MATH 210A, FALL 2017
HW 5 SOLUTIONS
WRITTEN BY DAN DORE

(If you find any errors, please email ddore@stanford.edu)

Question 1. Let $R = \mathbf{Z}[t]/(t^2-1)$. Regard $\mathbf{Z}$ as an R-module by letting t act by the identity. Compute $\mathrm{Tor}_k^R(\mathbf{Z},\mathbf{Z})$ and $\mathrm{Ext}_R^k(\mathbf{Z},\mathbf{Z})$ for all $k \geq 0$.

Solution. We computed a free resolution for $\mathbf{Z}$ on the previous assignment:

$$\cdots \xrightarrow{f_{n+1}} R \xrightarrow{f_n} R \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_2} R \xrightarrow{d_1} R \xrightarrow{d_0} \mathbf{Z} \longrightarrow 0$$

Here, f_n is multiplication by $t-1$ when n is odd and multiplication by $t+1$ when $n>0$ is even. Since $R \otimes_R M \simeq M$ for any R-module M, when we apply the functor $(\cdot) \otimes_R \mathbf{Z}$ to this resolution (dropping the last term), we get:

$$\cdots \xrightarrow{\delta_{n+1}} \mathbf{Z} \xrightarrow{\delta_n} \cdots \longrightarrow \mathbf{Z} \xrightarrow{\delta_1} \mathbf{Z}$$

Here, $\delta_n = d_n \otimes_R \mathrm{id}_{\mathbf{Z}} \colon R \otimes_R \mathbf{Z} \to R \otimes_R \mathbf{Z}$. Under the isomorphism $\mathbf{Z} \to R \otimes_R \mathbf{Z}$, which is given by $n \mapsto 1 \otimes n$, $\delta_n \colon \mathbf{Z} \to \mathbf{Z}$ becomes the map $n \mapsto (t \pm 1) \cdot n = n \pm n$. For n odd, this is $n \mapsto (t-1)\cdot n = 0$; for $n > 0$ even, this is $n \mapsto (t+1) \cdot n = 2n$. So we can rewrite this complex as:

$$\cdots \longrightarrow \mathbf{Z} \xrightarrow{0} \mathbf{Z} \xrightarrow{2} \mathbf{Z} \xrightarrow{0} \mathbf{Z}$$

So for $k > 0$ even, we have $\mathrm{Tor}_k^R(\mathbf{Z},\mathbf{Z}) = \ker(\delta_k)/\operatorname{im}(\delta_{k+1}) = \ker(\delta_k)/0 = \ker(\delta_k)$. Since δ_k is multiplication by 2, which is injective on $\mathbf{Z}$, we have $\mathrm{Tor}_k^R(\mathbf{Z},\mathbf{Z}) = 0$ in this case. For k odd, we have $\operatorname{im}(\delta_{k+1}) = 2\mathbf{Z}$ and $\ker(\delta_k) = \mathbf{Z}$, so $\mathrm{Tor}_k^R(\mathbf{Z},\mathbf{Z}) = \mathbf{Z}/2\mathbf{Z}$ (viewed as an R-module by having t act as the identity). What about $k=0$? Then $\mathrm{Tor}_0^R(\mathbf{Z},\mathbf{Z}) = \mathbf{Z}/\operatorname{im}(\delta_1) = \mathbf{Z}$. This makes sense: $\mathbf{Z} \simeq R/(t-1)$, so $\mathrm{Tor}_0^R(\mathbf{Z},\mathbf{Z}) = \mathbf{Z} \otimes_R \mathbf{Z} = \mathbf{Z}/(t-1)\cdot\mathbf{Z} = \mathbf{Z}/0 = \mathbf{Z}$.

To summarize:

$$\mathrm{Tor}_k^R(\mathbf{Z},\mathbf{Z}) = \begin{cases} \mathbf{Z} & k = 0 \\ 0 & k > 0, k \text{ is even} \\ \mathbf{Z}/2\mathbf{Z} & k \text{ is odd} \end{cases}$$

All of these are given an R-module structure by having t act as the identity.

