TALK NOTES: CARRYING AND GROUP COHOMOLOGY

JACOB SWENBERG

1. What's up with carrying?

Let $C \subset \mathbb{Z}$ be a set of coset representatives for $\mathbb{Z}/10\mathbb{Z}$. In other words, every $n \in \mathbb{Z}$ can be written uniquely as $10a + b$ for $a \in \mathbb{Z}$ and $b \in C$. Thus, we have a bijection

$$\mathbb{Z} \times C \cong \mathbb{Z}, \qquad (a, b) \mapsto 10a + b.$$

Identifying C with $\mathbb{Z}/10\mathbb{Z}$, we see that the group law on the right of the bijection above does not agree with the natural one on the left. Indeed, let $(a, b), (c, d) \in \mathbb{Z} \times C$. Then while

$$(10a + b) + (10c + d) = 10(a + c) + (b + d),$$

we do not necessarily have $b + d \in C$. However, there exists $e \in C$ such that $b + d = e \in \mathbb{Z}/10\mathbb{Z}$, and so we have a function

$$\sigma : \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$$

such that for all $b, d \in C$, we have

$$b + d - 10\sigma(b, d) \in C.$$

If we view the bijection above as a bijection

$$\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}, \qquad (a, b) \mapsto [a, b],$$

then we have

$$[a, b] + [c, d] = [a + c + \sigma(b, d), b + d].$$

We view the second coordinates above as the 1's digits, and the first coordinates as "everything else." The function $\sigma(b, d)$ is therefore the "carrying the 1" that happens in long addition.

2. Newfangled digits

There are a couple ways we could try to push this. First, what happens if we change our set of coset representatives C? To reframe this choice of coset representatives, we instead consider set-theoretic sections s of the quotient map

$$\pi : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}.$$

In other words, these are functions $s : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$ that satisfy $\pi(s(n)) = n$ for all n. One checks that the choice of a set C of coset representatives for $\mathbb{Z}/10\mathbb{Z}$ is equivalent to the choice of a section s of π. We then think of these sections as choices of meaning for the digits $0, \ldots, 9$. For example, we could just pretend like the digit 9 actually means 19, and that would correspond to a section s with $s(9) = 19$.

Given a section $s : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$, we have a bijection

$$\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}, \qquad (a, b) \mapsto [a, b]_s := 10a + s(b).$$

We would like to understand what the group law on the right corresponds to on the left. To do this, we first observe that for all $b, d \in \mathbb{Z}/10\mathbb{Z}$,

$$\pi(s(b) + s(d) - s(b + d)) = b + d - (b + d) = 0.$$

Therefore, there exists a function

$$\sigma_s : \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$$

such that for all $b, d \in \mathbb{Z}/10\mathbb{Z}$, we have

$$s(b) + s(d) - s(b + d) = 10\sigma_s(b, d).$$

Then

$$[a, b]_s + [c, d]_s = [a + c + \sigma_s(b, d), b + d]_s.$$

Thus the choice of section s affects the carrying function! But how, exactly? Let $s_1, s_2 : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$ be two sections. Then there exists a function $\alpha : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$ such that $s_1(x) - s_2(x) = 10\alpha(x)$. Then

$$\begin{aligned} 10(\sigma_{s_1}(b, d) - \sigma_{s_2}(b, d)) &= (s_1(b) - s_2(b)) \\ &\quad + (s_1(d) - s_2(d)) \\ &\quad - (s_1(b + d) - s_2(b + d)) \\ &= 10(\alpha(b) + \alpha(d) - \alpha(b + d)). \end{aligned}$$

So

$$\sigma_{s_1}(b, d) - \sigma_{s_2}(b, d) = \alpha(b) + \alpha(d) - \alpha(b + d).$$

So changing the choice of section changes the "carrying function" by a function of the form

$$(b, d) \mapsto \alpha(b) + \alpha(d) - \alpha(b + d).$$

A function satisfying this identity is called a ***2-coboundary.***

One could ask how much we could change the section s (i.e. change an α) without changing the carry function. Note that choosing α to be a homomorphism changes the section, but does not change the carrying function. However, in this case, there is no homomorphism $\mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$. Indeed,

$$H^1(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z}) \cong \mathrm{Hom}(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z}) = 0.$$

This isn't the last time we will see group cohomology, however!

