Topics In Algebra, Homework 4

Nick Pratarelli, Charlie Scherer

March 18, 2010

Problem (3)**.** *Suppose a, b, m are positive integers with $a, b|m$ so that $\mathbb{Z}_a$ and $\mathbb{Z}_b$ are $\mathbb{Z}_m$-modules.*

1. $\mathrm{Tor}_0^{\mathbb{Z}_m}(\mathbb{Z}_a, \mathbb{Z}_b) \cong \mathbb{Z}_c$ *with* $c = \gcd(a, b)$.
2. *For $n > 0$,* $\mathrm{Tor}_n^{\mathbb{Z}_m}(\mathbb{Z}_a, \mathbb{Z}_b) \cong \mathbb{Z}_d$ *with* $d = \frac{\gcd(a,b)m}{\mathrm{lcm}(ab,m)}$.

Proof. Note that the following is a free (hence projective) resolution of $\mathbb{Z}_a$

$$\cdots \to \mathbb{Z}_m \xrightarrow{d_3} \mathbb{Z}_m \xrightarrow{d_2} \mathbb{Z}_m \xrightarrow{d_1} \mathbb{Z}_m \xrightarrow{d_0} \mathbb{Z}_a \to 0$$

where

$$d_0(1 + m\mathbb{Z}) = 1 + a\mathbb{Z}$$

$$d_{2k+1}(1 + m\mathbb{Z}) = a + m\mathbb{Z}$$

$$d_{2k+2}(1 + m\mathbb{Z}) = m/a + m\mathbb{Z}$$

for all non-negative integers k. Recall that since $\mathbb{Z}_b$ is a $\mathbb{Z}_m$-module, $\mathbb{Z}_b \cong \mathbb{Z}_m \otimes_{\mathbb{Z}_m} \mathbb{Z}_b$ via the map $\iota : n + b\mathbb{Z} \mapsto (1 + m\mathbb{Z}) \otimes (n + b\mathbb{Z})$. So we may transfer the structure of the complex

$$\cdots \to \mathbb{Z}_m \otimes_{\mathbb{Z}_m} \mathbb{Z}_b \xrightarrow{d_3 \otimes \mathrm{id}_{\mathbb{Z}_b}} \mathbb{Z}_m \otimes_{\mathbb{Z}_m} \mathbb{Z}_b \xrightarrow{d_2 \otimes \mathrm{id}_{\mathbb{Z}_b}} \mathbb{Z}_m \otimes_{\mathbb{Z}_m} \mathbb{Z}_b \xrightarrow{d_1 \otimes \mathrm{id}_{\mathbb{Z}_b}} \mathbb{Z}_m \otimes_{\mathbb{Z}_m} \mathbb{Z}_b \to 0$$

to the less typographically exacerbating complex

$$\cdots \to \mathbb{Z}_b \xrightarrow{d_3} \mathbb{Z}_b \xrightarrow{d_2} \mathbb{Z}_b \xrightarrow{d_1} \mathbb{Z}_b \to 0$$

where $d_n = \iota^{-1}(d_n \otimes \mathrm{id}_{\mathbb{Z}_b})\iota$.

Let's determine the boundary operators $d_n : \mathbb{Z}_b \to \mathbb{Z}_b$. Suppose $n = 2k$ for some positive integer k. Then

$$d_n \otimes \mathrm{id}_{\mathbb{Z}_b}((1+m\mathbb{Z}) \otimes (1+b\mathbb{Z})) = (m/a+m\mathbb{Z}) \otimes (1+b\mathbb{Z}) = (1+m\mathbb{Z}) \otimes (m/a+b\mathbb{Z})$$

Thus, $d_n(1 + b\mathbb{Z}) = a + b\mathbb{Z}$. So we get $\mathrm{im}(d_n) = \langle m/a + b\mathbb{Z} \rangle$ which has order $\frac{b}{\gcd(m/a,b)}$ so that $|\ker(d_n)| = \gcd(m/a, b)$.

Now suppose that $n = 2k + 1$ for some non-negative integer k. Then

$$d_n \otimes \mathrm{id}_{\mathbb{Z}_b}((1 + m\mathbb{Z}) \otimes (1 + b\mathbb{Z})) = (a + m\mathbb{Z}) \otimes (1 + b\mathbb{Z}) = (1 + m\mathbb{Z}) \otimes (a + b\mathbb{Z})$$

So $d_n(1+b\mathbb{Z}) = a+b\mathbb{Z}$. Hence, as above, $\mathrm{im}(d_n) = \langle a+b\mathbb{Z}\rangle$ which has order $\frac{b}{\gcd(a,b)}$ so $|\ker(d_n)| = \gcd(a,b)$.

Therefore, when n is positive and even

$$|\operatorname{Tor}_n^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b)| = \frac{|\ker(d_n)|}{|\mathrm{im}(d_{n+1})|} = \frac{\gcd(m/a,b)}{b/\gcd(a,b)}$$

and when n is positive and odd

$$|\operatorname{Tor}_n^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b)| = \frac{\gcd(a,b)}{b/\gcd(m/a,b)}$$

So whenever $n>0$ we have $d := |\operatorname{Tor}_n^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b)| = \frac{\gcd(a,b)\gcd(m/a,b)}{b}$. But as a group $\operatorname{Tor}_n^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b)$ is cyclic because it is a quotient of subgroups of $\mathbb{Z}_b$. There is only one cyclic group of order d, namely $\mathbb{Z}_d$. Thus $\operatorname{Tor}_n^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b) \cong \mathbb{Z}_d$ as groups for all $n>0$.

An elementary calculation involving the prime factorizations of a,b and m shows that $\frac{\gcd(a,b)m}{\mathrm{lcm}(ab,m)} = \frac{\gcd(a,b)\gcd(m/a,b)}{b}$, the former expression being more interesting because it is symmetric in a and b. Indeed, if $\prod {p_i}^{e_i}$,$\prod {p_j}^{f_i}$ and $\prod {p_i}^{g_i}$ are the prime factorizations of a,b and m respectively then

$$\frac{m}{\mathrm{lcm}(ab,e)} = \prod {p_i}^{g_i-\max(e_i+f_i,g_i)} = \prod {p_i}^{\min(f_i,g_i-e_i)-f_i} = \frac{\gcd(m/a,b)}{b}$$

The identity $g_i - \max(e_i+f_i,g_i) = \min(f_i,g_i-e_i)-f_i$ is easily verified in cases.

Lastly, consider $n=0$. We know

$$|\operatorname{Tor}_0^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b)| = \frac{|\mathbb{Z}_b|}{\mathrm{im}(d_1)} = \frac{b}{b/\gcd(a,b)}$$

As before, $\operatorname{Tor}_0^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b)$ must be cyclic as a group and have order $c := \gcd(a,b)$. So $\operatorname{Tor}_0^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b) \cong \mathbb{Z}_c$.

One might observe that since $\mathbb{Z}_m$ is commutative the tensor product of $\mathbb{Z}_m$-modules has a natural $\mathbb{Z}_m$-module structure. Therefore, one might demand also to know the $\mathbb{Z}_m$-multiplication on $\operatorname{Tor}_n^{\mathbb{Z}_m}(\mathbb{Z}_a,\mathbb{Z}_b)$. But since $\mathbb{Z}_m$ is unital and is generated as an additive group by its identity element there is one and only one $\mathbb{Z}_m$-multiplication on any $\mathbb{Z}_m$-module, M. To wit, if $x \in M$ then $(n+m\mathbb{Z})\cdot x$ is the n-fold sum of x with itself. $\square$