots, \sigma_{n+1}) = \sigma_1 f(\sigma_2, \dots, \sigma_{n+1}) +$$

$$+ \sum_{r=1}^{n} (-1)^r f(\sigma_1, \dots, \sigma_r\sigma_{r+1}, \dots, \sigma_{n+1}) + (-1)^{n+1} f(\sigma_1, \dots, \sigma_n),$$

$(d_o f)(\sigma) = \sigma c - c$, where $c = f([\ ])$.

Again, if G acts trivially on C, the same cohomology groups are obtained when G acts on the left as when G acts on the right.

Now let G be a group. We transform the standard complex to a homogeneous form. Define

$(\sigma_o, \dots, \sigma_n) = \sigma_o[\sigma_o^{-1}\sigma_1, \dots, \sigma_{n-1}^{-1}\sigma_n]$. Then $\sigma(\sigma_o, \dots, \sigma_n) =$

$= \sigma\sigma_o[\sigma_o^{-1}\sigma^{-1}\sigma\sigma_1, \dots, \sigma_{n-1}^{-1}\sigma^{-1}\sigma\sigma_n] = (\sigma\sigma_o, \dots, \sigma\sigma_n)$, and

$[\sigma_1, \ldots, \sigma_n] = (1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \cdots \sigma_n)$. Thus $X_n(G)$ is the free Z-module generated by the elements $(\sigma_o, \ldots, \sigma_n)$ or the free G-module generated by the elements $(1, \sigma_1, \ldots, \sigma_n)$ with G-action as above. Finally, the differentiation takes the form $d_n(\sigma_o, \ldots, \sigma_n) = \sum_{i=o}^{n} (-1)^i(\sigma_o, \ldots, \hat{\sigma}_i, \ldots, \sigma_n)$, where the $\hat{\sigma}_i$ means that σ_i is to be omitted from the expression. This results from

$$d_n(\sigma_o[\sigma_o^{-1}\sigma_1, \ldots, \sigma_{n-1}^{-1}\sigma_n]) = \sigma_1[\sigma_1^{-1}\sigma_2, \ldots, \sigma_{n-1}^{-1}\sigma_n] + \sum_{r=1}^{n-1} (-1)^r\sigma_o[\sigma_o^{-1}\sigma_1, \ldots, \sigma_{r-1}^{-1}\sigma_{r+1}, \ldots, \sigma_{n-1}^{-1}\sigma_n] + (-1)^n\sigma_o[\sigma_o^{-1}\sigma_1, \ldots, \sigma_{n-Z}^{-1}\sigma_{n-1}].$$

Definition 2.2: The complex $X_n(G)$ as described above is called the standard homogeneous free resolution of Z.

Remark 2.3: A second fundamental difference between groups and monoids is that for a group G, the map $\Phi: G \to G$ defined by $\Phi(x) = x^{-1}$ gives an isomorphism of Z(G) with Z(G)*, the opposite ring. Thus if A is a left G-module, A may be given a structure as right G-module by defining $a\sigma = \sigma^{-1}a$. Hence we need use only left G-modules in constructing the homology and cohomology theories of groups.

We now will give a brief general discussion of the first homology and cohomology groups, using the standard non-homogeneous resolution of Z.

Let G be a monoid, A a left G-module. The exact sequence $0 \to I \to Z(G) \to Z_\epsilon \to 0$ implies the exact sequence

$0 = \mathrm{Tor}_1^G(Z(G), A) \to \mathrm{Tor}_1^G(Z_\epsilon, A) \to I \otimes_G A \to Z(G) \otimes_G A$. Thus $H_1(G, A) \cong \mathrm{Ker}\,(I \otimes_G A \to Z(G) \otimes_G A)$. If G acts trivially on A, we have, for $(\sigma-1) \otimes a \in I \otimes_G A$, $(\sigma-1) \otimes a \to 1 \otimes (\sigma-1)a = 0 \in Z(G) \otimes_G A$. Thus $H_1(G, A) \cong I \otimes_G A \cong I \otimes_G ({}_\epsilon Z \otimes_Z A) \cong (I \otimes_G {}_\epsilon Z) \otimes_Z A$. Since $I \otimes_G {}_\epsilon Z \cong {}^I/I^2$, $H_1(G, A) \cong {}^I/I^2 \otimes_Z A$.

Now let G be a group. Let $[G, G]$ denote the commutator subgroup of G.

<u>Lemma 2.4</u>: ${}^I/I^2 \cong {}^G/[G, G]$

<u>Proof</u>: Define $G \to {}^I/I^2$ by $\sigma \to \overline{\sigma-1} = \sigma - 1 \pmod{I^2}$. Since $\sigma\tau - 1 = (\sigma - 1)(\tau - 1) + (\sigma - 1) + (\tau - 1)$, we obtain a morphism of Abelian groups Φ: ${}^G/[G, G] \to {}^I/I^2$, $\Phi(\bar{\sigma}) = \overline{\sigma - 1}$.
Define $I \to {}^G/[G, G]$ by $\sigma - 1 \to \bar{\sigma}$.
$(\sigma - 1)(\tau - 1) = (\sigma\tau - 1) - (\sigma - 1) - (\tau - 1) \to \overline{\sigma\tau\sigma^{-1}\tau^{-1}} = 0$, so we obtain ψ: ${}^I/I^2 \to {}^G/[G, G]$, $\psi(\overline{\sigma - 1}) = \bar{\sigma}$. Since $\psi\Phi$ and $\Phi\psi$ are identity maps, this gives the result.

