Some Motivation for the Study of Group Cohomology

May 7, 2013

This short note is meant as a motivation for the study of group cohomology. Everything that is not immediately clear to you is an implicit exercise.

§1 G-Modules

In this § we define the group ring $\mathbf{Z}[G]$ of a group over the integers $\mathbf{Z}$. Moreover, we show that any module over the group ring $\mathbf{Z}[G]$ of a finite cyclic group G occurs in a certain periodic chain complex.

§1.1 Fix a group G. We denote by $\mathbf{Z}[G]$ the *group ring* of G over the integers $\mathbf{Z}$. Elements of $\mathbf{Z}[G]$ are formal linear combinations $\sum_{g\in G} a_g g$ with $a_g \in \mathbf{Z}$. The sum and product of two elements in $\mathbf{Z}[G]$ is given by

$$\Big(\sum_{g\in G} a_g g\Big) + \Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G} (a_g + b_g) g$$

and

$$\Big(\sum_{g\in G} a_g g\Big) \cdot \Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G} \Big(\sum_{h\in G} a_{gh^{-1}} b_h\Big) g,$$

respectively.

As the name suggests, $\mathbf{Z}[G]$ is a ring. Moreover, there is a one-to-one correspondence between $\mathbf{Z}[G]$-modules and abelian groups equipped with an action of G. This correspondence even extends to morphisms, where it reads as follows: A $\mathbf{Z}[G]$-linear map $f\colon A \to B$ is nothing but a G-equivariant homomorphism of abelian groups, i.e., a group homomorphism $f\colon A \to B$, such that $f(g.x) = g.f(x)$ for all $x \in A$ and $g \in G$.

§1.2 Now suppose that G is a finite cyclic group $G = \langle\sigma\rangle$ of order n. We denote by N the element $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$ of $\mathbf{Z}[G]$. Moreover, we let $\mathfrak{I} = \{a \in \mathbf{Z}[G] \mid Na = 0\}$. There are short exact sequences

$$0 \longrightarrow \mathfrak{I} \longrightarrow \mathbf{Z}[G] \xrightarrow{N} \mathbf{Z} \cdot N \longrightarrow 0$$

and

$$0 \longrightarrow \mathbf{Z} \cdot N \longrightarrow \mathbf{Z}[G] \xrightarrow{\sigma - 1} \mathfrak{I} \longrightarrow 0$$

of $\mathbf{Z}[G]$-modules. Splicing these sequences together, we obtain a long exact sequence

$$0 \longleftarrow \mathbf{Z} \cdot N \xleftarrow{N} \mathbf{Z}[G] \xleftarrow{\sigma - 1} \mathbf{Z}[G] \xleftarrow{N} \mathbf{Z}[G] \xleftarrow{\sigma - 1} \cdots \tag{1}$$

of $\mathbf{Z}[G]$-modules.

§1.3 Let A be an arbitrary $\mathbf{Z}[G]$-module. We want to apply the functor $\hom_{\mathbf{Z}[G]}(-, A)$ from $\mathbf{Z}[G]$-modules to abelian groups to the sequence (1). For this purpose, we identify $\hom_{\mathbf{Z}[G]}(\mathbf{Z}[G], A) = A$ and $\mathbf{Z} \cdot N = \mathbf{Z}$. An easy calculation shows that $\hom_{\mathbf{Z}[G]}(\mathbf{Z}, A) = \{x \in A \mid \forall \tau \in G : \tau x = x\}$, which we agree to abbreviate by A^G. The composition of any two consecutive maps in the resulting sequence

$$0 \longleftarrow A^G \xleftarrow{N} A \xleftarrow{\sigma - 1} A \xleftarrow{N} A \xleftarrow{\sigma - 1} \cdots \tag{2}$$

is still equal to zero, even though the sequence is not necessarily exact. Put differently, (2) is a chain complex of abelian groups. We are thus led to the study of the quotient groups $\ker(N)/\operatorname{im}(\sigma - 1)$ and $\ker(\sigma - 1)/\operatorname{im}(N)$, which are well-defined and possibly non-zero. In **§2.3** we will study a situation, where it is highly desirable that these quotients vanish.

§2 Characteristic Polynomial and Norm

In this § we briefly recall some relevant notions from number theory and present a situation, where the chain complex (2) of **§1.3** occurs naturally. For this purpose, we fix a finite field extension L/k. It is not absolutely necessary to understand the rather terse proof of equation (4), but we need that equality in what follows below.

§2.1 Recall that the *characteristic polynomial* $\chi_a \in k[T]$ of some $a \in L$ is the characteristic polynomial $\chi_a(T) = \det(m_a - T)$ of the k-linear map $m_a : L \to L$ given by $x \mapsto ax$.

