On the extension giving the truncated Witt vectors

Torgeir Skjøtskift

January 5, 2015

Contents

Abstract

We explore the theory of cohomology of groups and the classification of group extensions with abelian kernel. We then look at the group extensions that underlie the truncated Witt vectors on the truncation set $\{1, p\}$ where p is a prime number. It turns out that we can do without the multiplicative structure on the source ring A by factoring the extension's representing cocycle through a map into the p-fold tensor product of A divided out by the C_p-action.

1 Introduction

Given two groups G and N, we can ask the following question: What are the essentially different ways we can express the group G as a quotient of some group E by N? Answering this question amounts to classifying certain objects called extensions, which are short exact sequences of groups

$$1 \to N \to E \to G \to 1 \, .$$

Restricting ourselves to extensions with abelian kernel, i.e. where N is an abelian group A, we solve the classification problem by using the theory of cohomology of groups.

Turning our attention to the truncated Witt vectors on a commutative ring A, we examine the extension we get from the projection of the Witt vectors onto A by forgetting down to abelian groups. This yields an extension

$$0 \to A \to W \to A \to 0$$

which is represented in the second cohomology group $H^2(A, A)$ by a cocycle depending on the multiplication in A. It turns out that this cocycle factors through a map into the p-fold tensor product of A divided out by the C_p-action, yielding another extension

$$0 \to A^{\otimes p}/C_p \to W' \to A \to 0 \, ,$$

in which the group structure in W' does not depend on the multiplication in A. We discover that tensoring this extension with $\mathbf{F}_p$ yields a long exact sequence in homology in which the connecting homomorphism is equal to a certain normalized cochain $A \to A$.

1.1 Why do we care?

In this section we will give some background information that lies outside the scope of this thesis, but which may help the reader place it in a wider context.

The motivation for this thesis is questions in equivariant homotopy theory, more precisely the equivariant structure of smash powers. If E is a spectrum, G a finite group and S a finite G-set, let

$$E^{\wedge S} = E \wedge \cdots \wedge E$$

be the smash product of E with itself indexed over the elements of S. The motivation lies in an attempt to understand the G-spectrum $E^{\wedge S}$, and in particular its fixed points $(E^{\wedge S})^G$ under the G-action.

A variant of the Redshift conjecture is that the chromatic level of $(E^{\wedge S})^G$ is higher than that of E itself. In particular, if multiplication by p is null-homotopic in E then it is not null-homotopic in $(E^{\wedge p})^{C_p}$, where C_p is the cyclic group of order p. We wish to study this more closely by examining the fundamental cofiber sequence

$$(E^{\wedge p})_{hC_p} \to (E^{\wedge p})^{C_p} \to E \, ,$$

where $(E^{\wedge p})_{hC_p}$ are the homotopy orbits under the C_p-action. If the fixed points are going to have higher chromatic filtration than E, then this cofiber

sequence must be non-trivial. One way to understand such a cofiber sequence is to understand the boundary map

$$E \to \Sigma(E^{\wedge p})_{hC_p} ,$$

which should be easier to understand since both E and $(E^{\wedge p})_{hC_p}$ are easier to understand than the fixed points.

Such questions arise in connection with topological Hochschild homology: If E is a commutative ring spectrum then

$$S \mapsto E^{\wedge S}$$

becomes a functor and we can give meaning to $E^{\wedge X}$, where X is a simplicial set. In particular, $\mathrm{THH}(E)$ arises as $E^{\wedge S^1}$ where S^1 is a simplicial model for the circle. Note that this case does not require that E be commutative. Let C_p be the cyclic group of order p, acting on S^1 by multiplication by the p-th roots of unity. This leads to the following variant of the fundamental cofiber sequence above

$$\mathrm{THH}(E)_{hC_p} \to \mathrm{THH}(E)^{C_p} \to \mathrm{THH}(E) ,$$

where $\mathrm{THH}(E)_{hC_p}$ are the homotopy orbits and $\mathrm{THH}(E)^{C_p}$ are the fixed points of $\mathrm{THH}(E)$.

We wish to understand this cofiber sequence by studying the boundary map

$$\mathrm{THH}(E) \to \Sigma\,\mathrm{THH}(E)_{hC_p}$$

To discover higher periodic classes one must work with coefficients. In particular, to discover increased divisibility by p, it is fair to start out with working with homotopy mod p.

In this thesis we study the lowest homotopy groups for the fixed points and the boundary maps in mod p. Here we rediscover the well known truncated Witt vectors for THH, while for the finite fixed points discover "new" extensions of $\pi_0 E$. In the last case we get an explicit version of the boundary map and an open question is how our formulas should generalize from π_0 to a map of spectra.

Concretely, letting A be an abelian group, $E = HA$ the Eilenberg-MacLane spectrum on A and $G = C_p$ be the cyclic group of order p, the fundamental cofiber sequence becomes

$$(HA^{\wedge p})_{hC_p} \to (HA^{\wedge p})^{C_p} \to HA .$$

In this case the boundary map is the map $\partial : HA \to \Sigma(HA^{\wedge p})_{hC_p}$, which in mod p homotopy becomes the map

$$\pi_*\partial : \pi_* HA \wedge \mathbf{S}/p \to \pi_*\Sigma(HA^{\wedge p})_{hC_p} \wedge \mathbf{S}/p .$$

Looking at the long exact sequence in homotopy given by smashing with the cofiber sequence

$$\mathbf{S} \xrightarrow{p} \mathbf{S} \to \mathbf{S}/p ,$$

where $\mathbf{S}$ is the sphere spectrum, we see that for $i < 1$, $\pi_i\Sigma(HA^{\wedge p})_{hC_p} \wedge \mathbf{S}/p$ is equal to zero since taking homotopy orbits preserves connectivity. Moreover, for $i > 1$ we have that $\pi_i HA \wedge \mathbf{S}/p$ is equal to zero. Thus, the only non-zero part of $\pi_*\partial$ is the connecting homomorphism

$$\pi_1 HA \wedge \mathbf{S}/p \to \pi_0(HA^{\wedge p})_{hC_p} \wedge \mathbf{S}/p .$$

This map is actually the connecting homomorphism

$$\mathrm{Tor}_1(\mathbf{F}_p, A) \to \mathbf{F}_p \otimes A^{\otimes p}/C_p \ ,$$

for which we discover a concrete formula in Section 3.

2 Cohomology of groups

We will start by defining a set of basic objects that will be of use later. Most of the contents of this section is taken from [1, ch. I-III] while expanding on those parts requiring additional details. The goal of this section is to be able to give a definition of the cohomology of a group G with coefficients in a $\mathbf{Z}G$-module M.

2.1 Chain complexes and homology

Let R be a ring. A *chain complex* C over R is a graded R-module $C = (C_n)$ together with an endomorphism d of C, called the *differential* of C, with degree -1 satisfying $d^2 = 0$. If d instead has degree $+1$, we write $C = (C^n)$ and say that C is a *cochain complex*. If M is a module, we will let M denote the chain complex $\cdots \to 0 \to 0 \to M$, concentrated in degree 0.

If C is a chain complex, we define the *homology* of C to be the graded R-module $H(C) = (H_n(C)) = \ker d/\operatorname{im} d$. If C is a cochain complex, we write $H(C) = (H^n(C))$ and call it the *cohomology* of C.

A graded module homomorphism $f : C \to C'$ of degree 0 between two chain complexes is called a *chain map* if $d'f = fd$. A chain map $f : C \to C'$ whose induced map $H(f) : H(C) \to H(C')$ is an isomorphism, is called a *weak equivalence*. In particular, homotopy equivalences of chain complexes are weak equivalences.

2.2 Resolutions

Definition 2.2.1. Given an R-module M, a *resolution* $\varepsilon : F \to M$ of M over R is an exact sequence

$$\cdots \to F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M \to 0$$

of R-modules. A *free resolution* is a resolution where all the F_i are free.