<u>Proposition 2.5</u>: If G is a group, A a left G-module with trivial G-action, then $H_1(G, A) \cong {}^G/[G, G] \otimes_Z A$.

We turn now to the first cohomology group and let G be a monoid, C a left G-module. A 1-cochain is a mapping $F: G \to C$ since $X_1(G)$ is G-free on generators $[\sigma]$, $\sigma \in G$).
$df(\sigma, \tau) = \sigma f(\tau) - f(\sigma\tau) + f(\sigma)$, so f is a 1-cocycle if and only if $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$. A 1-cocycle is also called a crossed homomorphism. If $h \in \mathrm{Hom}_G(X_0(G), C) \cong \mathrm{Hom}_G(Z(G), C)$ corresponds to

$c \in C$, then $(dh)(\sigma) = \sigma c - c$. $f: G \to C$ is a 1-coboundary if and only if $f(\sigma) = \sigma c - c$ for some $c \in C$. Such an f is also called a principal crossed homomorphism. If G acts trivially on C, then $H^1(G, C)$ is the group of monoid morphisms $f: G \to C$, that is, the set of maps f such that $f(\sigma\tau) = f(\sigma) + f(\tau)$, where $(f + g)(\sigma) = f(\sigma) + g(\sigma)$. If G is a group, each such map will vanish on $[G, G]$ (since C is an Abelian group).

Proposition 2.5′: If G is a group, C a left G-module with trivial G-action, then $H^1(G, C) \cong \mathrm{Hom}_Z(G/[G, G], C)$.

§3. The mapping theorem

We return briefly to the general theory of augmented rings. Let $(\Lambda, \epsilon_\Lambda, Q_\Lambda)$ and $(\Gamma, \epsilon_\Gamma, Q_\Gamma)$ be left augmented rings with augmentation ideals I_Λ and I_Γ. A ring morphism $\Phi: \Lambda \to \Gamma$ is a morphism of augmented rings if $\Phi(I_\Lambda) \subset I_\Gamma$. Let $\psi: Q_\Lambda \to Q_\Gamma$ be the morphism induced by a morphism $\Phi: \Lambda \to \Gamma$ of augmented rings. The diagram

$$\begin{array}{ccc} \Lambda & \xrightarrow{\epsilon_\Lambda} & Q_\Lambda \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ \Gamma & \xrightarrow[\epsilon_\Gamma]{} & Q_\Gamma \end{array}$$

commutes. Thus $\psi(\lambda x) = (\Phi\lambda)(\psi x)$, $\lambda \epsilon \Lambda$, $x \epsilon Q_\Lambda$, so that ψ is a Λ-morphism where Q_Γ is given a structure as Λ-module by means of Φ. Let X_Λ be a Λ-projective resolution of Q_Λ, X_Γ a Γ-projective resolution of Q_Γ. $\Gamma \otimes_\Lambda X_\Lambda$ is a Γ-projective complex over $\Gamma \otimes_\Lambda Q_\Lambda$ (since $\mathrm{Hom}_\Lambda(P, C) = \mathrm{Hom}_\Gamma(\Gamma \otimes_\Lambda P, C)$, where P is Λ-projective, is an exact functor of left Γ-modules C). Let $g: \Gamma \otimes_\Lambda Q_\Lambda \to Q_\Gamma$ be defined by $g(\gamma \otimes x) = \gamma(\psi x)$. By propositions 1.7 and 1.8 of chapter 8, there exists a translation $\tilde{g}: \Gamma \otimes_\Lambda X_\Lambda \to X_\Gamma$ lying over g, and $\tilde{g}$ is unique up to a homotopy. $\tilde{g}$ induces morphisms

$$F_n^\Phi: H_n(A \otimes_\Lambda X_\Lambda) = H_n(A \otimes_\Gamma (\Gamma \otimes_\Lambda X_\Lambda)) \to H_n(A \otimes_\Gamma X_\Gamma)$$

$$F_\Phi^n: H^n(\mathrm{Hom}_\Gamma(X_\Gamma, C)) \to H^n(\mathrm{Hom}_\Gamma(\Gamma \otimes_\Lambda X_\Lambda, C)) = H^n(\mathrm{Hom}_\Lambda(X_\Lambda, C))$$

defined for right Γ-modules A and left Γ-modules C.

Theorem 3.1: F_n^{Φ} is an isomorphism for all n and for all right Γ-modules A if and only if

i) $g: \Gamma \otimes_{\Lambda} Q_{\Lambda} \to Q_{\Gamma}$ is an isomorphism

ii) $\mathrm{Tor}_n^{\Lambda}(\Gamma, Q_{\Lambda}) = 0$ for $n > 0$.

If i) and ii) hold, then F_{Φ}^n is also an isomorphism for all n and for all left Γ-modules C and $\Gamma \otimes_{\Lambda} X_{\Lambda}$ is a Γ-projective resolution of Q_{Γ}.

Proof: If F_n^{Φ} is always an isomorphism, conditions i) and ii) result from taking $A = \Gamma$. Conversely, if i) and ii) hold, then $\Gamma \otimes_{\Lambda} X_{\Lambda}$ is a projective resolution for Q_{Γ}, where X_{Λ} is any Λ-projective resolution of Q_{Λ}. This implies the conclusions.