Now, we can apply the contravariant functor $\mathrm{Hom}_R(\cdot, \mathbf{Z})$ to our free resolution of $\mathbf{Z}$, using the fact that $\mathrm{Hom}_R(R, M) \simeq M$ for any R-module M:

$$\mathbf{Z} \xrightarrow{\delta^1} \mathbf{Z} \xrightarrow{\delta^2} \mathbf{Z} \xrightarrow{\delta^3} \cdots$$

Via the natural isomorphism $\mathrm{Hom}_R(R, M) \xrightarrow{\sim} M$ sending φ to $\varphi(1)$, the maps $\delta^n \colon f \mapsto f \circ \delta^n$ become $n \mapsto (t \pm 1)\cdot m = m \pm m$. Thus, $\delta^n = 0$ when n is odd and $\delta^n = 2$ when n is even. So the complex is:

$$\mathbf{Z} \xrightarrow{0} \mathbf{Z} \xrightarrow{2} \mathbf{Z} \xrightarrow{0} \cdots$$

When $k > 0$ is even, we have $\mathrm{Ext}_k^R(\mathbf{Z},\mathbf{Z}) = \ker \delta^{k+1}/\operatorname{im}\delta^k = \mathbf{Z}/2\mathbf{Z}$. When k is odd, $\mathrm{Ext}_k^R(\mathbf{Z},\mathbf{Z}) = \ker \delta^{k+1}/\operatorname{im}\delta^k = 0$, and when $k = 0$, we have $\mathrm{Ext}_k^R(\mathbf{Z},\mathbf{Z}) = \ker \delta^0 = \mathbf{Z}$. These have R-module structures via t acting by the identity, as before. To summarize:

$$\operatorname{Ext}_k^R(\mathbf{Z},\mathbf{Z}) = \begin{cases} \mathbf{Z} & k = 0 \\ \mathbf{Z}/2\mathbf{Z} & k > 0, k \text{ is even} \\ 0 & k \text{ is odd} \end{cases}$$

Question 2. Let $R = \mathbf{Z}[\sqrt{-30}]$. Regard $\mathbf{F}_2$ as an R-module by letting $\sqrt{-30}$ act by 0. Compute $\operatorname{Tor}_k^R(\mathbf{F}_2,\mathbf{F}_2)$ and $\operatorname{Ext}_R^k(\mathbf{F}_2,\mathbf{F}_2)$ for all $k \geq 0$.

Solution. Recall from last week that $\mathbf{F}_2 \cong R/I$ where $I = (2, \sqrt{-30})$. Since I is projective, as we know from class[1], we have a projective resolution

$$\cdots \to 0 \to 0 \to 0 \to I \xrightarrow{i} R \to \mathbf{F}_2 \to 0.$$

where $i\colon I \hookrightarrow R$ is the inclusion. Applying $(\cdot) \otimes_R R/I$ and dropping the last term, we get the complex:

$$\cdots \to 0 \to 0 \to 0 \to I \otimes (R/I) \xrightarrow{i\otimes 1} R \otimes (R/I) \to 0$$

which we can simplify to

$$\cdots \to 0 \to 0 \to 0 \to I/I^2 \xrightarrow{0} R/I \to 0$$

Note that the map is 0 since the image of $i\colon I \hookrightarrow R$ is zero in R/I), so the kernels and images are even easier to compute, and we just get

$$\operatorname{Tor}_k^R(\mathbf{F}_2,\mathbf{F}_2) = \begin{cases} \mathbf{F}_2 & k = 0 \\ I/I^2 & k = 1 \\ 0 & k \geq 2 \end{cases}$$

The last thing to do is compute what I/I^2 is. Recall that $I = \{x + y\sqrt{-30} \mid x \in 2\mathbb{Z}, y \in \mathbb{Z}\}$. Multiplying out

$$(2a + b\sqrt{-30})(2c + d\sqrt{-30}) = (4ac - 30bd) + (2ad + 2bc)\sqrt{-30}$$

shows that $I^2 \subset \{x + y\sqrt{-30} \mid x \in 2\mathbb{Z}, y \in 2\mathbb{Z}\} = (2)$, and we can guess that this might be equality. To show that this guess is correct, we just need to show that $(2) \subset I^2$, i.e. that $2 \in I^2$. This is easy: $2 \cdot 2 = 4$ belongs to I^2, and $(\sqrt{-30}) \cdot (\sqrt{-30}) = -30$ belongs to I^2, so $-30 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 = 2$ belongs to I^2. In particular, I^2 is an index-2 subgroup of I, and so $I/I^2 \simeq \mathbf{F}_2$ (it is easy to check that this has the same R-module structure as the $\mathbf{F}_2$ we started with).[2] Therefore:

$$\operatorname{Tor}_k^R(\mathbf{F}_2,\mathbf{F}_2) = \begin{cases} \mathbf{F}_2 & k = 0 \\ \mathbf{F}_2 & k = 1 \\ 0 & k \geq 2 \end{cases}$$