Since every exact sequence is a chain complex, we can view a resolution in terms of chain complexes by regarding ε as a chain map from the chain complex $F = (F_n)_{n\geq 0}$ to M, where M is the chain complex concentrated in degree 0:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & F_2 & \xrightarrow{d_2} & F_1 & \xrightarrow{d_1} & F_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \varepsilon} & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Proposition 2.2.2. *The exactness condition on the sequence*

$$\cdots \to F_1 \to F_0 \to M \to 0$$

holds if and only if ε is a weak equivalence

Proof. If the sequence is exact, then $H_i(\varepsilon) : H_i(F) \to H_i(M)$ is the isomorphism $0 \to 0$ for $i > 0$ and $H_0(F) \to H_0(M)$ is the isomorphism $F_0/\ker\varepsilon \to M$. Conversely, if ε is a weak equivalence then $H_i(\varepsilon)$ is an isomorphism for all i which implies that the sequence is exact. The implication can be seen in the case $i = 0$ from the diagram

$$\begin{array}{ccc} F_0 & \xrightarrow{\varepsilon} & M \\ \downarrow & \nearrow & \\ H_0(F) & & \end{array} .$$

□

Proposition 2.2.3. *Every module has a free resolution.*

Proof. Let M be a module and let d_{-1} be the zero map $M \to 0$ and let $F_{-1} = M$. For each $i \geq 0$, let F_i be the free R-module on $\ker d_{i-1}$ and let $d_i : F_i \to F_{i-1}$ be the map sending each generator to its corresponding element. □

Proposition 2.2.4. *A module M over a principal ideal domain R admits a resolution*

$$0 \to F_1 \to F_0 \to M \to 0 .$$

Proof. By Proposition 2.2.3, M has a free resolution $F \to M$. Since R is a principal ideal domain, submodules of free R-modules are free. Thus F_1 is equal to the kernel of the map $F_0 \to M$ and hence $F_2 = 0$. □

Since free modules are direct summands of themselves, free modules are projective and it follows from 2.2.3 that every module has a projective resolution. Note that a free R-module M admits the free resolution $0 \to M \xrightarrow{1} M \to 0$.

2.3 The integral group ring

Let G be a group and let M be the free $\mathbf{Z}$-module on the set G. As a set, M consists of the functions $f : G \to \mathbf{Z}$ having finite support, with sum and scalar multiplication defined pointwise. Consider the map $\mu : M \times M \to M$ sending (f, g) to $x \mapsto \sum_{uv=x} f(u)g(v) = \sum_u f(u)g(u^{-1}x)$.

Proposition 2.3.1. *The map μ is $\mathbf{Z}$-bilinear and associative, giving a product on M.*

Proof. Let $f, g \in M$ and $x \in G$. Let $\mu(f, g)$ be denoted by fg. To prove that μ is $\mathbf{Z}$-bilinear, we must show that $(nf + mf')g = nfg + mf'g$:

$$\begin{aligned} (nf + mf')g(x) &= \sum_{uv=x} (nf + mf')(u)g(v) \\ &= \sum_{uv=x} (nf(u) + mf'(u))g(v) \\ &= n \sum_{uv=x} f(u)g(v) + m \sum_{uv=x} f'(u)g(v) \\ &= nfg(x) + mf'g(x) . \end{aligned}$$

The calculation for the second coordinate is similar. Next, let h be another element of M. To prove associativity, we need to show that $(fg)h = f(gh)$:

$$\begin{aligned}(fg)h(x) = \sum_u fg(u)h(u^{-1}x) &= \sum_u \sum_v f(v)g(v^{-1}u)h(u^{-1}x) \\ &= \sum_v f(v)gh(v^{-1}x) \\ &= f(gh)(x)\ .\end{aligned}$$

Let 1_G denote the unit element of G. The unit with respect to μ is then the function $1 : G \to \mathbf{Z}$ mapping 1_G to 1 and every other element to 0. □

Definition 2.3.2. The ring given by endowing M with the product μ is called the *integral group ring* of G and is denoted $\mathbf{Z}G$.

The functors $G \mapsto \mathbf{Z}G$ and $R \mapsto R^*$, where R^* is the multiplicative group of units of R, form an adjoint pair

$$\mathrm{Grp} \underset{(-)^*}{\overset{\mathbf{Z}-}{\rightleftarrows}} \mathrm{Rng}\ .$$

This gives a bijection

$$\mathrm{Grp}(G, R^*) \cong \mathrm{Rng}(\mathbf{Z}G, R)$$

which is natural in G and R. Letting $R = \mathrm{End}(A)$ be the ring of endomorphisms of A then since $\mathrm{End}(A)^*$ is equal to $\mathrm{Aut}(A)$, the group of automorphisms of A, we get a bijection

$$\mathrm{Grp}(G, \mathrm{Aut}(A)) \cong \mathrm{Rng}(\mathbf{Z}G, \mathrm{End}(A))\ ,$$

giving that there is a one-to-one correspondence between $\mathbf{Z}G$-module structures on A and G-actions on A. We will usually not distinguish between these two concepts.

2.4 The cohomology of a group

We are now ready to define the cohomology of a group G with coefficients in a $\mathbf{Z}G$-module M. Let $\varepsilon : F \to \mathbf{Z}$ and $\eta : P \to M$ be projective resolutions of respectively $\mathbf{Z}$ and M over $\mathbf{Z}G$, and let C and C' be chain complexes over a ring R with differentials d and d' respectively. There is a chain complex

$$\mathscr{H}om_R(C, C')$$

defined in degree n as the R-module of graded module homomorphisms from C to C' with differential D defined by

$$D(f) = d'f + (-1)^{n+1} fd\ .$$

Observe that $\mathscr{H}om_R(C, C')_n = \prod_{q \in \mathbf{Z}} \mathrm{Hom}_R(C_q, C'_{q+n})$. If C' were concentrated in degree 0, we would get that

$$\mathscr{H}om_R(C, C')_n = \prod_{q \in \mathbf{Z}} \mathrm{Hom}_R(C_q, C'_{q+n}) = \mathrm{Hom}_R(C_{-n}, C'_0)\ ,$$

which would be natural to view as the degree n part of a cochain complex defined in degree n by

$$\mathscr{H}om_R(C,C')^n = \mathscr{H}om_R(C,C')_{-n} = \mathrm{Hom}_R(C_n, C'_0) \ .$$

In this case, the differential $\delta = (D_{-n} : \mathrm{Hom}_R(C,C')^n \to \mathrm{Hom}_R(C,C')^{n+1})$ would take the form

$$\delta(f) = (-1)^{n+1} f d \ . \tag{2.4.1}$$

Definition 2.4.1. The cohomology $H^*(G,M)$ of G with coefficients in M is the homology of the cochain complex $\mathscr{H}om_{\mathbf{Z}G}(F,M)$ where M is concentrated in degree 0.

We will now construct a concrete resolution F of $\mathbf{Z}$ over $\mathbf{Z}G$, allowing us to compute the cohomology of a group according to Definition 2.4.1.

Proposition 2.4.2. *Let X be a simplicial abelian group having the face maps $d_i : X_n \to X_{n-1}$ for $0 \le i \le n$. The sequence*

$$\cdots \to X_n \xrightarrow{\partial_n} X_{n-1} \to \cdots \to X_1 \xrightarrow{\partial_1} X_0 \ ,$$

where $\partial_n(x) = \sum_{i=0}^n (-1)^i d_i(x)$, is a chain complex of abelian groups.

Proof. Since the face maps are group homomorphisms, so are the ∂_n's. Left to show is that $\partial_{n-1}\partial_n = 0$. We have

$$\partial_{n-1}\partial_n(x) = \sum_{i=0}^{n-1} (-1)^i d_i \left(\sum_{j=0}^{n} (-1)^j d_j(x) \right) = \sum_{i=0}^{n-1} \sum_{j=0}^{n} (-1)^{i+j} d_i d_j(x) \ .$$

The simplicial identity $d_i d_j = d_{j-1} d_i$ holds for $i < j$ and hence this double sum splits into the following three sums

$$\sum_{i<j} (-1)^{i+j} d_{j-1} d_i(x) + \sum_{i=j} (-1)^{i+j} d_i d_j(x) + \sum_{j<i} (-1)^{i+j} d_i d_j(x) \ .$$

Observing that the terms indexed by the i's and j's satisfying $i = j+1$ cancel the terms indexed by the i's and j's satisfying $i = j$, we have:

$$\begin{aligned} \partial_{n-1}\partial_n(x) &= \sum_{i+1<j} (-1)^{i+j} d_{j-1} d_i(x) + \sum_{j<i} (-1)^{i+j} d_i d_j(x) \\ &= \sum_{j<i} (-1)^{j+i+1} d_i d_j(x) + \sum_{j<i} (-1)^{i+j} d_i d_j(x) \\ &= 0 \ . \end{aligned}$$

□

Definition 2.4.3. If X is a simplicial abelian group then the *Moore complex* MX is the chain complex given by Proposition 2.4.2