Now let G and G' be monoids and let $\Phi: G' \to G$ be a morphism of monoids. Φ induces a morphism $\Phi: Z(G') \to Z(G)$ and if ϵ and ϵ' are the respective unit augmentations, $\epsilon\Phi = \epsilon'$. Thus Φ is a morphism of augmented rings and morphisms

$$F_n^{\Phi}: H_n(G', A) \to H_n(G, A)$$

$$F_{\Phi}^n: H^n(G, C) \to H^n(G', C)$$

are defined for right G-modules A and left G-modules C.

Corollary 3.2: F_n^{Φ} is an isomorphism for all n and for all right G-modules A if and only if

i) $g: Z(G) \otimes_{G'} {}_{\epsilon'}Z \to Z$ given by $g(x \otimes q) = \epsilon(x)q$ is an isomorphism.

ii) $H_n(G', Z(G)) = \mathrm{Tor}_n^{G'}(Z(G), {}_{\epsilon'}Z) = 0$ for $n > 0$.

If i) and ii) hold then F_Φ^n is an isomorphism for all n and all left G-modules C, and $Z(G) \otimes_{G'} X$ is a G-projective resolution of A for any G'-projective resolution of X of Z.

Remarks 3.3: Since Z(G) and Z(G') are both left and right augmented rings, similar results hold for left G-modules A and right G-modules C. Also, condition i) will hold whenever $\Phi: G' \to G$ is an epimorphism: g will clearly be an epimorphism; if

$x \otimes q \in \ker g$, $x = \Sigma n_\sigma \sigma$, then $\Sigma n_\sigma = 0$

and $x \otimes q = \Sigma n_\sigma \sigma \otimes q$

$= \Sigma n_\sigma \Phi(\tau) \otimes q$ for some elements $\tau \in G'$

$= \Sigma n_\sigma 1_G \tau \otimes q$ by G' action on Z(G)

$= \Sigma n_\sigma 1_G \otimes \tau q$

$= \Sigma n_\sigma 1_G \otimes q = 0$ by G' action on Z.

Proposition 3.4: Let G be a group, G' a monoid contained in G and such that $\sigma \in G$ implies $\sigma = \alpha^{-1}\beta$, $\alpha \in G'$, $\beta \in G'$. Then if $\Phi: G' \to G$ is the inclusion map, F_n^Φ and F_Φ^n are isomorphisms and if X is a G'-projective resolution of Z, then $Z(G) \otimes_{G'} X$ is a G-projective resolution of Z.

Proof: We must verify conditions i) and ii) of the corollary. For i) it suffices to show $\sigma \otimes 1 = 1_G \otimes 1$ for $\sigma \in G$; but if $\sigma = \alpha^{-1}\beta$, $\alpha \in G'$, $\beta \in G'$, then

$$\sigma \otimes 1 = \alpha^{-1}\beta \otimes 1 = \alpha^{-1} \otimes \beta 1 = \alpha^{-1} \otimes 1 = \alpha^{-1} \otimes \alpha 1 = 1_G \otimes 1.$$

For ii) we must prove $\mathrm{Tor}_n^{G'}(Z(G), Z) = 0$ for $n > 0$, and, since

Tor commutes with direct limits (by propositions 5.12 and 5.17 of chapter 3), it suffices to prove that $Z(G)$ is the direct limit of a directed system of G'-projective right G'-modules. For $\sigma \varepsilon G$, define the map $f_\sigma: G' \to G$ by $f_\sigma(x) = \sigma x$. f_σ gives a G'-isomorphism of $Z(G')$ with a right G'-submodule A_σ of $Z(G)$. $\sigma \varepsilon A_\sigma$, so $Z(G)$ is the union of the submodules A_σ. Finally, the family $\{A_\sigma\}$ is directed: if $\sigma \varepsilon G$, $\tau \varepsilon G$, $\sigma^{-1}\tau = \alpha^{-1}\beta$, $\alpha \varepsilon G'$, $\beta \varepsilon G'$ and $\sigma\alpha^{-1} = \tau\beta^{-1} = \gamma$, say; then $\sigma x = \gamma(\alpha x) \varepsilon A_\gamma$, $\tau x = \gamma(\beta x) \varepsilon A_\gamma$ for $x \varepsilon G'$ and $A_\sigma \subset A_\gamma$, $A_\tau \subset A_\gamma$.

4. Free monoids and groups

In this section we discuss the homology and cohomology theories of free monoids and groups.

We consider first the non-Abelian case. We need a lemma.

Lemma 4.1: Let G be either the free monoid or the free group generated by a set S. Let A be a left G-module and $f: S \to A$ be an arbitrary mapping. Then there exists one and only one extension of f to a crossed homomorphism of G into A.

Proof: For the case of a free monoid, define

$$\tilde{f}(1) = 0,\ \tilde{f}(s) = f(s),\ \tilde{f}(s_1 \dots s_p s_{p+1}) = s_1 \dots s_p \tilde{f}(s_{p+1}) + \tilde{f}(s_1 \dots s_p).$$

Then a simple induction on the length of τ gives $\tilde{f}(\sigma\tau) = \sigma\tilde{f}(\tau) + \tilde{f}(\sigma)$, $\sigma, \tau \varepsilon G$. For the case of a free group, define

$$\tilde{f}(1) = 0,\ \tilde{f}(s) = f(s),\ \tilde{f}(s^{-1}) = -s^{-1}\tilde{f}(s),\ \tilde{f}(s_1 \dots s_p s_{p+1}) =$$
$$= s_1 \dots s_p \tilde{f}(s_{p+1}) + \tilde{f}(s_1 \dots s_p),$$

where $s_1 \dots s_p s_{p+1}$ is irreducible $(s_i \neq s_{i+1}^{-1},\ 1 \leq i \leq p)$, and $s_i \varepsilon S$ or $s_i^{-1} \varepsilon S$. $\tilde{f}(s^{-1}) = -s^{-1}\tilde{f}(s)$ for $s \varepsilon S$ or $s^{-1} \varepsilon S$. If $\sigma = s_1 \dots s_p$ and τ is of length one, $\tau \neq s_p^{-1}$, $\tilde{f}(\sigma\tau) = \sigma\tilde{f}(\tau) + \tilde{f}(\sigma)$.