[1] If you wanted to prove it (you didn't have to) the easiest way is to show that $I_\mathfrak{m}$ is free for all maximal ideals $\mathfrak{m}$ of R. Since $R/I \simeq \mathbf{F}_2$ is a field, I is a maximal ideal, so $I_\mathfrak{m} = R_\mathfrak{m}$ for $\mathfrak{m} \neq I$. Then it's not so hard to see directly that for $\mathfrak{m} = I$, $I_\mathfrak{m} = \mathfrak{m}R_\mathfrak{m}$ is principal, i.e. that $R_\mathfrak{m}$ is a principal ideal domain (this also follows from some general theory about rings like $\mathbf{Z}[-\sqrt{30}]$, called *Dedekind domains*). Then we wrote down a finite presentation for I, so by HW3 Q10, I is projective.

[2] For a maximal ideal $\mathfrak{m}$ of a ring R, such as I above, the space $\mathfrak{m}/\mathfrak{m}^2$ can be thought of as the "cotangent space" of R at the "point" $\mathfrak{m}$. It's a vector space over the field $R/\mathfrak{m}$. This turns out to be a useful construction throughout commutative algebra and algebraic geometry. When a ring is sufficiently 'nice', such as $\mathbf{Z}[\sqrt{-30}]$, this dimension is the same for all $\mathfrak{m}$.

For Ext, we can apply the contravariant functor $\mathrm{Hom}_R(\cdot, \mathbf{F}_2)$ to the projective resolution $\cdots \to 0 \to 0 \to I \xrightarrow{i} R \to \mathbf{F}_2 \to 0$ (dropping the first term) to obtain

$$0 \to \mathrm{Hom}_R(R, \mathbf{F}_2) \xrightarrow{i^*} \mathrm{Hom}_R(I, \mathbf{F}_2) \to 0 \to 0 \to 0 \to \cdots$$

Note that $\mathrm{Hom}_R(R, \mathbf{F}_2) \cong \mathbf{F}_2$ has only one nonzero element, namely $f\colon R \to \mathbf{F}_2$ sending $x + y\sqrt{-30}$ to $x \bmod 2$. Since this restricts to 0 on $I \subset R$, the map i^* here is 0. So it remains only to compute $\mathrm{Hom}_R(I, \mathbf{F}_2)$.

Note that as *abelian groups* I is isomorphic to $\mathbb{Z}^2$, so there are only three nonzero group-homomorphisms from I to $\mathbf{F}_2$: $\alpha(2a+b\sqrt{-30}) = a \bmod 2$; $\beta(2a+b\sqrt{-30}) = b \bmod 2$; and $\gamma(2a+b\sqrt{-30}) = a+b \bmod 2$. So we need only check which of these are R-linear. Since 1 and $\sqrt{-30}$ additively generate R, we need only check that they preserve multiplication by these elements (and for 1 this is automatic).

Recalling that $\sqrt{-30}$ acts by 0 on $\mathbf{F}_2$, we just need to check whether

$$\alpha\big(\sqrt{-30} \cdot (2a + b\sqrt{-30})\big) \stackrel{?}{=} 0 = \sqrt{-30} \cdot \alpha(2a + b\sqrt{-30})$$

nd so on.

$$\begin{aligned}
\alpha\big(\sqrt{-30} \cdot (2a + b\sqrt{-30})\big) &= \alpha(-30b + 2a\sqrt{-30}) = -15b \bmod 2 = b \bmod 2 \neq 0 \\
\beta\big(\sqrt{-30} \cdot (2a + b\sqrt{-30})\big) &= \beta(-30b + 2a\sqrt{-30}) = 2a \bmod 2 = 0 \bmod 2 \stackrel{\checkmark}{=} 0 \\
\gamma\big(\sqrt{-30} \cdot (2a + b\sqrt{-30})\big) &= \gamma(-30b + 2a\sqrt{-30}) = -15b + 2a \bmod 2 = b \bmod 2 \neq 0
\end{aligned}$$