Let EG be the simplicial set given in degree n by $G^{\times n+1}$. The face and degeneracy maps in EG are defined respectively by

$$d_i(g_0,\dots,g_n) = (g_0,\dots,\hat{g_i},\dots,g_n)$$
$$s_i(g_0,\dots,g_n) = (g_0,\dots,g_i,g_i,\dots,g_n)\ .$$

The group G acts freely on each degree EG_n of EG by

$$g(g_0,\dots,g_n) = (gg_0,\dots,gg_n)\ ,$$

making EG a free simplicial G-set. Extending this action linearly, $\mathbf{Z}EG$ becomes a free simplicial $\mathbf{Z}G$-module by [1, I.3.1], each degree $\mathbf{Z}EG_n$ having basis the set of representatives of G-orbits of elements $(g_0,\dots,g_n)$. The Moore complex $M\mathbf{Z}EG$ becomes a chain complex of free $\mathbf{Z}G$-modules and since EG is contractible, we obtain weak equivalences

$$M\mathbf{Z}EG \to M\mathbf{Z} \to \mathbf{Z}\ .$$

Definition 2.4.4. The *standard resolution* of $\mathbf{Z}$ over $\mathbf{Z}G$ is the weak equivalence $M\mathbf{Z}EG \to \mathbf{Z}$ given by composing the two weak equivalences above.

Each G-orbit in $\mathbf{Z}EG_n$ is represented by an element $(1, g_1, g_2, \dots, g_n)$, which can be written in the form

$$[h_1|\cdots|h_n] = (1, h_1, h_1h_2, \dots, h_1\cdots h_n)$$

by letting $h_1 = g_1$ and $h_i = g_{i-1}^{-1}g_i$ for $1 < i \leq n$. In this basis, the face maps are given by

$$d_i[g_1|\cdots|g_n] = \begin{cases} g_1[g_2|\cdots|g_n] & i = 0 \\ [g_1|\cdots|g_ig_{i+1}|\cdots|g_n] & 0 < i < n \\ [g_1|\cdots|g_{n-1}] & i = n\ . \end{cases}$$

Definition 2.4.5. The *bar resolution* of $\mathbf{Z}$ over $\mathbf{Z}G$ is the standard resolution where each degree of $\mathbf{Z}EG$ is given the basis described above.

If $F \to \mathbf{Z}$ is the standard resolution, there is for each n a submodule D_n of F_n generated by the elements $(g_0,\dots,g_n)$ such that $g_i = g_{i+1}$ for some $0 \leq i < n$. Orbits of such elements are represented by elements $[h_1|\cdots|h_n]$ where $h_i = 1$ for some $0 < i \leq n$.

Definition 2.4.6. The *normalized* bar resolution of $\mathbf{Z}$ over $\mathbf{Z}G$ is the resolution defined in degree n by F_n/D_n and is generated by elements $[h_1|\cdots|h_n]$ such that $h_i \neq 1$ for all i.

Since any two projective resolutions of a module are homotopy equivalent, and homotopy equivalences are weak equivalences, the cohomology $H^*(G, M)$ does not depend on the choice of resolutions F and P. Thus we may choose F to be the bar resolution, and we get

$$\begin{aligned} \mathscr{H}om_{\mathbf{Z}G}(F, M)^n &= \mathbf{Z}G\text{-mod}(M\mathbf{Z}EG_n, M) \\ &= \mathbf{Z}G\text{-mod}(\mathbf{Z}[G^{\times n+1}], M) \\ &\cong G\text{-set}(G^{\times n+1}, \mathcal{U}M) \\ &\cong \text{Set}(G^{\times n}, \mathcal{U}'\mathcal{U}M)\ , \end{aligned}$$

where the two isomorphisms are given respectively by the adjoint pairs

$$G\text{-set} \underset{\mathcal{U}}{\overset{\mathbf{Z}[-]}{\rightleftarrows}} G\text{-mod} ,$$

and

$$\text{Set} \underset{\mathcal{U}'}{\overset{G\times -}{\rightleftarrows}} G\text{-set} .$$

Explicitly, the isomorphism $\text{Set}(G^{\times n}, \mathcal{U}'X) \cong G\text{-set}(G^{\times n+1}, X)$ is given by sending a function $f : G^{\times n} \to \mathcal{U}'X$ to the G-set homomorphism

$$(g_0, \ldots, g_n) \mapsto g_0 f(g_0^{-1}g_1, \ldots, g_0^{-1}g_n) ,$$

with the inverse sending a G-set homomorphism $f' : G^{\times n+1} \to X$ to the function

$$(g_1, \ldots, g_n) \mapsto f'(1, g_1, \ldots, g_n) .$$

Definition 2.4.7. If F is the bar resolution, then $\mathscr{H}om_{\mathbf{Z}G}(F, M)$ is called the *standard* complex and is denoted $C^*(G, M)$.

Taking F instead to be the normalized bar resolution, we get the subcomplex $C^*_N(G, M)$ of $C^*(G, M)$ consisting in degree n of those functions $f : G^{\times n} \to M$ satisfying

$$f(g_1, \ldots, g_n) = 0$$

whenever at least one $g_i = 1$.

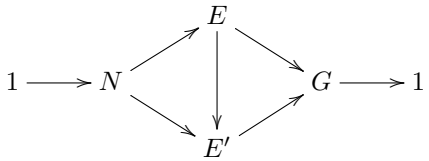
Definition 2.4.8. The cochain complex $C^*_N(G, M)$ is called the *normalized* standard complex. A function $f : G^n \to M$ is said to be *normalized* if it is a cochain in $C^n_N(G, M)$.

2.5 Group extensions

Definition 2.5.1. Let G and N be groups. An *extension* of G by N is a short exact sequence

$$1 \to N \to E \to G \to 1 \qquad (*)$$

of groups. Another extension $1 \to N \to E' \to G \to 1$ is equivalent to $(*)$ if there is a homomorphism $E \to E'$ of groups such that the following diagram commutes:



By the Five lemma, any equivalence of extensions is necessarily an isomorphism.

Definition 2.5.2. An extension $1 \to N \to E \to G \to 1$ is said to be a *split* extension if it is split as a short exact sequence of groups.

Restricting ourselves to those extensions where N is an abelian group A, there is to each extension an associated action of G on A:

Proposition 2.5.3. *An extension of a group G by an abelian group A gives rise to an action of G on A, giving A the structure of a $\mathbf{Z}G$-module.*

Proof. Consider the extension $0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1$. By exactness, A is isomorphic to the kernel of π, which means that A is embedded as a normal subgroup of E. E acts on A by conjugation, which restricts to the trivial action on A. We get an induced action of the quotient group $E/A \cong G$ on A, given explicitly by $i(ga) = \tilde{g}i(a)\tilde{g}^{-1}$ for some $\tilde{g} \in \pi^{-1}(g)$. Viewing the action as a group homomorphism $G \to \mathrm{Aut}(A)$ from G to the group of automorphisms of A, we obtain the corresponding $\mathbf{Z}G$-module structure by the bijection $\mathrm{Grp}(G, \mathrm{Aut}(A)) \cong \mathrm{Rng}(\mathbf{Z}G, \mathrm{End}(A))$. □

Definition 2.5.4. For a fixed $\mathbf{Z}G$-module structure on A, $\mathcal{E}(G, A)$ is the set of equivalence classes of extensions of G by A giving rise to the given group action of G on A.

Definition 2.5.5. Given an action of G on A, the set $A \times G$ together with the multiplication

$$(a, g)(b, h) = (a + gb, gh)$$

is called the *semi-direct product of G and A relative to the given action of G on A* and is denoted $A \rtimes G$.

The unit element of $A \rtimes G$ is $(0, 1)$ and inverses are defined by

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

Note that we get an equality $A \rtimes G = A \times G$ exactly when the G-action on A is trivial, in particular when E is abelian. The canonical inclusion and projection gives us a split extension

$$0 \to A \xrightarrow{\text{incl}} A \rtimes G \xrightarrow{\text{proj}} G \to 1 \, . \tag{2.5.1}$$

Definition 2.5.6. Given an action of G on A, the extension (2.5.1) is called the *canonical split extension of G by A*

Since splittings $s : G \to A \rtimes G$ of the extension (2.5.1) are of the form

$$s(g) = (a, g)$$

for some a in A, with a depending on g, and since

$$s(gh) = s(g)s(h) = (a, g)(b, h) = (a + gb, gh) \, ,$$

the splittings of the extension (2.5.1) are in one to one correspondence with functions $d : G \to A$ satisfying $d(gh) = d(g) + gd(h)$.

