MATH 210A, FALL 2017
HW 7 SOLUTIONS
WRITTEN BY DAN DORE, EDITS BY PROF. CHURCH
(If you find any errors, please email ddore@stanford.edu)

Question 1. Recall that in class we used the free resolution from HW4 Q4(g) to compute for $G = \mathbf{Z}/2 = \{1, s\}$ that

$$H^k(\mathbf{Z}/2;\, M) = \begin{cases} M^G & k = 0 \\ \frac{\{m\in M | sm+m=0\}}{\{sn-n | n\in M\}} & k = 1, 3, 5, \dots \\ \frac{\{m\in M | sm=m\}}{\{sn+n | n\in M\}} & k = 2, 4, 6, \dots \end{cases}$$

For $G = \mathbf{Z}/n = \{1, s, \dots, s^{n-1}\}$, find a similar description of $H^k(\mathbf{Z}/n;\, M)$ for a $\mathbf{Z}G$-module M. (Hint: find a free resolution of $\mathbf{Z}$ as a $\mathbf{Z}G$-module; note that $\mathbf{Z}G \cong \mathbf{Z}[s]/(s^n - 1)$.
The resolution will again be 2-periodic just like for $\mathbf{Z}[s]/(s^2 - 1)$.

Solution. Let $R = \mathbf{Z}G \simeq \mathbf{Z}[s]/(s^n - 1)$. We want to compute a resolution for the R-module $\mathbf{Z}$, where s acts by the identity. This is generated by the single element 1, so we have a surjection $d_0\colon R \twoheadrightarrow \mathbf{Z}$ sending $1 \in$ R to $1 \in \mathbf{Z}$. Then R-linearity forces d_0 to send $a_0 + a_1 s + \cdots + a_{n-1}s^{n-1}$ to $a_0 + a_1 + \cdots + a_{n-1}$. Thus, the kernel of d_0 is the "augmentation ideal" $I = \{a_0 + a_1 s + \cdots + a_{n-1}s^{n-1} \mid a_0 + \cdots + a_{n-1} = 0\}$.

We claim that $I = (s - 1)$. Certainly $s - 1 \in I$, so we have $(s - 1)R \subseteq I$. To see the other inclusion, consider some $r = a_0 + a_1 s + \cdots + a_k s^k \in I$. We prove that $r \in (s - 1)$ by induction on k. If $k = 0$, since $r \in I$ we know $a_0 = 0$, and certainly $r = 0$ belongs to $(s - 1)$. If $k \geq 1$, consider

$$r' = r - (s-1)a_k s^{k-1} = r - a_k s^k + a_k s^{k-1} = a_0 + a_1 s + \cdots + (a_{k-1} + a_k)s^{k-1}.$$

By induction $r' \in (s - 1)$, and thus $r \in (s - 1)$ as well.

Thus, we have a presentation:

$$R \xrightarrow[(s-1)]{d_1} R \xrightarrow{d_0} \mathbf{Z} \longrightarrow 0$$

Now, we need to compute the kernel of d_1, i.e. the ideal $\{r \in R \mid (s - 1)r = 0\}$. Given $r = a_0 + a_1 s + \cdots + a_{n-1}s^{n-1}$, we compute

$$(s-1)r = (a_{n-1} - a_0) + (a_0 - a_1)s + \cdots + (a_{n-2} - a_{n-1})s^{n-1}.$$

Therefore $(s - 1)r = 0$ iff $a_0 = a_1$ and $a_1 = a_2$ and ... and $a_{n-2} = a_{n-1}$ and $a_{n-1} = a_0$. Therefore

$$\ker d_1 = \{r \in R \mid (s-1)r = 0\} = \{a_0(1 + s + \cdots + s^{n-1})\}.$$

Let N_n denote $N_n = 1 + s + \cdots + s^{n-1} \in \mathbf{Z}G$, so $\ker d_1 = (N_n)$. This gives us the next term of our free resolution:

$$R \xrightarrow[N_n]{d_2} R \xrightarrow[(s-1)]{d_1} R \xrightarrow{d_0} \mathbf{Z} \longrightarrow 0$$