Therefore the only two R-linear homomorphisms from I to $\mathbf{F}_2$ are the zero map and β. So as an abelian group $\mathrm{Hom}_R(I, \mathbf{F}_2) \cong \mathbf{F}_2$, and the fact that multiplication by $\sqrt{-30}$ annihilates β means this is the same R-module structure as always. We conclude:

$$\mathrm{Ext}^k_R(\mathbf{F}_2, \mathbf{F}_2) = \begin{cases} \mathbf{F}_2 & k = 0 \\ \mathrm{Hom}_R(I, \mathbf{F}_2) \cong \mathbf{F}_2 & k = 1 \\ 0 & k \geq 2 \end{cases}$$

Question 3. Let $R = \mathbf{R}[T]$. Let $M = \mathbf{R}^2$, with R-module structure where T acts by $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$. Let $N = \mathbf{R}$ with R-module structure where T acts by 0.
Compute $\mathrm{Tor}^R_k(M, N)$ and $\mathrm{Ext}^k_R(M, N)$ and $\mathrm{Ext}^k_R(N, M)$ for all $k \geq 0$.

Solution. On the last assignment, we computed a free resolution for M:

$$\cdots \to 0 \to 0 \longrightarrow R \xrightarrow{d_1} R \xrightarrow{d_0} M \longrightarrow 0$$

Here, d_1 is multiplication by $(T-1)^2$. If we apply the functor $(\cdot) \otimes N$ to this, after dropping the M term, we get the complex:

$$\cdots \to 0 \to 0 \longrightarrow N \xrightarrow{(T-1)^2} N \to 0$$

We used the same reasoning as in Question 1 to determine the complex: $R \otimes_R N \simeq N$, and the map $f_0 \otimes \mathrm{id}_N$ becomes the action by $(T-1)^2$ under this isomorphism. Now, since T acts by 0 on N, the element $T - 1$ acts by $(T-1) \cdot n = -n$. In particular $(T-1)^2 \cdot n = (-1)^2 \cdot n = n$, so the action of $(T-1)^2$ on N is the identity map.

Thus, we have $\operatorname{Tor}_R^0(M,N) = N/N = 0$, $\operatorname{Tor}_R^1(M,N) = 0/0 = 0$, and of course the higher Tor's vanish since the complex is 0 after the first two terms. So we have $\operatorname{Tor}_R^k(M,N) = 0$ for all k.

If we apply $\operatorname{Hom}_R(\cdot, N)$ to the sequence, we get:

$$0 \to N \xrightarrow{(T-1)^2} N \longrightarrow 0 \to 0 \to \cdots$$

Again, by the same reasoning as in Question 1, $\operatorname{Hom}_R(R,N) \simeq N$ and multiplication by $(T-1)^2$ becomes the action by $(T-1)^2$ under this isomorphism. Since $(T-1)^2$ acts by the identity map on N, we get that $\operatorname{Ext}_k^R(M,N) = 0$ for all k just as above.

In order to compute $\operatorname{Ext}_R^k(N,M)$, we either need a projective resolution of N or an injective resolution of M. In general, it's much easier to compute projective resolutions, so that's what we'll do.

We have a surjective map $\pi\colon R \to \mathbf{R}$ sending $p(T)$ to $p(T)\cdot 1$. Since T acts by 0, the kernel is (T). Since R is a domain, the map $R \to R$ given by multiplication by T is injective, so we have a free resolution:

$$\cdots \to 0 \to 0 \longrightarrow R \xrightarrow{T} R \xrightarrow{\pi} N \to 0$$

Applying the functor $\operatorname{Hom}_R(\cdot, M)$ (after dropping the N term) and using the same reasoning as before, we get the complex:

$$0 \longrightarrow M \xrightarrow{T} M \longrightarrow 0 \to 0 \to \cdots$$

So $\operatorname{Ext}_R^0(N,M) = \ker T$ and $\operatorname{Ext}_R^1(N,M) = \operatorname{coker} T$, where we think of T as the linear transformation $\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)$ acting on M. But T is an isomorphism ($\det T = 1$), so $\operatorname{Ext}_R^k(N,M) = 0$ for all k.

Question 4. Let $R = \mathbf{C}[T]$. Given $\lambda \in \mathbb{C}$, let $\mathbf{C}_\lambda$ denote $\mathbf{C}$ regarded as an R-module by letting T act by λ. Compute $\operatorname{Ext}_R^k(\mathbf{C}_\lambda, \mathbf{C}_\mu)$ for all $k \geq 0$, for all $\lambda, \mu \in \mathbf{C}$.