The canonical split extension (2.5.1) gives rise to the given action of G on A. To see this, let $g \in G$. Then $\tilde{g} \in \pi^{-1}(g)$ is of the form (a, g) for some $a \in A$

and so if $b \in A$, the the induced G-action $*$ on A is given by

$$\begin{aligned} i(g * b) = \tilde{g} i(b) \tilde{g}^{-1} &= (a, g)(b, 1)(a, g)^{-1} \\ &= (a + gb, g)(g^{-1}(-a), g^{-1}) \\ &= (a + gb - a, 1) \\ &= (gb, 1) \\ &= i(gb) \ , \end{aligned}$$

showing that the induced action is is indeed the action we started out with.

Now, let

$$0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1 \tag{2.5.2}$$

be another extension giving rise to the same action of G on A.

Proposition 2.5.7. *The extension* (2.5.2) *splits if and only if it is equivalent to the canonical split extension of G by A.*

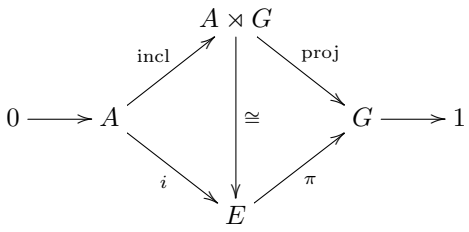
Proof. Assume that the extension splits and let $s : G \to E$ be a splitting. If e is an element of E then $e = e(s\pi e)^{-1}(s\pi e)$ where $e(s\pi e)^{-1} \in \ker \pi$ and $s\pi e \in \operatorname{im} s$. Moreover, if e is in both the the kernel of π and image of s, then $\pi e = 1 = \pi s g = g$ so that $e = 1$. By exactness, $\ker \pi$ is equal to $\operatorname{im} i$ which is isomorphic to A, and since πs is a bijection, s is an injection so that $\operatorname{im} s$ is isomorphic to G. Thus, we get a bijection $A \times G \to E$ of sets by

$$(a, g) \mapsto i(a) s(g) \ .$$

The unique group structure on the set $A \times G$ making this bijection an isomorphism is calculated by noting that $i(ga) = \tilde{g} i(a) \tilde{g}^{-1}$ implies $i(ga)\tilde{g} = \tilde{g} i(a)$, so that

$$\begin{aligned} i(a)s(g)i(b)s(h) &= i(a)i(gb)s(g)s(h) \\ &= i(a + gb)s(gh) \ , \end{aligned}$$

giving the multiplication $(a, g)(b, h) = (a + gb, gh)$ on $A \times G$, which is just $A \rtimes G$. Since the diagram



commutes, we have the required equivalence. Conversely, assuming we have such an equivalence, we get a splitting s by letting $s(g) = \phi s'(g)$ where ϕ is the isomorphism $A \rtimes G \to E$ given by the equivalence and s' a splitting of (2.5.1). □

From this proposition, we see that for a given $\mathbf{Z}G$-module structure A, there is, up to equivalence, only one split extension of G by A giving rise to the given action of G on A.

Given the extension (2.5.2), we may always choose a normalized set-theoretic section of π, i.e. a function $s : G \to E$ such that $\pi s = id_G$ and such that $s(1) = 1$. Since

$$\pi(s(g)s(h)) = \pi s(g)\pi s(h) = gh = \pi s(gh)$$

we have that $s(g)s(h)s(gh)^{-1}$ is in $i(A)$. This gives a function

$$f : G \times G \to A$$

defined by $i(f(g,h)) = s(g)s(h)s(gh)^{-1}$. Note that if s is normalized, then this implies that f too is normalized, i.e.

$$f(g,1) = f(1,g) = 0\ . \tag{2.5.3}$$

This is true since $i(f(1,g)) = s(g)s(1)s(g)^{-1} = s(g)s(g)^{-1} = 1$ and

$$i(f(g,1)) = s(1)s(g)s(g)^{-1} = 1\ .$$

Since f is identically 1 if and only if s is a homomorphism, f measures the failure of s being a splitting. Letting ϕ be the bijection $\phi : A \times G \to E$, defined by

$$\phi(a,g) = i(a)s(g)\ ,$$

we have that

$$\begin{aligned} i(a)s(g)i(b)s(h) &= i(a)i(gb)s(g)s(h) \\ &= i(a+gb)i(f(g,h))s(gh) \\ &= i(a+gb+f(g,h))s(gh)\ . \end{aligned}$$

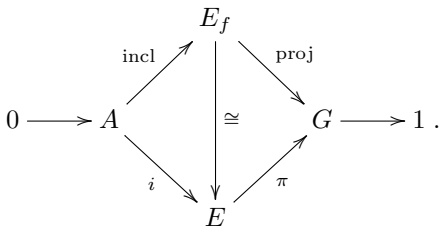
Thus, the group law on the set $A \times G$ making ϕ an isomorphism is defined by

$$(a,g)(b,h) = (a+gb+f(g,h), gh)\ .$$

Letting E_f denote the set $A \times G$ together with this group structure, we get an extension

$$0 \to A \xrightarrow{\text{incl}} E_f \xrightarrow{\text{proj}} G \to 1\ , \tag{2.5.4}$$

which is equivalent to (2.5.2), seen again from the commutativity of the diagram



Moreover, the G-action $*$ on A induced by the extension (2.5.4), is the given G-action:

$$\begin{aligned} \text{incl}(g*a) &= \tilde{g}\,\text{incl}(a)\tilde{g}^{-1} \\ &= (b,g)(a,1)(b,g)^{-1} \\ &= (b+ga+f(g,1),g)(-g^{-1}f(g,g^{-1}) - g^{-1}b, g^{-1}) \\ &= (b+ga-f(g,g^{-1})-b+f(g,g^{-1}),1) \\ &= (ga,1) = \text{incl}(ga)\ . \end{aligned}$$

Thus, given the function f defined above we can, up to equivalence, reconstruct the extension (2.5.2).

Proposition 2.5.8. *Let A be a $\mathbf{Z}G$-module and let $f : G\times G \to A$ be a function satisfying* (2.5.3)*. The binary operation $(a,g)(b,h) = (a + bg + f(g,h), gh)$ defines a group structure on $A \times G$ if and only if*

$$gf(h,k) - f(gh,k) + f(g,hk) - f(g,h) = 0\ . \tag{2.5.5}$$

Moreover, if f satisfies (2.5.5)*, the canonical inclusion and projection gives an extension*

$$0 \to A \xrightarrow{\text{incl}} (A \times G)_f \xrightarrow{\text{proj}} G \to 1 \tag{2.5.6}$$

inducing the given G-action on A. This extension also has the property that if $s' : G \to A \times G$ is the canonical cross-section $g \mapsto (0,g)$, then the function $f' : G \times G \to A$ defined by $\text{incl}(f'(g,h)) = s'(g)s'(h)s'(gh)^{-1}$, is the function f.

Proof. Assume that the given operation defines a group structure, then associativity holds only if

$$[(a,g)(b,h)](c,k) = (a + gb + f(g,h) + ghc + f(gh,k), ghk)$$

is equal to

$$(a,g)[(b,h)(c,k)] = (a + gb + ghc + gf(h,k) + f(g,hk), ghk)\ .$$

This holds only if f satisfies (2.5.5). Conversely, if f satisfies the given condition, then associativity obviously holds. Now assume f satisfies the condition (2.5.5). The canonical inclusion and projection define homomorphisms in the sequence (2.5.6) since

$$\text{incl}(a+b) = (a+b,1) = (a+b+f(1,1),1) = \text{incl}(a)\,\text{incl}(b)$$

and

$$\text{proj}((a,g)(b,h)) = \text{proj}(a + bg + f(g,h), gh) = gh = \text{proj}(a,g)\,\text{proj}(b,h)\ .$$

Thus, by the injectivity of incl and surjectivity of proj, the sequence (2.5.6) is an extension, inducing the G- action $*$ on A defined by

$$\begin{aligned}
\text{incl}(g * a) &= \tilde{g}\,\text{incl}(a)\tilde{g}^{-1} \\
&= (b,g)(a,1)(b,g)^{-1} \\
&= (b + ga + f(g,1), g)(-g^{-1}f(g,g^{-1}) - g^{-1}b, g^{-1}) \\
&= (b + ga - f(g,g^{-1}) - b + f(g,g^{-1},1) \\
&= (ga,1) = \text{incl}(ga)\ ,
\end{aligned}$$

which is the given G-action. Lastly,

$$\begin{aligned}
\text{incl}(f'(g,h)) &= (0,g)(0,h)(0,gh)^{-1} \\
&= (f(g,h),gh)(-(gh)^{-1}f(gh,(gh)^{-1}),(gh)^{-1}) \\
&= (f(g,h) - f(gh,(gh)^{-1}) + f(gh,(gh)^{-1}),1) \\
&= (f(g,h),1) = \text{incl}(f(g,h))\ ,
\end{aligned}$$

showing that f' is equal to f. □

Observe that functions $G \times G \to A$ satisfying (2.5.3) correspond to 2-cochains in the normalized chain complex $C_N^*(G, A)$, and that (2.5.5) holds if and only if f is a cocycle.