To find $\ker d_2$ we compute that given $r = a_0 + a_1 s + \cdots + a_{n-1}s^{n-1}$,

$$N_n r = (\sum a_i) + (\sum a_i)s + \cdots + (\sum a_i)s^{n-1} = (\sum a_i)N_n.$$

It follows that $\ker d_2$ is the ideal I from above where $\sum a_i = 0$, which we already proved is equal to $(s-1)$.Thus, we have a 2-periodic resolution:

$$\cdots \longrightarrow R \xrightarrow[N_n]{d_{2n}} R \xrightarrow[(s-1)]{d_{2n-1}} R \longrightarrow \cdots \longrightarrow R \xrightarrow[N_n]{d_2} R \xrightarrow[(s-1)]{d_1} R \xrightarrow{d_0} \mathbf{Z} \longrightarrow 0$$

i.e. the even differentials are multiplication by N_n and the odd differentials are multiplication by $(s-1)$.

To calculate $H^k(\mathbf{Z}/n; M) = \mathrm{Ext}^k_{\mathbf{Z}G}(\mathbf{Z}, M)$ we will apply the contravariant right-exact functor $\mathrm{Hom}_R(\cdot, M)$ to the above free resolution. We use the fact (explained in more detail in the solutions for HW5) that $\mathrm{Hom}_R(R, M) \simeq M$ and that if $d\colon R \to R$ is a map given by multiplication by r, then the induced map $\mathrm{Hom}_R(R, M) \to \mathrm{Hom}_R(R, M)$ becomes the action of r on M under this isomorphism. Thus, $H^k(\mathbf{Z}/n; M)$ is the degree-k cohomology of the following complex:

$$0 \to M \xrightarrow[(s-1)]{\delta^1} M \xrightarrow[N_n]{\delta^2} M \longrightarrow \cdots \longrightarrow M \xrightarrow[N_n]{\delta^{2n}} M \xrightarrow[(s-1)]{\delta^{2n+1}} M \longrightarrow \cdots$$

Thus, we have $H^k(\mathbf{Z}/n; M) = \ker(\delta^{k+1})/\operatorname{im}(\delta^k)$. For k odd, this is $\ker(N_n)/\operatorname{Im}((s-1))$. We have $\ker(N_n) = \{m \in M \mid s^{n-1} \cdot m + s^{n-2} \cdot m + \cdots + m = 0\}$. Defining[1] $N\colon M \to M$ by

$$N(m) = N_n \cdot m = s^{n-1} \cdot m + \cdots + m = \sum_{g \in \mathbf{Z}/n} g \cdot m.$$

$\operatorname{Im}((s-1)) = \{s \cdot n - n \mid n \in M\}$.

For k even, we have

$$H^k(\mathbf{Z}/n; M) = \frac{\ker((s-1))}{\operatorname{Im}(N_n)} = \{m \in M \mid sm = m\}/\{N(n) \mid n \in M\} = M^G/N(M)$$

Finally, for $k = 0$, we have $H^0(\mathbf{Z}/n; M) = \ker \delta^1 = \{m \in M \mid sm = m\} = M^G$, as we know we must. Putting this all together, we have:

$$H^k(\mathbf{Z}/n; M) = \begin{cases} M^G & k = 0 \\ \{m \in M \mid N(m) = 0\}/\{sn - n \mid n \in M\} & k = 1, 3, 5, \ldots \\ M^G/N(M) & k = 2, 4, 6, \cdots \end{cases}$$

Question 2. Let G be a group.

(a) Prove that $H^0(G; \mathbf{Z}G) \cong \mathbf{Z}$ if G is finite, and $H^0(G; \mathbf{Z}G) = 0$ if G is infinite.

(b) Prove that $H^1(G; \mathbf{Z}G) \neq 0$ if $G = \mathbf{Z} = \{\ldots, t^{-1}, 1, t, \ldots\}$.

(c) (Hard, very optional) Can you find another group for which $H^1(G; \mathbf{Z}G) \neq 0$?

[1] If $\mathbf{Z}/n$ is the Galois group of a field extension L/K and $M = L^\times$, then N is the norm map $N_{L/K}$ as in Question 3. (If M is the additive group $M = L$, then N is the trace map $\mathrm{Tr}_{L/K}$.) This is an important construction in algebraic number theory.