Solution. We need to compute a projective resolution of $\mathbf{C}_\lambda$. Since $\mathbf{C}_\lambda$ is generated by 1 as a $\mathbf{C}$-module and therefore as an R-module, we have a surjection $\pi\colon R \to \mathbf{C}_\lambda$ sending $p(T)$ to $p(T)\cdot 1 = p(\lambda)$. So the kernel is $\{p(T) \in R \mid p(\lambda) = 0\}$. This is the principal ideal $(T-\lambda)$: if $p(T) \in R$, we can write $p(T) = (T-\lambda)q(T) + r$ with $\deg r < \deg(T-\lambda) = 1$, so r is a constant. Then $p(\lambda) = r$, so $p(\lambda) = 0$ iff $(T-\lambda) \mid p(T)$. So we have a free resolution:

$$\cdots \to 0 \to 0 \longrightarrow R \xrightarrow{T-\lambda} R \longrightarrow \mathbf{C}_\lambda \longrightarrow 0$$

Now, dropping the $\mathbf{C}_\lambda$ term and applying the contravariant functor $\operatorname{Hom}(\cdot, \mathbf{C}_\mu)$, we get:

$$0 \to \mathbf{C}_\mu \xrightarrow{T-\lambda} \mathbf{C}_\mu \to 0 \to 0 \to \cdots$$

As before, we use $\operatorname{Hom}_R(R,M) \simeq M$, and that multiplication by $T-\lambda$ in R corresponds under this isomorphism to the action of $T-\lambda$. Since T acts by μ on $\mathbf{C}_\lambda$, we know that $T-\lambda$ acts by $\mu-\lambda$. So we have two cases: if $\mu = \lambda$, then the map is 0 and we have $\operatorname{Ext}_R^0(\mathbf{C}_\lambda, \mathbf{C}_\lambda) = \mathbf{C}_\lambda$ and $\operatorname{Ext}_R^1(\mathbf{C}_\lambda, \mathbf{C}_\lambda) = \mathbf{C}_\lambda$. We also clearly have $\operatorname{Ext}_R^k(\mathbf{C}_\lambda, \mathbf{C}_\lambda) = 0$ for $k \geq 2$.

$$\operatorname{Ext}_R^k(\mathbf{C}_\lambda, \mathbf{C}_\lambda) = \begin{cases} \mathbf{C}_\lambda & k = 0 \\ \mathbf{C}_\lambda & k = 1 \\ 0 & k \geq 2 \end{cases}$$

If we have $\mu \neq \lambda$, the map is multiplication by $\mu - \lambda$, which is an isomorphism, so we have $\operatorname{Ext}^0_R(\mathbf{C}_\lambda, \mathbf{C}_\mu) = \operatorname{Ext}^1_R(\mathbf{C}_\lambda, \mathbf{C}_\mu) = 0$, so

$$\operatorname{Ext}^k_R(\mathbf{C}_\lambda, \mathbf{C}_\mu) = 0 \quad \text{for all } k \geq 0.$$

Question 5. Let $R = \mathbf{C}[x, y]$.

(a) Regard $\mathbf{C}$ as an R-module by letting x and y act by 0. Compute $\operatorname{Tor}^R_k(\mathbf{C}, \mathbf{C})$ for all $k \geq 0$.

(b) Let $I \subset R$ be the ideal $I = (x, y)$. We would like to understand $I \otimes_R I$, so:

Give a basis for $I \otimes_R I$ as a complex vector space.
If you can also describe the R-module structure without too much pain, please do.

Solution. (a) We computed in the last assignment (for $R = \mathbf{R}[x, y]$ and $M = \mathbf{R}$ with R-module action by sending x, y to 0; but nothing changes when you replace $\mathbf{R}$ with any other field) the following free resolution:

$$\cdots 0 \to 0 \longrightarrow R \xrightarrow[\begin{pmatrix} y \\ -x \end{pmatrix}]{d_2} R^2 \xrightarrow[\begin{pmatrix} x & y \end{pmatrix}]{d_1} R \xrightarrow{d_0} M \longrightarrow 0$$