If $\tau = s_p^{-1}$,
$$f(\sigma\tau) = \sigma(\tilde{f}(\tau) + \tau\tilde{f}(\tau^{-1})) + \tilde{f}(\sigma\tau)$$
$$= \sigma\tilde{f}(\tau) + s_1 \dots s_{p-1}\tilde{f}(s_p) + \tilde{f}(s_1 \dots s_{p-1})$$
$$= \sigma\tilde{f}(\tau) + \tilde{f}(s_1 \dots s_p) = \sigma\tilde{f}(\tau) + \tilde{f}(\sigma).$$

Again, a simple induction on the length of τ gives $\tilde{f}(\sigma\tau) = \sigma\tilde{f}(\tau) + \tilde{f}(\sigma)$, $\sigma, \tau \varepsilon G$. Clearly if an extension of f to a crossed homomorphism exists, it must have the form indicated, hence the proof is complete.

Proposition 4.2: Let G be the free monoid or free group generated by a set S. Then the augmentation ideal $I \subset Z(G)$ is a free G-module generated by the elements $s - 1$, $s \in S$.

Proof: Let J be the ideal generated by $\{s - 1 \mid s \in S\}$. If $\sigma = s^{-1} \in G$ for the free group, $\sigma - 1 = (-s^{-1})(s - 1) \in J$. Inductively, if $\sigma = s_1 \dots s_p$ is irreducible, $\sigma - 1 = s_1 \dots s_{p-1}(s_p - 1) + (s_1 \dots s_{p-1} - 1) \in J$ and since $\{\sigma - 1 \mid \sigma \in G\}$ generates I, $I = J$. Consider the standard non-homogeneous resolution X of Z. Identifying X_0 with $Z(G)$, $X_0 \to Z$ becomes the augmentation morphism, hence has kernel I. $X_2 \to X_1 \xrightarrow{d_1} I \to 0$ is exact, $d_1[\sigma] = \sigma - 1$. If A is a left G-module, $0 \to \mathrm{Hom}_G(I, A) \to \mathrm{Hom}_G(X_1, A) \to \mathrm{Hom}_G(X_2, A)$ is exact, $\mathrm{Hom}_G(I, A) \cong \mathrm{Ker}\,(\mathrm{Hom}_G(X_1, A) \to \mathrm{Hom}_G(X_2, A))$, the right side being the group of crossed homomorphisms of G into A. If $h \in \mathrm{Hom}_G(I, A)$ corresponds to the crossed homomorphism f, $h(s - 1) = f(s)$. By the lemma, we obtain a G-morphism $I \to A$ for any arbitrary choice of the images of the $s - 1$, and since A is also arbitrary, this implies that the $s - 1$ form a G-base for I.

Corollary 4.3: $0 \to I \to Z(G) \to Z \to 0$ is a G-projective resolution of Z and $H^n(G, A) = H_n(G, A) = 0$, $n > 1$, where G is a free monoid or group.

Remark 4.4: If G is a free monoid or group generated by a non-void set S, I/I^2 is Z-free on the generators $\{\overline{s - 1} \mid s \in S\}$ (as follows from the identity $xy - 1 = (x - 1) + (y - 1) + (x - 1)(y - 1)$, $x, y \in G$).

Thus $H_1(G, Z) \cong \mathrm{Tor}_1^G(Z, Z) \cong I/I^2 \neq 0$ and $\ell \cdot dh_{Z(G)}Z = 1$, $r \cdot dh_{Z(G)}Z = 1$.

We now consider the case of a free Abelian monoid G generated by a finite set $s_1, \ldots, s_n$. $Z(G)$ is isomorphic to the polynomial ring $Z[s_1, \ldots, s_n]$, hence gl. dim $Z(G) = n + 1$ by theorem 3.4 of chapter 9. We will obtain a G-free resolution of Z of length n.

We need one preliminary result. Let G and G' be monoids, A a G-module and A' a G'-module. $A \otimes_Z A'$ can be given a structure as $(G\times G')$-module by defining $(\sigma, \sigma')(a \otimes a') = \sigma a \otimes \sigma' a'$, $\sigma \in G$, $\sigma' \in G'$, $a \in A$, $a' \in A'$. If A is G-free and A' is G'-free, then $A \otimes A'$ is $(G\times G')$-free. If X is a G-free complex, X' a G'-free complex, then $X \otimes_Z X'$ is a $(G\times G')$-free complex.

<u>Lemma 4.5</u>: Let X be a G-free resolution of Z, X' a G'-free resolution of Z. Then $X \otimes_Z X'$ is a $(G\times G')$-free resolution of $Z \otimes_Z Z = Z$.

<u>Proof</u>: $H_i(X \otimes_Z X') \cong \mathrm{Tor}_i^Z(Z, Z) = 0$ for $i \geq 1$, and $X_1 \otimes_Z X_o' \oplus X_o \otimes_Z X_1' \to X_o \otimes_Z X_o' \to Z \otimes_Z Z \to 0$ is exact by proposition 5.10 of chapter 8. This gives the result.