Solution. (a) Since $H^0(G; M) = M^G$ for any group G and G-module M, we need to compute $(\mathbf{Z}G)^G$. Consider an arbitrary $\alpha = \sum_{g \in G} a_g \cdot g \in \mathbf{Z}G$, where by definition $a_g = 0$ for all but finitely many g. To be G-invariant (i.e. to lie in $(\mathbf{Z}G)^G$) means that $h \cdot \alpha = \alpha$ for all $h \in g$; in other words, for any $h \in G$

$$\sum_{g \in G} a_g \cdot (hg) = \sum_{g \in G} a_g \cdot g.$$

Comparing coefficients of h on each side, we have that $a_1 = a_h$ for all $h \in G$. If G is infinite, this is a contradiction unless $a_1 = 0$ (since only finitely many coefficients can be nonzero), so $H^0(G; \mathbf{Z}G) = 0$ in this case. If G is finite, on the other hand, we find that $(\mathbf{Z}G)^G = \{a_1(\sum_{g \in G} g)\} \cong \mathbf{Z}$.

(b) Note that $\mathbf{Z}G \simeq \mathbf{Z}[s, s^{-1}] =: R$, the ring of Laurent polynomials in the variable s. We computed in class that $H^1(G = \mathbf{Z}; M) = \operatorname{coker}(t - 1\colon M \to M) \cong M_G$ (but see below for a reminder of the proof if you forgot it). Note that $\operatorname{coker}(t - 1\colon M \to M) = M/(t - 1)M = M \otimes_R (R/(t - 1))$. Therefore when we take $M = \mathbf{Z}G = R$, we find

$$H^1(G = \mathbf{Z}; \mathbf{Z}G) = R \otimes_R (R/(t - 1)) \cong R/(t - 1) \cong \mathbf{Z} \neq 0.$$

Refresher on $H^*(G = \mathbf{Z}; M)$: We need to compute at least the first two terms of a free resolution of the trivial G-module $\mathbf{Z}$. Since 1 generates $\mathbf{Z}$, we have a surjection $d_0\colon R \twoheadrightarrow \mathbf{Z}$ sending $a_{-n}s^{-n} + \cdots + a_m s^m$ to $a_{-n} + \cdots + a_m$. The kernel I of d_0 includes the principal ideal $(s - 1)R$, and we want to show that this is the entire kernel. The argument is nearly identical to the one in Question 1. We may induct on m to show that if $p(s) \in I$, then $p(s) = q(s)(s - 1) + r(s)$ with $r(s) \in \mathbf{Z}[s^{-1}]$ and $q(s) \in R$ (even $q(s) \in \mathbf{Z}[s]$). Then since $q(s)(s - 1) \in I$, we have that $r(s) \in I$ as well. But $(s - 1) = -s(s^{-1} - 1)$, and $-s$ is a unit in R. So now it suffices to show that $r(s) \in I \cap \mathbf{Z}[s^{-1}]$ is in $(s^{-1} - 1)\mathbf{Z}[s^{-1}]$, which is the same argument as before. Now, we have:

$$R \xrightarrow[(s-1)]{d_1} R \xrightarrow{d_0} \mathbf{Z} \longrightarrow 0$$

But $R = (\mathbf{Z}[s])[\frac{1}{s}]$ is a domain, so d_1 is injective, and we have:

$$\cdots \to 0 \xrightarrow{d_2} R \xrightarrow[(s-1)]{d_1} R \xrightarrow{d_0} \mathbf{Z} \longrightarrow 0$$

(and for $n \geq 3$, all terms are 0). Applying the contravariant functor $\operatorname{Hom}_R(\cdot, M)$, we get the following complex computing $H^k(\mathbf{Z}; M)$:

$$0 \to M \xrightarrow[(s-1)]{\delta^1} M \xrightarrow{\delta^2} 0 \to \cdots$$

Thus, we have $H^0(\mathbf{Z}; M) = \ker \delta^1 = \{m \in M \mid sm = m\} = M^G$ and

$$H^1(\mathbf{Z}; M) = \ker(\delta^2)/\operatorname{im}(\delta^1) = M/\{sm - m \mid m \in M\}$$

and $H^k(\mathbf{Z}; M) = 0$ for all $k \geq 2$ and all G-modules M. Now, taking $M = \mathbf{Z}G$, we compute $H^1(\mathbf{Z}; \mathbf{Z}G)$. But this is $R/\{sr - r \mid r \in R\} = R/(s - 1)R \simeq \mathbf{Z}$, as we saw above. Thus, $H^1(\mathbf{Z}; \mathbf{Z}G) = \mathbf{Z}$.