Here, f_0 and f_1 are given by $f_0(p, q) = xp + yq$ and $f_1(r) = (yr, -xr)$. Applying the functor $\otimes_R \mathbf{C}$, we get:

$$\cdots 0 \to 0 \to \mathbf{C} \xrightarrow{0} \mathbf{C}^2 \xrightarrow{0} \mathbf{C} \to 0$$

Here, we used the fact discussed earlier that $R^n \otimes_R (R/I) \simeq (R/I)^n$, and a matrix for $d \otimes \operatorname{id}_{R/I}$ is given by reducing a matrix for d mod I. But both the matrices $\begin{pmatrix} y \\ -x \end{pmatrix}$ and $\begin{pmatrix} x & y \end{pmatrix}$ become zero when we tensor with $\mathbf{C}$ (since x and y act by 0 there), which is how we know these maps are 0. This tells us that

$$\operatorname{Tor}^R_k(\mathbf{F}_2, \mathbf{F}_2) = \begin{cases} \mathbf{C} & k = 0 \\ \mathbf{C}^2 & k = 1 \\ \mathbf{C} & k = 2 \\ 0 & k \geq 3 \end{cases}$$

(b) [Note from TC: I think the simpler way to do this is to first show that $\ker(I \otimes_R I \to I^2) \cong \operatorname{Tor}_1(I, R/I)$, and then to show $\operatorname{Tor}_1(I, R/I) \cong \operatorname{Tor}_2(R/I, R/I)$, which we just proved is $\mathbf{C}$. Therefore once we find one element in this kernel (namely $x \otimes y - y \otimes x$) we just need any set that descends to a basis for I^2. But the approach below works as well.]

Note that I is the kernel of the map $d_0 \colon R \to M$ in the previous part, so our free resolution for M gives us a free resolution for I:

$$0 \longrightarrow R \xrightarrow[\begin{pmatrix} y \\ -x \end{pmatrix}]{d_1} R^2 \xrightarrow[\begin{pmatrix} x & y \end{pmatrix}]{d_0} I \longrightarrow 0$$

Using this free resolution, we can compute $I \otimes_R I = \operatorname{Tor}^R_0(I, I)$, by applying the functor $(\cdot) \otimes_R I$, which yields the complex:

$$I \xrightarrow[\begin{pmatrix} y \\ -x \end{pmatrix}]{\delta} I \oplus I$$

Here, we are identifying $R \otimes_R I$ with I and $R^2 \otimes_R I$ with $I \oplus I$ (this should not be referred to as I^2, since that typically refers to the ideal $I \cdot I$). Thus, $I \otimes_R I \simeq \operatorname{coker} \delta$. Note that the identification of this cokernel with $I \otimes I$ is via the map $\begin{pmatrix} x & y \end{pmatrix} \colon R^2 \to I$, so we should think of $I \oplus I$ as $(x \otimes I) \oplus (y \otimes I)$. In particular, the map $\pi \colon I \oplus I \to I \otimes I = \operatorname{coker} \delta$ is given by sending (p, q) to $(x \otimes p + y \otimes q)$. Similarly, we should think of δ as sending $p(x, y) \in I$ to $(x \otimes y \cdot p(x, y), -y \otimes x \cdot p(x, y))$. Certainly $x \otimes y \cdot p - y \otimes x \cdot p = 0$, and we've seen that this actually generates the kernel of π.

Let $(p, q) \in I \oplus I$. Then we can write p uniquely as

$$p(x, y) = xp_0(x) + yp_1(x) + y^2 p_2(x) + \cdots + y^n p_n(x)$$

for some polynomials $p_i(x) \in R$, and any choice of $p_i \in R$ give an element of I. Letting $p_1(x) = a + x \cdot p_1'(x)$ with $a \in \mathbf{C}$, we can then write p uniquely as

$$p = xp_0(x) + ya + y \cdot \left(xp_1'(x) + yp_2(x) + y^2 p_3(x) + \cdots + y^{n-1} p_n(x) \right) =: xp_0(x) + ya + yq(x, y)$$

Note that $q(x, y) \in I$, and that if $xp_0(x) + ya + yq(x, y) = xp_0'(x) + ya' + yq'(x, y)$ with $q, q' \in I$, then we can rearrange this to give:

$$y \left(q(x, y) - q'(x, y) \right) = x \left(p_0'(x) - p_0(x) \right) + y \left(a' - a \right)$$

Since the left hand side is divisible by y, the right hand side must be as well, so $p_0 = p_0'$. This implies that $a' - a = q - q' \in I$, which means that $a' = a$, since I is a proper ideal. Thus, any element $p \in I$ may be written uniquely as $p = xp_0(x) + ya + yq(x, y)$ with $q(x, y) \in I$. Therefore, we can write any element of $I \oplus I$ uniquely as $(xp_0(x) + ya, r(x, y)) + (y \cdot q(x, y), -x \cdot q(x, y))$ with $r(x, y), q(x, y) \in I$, so the second term is in $\operatorname{im} \delta$.