Let $s : G \to E$ be a normalized section of π in (2.5.2). If s' is any other normalized section, then due to the bijection $\phi : A \times G \to E$, the element $s'(g)$ in E can be written $i(a)s(g)$ for some $a \in A$, and so s' must be of the form

$$g \mapsto i(c(g))s(g)$$

for some function $c : G \to A$ satisfying $c(1) = 0$. The function $f' : G \times G \to A$ defined by $i(f'(g, h)) = s'(g)s'(h)s'(gh)^{-1}$ then has the values

$$\begin{aligned} i(f'(g,h)) &= i(c(g))s(g)i(c(h))s(h)(i(c(gh)s(gh))^{-1} \\ &= i(c(g))i(gc(h))s(g)s(h)s(gh)^{-1}i(c(gh))^{-1} \\ &= i(c(g) + gc(h) + f(g,h))i(c(gh))^{-1} \\ &= i(c(g) + gc(h) + f(g,h) - c(gh)) \ , \end{aligned}$$

and so $f'(g, h) = f(g, h) + c(g) + gc(h) - c(gh) = f(g, h) + (\delta c)(g, h)$. Thus, the change of section of π in (2.5.2) is reflected by modifying f by a coboundary in $C_N^2(G, A)$, and we have the following theorem [1, IV.3.12]:

Theorem 2.5.9. *For a fixed* $\mathbf{Z}G$*-module structure on* A*, there is a bijection*

$$\mathcal{E}(G, A) \cong H^2(G, A)$$

given by sending an extension $0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ *to the function*

$$f : G \times G \to A$$

defined by

$$i(f(g, h)) = s(g)s(h)s(gh)^{-1}$$

where s *is any normalized set-theoretic section of the extension. The inverse is given by sending a function* $f : G \times G \to A$ *to the extension*

$$0 \to A \xrightarrow{\text{incl}} (A \times G)_f \xrightarrow{\text{proj}} G \to 1 \ .$$

3 On the extension giving the truncated Witt vectors

For the remainder of this thesis, let A be a commutative ring and p a prime number.

3.1 Witt vectors in general

Definition 3.1.1. A set S of positive integers is a *truncation set* if $n \in S$ and $d \mid n$ implies $d \in S$.

A truncation set S gives rise to the *Witt ring* $W_S(A)$, defined as a set by $W_S(A) = A^S$. The *ghost map* $w : W_S(A) \to A^S$ is given in the n-th coordinate by

$$a \mapsto w_n(a) = \sum_{d|n} d a_d^{n/d} \ .$$

By [2, proposition 2], there is a unique ring structure on $W_S(A)$ such that the ghost map is a natural transformation of functors from rings to rings. This unique ring structure is obtained explicitly by forcing w to be a homomorphism of rings.

Definition 3.1.2. For n a non-negative integer, $W_n(A)$ is the Witt ring on the truncation set $S_n = \{1, p, p^2, \ldots, p^{n-1}\}$. The vectors in $W_n(A)$ and A^{S_n} are indexed over the set $\{0, \ldots, n-1\}$ of the powers of p in S_n

3.2 The extension underlying $W_2(A)$

Let $W = W_2(A)$. The ghost map $w : W \to A \times A$ is given by

$$(a_0, a_1) \mapsto (a_0, a_0^p + p a_1) \ .$$

If $a = (a_0, a_1)$ and $b = (b_0, b_1)$ are two vectors in W, the sum $a + b$ is given by solving the equation $w(a + b) = w(a) + w(b)$ for $a + b$. We have

$$\begin{aligned} w(a) + w(b) &= (a_0 + b_0, a_0^p + b_0^p + p(a_1 + b_1)) \\ w(a + b) = w(s) &= (s_0, s_0^p + p s_1) \ , \end{aligned}$$

which gives the following equations:

$$\begin{aligned} s_0 &= a_0 + b_0, \\ p s_1 &= -\sum_{i=1}^{p-1} \binom{p}{i} a_0^p b_0^{p-i} \ . \end{aligned}$$

Since $1 \leq i < p$, the binomial coefficients $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ are all divisible by p, and hence we can solve the second equation above for s_1, giving

$$s_1 = (a_0^p + b_0^p - (a_0 + b_0)^p)/p \ .$$

This forces the following group law on W

$$a + b = (a_0 + b_0, a_1 + b_1 + (a_0^p + b_0^p - (a_0 + b_0)^p)/p) \ .$$

Letting $f : A \times A \to A$ be the map $(x, y) \mapsto (x^p + y^p - (x + y)^p)/p$, this group law takes on the familiar form

$$a + b = (a_0 + b_0, a_1 + b_1 + f(a_0, b_0)) \ .$$

The identity element in W is $(0, 0)$ and the additive inverse of a is

$$-a = \begin{cases} (-a_0, -a_1) & p > 2 \\ (-a_0, a_0^2 - a_1) & p = 2 \ . \end{cases}$$

Since the ghost map restricts to the identity on A in its zeroth coordinate, the projection $W \to A$ from W to A sending (a, b) to a is a surjection of rings. The kernel of this projection is $I = \{(0, a) \mid a \in A\}$.

Forgetting down to abelian groups, we get an extension

$$0 \to I \xrightarrow{\text{incl}} W \xrightarrow{\text{proj}} A \to 0 \tag{3.2.1}$$

of A by I. Since W is abelian, the associated $\mathbf{Z}A$-module structure on I is trivial. Observing that the map $I \to A$ sending $(0, a)$ to a is an isomorphism of groups, and that interchanging the two coordinates in W yields an isomorphism $W \cong (A \times A)_f$, we see that f represents the class of this extension in $H^2(A, A)$. Indeed, by applying the coboundary map $\delta : C^2(A, A) \to C^3(A, A)$ described in (2.4.1) to the cochain f we find that

$$\begin{aligned}
\delta f(a_1, a_2, a_3) &= -\left(f(a_2, a_3) - f(a_1 + a_2, a_3) + f(a_1, a_2 + a_3) - f(a_1, a_2)\right) \\
&= -\frac{a_2^p + a_3^p - (a_2 + a_3)^p}{p} + \frac{(a_1 + a_2)^p + a_3^p - ((a_1 + a_2) + a_3)^p}{p} \\
&\quad - \frac{a_1^p + (a_2 + a_3)^p - (a_1 + (a_2 + a_3))^p}{p} \\
&\quad + \frac{a_1^p + a_2^p - (a_1 + a_2)^p}{p} \\
&= 0 \,,
\end{aligned}$$

showing that f is a cocycle. Moreover, the equations

$$\begin{aligned}
f(a, 0) &= \frac{a^p - a^p}{p} = 0 \\
f(0, b) &= \frac{b^p - b^p}{p} = 0
\end{aligned}$$

hold for any a, b in A, showing that f is normalized. The following diagram then shows that f represents the class of (3.2.1).