(c) It turns out that $H^1(G; \mathbf{Z}G) = 0$ whenever G is finite (though this is not easy to prove[2]), so we need to look to infinite groups.

An satisfactory, but perhaps unsatisfying, example would be to take $G = \mathbf{Z} \times \mathbf{Z}/n$. Then $H^1(G; \mathbf{Z}G) \simeq H^1(\mathbf{Z}; \mathbf{Z}G) \simeq \mathbf{Z}$, essentially by a combination of the argument for $G = \mathbf{Z}$ and a computation for $G = \mathbf{Z}/n$ (using the answer from Q1).

Remarks from TC: To find more interesting examples that do not essentially come from $\mathbf{Z}$, we must turn to infinite non-abelian groups. For specific groups, this can be computed by hand (if the right group is chosen).

For a general way to understand why some of these examples work, here is one way to think about it (which obviously you were not expected to do). Suppose there is a contractible space X on which G acts nicely by homeomorphisms, so that every point in X is fixed by at most finitely many elements, and so that the quotient X/G is compact. Then it turns out[3] that $H^1(G; \mathbf{Z}G) \simeq H^1_c(X; \mathbf{Z})$, where H^1_c is the *compactly-supported* cohomology of the topological space X.

Here are some examples where this setup applies and $H^1_c(X) \neq 0$:

- $G = F_n$, the free group on n generators; $X =$ an infinite $2n$-regular tree
- the infinite dihedral group D_∞; $X = \mathrm{R}$ (here the computation that $H^1_c(X) \neq 0$ is especially easy)
- $G = \mathrm{SL}_2(\mathbf{Z})$ or any finite-index subgroup of it; $X =$ the upper half plane $\mathbb{H}^2$ with balls around $\mathbf{Q} \cup \{\infty\}$ removed (so that X/G is the modular curve, with a neighborhood of the cusp removed to make it compact)

These are all "1-dimensional virtual duality groups" (see §VIII.10 of Brown's book), and such a group will always have $H^1(G; \mathbf{Z}G) \neq 0$, although other examples are possible.

Question 3. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. The unit group $L^\times$ is an abelian group with an action of G, so we may consider the group cohomology $H^k(G; L^\times)$. A theorem of Noether states that $H^1(G; L^\times) = 0$; you may assume this without proof.

(a) Use Noether's theorem to prove that if $\mathrm{Gal}(L/K)$ is generated by a single element s, then every element $\ell \in L$ with norm 1 has[4] the form $s(z)/z$ for some $z \in L$.

(b) Use part (a) to give a parametrization in two rational parameters of the rational points on the unit circle:

$$S^1(\mathbf{Q}) = \{(x \in \mathbf{Q}, y \in \mathbf{Q}) \mid x^2 + y^2 = 1\}.$$

That is, give two rational functions $x(a, b) \in \mathbf{Q}(a, b)$ and $y(a, b) \in \mathbf{Q}(a, b)$ such that the resulting function $f\colon \mathbf{Q}^2 \to \mathbf{Q}^2$ given by $(a, b) \mapsto \big(x(a, b), y(a, b)\big)$ has image $S^1(\mathbf{Q})$.

---

[2] for those who want a reference, it follows from the fact that $\mathbf{Z}G$ is "co-induced" from the trivial group when G is finite, together with Shapiro's lemma

[3] This is proved as Prop. VIII.7.5, pp. 209, in the book *Cohomology of Groups* by Brown (available for free download via the Stanford library by clicking here); plus Exercise VIII.7.4 for the finite stabilizers.

[4] Recall that for a Galois extension L/K the norm $N^L_K\colon L \to K$ is given by $N^L_K(\ell) = \prod_{g \in \mathrm{Gal}(L/K)} g \cdot \ell$.