This means that sub-$\mathbf{C}$-vector space of $I \oplus I$ given by elements of the form $(xp_0(x) + ya, r(x, y))$ maps isomorphically under π to $I \otimes_R I$. We can take

$$\{(x^a, 0)\}_{a \geq 1} \cup \{(0, x^b y^c)\}_{b+c \geq 1} \cup \{(y, 0)\}$$

as a $\mathbf{C}$-basis.

This says that a $\mathbf{C}$-basis for $I \otimes_R I$ is given by the elements $x \otimes x^a$ with $a \geq 1$, together with the elements $y \otimes x^b y^c$ with $b + c \geq 1$, as well as the element $x \otimes y$.

Question 6. Prove that if M is torsion-free and finitely generated, then

$$\operatorname{Tor}_k(M, X) = 0 \qquad \text{for all } k > 0 \qquad \text{and any } X.$$

Solution. One way to prove this where the hypothesis that M is finitely generated is to show that torsion-free finitely generated modules over a PID are free. Since this is an important part of the structure theorem for finitely generated modules over a PID, I won't include the proof here.

Alternatively, there is an elementary argument using the *equational criterion for flatness*. This was Q11 on HW3: a finitely presented module is projective iff every linear dependence is trivial.[3]

[3] In general, an R-module M is flat iff every linear dependence is trivial, without needing to worry about finite presentation hypotheses, and this is strictly weaker than projectivity away from the finitely generated case (for example, $\mathbf{Q}$ is flat over $\mathbf{Z}$ but not projective). The equational criterion of flatness usually refers to this more general statement. For a 'fun' exercise, see if you can prove the general criterion. The proof is not very hard, and uses similar ideas to ones appearing in this assignment, namely that flatness of a module M can be checked by showing that for every ideal I, $I \to R$ remains injective after tensoring with M

We can show fairly easily that any finitely generated module over a PID is finitely presented. Indeed, let $\pi\colon R^k \to M$ be a surjection. We want to show that $\ker \pi \subseteq R^k$ is finitely generated. In fact, this is true for *any* submodule $K \subseteq R^k$ by induction on k. When $k = 1$, this is the statement that any ideal of R is finitely generated. In fact, any ideal of R is generated by a single element, since R is a PID, so this settles $k = 1$. Now, we can induct on k. We have a short exact sequence:

$$0 \to (K \cap R^{k-1}) \to K \to K/(K \cap R^{k-1}) \to 0$$

Here, we embed R^{k-1} into R^k by sending a basis to the first n coordinates. By induction, $K \cap R^{k-1} \subseteq R^{k-1}$ is finitely generated, and $K/(K \cap R^{k-1}) \subseteq R^k/R^{k-1} \simeq R$, so $K/(K \cap R^{k-1})$ is also finitely generated. Therefore, K is finitely generated.

Now, it suffices to show the equational criterion. Let $a_1 m_1 + \cdots + a_n m_n$ be a linear dependence in M, and suppose without loss of generality that $a_i \neq 0$ for each i. Because R is a PID, the ideal $(a_1, \ldots, a_n)$ is principal, so it is of the form (r) for some $r \in R$. Since the a_i are nonzero, $r \neq 0$. Thus, for each i, $a_i = ra_i'$ for some $a_i' \in R$. So we can write:

$$0 = ra_1' m_1 + \cdots + ra_n' m_n = r \cdot \left(a_1' m_1 + \cdots + a_n' m_n\right)$$