Returning to the situation of the free Abelian monoid with n generators, let Y be a G-free module on n generators $y_1, \ldots, y_n$ and let $E(Y)$ be its exterior algebra. Let $E(Y)_q = X_q$, $X_o = Z(G)$. Define

$d_q\colon X_q \to X_{q-1}$, $1 \leq q \leq n$, by $d_q(y_{i_1} \cdots y_{i_q}) =$

$$= \sum_{\nu=1}^{q} (-1)^{\nu+1}(s_{i_\nu} - 1)y_{i_1} \cdots \hat{y}_{i_\nu} \cdots y_{i_q},$$

where $\hat{y}_j$ means that y_j is to be omitted from the product. Define $f: X_0 \to Z$ by $f(1) = 1$. X is easily seen to be a complex over Z.

Proposition 4.6: X is a G-free resolution of Z.

Proof: We use induction on n. If $n = 1$, G is the free monoid generated by s_1. $I = (s_1 - 1)$ by proposition 4.2. $(s_1 - 1) \to y_1$ defines an isomorphism $I \cong X_1$, and $0 \to X_1 \xrightarrow{d_1} X_0 \xrightarrow{f} Z \to 0$ is exact. Now let $n > 1$ and assume the result for free Abelian monoids with less than n generators. $G \cong G' \times G''$, where G' is the free Abelian monoid generated by $s_1, \ldots, s_{n-1}$ and G'' is the free monoid generated by s_n. If X' and X'' are the free resolutions of Z over G' and G'' respectively then, by the lemma, $X' \otimes X''$ is a G-free resolution of Z. A trivial verification shows that $X' \otimes X''$ may be identified with the complex X.

Corollary 4.7: If G is the free Abelian group generated by a finite set, $G' \subset G$ the free Abelian monoid generated by the same set and X the G'-free resolution of Z obtained above, then $Z(G) \otimes_{G'} X$ is a G-projective resolution of Z.

Proof: This follows from proposition 3.4.

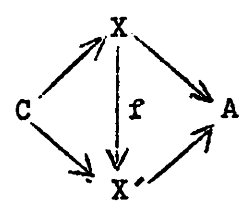
Corollary 4.8: If G is the free Abelian monoid or group generated by a set with n elements, then $H_q(G, A) = H^q(G, A) = 0$ for any $q > n$ and any G-module A.

§5. Extensions of modules

In this section, we digress from the subject of the chapter to give the theory of extensions of modules over an arbitrary ring. We will apply the result to group rings over a field, obtaining an interpretation of $H^1(G, \mathrm{Hom}_K(A, C))$ for $K(G)$-modules A and C.

Let Λ be a ring and let A and C be (left) Λ-modules.

Definitions 5.1: An extension (E) over A with kernel C is an exact sequence of Λ-modules $0 \to C \xrightarrow{\psi} X \xrightarrow{\Phi} A \to 0$. Let $0 \to C \xrightarrow{\psi'} X' \xrightarrow{\Phi'} A \to 0$ be another extension (E'). If there exists a Λ-morphism $f: X \to X'$ such that the diagram



commutes, then (E) and (E') are said to be equivalent (and f is then an isomorphism). $E(A, C)$ denotes the set of equivalence classes of extensions over A with kernel C. All split exact extensions are in one class, which is called the split class. We define a multiplication between elements (E) and (E') (as above) of $E(A, C)$: in $X \oplus X'$, consider $B = \{(x, x') | \Phi(x) = \Phi'(x')\}$ and $D = \{(-\psi(c), \psi'(c)) | c \in C\}$; $D \subset B$. Let $Y = B/D$. Let $\psi: C \to Y$ be given by $\psi(c) = (\overline{\psi(c), 0}) = (\overline{0, \psi'(c)})$ and let $\Phi: Y \to A$ be given by $\Phi(\overline{x, x'}) = \Phi(x) = \Phi'(x')$. Then $0 \to C \xrightarrow{\psi} Y \xrightarrow{\Phi} A \to 0$ is exact, and is called the Baer product of (E) and (E'). An extension (E): $0 \to C \to X \to A \to 0$ defines canonically a connecting morphism

$\delta_E : \mathrm{Hom}(A, A) \to \mathrm{Ext}^1(A, C) \cdot \delta_E(i)$, where i is the identity map, is called the characteristic class of the extension and is clearly the same for equivalent extensions.

Theorem 5.2: The map $E \to \delta_E(i)$ gives a one to one correspondence between $E(A, C)$ and $\mathrm{Ext}^1(A, C)$. Baer multiplication goes over to addition, the split class going to zero.

Proof: Choose and fix an exact sequence $0 \to C \xrightarrow{\alpha} Q \xrightarrow{\beta} N \to 0$, where Q is injective. Suppose $f \in \mathrm{Hom}(A, N)$ is given. Consider $A \oplus Q$. Define a morphism $\nu : A \oplus Q \to N$ by:

i) $\nu(a, q) = -f(a) + \beta(q)$.

Let $X = \mathrm{Ker}(\nu)$. Define further:

$\psi : C \to X$ by $\psi(c) = (o, \alpha(c))$ (a monomorphism, since α is)

ii) $\eta : X \to Q$ by $\eta(a, q) = q$

$\phi : X \to A$ by $\phi(a, q) = a$ (an epimorphism, since β is)

Then the following diagram is commutative and has exact rows, the upper row being denoted (E_f):

$$\text{iii)}\quad \begin{array}{ccccccccc} 0 & \to & C & \xrightarrow{\psi} & X & \xrightarrow{\phi} & A & \to & 0 \\ & & \downarrow j & & \downarrow \eta & & \downarrow f & & \\ 0 & \to & C & \xrightarrow{\alpha} & Q & \xrightarrow{\beta} & N & \to & 0, \end{array}$$

where j is the identity.