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I & \longrightarrow & W & \longrightarrow & A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cong} & & \| & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & W & \longrightarrow & A & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \cong} & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & (A \times A)_f & \longrightarrow & A & \longrightarrow & 0 \,.
\end{array}$$

Example 3.2.1. Let $A = \mathbf{F}_p$ be the field of characteristic p. As we have seen, the sum $a + b$ of two vectors a and b in W is determined by the value of the function $f : \mathbf{F}_p \times \mathbf{F}_p \to \mathbf{F}_p$ on the vector (a_0, b_0). Examining the case $p = 2$, we see that

$$a + b = (a_0 + b_0, a_1 + b_1 - a_0 b_0) \,.$$

For the vector $(1, 0)$ in W, we have that $2(1, 0) = (1, 0) + (1, 0) = (2, -1) = (0, 1)$, which is not zero in $\mathbf{F}_2 \times \mathbf{F}_2$. This implies that W cannot be isomorphic to

$\mathbf{F}_2 \times \mathbf{F}_2$, and since W is of order 4, then by the classification of finitely generated abelian groups, we must have

$$W \cong \mathbf{Z}/4\mathbf{Z} \, .$$

In fact, if p is any prime number and n a non-negative integer, then [3, corollary §6.8] characterizes $W_n(\mathbf{F}_p)$ by

$$W_n(\mathbf{F}_p) \cong \mathbf{Z}/p^n\mathbf{Z} \, .$$

If p acts injectively on $H^2(A, A)$, the extension (3.2.1) is a split extension. To see this, let $g : A \to A$ be the p-th power map $a \mapsto a^p$. Then

$$\begin{aligned} \delta g(a, b) &= ag(b) - g(a + b) + g(a) \\ &= a^p + b^p - (a + b)^p \\ &= pf(a, b) \, , \end{aligned}$$

so the class of pf is zero in $H^2(A, A)$, implying that the class of f is zero if p acts injectively. Note that g is a normalized cochain in $C^1(A, A)$.

Since A is commutative, the multiplication map $A^{\times p} \to A$ factors through the projection $A^{\times p} \to A^{\times p}/C_p$ of $A^{\times p}$ onto its C_p-orbits, and thus corresponds uniquely to the linear map

$$\mu : A^{\otimes p}/C_p \to A$$

defined by sending an element $a_1 \otimes \cdots \otimes a_p$ to the product $a_1 \cdots a_p$.

Let X be the set of surjective functions $\{1, \ldots, p\} \to \{0, 1\}$, and let the function $f' : A \times A \to A^{\otimes p}/C_p$ be given by

$$f'(a, b) = - \sum_{[x] \in X/C_p} [a_{x_1} \otimes \cdots \otimes a_{x_p}] \, ,$$

where $a_0 = a$ and $a_1 = b$. In words, $-f'(a, b)$ is the sum of all the orbits of tensors consisting of both a's and b's.

Lemma 3.2.2. *Let $a \neq b$. For each $1 \leq i < p$, the number of summands in $f'(a, b)$ whose representing tensors consist of exactly i a's is $\binom{p}{i}/p$. This gives a total of $(2^p - 2)/p$ summands.*

Proof. Let $1 \leq i < p$. There are $\binom{p}{i}$ functions in X that hit 0 exactly i times. Since p is prime, C_p is a simple group, and since each orbit $[x]$ in X is in one to one correspondence with the quotient group C_p/C_{p_x} (where C_{p_x} is the isotropy subgroup of x), we have that each orbit must be of order either p or 1. Suppose $[x]$ has order 1. Then for a generator t of C_p, we must have $t^j x = x$ for each $j = 0, \ldots, p - 1$. Since $t^j x(i) = x(i + j \mod p)$, this means that x is not surjective, a contradiction. Thus, every orbit of X has p elements, and so the total number of orbits of tensors consisting of exactly i a's is equal to $\binom{p}{i}/p$.

Using the Binomial theorem, we see that the total number of summands is

$$\begin{aligned}\sum_{i=1}^{p-1}\binom{p}{i}/p &= \frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}1^i 1^{p-i} \\ &= \frac{1}{p}\left(\sum_{i=0}^{p}\binom{p}{i}1^i 1^{p-i} - 2\right) \\ &= \frac{(1+1)^p - 2}{p} \\ &= \frac{2^p - 2}{p}\ .\end{aligned}$$

□

Proposition 3.2.3. *The diagram below commutes.*

$$\begin{array}{ccc} A\times A & \xrightarrow{f} & A \\ {\scriptstyle f'}\downarrow & \nearrow_{\mu} & \\ A^{\otimes p}/C_p & & \end{array}$$

Proof. Need to show that $\mu f' = f$. If $a, b \in A$, then

$$\begin{aligned}\mu f'(a,b) &= \mu\left(-\sum_{[x]\in X/C_p}[a_{x_1}\otimes\cdots\otimes a_{x_p}]\right) \\ &= -\sum_{[x]\in X/C_p}\mu[a_{x_1}\otimes\cdots\otimes a_{x_p}] \\ &= -\sum_{[x]\in X/C_p}a_{x_1}\cdots a_{x_p} \\ &= -\sum_{i=1}^{p-1}\frac{\binom{p}{i}}{p}a^i b^{p-i} \\ &= \frac{a^p + b^p - \sum_{i=0}^{p}\binom{p}{i}a^i b^{p-i}}{p} \\ &= \frac{a^p + b^p - (a+b)^p}{p} \\ &= f(a,b)\ .\end{aligned}$$

□

Since $x\otimes 0 = 0$, we have for any a, b in A

$$f'(a,0) = f'(0,b) = 0\ ,$$

showing that f' is normalized. To show that f' is also a cocycle, we need the following lemma.

Lemma 3.2.4. *Let a, b, c be elements of A and let Y be the set of surjective functions $\{1, \dots, p\} \to \{0, 1, 2\}$. Then the following two equations hold*

$$f'(a+b, c) = f'(a, c) + f'(b, c) - R$$
$$f'(a, b+c) = f'(a, b) + f'(a, c) - R\,,$$

where $R = \sum_{[y] \in Y/C_p} [\rho_{y_1} \otimes \cdots \otimes \rho_{y_p}]$, $\rho_0 = a$, $\rho_1 = b$ and $\rho_2 = c$.

Proof. In the first equality, the summands in $f'(a, c)$ are summands in $f'(a+b, c)$ since any summand $[\alpha_{x_1} \otimes \cdots \otimes \alpha_{x_p}]$ in $f'(a, c)$ is a term in the summand $[\beta_{x_1} \otimes \cdots \otimes \beta_{x_p}]$ in $f'(a+b, c)$. Since A is abelian, the same holds for $f'(b, c)$. The remaining summands are represented by tensors consisting of both a's, b's and c's, and hence are of the form $[\rho_{y_1} \otimes \cdots \otimes \rho_{y_p}]$. Let φ be the map $\{0, 1, 2\} \to \{0, 1\}$ defined by

$$0 \mapsto 0$$
$$1 \mapsto 0$$
$$2 \mapsto 1$$

Each summand $[\rho_{y_1} \otimes \cdots \otimes \rho_{y_p}]$ in R is a term in the summand $[\beta_{\varphi_{y_1}} \otimes \cdots \otimes \beta_{\varphi_{y_p}}]$ in $f'(a+b, c)$. This shows the first equality. Finally, since f' is symmetric,

$$f'(a, b+c) = f'(b+c, a) = f'(a, b) + f'(a, c) - R\,.$$

□

Let us now calculate $\delta f'$ where $\delta : C^2(A, A^{\otimes p}/C_p) \to C^3(A, A^{\otimes p}/C_p)$ is the coboundary map. Using Lemma 3.2.4, we have

$$\begin{aligned}
\delta f'(a, b, c) &= (-1)^3 f' d(a, b, c) \\
&= -f'(b, c) + f'(a+b, c) - f'(a, b+c) + f'(a, b) \\
&= -f'(b, c) + f'(b, c) - f'(a, b) + f'(a, b) \\
&= 0\,.
\end{aligned}$$

This shows f' is a normalized cocycle in $C^2(A, A^{\otimes p}/C_p)$, and f' represents the class of the extension

$$0 \to A^{\otimes p}/C_p \to W' \to A \to 0 \tag{3.2.2}$$

in $\mathcal{E}(A, A^{\otimes p}/C_p)$, where $W' \cong (A^{\otimes p}/C_p \times A)_{f'}$. Notice that unlike W, the group law on W' does not depend on the multiplication in A. We see that the extension (3.2.2) is still split if p acts injectively on $H^2(A, A^{\otimes p}/C_p)$. Indeed, if

$g' : A \to A^{\otimes p}/C_p$ is the cochain $a \mapsto [a^{\otimes p}]$, then

$$\begin{aligned}
\delta g'(a,b) &= ag'(b) - g'(a+b) + g'(a) \\
&= [b^{\otimes p}] - [(a+b)^{\otimes p}] + [a^{\otimes p}] \\
&= [b^{\otimes p}] - \left(\sum_{x \in X} [a_{x_1} \otimes \cdots \otimes a_{x_p}] + [a^{\otimes p}] + [b^{\otimes p}] \right) + [a^{\otimes p}] \\
&= - \sum_{x \in X} [a_{x_1} \otimes \cdots \otimes a_{x_p}] \\
&= - \sum_{[x] \in X/C_p} p[a_{x_1} \otimes \cdots \otimes a_{x_p}] \\
&= -p \sum_{[x] \in X/C_p} [a_{x_1} \otimes \cdots \otimes a_{x_p}] \\
&= pf'(a,b) \ .
\end{aligned}$$

If p acts injectively, this implies that the class of f' is zero in $H^2(A, A^{\otimes p}/C_p)$.