We claim that

$$\chi_a = f^{[L:k(a)]}, \tag{3}$$

where $f \in k[T]$ is the minimum polynomial of a and $[L : k(a)]$ denotes the degree of L over $k(a)$.

Let us first consider the case that $L = k(a)$. In this case, both f and χ_a are monic polynomials with $\deg(f) = [L : k] = \deg(\chi_a)$. Moreover, $f \mid \chi_a$ since $\chi_a(a) = \chi_a(m_a)(1) = 0$ by the Caley-Hamilton theorem. Therefore, $f = \chi_a$.

In the general case, choose bases $b_1, \ldots, b_r$ of $k(a)$ over k, and $c_1, \ldots, c_s$ of L over $k(a)$. Then $ab_ic_j = \sum_{k=1}^{r} \alpha_k b_k c_j$ and the matrix of m_a with respect to the basis $\{b_ic_j\}_{ij}$ thus consists of $s = [L : k(a)]$ blocks of dimension $r \times r$ on the diagonal. Equation (3) now follows, because each of these blocks contains the matrix of m_a restricted to $k(a)$ with respect to the basis $\{b_i\}_i$.

§2.2 Just as we have defined the characteristic polynomial of some $a \in L$, we might consider the determinant $\det_k(m_a)$ of multiplication by a. This value is usually called the *norm* of a and is denoted by $\mathrm{N}_{L/k}(a)$. Recall from linear algebra that the determinant $\mathrm{N}_{L/k}(a)$ of m_a is nothing but the constant term in $\chi_a(T)$. Hence

$$\mathrm{N}_{L/k}(a) = \Big(\prod_i a_i\Big)^{[L:k(a)]},$$

where the a_i are the roots of the minimum polynomial f of a in some splitting field $E \supseteq L$ of f.

Note that if L/k is separable, this implies that

$$\mathrm{N}_{L/k}(a) = \prod_\sigma \sigma(a),$$

where σ runs through all maps $L \to \bar{k}$ into the algebraic closure $\bar{k}$ of k fixing k. In the case that $L = k(a)$, this follows from the fact that $\sigma(a)$ runs through all roots of f. In the case that $L \supset k(a)$, one further notes that each map $k(a) \to \bar{k}$ has $[L : k(a)]$ extensions to L.

Note that if L/k is a Galois extension, L/k being normal implies that the Galois group G already contains the relevant restrictions of all the embeddings $L \to \bar{k}$. Hence

$$\mathrm{N}_{L/k}(a) = \prod_{\sigma \in G} \sigma(a). \tag{4}$$

§2.3 Now let L/k be a cyclic Galois extension with Galois group $G = \langle \sigma \rangle$ of order n. The multiplicative group L^* becomes a $\mathbf{Z}[G]$-module via

$$\Big(\sum_{\tau \in G} a_\tau \tau\Big).x = \prod_{\tau \in G} a_\tau \tau(x).$$

Using the notation of **§1.3**, we write $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$. Computing the action of N on $a \in L^*$, we find that

$$N.a = \prod_{\tau \in G} \tau(a) = \mathrm{N}_{L/k}(a),$$

where the last equality follows from equation (4).

Further note that some $a \in L^*$ is contained in $\mathrm{im}(\sigma - 1)$ if and only if there is some $b \in L^*$ such that $a = \sigma(b)/b$.

Vanishing of the groups $\ker(N)/\mathrm{im}(1-\sigma)$ that we looked at in **§1.3** is hence equivalent to the fact that any element $a \in L^*$ of norm 1 may be written as $a = \sigma(b)/b$ for some $b \in L^*$.

Exercise: After you have worked through this text, you should read `http://en.wikipedia.org/wiki/Hilbert's_Theorem_90` and convince yourself that this excurse into number theory was not pointless. Note that we have not proven that $\ker(N)/\mathrm{im}(1-\sigma) = 0$. However, there are proofs of this fact – even not too difficult ones.

Exercise: After listening to Manuel's talk, you should reconsider the exact sequence (1) and the resulting chain complex (2) of **§1.3**. In order to sort things out, you should note that Ext-groups can be calculated both by a resolution of the left and a resolution of the right argument[1]. You should be able to give a complete description of the cohomology of a finite cyclic group G with coefficients in some arbitrary $\mathbf{Z}[G]$-module A. What happens if you specialize to the case $A = \mathbf{Z}$?

Exercise: Discuss what of **§2.2** and **§2.3** remains true if one replaces the norm $\mathrm{N}_{L/k}(a)$ by the trace $\mathrm{Tr}_{L/k}(a) = \mathrm{Tr}_k(m_a)$ of an element $a \in L$.

[1] We will see a proof of this fact in a later talk.