It is important to remember that while we have changed the representation of integers into digits, we have not changed the isomorphism class of the group of integers $\mathbb{Z}$ itself. Let us witness this isomorphism. Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Then for all $(c, d) \in \mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$,

$$[a, b]_{s_1} - [c, d]_{s_2} = 10(a - c) + s_1(b) - s_2(d).$$

We would like this to be zero for some choice of (c, d). For this, we choose

$$(c, d) = (a + \alpha(b), b)$$

And one checks that

$$[a + \alpha(b), b]_{s_2} = [a, b]_{s_1}.$$

We say that the map

$$\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}, \qquad (a, b) \mapsto (a + \alpha(b), b)$$

intertwines the group structure induced by s_1 on the left and the group structure induced by s_2 on the right.

3. What if we carried differently?

One can ask what happens when we change the carrying function σ itself directly. We could ask if the binary operation given by the formula

$$[a, b]_\sigma + [c, d]_\sigma = [a + c + \sigma(b, d), b + d]_\sigma$$

is even a group structure. At the very least, we need this operation to be associative. A simple computations shows that this is the same as requiring that:

$$\sigma(x, y) + \sigma(x + y, z) = \sigma(y, z) + \sigma(x, y + z).$$

This is called the ***2-cocycle condition*** and functions

$$\sigma : \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$$

satisfying the 2-cocycle condition are called ***2-cocycles.*** Note that the set of 2-cocycles $Z^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z})$ is a group under pointwise addition of functions, and has the set of 2-coboundaries $B^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z})$ as a subgroup. We define

$$H^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z}) := \frac{Z^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z})}{B^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z})}.$$

We discover that this H^2 captures all possible associative addition laws on $\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ of the form

$$[a, b]_\sigma + [c, d]_\sigma = [a + c + \sigma(b, d), b + d]_\sigma$$

up to isomorphism.

Lemma 3.1. *For all $\sigma \in Z^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z})$, the addition law given by*

$$[a, b]_\sigma + [c, d]_\sigma = [a + c + \sigma(b, d), b + d]_\sigma$$

makes $\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ into a group, which we denote by $[\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}]_\sigma$.

Proof. We must check that there is an identity and that there are inverses. Note first that for all $x \in \mathbb{Z}/10\mathbb{Z}$, we have

$$\sigma(x, 0) + \sigma(x, 0) = \sigma(0, 0) + \sigma(x, 0).$$

In particular, $\sigma(x, 0) = \sigma(0, 0)$. Similarly, $\sigma(0, x) = \sigma(0, 0)$. Then one easily checks that $[-\sigma(0, 0), 0]_\sigma$ is an identity element.

Also for all $[x, y]_\sigma$, we have an inverse given by

$$[-x - \sigma(-y, y), -y],$$

where one uses the fact that

$$\sigma(-y, y) + \sigma(0, -y) = \sigma(y, -y) + \sigma(-y, 0).$$

$\square$

For now, we won't care if the group law is abelian.

What properties do these groups have? One first easily checks that projection onto the second factor $[\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}]_\sigma \to \mathbb{Z}/10\mathbb{Z}$ is a surjective group homomorphism, and the kernel is

$$\{[x,0]_\sigma : x \in \mathbb{Z}\}.$$

We will use this later!

4. How many flavors of carrying are there??

We now seek to understand the structure of the group $H^2(\mathbb{Z}/10\mathbb{Z},\mathbb{Z})$. It is certainly finitely generated as a sub-quotient of a free abelian group of finite rank (namely, the set of functions $\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}\to\mathbb{Z}$). But it will turn out that this group is actually a finite group *in this specific example.*

First, we need to explain why it's called "group cohomology" and where it fits in the bigger picture of algebra.

Definition 4.1. Let G be a group. A *G-module* is an abelian group A equipped with a homomorphism

$$G \to \mathrm{Aut}(A), \qquad g \mapsto (a \mapsto ga).$$

In particular, we have

$$1a = a, \quad g(a+b) = ga + gb, \quad g(ha) = (gh)a.$$

A *morphism of G-modules* is a group homomorphism $f : A \to B$ between G-modules satisfying

$$f(ga) = gf(a)$$

for all $g \in G$ and $a \in A$.

The category of G-modules is a lot like the category of abelian groups. In particular, we have a first isomorphism theorem, and every subgroup is the kernel of a quotient map.

Definition 4.2. We say that a sequence $A \xrightarrow{f} B \xrightarrow{h} C$ of G-module maps is *exact* if $\ker(h) = \operatorname{im}(f)$.