Definition 3.2.5. Let R be a ring and let M and N be R-modules. If $F \to M$ and $P \to N$ are projective resolutions of M and N over R, then

$$\mathrm{Tor}_*^R(M,N) = H_*(F \otimes_R N) = H_*(F \otimes_R P) = H_*(M \otimes_R P) \ .$$

Note that when $R = \mathbf{Z}$, we write $\mathrm{Tor}_*(M,N)$ instead of $\mathrm{Tor}_*^{\mathbf{Z}}(M,N)$.

Proposition 3.2.6. *For any abelian group A, $\mathrm{Tor}_i(\mathbf{Z}, A) = 0$ for $i > 0$ and $\mathrm{Tor}_0(\mathbf{Z}, A) = A$.*

Proof. Let $\varepsilon : F \to A$ be a projective resolution of A over $\mathbf{Z}$. By definition, we have $\mathrm{Tor}_i(\mathbf{Z}, A) = H_i(\mathbf{Z} \otimes F) = H_i(F)$. Since F is exact at all positive degrees, $H_i(F) = 0$ for $i > 0$. If $i = 0$ then, since ε is a weak equivalence, $H_0(F) = A$. □

Let now $\varepsilon : P \to \mathbf{F}_p$ denote the sequence

$$0 \to \mathbf{Z} \xrightarrow{p} \mathbf{Z} \xrightarrow{\varepsilon} \mathbf{F}_p \to 0 \ ,$$

where p is multiplication with p and ε is the quotient map. Since the sequence above is exact and each P_i is free, this forms a projective resolution of $\mathbf{F}_p$ over $\mathbf{Z}$. Since projective modules are flat, tensoring P with the extension (3.2.2) yields a short exact sequence

$$0 \to P \otimes A^{\otimes p}/C_p \to P \otimes W' \to P \otimes A \to 0 \tag{3.2.3}$$

of chain complexes. The chain complexes in (3.2.3) are the columns in the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbf{Z} \otimes A^{\otimes p}/C_p & \longrightarrow & \mathbf{Z} \otimes W' & \longrightarrow & \mathbf{Z} \otimes A & \longrightarrow & 0 \\
 & & \downarrow p & & \downarrow p & & \downarrow p & & \\
0 & \longrightarrow & \mathbf{Z} \otimes A^{\otimes p}/C_p & \longrightarrow & \mathbf{Z} \otimes W' & \longrightarrow & \mathbf{Z} \otimes A & \longrightarrow & 0
\end{array}$$

Applying the Snake lemma to the diagram above yields the following long exact sequence in homology:

$$\begin{aligned} 0 \to \mathrm{Tor}_1(\mathbf{F}_p, A^{\otimes p}/C_p) \to \mathrm{Tor}_1(\mathbf{F}_p, W') \to \mathrm{Tor}_1(\mathbf{F}_p, A) \to \\ \mathbf{F}_p \otimes A^{\otimes p}/C_p \to \mathbf{F}_p \otimes W' \to \mathbf{F}_p \otimes A \to 0 \, . \end{aligned} \tag{3.2.4}$$

By Proposition 2.2.3, A has a projective resolution F over $\mathbf{Z}$. The tensor product of P with F yields another short exact sequence

$$0 \to \mathbf{Z} \otimes F \to \mathbf{Z} \otimes F \to \mathbf{F}_p \otimes F \to 0 \tag{3.2.5}$$

of chain complexes. The chain complexes in (3.2.5) are the columns in the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z} \otimes F_1 & \xrightarrow{p} & \mathbf{Z} \otimes F_1 & \longrightarrow & \mathbf{F}_p \otimes F_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbf{Z} \otimes F_0 & \xrightarrow{p} & \mathbf{Z} \otimes F_0 & \longrightarrow & \mathbf{F}_p \otimes F_0 & \longrightarrow & 0 \end{array}$$

This yields another long exact sequence in homology:

$$0 \to \mathrm{Tor}_1(\mathbf{F}_p, A) \to A \xrightarrow{p} A \to \mathbf{F}_p \otimes A \to 0 \, . \tag{3.2.6}$$

If p is zero in A then $p : A \to A$ is the zero map, and so (3.2.6) becomes

$$0 \to \mathrm{Tor}_1(\mathbf{F}_p, A) \to A \to 0 \to A \to \mathbf{F}_p \otimes A \to 0$$

giving the following isomorphisms:

$$\mathrm{Tor}_1(\mathbf{F}_p, A) \cong A \cong \mathbf{F}_p \otimes A \, . \tag{3.2.7}$$

Moreover, if p is zero in A then we have

$$\mathrm{Tor}_1(\mathbf{F}_p, A^{\otimes p}/C_p) \cong A^{\otimes p}/C_p \cong \mathbf{F}_p \otimes A^{\otimes p}/C_p \, . \tag{3.2.8}$$

Applying the isomorphisms in (3.2.7) and (3.2.8) to (3.2.4), we get the long exact sequence

$$0 \to A^{\otimes p}/C_p \to \mathrm{Tor}_1(\mathbf{F}_p, W') \to A \xrightarrow{\partial} A^{\otimes p}/C_p \to W' \otimes \mathbf{F}_p \to A \to 0 \, .$$

Note that the map ∂ in the sequence above is the connecting homomorphism

$$\mathrm{Tor}_1(\mathbf{F}_p, A) \to \mathbf{F}_p \otimes A^{\otimes p}/C_p$$

in (3.2.4). Chasing the diagram given by (3.2.3), an element x_1 in A is the image of the element $(0, x_1)$ in W'. Applying the multiplication map p to the element $(0, x_1)$, we get that $\partial(x_1)$ is the first coordinate of $p(0, x_1)$.

Definition 3.2.7. Let $(0, x_1), \ldots, (0, x_n)$ be elements of W'. Define h to be the function $A^{\times n} \to A^{\otimes p}/C_p$ satisfying the following relation in W'.

$$(0, x_1) + \cdots + (0, x_n) = (h(x_1, \ldots, x_n), x_1 + \cdots + x_n) \, .$$

To be able to define the connecting homomorphism ∂ explicitly, we need a concrete formula for the function h from Definition 3.2.7.

Lemma 3.2.8. *Let $x = (x_1, \ldots, x_n)$ be a sequence in $A^{\times n}$ and let Z be the set of non-constant functions $\{1, \ldots, p\} \to \{1, \ldots, n\}$. The following equality holds*

$$ph(x) = -p \sum_{[z] \in Z/C_p} [x_{z_1} \otimes \cdots \otimes x_{z_p}].$$

Proof. Let X be the sum $\sum_{i=1}^{n} x_i$ and observe that

$$-\sum_{z \in Z} [x_{z_1} \otimes \cdots \otimes x_{z_p}] = -[X^{\otimes p} - x_1^{\otimes p} - \cdots - x_n^{\otimes p}].$$

Since each C_p-orbit in Z has exactly p elements, this implies that

$$-p \sum_{[z] \in Z/C_p} [x_{z_1} \otimes \cdots \otimes x_{z_p}] = -[X^{\otimes p} - x_1^{\otimes p} - \cdots - x_n^{\otimes p}] \, .$$

For the case $n = 1$, we have $ph(x) = 0 = -[(x_1)^{\otimes p} - x_1^{\otimes p}]$. Assume the statement holds for some $n = k > 1$. By definition of h and the group law in W', we get

$$\begin{aligned} \sum_{i=1}^{k+1} (0, x_i) &= \sum_{i=1}^{k} (0, x_i) + (0, x_{k+1}) \\ &= (h(x), X) + (0, x_{k+1}) \\ &= (h(x) + f'(X, x_{k+1}), X + x_{k+1}) \end{aligned}$$