On the other hand, since Q is injective, given an extension (E) we obtain an η and f such that diagram iii) is valid. Here, if $\nu : A \oplus Q \to N$ is given as in i), X may be identified with $\mathrm{Ker}(\nu)$ (via $x \to (\phi(x), n(x))$) and relations ii) will hold. Now (E) and (E_f) are clearly equivalent. Diagram iii) gives rise to a commutative diagram with exact row.

iv)

$$\begin{array}{ccccccc}
 & & \operatorname{Hom}(A, A) & \xrightarrow{\ \delta_{E_f}\ } & & & \\
 & & \Big\downarrow{\scriptstyle \operatorname{Hom}(i,\, f)} & \searrow & & & \\
\operatorname{Hom}(A, Q) & \xrightarrow{\operatorname{Hom}(i,\beta)} & \operatorname{Hom}(A, N) & \xrightarrow{\ \delta\ } & \operatorname{Ext}^1(A, C) & \longrightarrow & 0,
\end{array}$$

where δ is the connecting morphism arising from the bottom row of iii), and $\delta(f) = \delta_{E_f}(i)$. Since δ is an epimorphism, the map $E \to \delta_E(i)$ from $E(A, C)$ to $\operatorname{Ext}^1(A, C)$, is onto. To show that it is one to one, suppose $\delta(f_1) = \delta(f_2)$. We must show that (E_{f_1}) and (E_{f_2}) are equivalent. By iv), $f_1 - f_2 = \beta g$ for some $g \in \operatorname{Hom}(A, Q)$. Define an automorphism $w : A \oplus Q \to A \oplus Q$ by $w(a, q) = (a, q + g(a))$. Since $\nu_1 w(a, q) = -f_1(a) + \beta g(a) + \beta(q) = -f_2(a) + \beta(q) = \nu_2(a, q)$, w induces an isomorphism $w' : X_2 \to X_1$, where $X_1 = \operatorname{Ker}(\nu_1)$, $X_2 = \operatorname{Ker}(\nu_2)$, such that $w'\psi_2 = \psi_1$ and $\phi_1 w' = \phi_2$. Thus (E_{f_1}) and (E_{f_2}) are equivalent. If we take $f = 0$ and construct E_f, $X = \operatorname{Ker}(\nu) \cong A \oplus C$ and the split class goes to zero in $\operatorname{Ext}^1(A, C)$. Finally, to show that Baer multiplication goes into addition, let (E), $0 \to C \xrightarrow{\psi} X \xrightarrow{\phi} A \to 0$, be the Baer product of (E_{f_1}) and (E_{f_2}) and let $f = f_1 + f_2$. Define $\eta : X \to Q$ by

$\eta(\overline{x_1, x_2}) = \eta_1(x_1) + \eta_2(x_2)$.

$f\phi(\overline{x_1, x_2}) = f_1\phi_1(x_1) + f_2\phi_2(x_2) = \beta\eta_1(x_1) + \beta\eta_2(x_2) = \beta\eta(\overline{x_1, x_2})$ and $\eta\psi = \alpha$ since $\eta_1\psi_1 = \alpha$. Thus we obtain a diagram like iii), so that (E) is defined by f. This completes the proof.

Before applying our result to group rings over a field, we need some preliminary results. Let G be a group. Let K be any commutative ring and let C be a $K(G)$-module. Clearly $K \otimes_{K(G)} C \cong Z \otimes_{Z(G)} C$ and $\mathrm{Hom}_{K(G)}(K, C) \cong \mathrm{Hom}_{Z(G)}(Z, C)$ as $K(G)$-modules. If $X(G)$ is the standard free resolution of Z, $K \otimes_Z X(G)$ is a $K(G)$-free resolution of $K \otimes_Z Z = K$. Further, we have $X(G) \otimes_Z K \otimes_{K(G)} C \cong X(G) \otimes_Z Z \otimes_{Z(G)} C \cong X(G) \otimes_{Z(G)} C$ and

$$\mathrm{Hom}_{K(G)}(K \otimes_Z X(G), C) \cong \mathrm{Hom}_Z(X(G), \mathrm{Hom}_{K(G)}(K, C)) \cong \mathrm{Hom}_Z(X(G), \mathrm{Hom}_{Z(G)}(Z, C))$$
$$\cong \mathrm{Hom}_{Z(G)}(X(G), C).$$

Thus $\mathrm{Tor}_n^{K(G)}(K, C) \cong \mathrm{Tor}_n^{Z(G)}(Z, C) = H_n(G, C)$ and

$\mathrm{Ext}^n_{K(G)}(K, C) \cong \mathrm{Ext}^n_{Z(G)}(Z, C) = H^n(G, C)$, $n \geq 0$. This result motivated our previous use only of Z.