Solution. (a) If $G = \mathrm{Gal}(L/K)$ is generated by a single element s, then $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/n$, where n is the order of s. Then we can use Question 1 to compute the group cohomology

$$H^1(G; L^\times) = H^1(\mathbf{Z}/n; L^\times) = \{\ell \in L^\times \mid N(\ell) = 1\}/\{sz - z \mid z \in L^\times\}$$

Here, $N(\ell) = (\ell) * (s \cdot \ell) * (s^2 \cdot \ell) * \cdots * (s^{n-1} \cdot \ell)$ is as defined in Question 1. We can see that $N(\ell) = N_K^L(\ell)$. (Note that in Question 1, we write the group operation on the abelian group M as $+$ and the identity as 0, but for $L^\times$, the group operation is multiplication and the identity is 1). Thus, Noether's theorem tells us that since $H^1(G; L^\times) = 0$, any $\ell \in L^\times$ with $N_K^L(\ell) = 1$ is of the form $s(z)/z$ for some $z \in L^\times$.

(b) Let $K = \mathbf{Q}(i) = \{a + bi \mid a, b \in \mathbf{Q}, i^2 = -1\}$. This is a degree two field extension of $\mathbf{Q}$, which is therefore Galois with Galois group $\mathbf{Z}/2$. The nontrivial element of the group is $s\colon i \mapsto -i$ (i.e. because the minimal polynomial of i is $x^2 + 1$, and the roots of this are exactly $\pm i$). Therefore, we have $N_{\mathbf{Q}}^K(x + yi) = (x + yi)s(x + yi) = x^2 + y^2$. Thus, the previous part of the problem implies that if $x^2 + y^2 = 1$ for $(x, y) \in \mathbf{Q}^2$, then there is some $a + ib \in K^\times$ with

$$x + iy = \frac{s(a + bi)}{(a + bi)} = \frac{(a - bi)}{(a + bi)} = \frac{(a - bi)^2}{a^2 + b^2} = \frac{a^2 - b^2}{a^2 + b^2} + \frac{-2ab}{a^2 + b^2} i \tag{1}$$

Thus, $x = x(a, b) := \frac{a^2 - b^2}{a^2 + b^2}$ and $y = y(a, b) := \frac{-2ab}{a^2 + b^2}$. Thus, the map $(a, b) \mapsto (x(a, b), y(a, b))$ from $\mathbf{Q}^2$ to $\mathbf{Q}^2$ contains $S^1(\mathbf{Q})$ in its image. Note that this map is defined everywhere on $\mathbf{Q}^2 \setminus \{(0, 0)\}$, since $a^2 + b^2 \neq 0$ unless $(a, b) = (0, 0)$.

We should also check that the image is contained in $S^1(\mathbf{Q})$. This can be checked simply by summing the squares of the right hand side; alternately, our computation in (a) [or in Q1] shows that any element of the form $w = s(z)/z$ automatically has $N(w) = N(s(z))/N(z) = 1$.

Given a chain complex $C_\bullet = \to \cdots C_2 \to C_1 \to C_0 \to 0$ and a chain map $f\colon C_\bullet \to C_\bullet$:

We call f an *involution* if $f \circ f = \text{id}$.

We call f a *weak involution* if there is a *homotopy* $f \circ f \sim \text{id}$.

Question 4. Give an example of a chain complex $C_\bullet$ and a weak involution $f\colon C_\bullet \to C_\bullet$ that is not an involution.

Solution. If all maps d of the complex $C_\bullet$ are 0, then a chain homotopy between two maps from $C_\bullet$ to $C_\bullet$ must vanish, so f is an involution iff it is a weak involution. Therefore, we need a sequence with at least one non-zero map. Let's pick the easiest possible sequence:

$$C_\bullet = \ \cdots \to 0 \to \mathbf{Z} \xrightarrow[\text{id}]{d} \mathbf{Z} \to 0$$

We consider the left-hand term to be in degree 1 and the right-hand term to be in degree 0 (although this doesn't affect anything).