Multiplying the first coordinate in the sum above by p yields

$$\begin{aligned} ph(x) + pf'(X, x_{k+1}) &= -[X^{\otimes p} - x_1^{\otimes p} - \cdots - x_k^{\otimes p}] \\ &\quad - [(X + x_{k+1})^{\otimes p} - X^{\otimes p} - x_{k+1}^{\otimes p}] \\ &= -[(X + x_{k+1})^{\otimes p} - x_1^{\otimes p} - \cdots - x_{k+1}^{\otimes p}] \, , \end{aligned}$$

which is the statement for $n = k + 1$, completing the proof. □

Proposition 3.2.9. *If Z is the set of non-constant functions $\{1, \ldots, p\} \to \{1, \ldots, n\}$ then*

$$h(x) = -\sum_{[z] \in Z/C_p} [x_{z_1} \otimes \cdots \otimes x_{z_p}] \, .$$

Proof. Let $B = \mathbf{Z}A$ be the free abelian group on A and let $g : A^{\times n} \to A^{\otimes p}/C_p$ be defined by

$$g(x) = -\sum_{[z] \in Z/C_p} [x_{z_1} \otimes \cdots \otimes x_{z_p}] \, .$$

We will prove the Proposition by showing that $h - g = 0$. Since $B = \oplus_A \mathbf{Z}$ we have

$$\begin{aligned} B^{\otimes p} &= (\oplus_A \mathbf{Z})^{\otimes p} \\ &\cong \oplus_{A^{\times p}} (\mathbf{Z}^{\otimes p}) \\ &\cong \oplus_{A^{\times p}} \mathbf{Z} \\ &= \mathbf{Z}[A^{\times p}] \end{aligned}$$

so that $B^{\otimes p}$ is isomorphic to the free abelian group on $A^{\times p}$. Since $\mathbf{Z}[-]$ is the left adjoint to the forgetful functor from abelian groups to sets, it takes colimits to colimits. Thus,

$$\begin{aligned} B^{\otimes p}/C_p &\cong \mathbf{Z}[A^{\times p}]/C_p \\ &\cong \mathbf{Z}[A^{\times p}/C_p] \end{aligned}$$

so that $B^{\otimes p}/C_p$ is the free abelian group on $A^{\times p}/C_p$. The naturality of $\eta = h - g$ now yields the commutative diagram

$$\begin{array}{ccc} B^{\times n} & \longrightarrow & A^{\times n} \\ \downarrow{\scriptstyle \eta_B} & & \downarrow{\scriptstyle \eta_A} \\ B^{\otimes p}/C_p & \longrightarrow & A^{\otimes p}/C_p \ . \end{array}$$

The horizontal maps are given by sending each generator to its corresponding element. Since $B^{\otimes p}/C_p$ is torsion free, Lemma 3.2.8 implies that η_B is zero and since the top horizontal map in the diagram above is surjective, we have that η_A must also be zero. □

The sum $n(0,x)$ in W' is given by the last proposition as $(h(x,\ldots,x), nx)$, where $h(x,\ldots,x)$ is equal to the sum $-\sum_{[z]\in Z/C_p}[x^{\otimes p}]$. Since there are exactly $n^p - n$ functions in Z, there are $(n^p - n)/p$ orbits in Z/C_p. Thus,

$$n(0,x) = \left(-\frac{n^p - n}{p}[x^{\otimes p}], nx\right) \ .$$

This shows that $\partial(x) = -\frac{p^p - p}{p}[x^{\otimes p}]$. If p is zero in A then since $p \geq 2$, we have

$$\begin{aligned} -\frac{p^p - p}{p} &= \frac{p - p^p}{p} \\ &= 1 - p^{p-1} \\ &= 1 \ , \end{aligned}$$

showing that the connecting homomorphism

$$\partial : A \to A^{\otimes p}/C_p$$

is equal to the map g'. Observe that p is zero in A, this implies that p is not zero in W' since $p(0,1)$ in W' would then be equal to $(g'(1), 0)$ which is not zero.

What we have discovered is that in the case of an extension of A by $A^{\otimes p}/C_p$ represented by the 2-cocycle f', the connecting homomorphism ∂ coincides with a particular given 1-cochain g' when p is zero in A. An effort to generalize this discovery provokes the following question:

Question. Given a module M and a cocycle φ in $C^2_N(A, M)$ satisfying

$$p\varphi = \delta\gamma$$

for some cochain $\gamma : A \to M$ in $C^1_N(A, M)$, will tensoring the resolution P with extensions $0 \to M \to E \to A \to 0$ represented by φ always give long exact

sequences

$$0 \to \mathrm{Tor}_1(\mathbf{F}_p, M) \to \mathrm{Tor}_1(\mathbf{F}_p, E) \to \mathrm{Tor}_1(\mathbf{F}_p, A) \xrightarrow{\partial}$$
$$\mathbf{F}_p \otimes M \to \mathbf{F}_p \otimes E \to \mathbf{F}_p \otimes A \to 0$$

in which the connecting homomorphism ∂ is equal to γ?

Observe that the question above assumes a priori that p times the representing cocycle φ is equal to the coboundary of some cochain γ, while the assumption that p is zero in A and M is removed.

To answer the question, let us again construct the connecting homomorphism ∂ by chasing the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \\ 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

We start by picking an element a in A in the kernel of p, i.e. such that $pa = 0$. This element is the image of the element $(0, a)$ in E. Applying the multiplication map p to $(0, a)$, we have that $\partial(a)$ is the first coordinate of $p(0, a)$. Recall that the group operation in E is determined by the cocycle φ in the following way:

$$(m, a) + (n, b) = (m + n + \varphi(a, b), a + b) \; .$$

Calculating $p(0, a)$ according to this group law then gives

$$\begin{aligned} p(0, a) &= (\varphi(a, a) + \varphi(2a, a) + \cdots + \varphi((p-1)a, a), pa) \\ &= \left(\sum_{i=1}^{p-1} \varphi(ia, a), pa \right) \; . \end{aligned}$$

Multiplying the first coordinate of $p(0, a)$ by p, we get

$$p \left(\sum_{i=1}^{p-1} \varphi(ia, a) \right) = \sum_{i=1}^{p-1} p\varphi(ia, a) \; .$$

By assumption, $p\varphi(ia, a) = \delta\gamma(ia, a)$. Substituting this in the sum above yields

$$\begin{aligned} \sum_{i=1}^{p-1} p\varphi(ia, a) &= \sum_{i=1}^{p-1} \delta\gamma(ia, a) \\ &= \sum_{i=1}^{p-1} \gamma(a) - \gamma(ia + a) + \gamma(ia) \\ &= \sum_{i=1}^{p-1} \gamma(a) - \gamma((i+1)a) + \gamma(ia) \; . \end{aligned}$$

For example if $p = 2$ we have

$$2\varphi(a, a) = \gamma(a) - \gamma(2a) + \gamma(a) = 2\gamma(a) \; .$$

In general, the terms $-\gamma((j+1)a)$ and $\gamma(ia)$ cancel for $j = i-1$ whenever $1 < i < p$. The remaining terms in the sum above are then

$$\begin{aligned}\sum_{i=1}^{p-1} \gamma(a) - \gamma((i+1)a) + \gamma(ia) &= \left(\sum_{i=1}^{p-1} \gamma(a)\right) - \gamma(pa) + \gamma(a) \\ &= (p-1)\gamma(a) + \gamma(a) \\ &= p\gamma(a)\ ,\end{aligned}$$

which shows that $p\partial(a) = p\gamma(a)$. By modifying the proof of Proposition 3.2.9 we see that $\partial = \gamma$ and we have proved the following theorem.

Theorem 3.2.10. *Let M be a module, A an abelian group and φ a cocycle in $H^2(A, M)$ representing an extension $0 \to M \to E \to A \to 0$. If φ has the property that*

$$p\varphi = \delta\gamma$$

for some cochain γ in $C_N^1(A, M)$, then the connecting homomorphism ∂ in the long exact sequence

$$\begin{gathered}0 \to \mathrm{Tor}_1(\mathbf{F}_p, M) \to \mathrm{Tor}_1(\mathbf{F}_p, E) \to \mathrm{Tor}_1(\mathbf{F}_p, A) \xrightarrow{\partial} \\ \mathbf{F}_p \otimes M \to \mathbf{F}_p \otimes E \to \mathbf{F}_p \otimes A \to 0\end{gathered}$$

is equal to γ.

References

[1] Kenneth S. Brown. *Cohomology of Groups*. Springer-Verlag, 1982.

[2] Lars Hesselholt. Lecture notes on Witt vectors. `http://www.math.nagoya-u.ac.jp/~larsh/papers/s03/wittsurvey.pdf`, 2005.

[3] Jean-Pierre Serre. *Local Fields*. Springer-Verlag, 1979.