Now let A and C be $K(G)$-modules and consider $\mathrm{Hom}_K(A, C)$ as a $K(G)$-module under diagonal G-action, $(\sigma f)(a) = \sigma f(\sigma^{-1}a)$, $\sigma \varepsilon G$. We assume that K is a field. If P is a $K(G)$-projective module, C any $K(G)$-module, then, since $\mathrm{Hom}_K(A, C)$ is an exact functor of $K(G)$-modules A, so is $\mathrm{Hom}_{K(G)}(A, \mathrm{Hom}_K(P, C)) \cong$ $\cong \mathrm{Hom}_K(A \otimes_{K(G)} P, C) \cong \mathrm{Hom}_{K(G)}(P, \mathrm{Hom}_K(A, C))$. Thus $\mathrm{Hom}_K(P, C)$ is $K(G)$-injective and if X is a $K(G)$-projective resolution of a $K(G)$-module A, then $\mathrm{Hom}_K(X, C)$ is a $K(G)$-injective resolution of $\mathrm{Hom}_K(A, C)$. Further, $\mathrm{Hom}_{K(G)}(A, C) \cong \mathrm{Hom}_{K(G)}(A, \mathrm{Hom}_K(K, C) \cong$ $\mathrm{Hom}_{K(G)}(K, \mathrm{Hom}_K(A, C))$. Therefore we have

$$\mathrm{Ext}^n_{K(G)}(A, C) \cong \mathrm{Ext}^n_{K(G)}(K, \mathrm{Hom}_K(A, C)), \; n \geq 0.$$

Corollary 5.3: Let A and C be $K(G)$-modules (representation modules for G with corfficients in the field K). Then there is a one to one correspondence between $E(A, C)$ and $H^1(G, \mathrm{Hom}_K(A, C))$ in which the split class goes to zero.

Proof: $H^1(G, \mathrm{Hom}_K(A, C)) \cong \mathrm{Ext}^1_{K(G)}(K, \mathrm{Hom}_K(A, C)) \cong \mathrm{Ext}^1_{K(G)}(A, C)$.

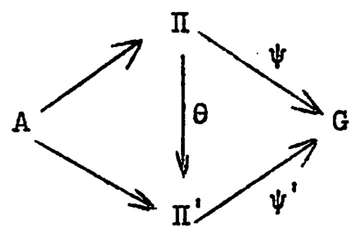
We conclude this section by obtaining a classical theorem (due to Maschke):

Theorem 5.4: Let G be a finite group of order q and K a field of characteristic zero or p, where $(p, q) = 1$. Then $K(G)$ is a semi-simple ring.

Proof: By 8.6 of chapter 9, we must prove that every $K(G)$-module is projective, or that every exact sequence $0 \to C \to F \to A \to 0$ splits, where F is free. By 5.3, it suffices to prove $H^1(G, \mathrm{Hom}_K(A, C)) = X = 0$. Now for any G-module B, $qH^1(G, B) = 0$ since if $f : Z(G) \to B$ is a 1-cocycle, $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$, and if $a = \sum_{\sigma \varepsilon G} f(\sigma)$, $\sigma a - a = -qf(\sigma)$, or qf is a 1-coboundary. Therefore $qX = 0$, and since X is a K-space, $X = 0$.

§6. Extensions of groups

Definition 6.1: Let G be a group. A pair (Π, ψ) where Π is a group and $\psi : \Pi \to G$ is a group epimorphism with kernel A is called an extension of A by G. A is then necessarily a normal subgroup of Π. Let (Π', ψ') be a second extension of A by G. (Π, ψ) is said to be equivalent to (Π', ψ') if there exists a morphism of groups $\theta : \pi \to \Pi'$ such that the diagram



is commutative. θ must then be an isomorphism. We assume that A is a commutative group. For each $\sigma \varepsilon G$, choose $\pi_\sigma \varepsilon \Pi$ such that $\psi(\pi_\sigma) = \sigma$. $\{\pi_\sigma\}$ is called a section of Π. Since A is a normal commutative subgroup of Π, the map $a \to \pi_\sigma a \pi_\sigma^{-1}$ is an automorphism of A depending only on σ. Defining

$a^\sigma = \pi_\sigma a \pi_\sigma^{-1}$, $a^1 = a, (a_1\ a_2)^\sigma = a_1^\sigma\ a_2^\sigma$, and $(a^\sigma)^\tau = a^{\tau\sigma}$. Thus an extension (Π, ψ) of A by G induces a structure of G-module on A.

Theorem 6.2: Let G be a group and A a G-module. The equivalence classes of extensions of A by G which induces the given G-module structure on A are in one to one correspondence with the elements of $H^2(G, A)$.

Proof: Using the standard non-homogeneous G-free resolution of Z, a 2-cocycle is a map $f : G \times G \to A$ such that

$\sigma f(\tau, p) - f(\sigma\tau, p) + f(\sigma, \tau p) - f(\sigma,\tau) = 0$, or, writing $f(\sigma, \tau) = a_{\sigma,\tau}$

for all $\sigma, \tau \in G$. Conversely, if we can so choose $\{\pi^*_\sigma\}$, the map $\Pi \to \Pi^*$ given by $a\pi_\sigma \to a\pi^*_\sigma$, $a \in A$, is clearly an isomorphism which reduces to the identity on A (since $\pi_1 = \pi^*_1 = 1$) and therefore defines an equivalence. Since the choice of section does not effect the cohomology class, (Π, ψ) and (Π^*, ψ) are equivalent if and only if $\{a_{\sigma,\tau}\}$ and $\{a^*_{\sigma,\tau}\}$ (resulting from any choice of sections) represent the same element of $H^2(G, A)$. It remains to prove that every element of $H^2(G, A)$ results in this manner from an extension. Let $\{a_{\sigma,\tau}\}$ represent $\alpha \in H^2(G, A)$. We may assume $a_{1,1} = 1$, whence