Example 4.3. The groups $\mathbb{C}$, $\mathbb{C}^\times$, and $2\pi i\mathbb{Z}$ are $\mathbb{Z}/2\mathbb{Z}$-modules by the action of complex conjugation. The sequence

$$0 \to 2\pi i\mathbb{Z} \to \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \to 1$$

is exact. Exactness at $2\pi i\mathbb{Z}$ follows from injectivity of the map $2\pi i\mathbb{Z} \to \mathbb{C}$, and exactness at $\mathbb{C}^\times$ follows from surjectivity of the complex exponential map. Exactness at $\mathbb{C}$ is simply the fact that $2\pi i\mathbb{Z}$ is the kernel of exp.

Definition 4.4. Let A be a G-module. The *invariants* of A are

$$A^G := \{a \in A : ga = a \quad \forall g \in G\}.$$

Note that A^G is a subgroup of A.

Unfortunately, while taking invariants is *functorial*, it does not preserve exactness. However, there are functorial *cohomology groups*

$$H^n(G, A), \qquad n \geq 0$$

such that $H^0(G, A) = A^G$ and for any *short exact sequence*

$$0 \to A \to B \to C \to 0,$$

there is a *long exact sequence*

$$0 \to A^G \to \cdots \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \cdots$$

The cohomology groups are defined as follows:

We let

$$C^n(G, A) := \{f \in \mathrm{Fun}(G^{n+1}, A) : f(g\vec{v}) = gf(\vec{v})\}.$$

We have maps

$$d : C^n(G, A) \to C^{n+1}(G, A),$$

$$df(g_0, \ldots, g_n) = \sum_{k=0}^{n} (-1)^k f(g_0, \ldots, \widehat{g_k}, \ldots, g_n).$$

Here, the hat means we omit this element from the list. These maps fit into a sequence

$$0 \to C^0(G, A) \xrightarrow{d} C^1(G, A) \xrightarrow{d} \cdots \xrightarrow{d} C^n(G, A) \xrightarrow{d} \cdots$$

such that $d \circ d = 0$. Thus, we may define

$$Z^n(G, A) := \ker(d : C^n(G, A) \to C^{n+1}(G, A)),$$

$$B^n(G, A) := \mathrm{im}(d : C^{n-1}(G, A) \to C^n(G, A)) \subseteq Z^n(G, A),$$

$$H^n(G, A) := \frac{Z^n(G, A)}{B^n(G, A)}.$$

In our example, $\mathbb{Z}$ is a $\mathbb{Z}/10\mathbb{Z}$-module by the trivial action. We now wish to compute $H^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z})$. In general, $H^2(G, A)$ has a description as follows:

$$Z^2(G, A) := \{\sigma : G^2 \to A : a\sigma(b, c) - \sigma(ab, c) + \sigma(a, bc) - \sigma(a, b) = 0\},$$

$$B^2(G, A) := \{(x, y) \mapsto x\alpha(y) - \alpha(xy) + \alpha(x)\} \subseteq Z^2(G, A)$$

We use the following Lemma:

Lemma 4.5. *Let G be a finite cyclic group of order n, generated by $g \in G$, and let A be a G-module. Let*

$$N_G : A \to A, \qquad a \mapsto \sum_{i=0}^{n-1} g^i a.$$

Then

$$H^2(G, A) \cong A^G / N_G(A), \qquad [\sigma] \mapsto \epsilon_\sigma := \sum_{i=0}^{n-1} \sigma(g^i, g).$$

Proof. Omitted. □

Corollary 4.6. *We have*

$$H^2(\mathbb{Z}/10\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/10\mathbb{Z}.$$

5. How different really are these?

In general, $H^2(G, A)$ classifies short exact sequences

$$0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$$

such that $x\iota(a)x^{-1} = \iota(\pi(x)a)$ for all $x \in E$ and $a \in A$. Two such sequences are considered equivalent if there is an isomorphism $E \cong E'$ making the diagram commute:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, equal] & E \arrow[r, "\pi"] \arrow[d, "\cong"] & G \arrow[r] \arrow[d, equal] & 1 \\
0 \arrow[r] & A \arrow[r, "\iota'"] & E' \arrow[r, "\pi'"] & G \arrow[r] & 1.
\end{tikzcd}$$

However, what if we have an isomorphism $E \cong E'$ that doesn't preserve the image of A?