Our first claim is that a chain map $g\colon C_\bullet \to C_\bullet$ must have g_0 and g_1 being the same map (i.e. multiplication by the same n). Since all homomorphisms from $\mathbf{Z}$ to $\mathbf{Z}$ are given by multiplication by some element of $\mathbf{Z}$, a chain map from $C_\bullet$ to $C_\bullet$ is a diagram of the following form:

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{d} & \mathbf{Z} \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle n} \\ \mathbf{Z} & \xrightarrow{d} & \mathbf{Z} \end{array}$$

The fact that it is a chain map implies that $n \circ d = d \circ m$, so $n = m$ (since $d = \text{id}$).

Our second claim is that *any* chain map $C_\bullet \to C_\bullet$ is homotopic to *any* other; equivalently, that any chain map $g\colon C_\bullet \to C_\bullet$ is homotopic to 0. Indeed, a homotopy from g to 0 is a choice of map $h_0\colon C_0 \to C_1$ such that $g_0 = d \circ h_0$ and $g_1 = h_0 \circ d$ (since all other terms in the definition vanish). But we have already seen that $g_0 = g_1$ and $d = \text{id}$, so we can simply take $h_0 = g_0$.

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\text{id}} & \mathbf{Z} \\ {\scriptstyle n}\downarrow & \overset{n}{\swarrow} & \downarrow{\scriptstyle n} \\ \mathbf{Z} & \xrightarrow{\text{id}} & \mathbf{Z} \end{array}$$

In particular, this means that *every* $f\colon C_\bullet \to C_\bullet$ is a weak involution (since $f \circ f$ will be homotopic to id no matter what it is). Therefore we can take any f which is not actually an involution; this is accomplished by taking any $n \in \mathbf{Z} \setminus \{-1, 1\}$.

Question 5. (Optional, replaces Q4) Give an example of a chain complex $C_\bullet$ and a weak involution $f\colon C_\bullet \to C_\bullet$ that is not *homotopic* to an involution.

(That is, there does not exist any involution $g\colon C_\bullet \to C_\bullet$ with $g \circ g = \text{id}$ and $f \sim g$.)

Solution. Let us return to our example with $C_0 = C_1 = \mathbf{Z}$ and $d\colon C_1 \to C_0$ is multiplication by some $d \in \mathbf{Z} \setminus \{0\}$, but this time we will take some other d than 1:

$$C_\bullet = \ \mathbf{Z} \xrightarrow{d} \mathbf{Z}$$

The same argument as before shows that any chain map $g\colon C_\bullet \to C_\bullet$ has to have both g_0 and g_1 be multiplication by the same $m \in \mathbf{Z}$ (using just that $\mathbf{Z}$ is a domain and $d \neq 0$). Therefore we can speak simply about the chain map $m\colon C_\bullet \to C_\bullet$ for $m \in \mathbf{Z}$.

First, let us understand when two such maps are homotopic. A homotopy $n \sim m$ means exactly that there is some map $h_0\colon C_0 \to C_1$ with $n - m = d \circ h_0$ and $n - m = h_0 \circ d$. This is possible if and only if d divides $n - m$ (in which case we take $h_0\colon C_0 \to C_1$ to be multiplication by $\frac{n-m}{d}$). To sum up, two chain maps n and m are homotopic if and only if $n \equiv m \bmod d$.

Therefore if $f\colon C_\bullet \to C_\bullet$ is multiplication by n, we see that f is a weak involution iff $n^2 \equiv 1 \bmod d$. As for *actual* involutions, the only involutions are multiplication by 1 or -1. Therefore f is homotopic to an *actual* involution iff $n \equiv \pm 1 \bmod d$.

So to find a weak involution that is not homotopic to an involution, we must find some n such that $n^2 \equiv 1 \bmod d$ but $n \not\equiv \pm 1 \bmod d$. This is impossible if d is prime, but as long as d has more than 1 odd prime factor (or d is divisible by 8, or d is divisible by both 4 and an odd prime) we can do it (thanks to the Chinese Remainder Theorem, plus knowledge of the structure of $(\mathbf{Z}/p^k)^\times$). For example, we could take $d = 15$ and $n = 4$; or $d = 8$ and $n = 3$; or $d = 12$ and $n = 5$.