$a_{\sigma,1} = \dfrac{a^\sigma_{1,1}\, a_{\sigma,1}}{a_{\sigma,1}} = 1$, $a_{1,\sigma} = 1$, $\sigma \in G$. Define $\Pi = \{(a, \sigma) \mid a \in A, \sigma \in G\}$,

and define multiplication by $(a, \sigma)(b, \tau) = (ab^\sigma a_{\sigma,\tau}, \sigma\tau)$. Since

$a_{\sigma,\tau}a_{\sigma\tau,\rho} = a^\sigma_{\tau,\rho}a_{\sigma,\tau\rho}$, $((a,\sigma)(b,\tau))(c,\rho) = (ab^\sigma c^{\sigma\tau}a_{\sigma,\tau}a_{\sigma\tau,\rho}, \sigma\tau\rho) =$

$(ab^\sigma c^{\sigma\tau}a^\sigma_{\tau,\rho}a_{\sigma,\tau\rho}, \sigma\tau\rho) = (a,\sigma)((b,\tau)(c,\rho))$. Let

$e = (1, 1)$; $e(a, \sigma) = (a \cdot a_{1,\sigma}, \sigma) = (a, \sigma) = (a \cdot a_{\sigma,1}, \sigma) = (a, \sigma)e$.

$(a, 1)(a^{-1}, 1) = e$; since $(a, \sigma)(1, \sigma^{-1}) = (b, 1)$, $(1, \sigma^{-1})(a, \sigma) = (c, 1)$,

every element has a left and right inverse. We have proven therefore that Π is a group. (Π, ψ) is an extension of A by G, $\psi(a, g) = g$, where $A \subset \Pi$ under $a \to (a, 1)$. $\{(1, \sigma)\}$ is a section of Π.

$(1, \sigma)(a, 1)(1, \sigma)^{-1} = (a^\sigma, \sigma)(1, \sigma)^{-1} = (a^\sigma,1)(1, \sigma)(1, \sigma)^{-1} = (a^\sigma, 1)$,

so that (Π, ψ) induces the given G-module structure on A. Finally, $(1, \sigma)(1, \tau) = (a_{\sigma,\tau}, \sigma\tau) = (a_{\sigma,\tau}, 1)(1, \sigma\tau)$ so that the resulting factor system is just $\{a_{\sigma,\tau}\}$, as desired.

Definition 6.3: an extension (Π, ψ) of A by G is called inessential if there exists a morphism $\phi : G \to \Pi$ such that $\psi\phi$ is the identity of G. Then $\{\phi(\sigma)\}$ is a section such that $a_{\sigma,\tau} = 1$ for all $\sigma, \tau \varepsilon G$. Thus $o \varepsilon H^2(G, A)$ corresponds to the class of inessential extensions.

We next obtain an interpretation of $H^1(G, A)$. Let (Π, ψ) be a fixed extension of the commutative group A by G, and consider A as a G-module under the induced structure. An automorphism ϕ of Π such that $\phi(a) = a$ and $\psi\phi = \psi$ is said to be trivial for both A and G. The set of all such automorphisms forms a group denoted $U(\Pi)$. Since A is commutative and $A = \ker \psi$, if $a \varepsilon A$, then $\phi_a : \Pi \to \Pi$ given by $\phi_a(\pi) = a\pi a^{-1}$ ia an element of $U(\Pi)$. The set of such elements forms a subgroup $V(\Pi)$, the set of inner automorphisms of Π determined by elements of A.

Theorem 6.4: $U(\Pi)$ is a commutative group and $U(\Pi)/V(\Pi) \cong H^1(G, A)$.

Proof: Choose a section $\{\pi_\sigma\}$ of Π. Let $\phi \varepsilon U(\Pi)$. $\psi\phi(\pi_\sigma) = \sigma$, say $\phi(\pi_\sigma) = a\pi_\sigma$, $a \varepsilon A$. If $\pi'_\sigma = b\pi_\sigma$, $b \varepsilon A$, then $\phi(\pi'_\sigma) = b\phi(\pi_\sigma) = ab\pi_\sigma = a\pi'_\sigma$, so that $a = a_\sigma$ depends only on σ.

$a_{\sigma\tau}\pi_\sigma\pi_\tau = \phi(\pi_\sigma\pi_\tau) = \phi(\pi_\sigma)\phi(\pi_\tau) = a_\sigma\pi_\sigma a_\tau\pi_\sigma^{-1}\pi_\sigma\pi_\tau = a_\sigma a_\tau^\sigma\pi_\sigma\pi_\tau$. Therefore $a_{\sigma\tau} = a_\tau^\sigma a_\sigma$ and $\{a_\sigma\}$ is a 1-cocycle. Clearly the map $f : U(\Pi) \to Z(A)$, $f(\phi) = \{a_\sigma\}$, is a monomorphism of groups, $Z(A)$ the group of 1-cocycles of A. Given $\{a'_\sigma\} \varepsilon Z(A)$, define $\phi' \varepsilon U(\Pi)$ by $\phi'(a\pi_\sigma) = a'_\sigma a\pi_\sigma$, $a \varepsilon A$. $f(\phi') = \{a'_\sigma\}$, so that f is an epimorphism. If $a \varepsilon A$, we have $a\pi_\sigma a^{-1} = a\pi_\sigma a^{-1}\pi_\sigma^{-1}\pi_\sigma = {}^a/a^\sigma \cdot \pi_\sigma$ and $f(\phi_a) = \{{}^a/a^\sigma\}$, $f(V(\Pi)) = B(A)$, the group of 1-coboundaries of A.