Since M is torsion-free and $r \neq 0$, we have

$$a_1' m_1 + \cdots + a_n' m_n = 0$$

Now, consider the ideal $(a_1', \ldots, a_n') = (r')$ for some $r' \in R$. Then we know that $r' \mid a_i'$ for all i, so $rr' \mid ra_i' = a_i$ for all i. Thus, $(r) = (a_1, \ldots, a_n) \subseteq (rr')$, so we have $r = (rr')r''$ for some $r'' \in R$; since R is a domain, this implies that $r'r'' = 1$, so r' is a unit, i.e. $(a_1', \ldots, a_n') = R$. We can multiply a trivializing relation for the linear dependence $0 = a_1' m_1 + \cdots + a_n' m_n$ by r to get one for $0 = a_1 m_1 + \cdots + a_n m_n$, so by renaming a_i' to a_i, we may now assume that $(a_1, \ldots, a_n) = R$. Thus, there are $r_i \in R$ such that $r_1 a_1 + \cdots + r_n a_n = 1$.

Now, for each i, we can write:

$$\begin{aligned} m_i &= (r_1 a_1 + \cdots + r_n a_n) \cdot m_i \\ &= \left(\sum_{j \neq i} r_j a_j\right) \cdot m_i + r_i a_i m_i \\ &= \left(\sum_{j \neq i} r_j a_j\right) \cdot m_i - r_i \cdot (a_1 m_1 + \cdots + a_{i-1} m_{i-1} + a_{i+1} m_{i+1} + \cdots + a_n m_n) \\ &= \left(\sum_{j \neq i} r_j a_j\right) \cdot m_i + \sum_{j \neq i} (-r_i a_j) m_j \end{aligned}$$

Define $v^j = m_j$ and b_i^j to be the coefficient of m_j in the last equation above: if $i \neq j$, $b_i^j = (-r_i a_j)$ and if $i = j$, then $b_i^i = \sum_{j \neq i} r_j a_j$. Thus, $m_i = \sum_j b_i^j v^j$.

Now, it suffices to show that for each j, $\sum_{i=1}^n a_i b_i^j = 0$. But this is:

$$\begin{aligned}\sum_{i=1}^n a_i b_i^j &= \sum_{i\neq j} a_i(-r_i a_j) + a_j b_j^j \\ &= -a_j \cdot \sum_{i\neq j} r_i a_i + a_j \cdot \left(\sum_{i\neq j} r_i a_i\right) \\ &= 0\end{aligned}$$

This concludes the proof.

Question 6′. (replaces Q6) Prove that if M is torsion-free, then

$$\mathrm{Tor}_k(M, X) = 0 \qquad \text{for all } k > 0 \qquad \text{and any \textit{finitely generated} } X.$$

Solution. We induct on the number of generators of X. If X is generated by a single element, then $X \simeq R/I$ for some ideal I. Since R is a PID, $I = (r)$ for some $r \in R$, so $X \simeq R/(r)$. If $r = 0$, then $X \simeq R$ is free, and therefore projective, so $\mathrm{Tor}_k(M, X) = 0$ for all k and all m. Consider the exact sequence:

$$0 \longrightarrow R \xrightarrow{r} R \longrightarrow X \longrightarrow 0$$

Applying the functor $M \otimes_R (\cdot)$ and using the long exact Tor sequence, we get an exact sequence:

$$\mathrm{Tor}_1^R(M, R) = 0 \longrightarrow \mathrm{Tor}_1^R(M, X) \longrightarrow M \otimes_R R \xrightarrow{r} M \otimes_R R \longrightarrow M \otimes_R R/(r) \longrightarrow 0$$

Thus, we may identify $\mathrm{Tor}_1^R(M, X)$ with the kernel of the map $M \otimes_R R \to M \otimes_R R$ given by multiplication by r on the second factor. We may identify $M \otimes_R R$ with M, so this is just the map $M \to M$ given by multiplication by r. The kernel of this map is then exactly the set of $m \in M$ with $r \cdot m = 0$. Since M is torsion-free and $r \neq 0$, this implies $m = 0$. Thus, we know that $\mathrm{Tor}_1^R(M, R/(r)) = 0$ for any $r \in R$.

Now, let $x_1, \ldots, x_n$ generate X, and let X' be the R-submodule of X generated by $x_1, \ldots, x_{n-1}$. We have a short exact sequence:

$$0 \to X' \to X \to X/X' \to 0$$

Here, X/X' is generated by a single element, so it is isomorphic to $R/(r)$ for some $r \in R$. Now, we can take the Tor long exact sequence to get:

$$\cdots \longrightarrow \mathrm{Tor}_k(M, X') \longrightarrow \mathrm{Tor}_k(M, X) \longrightarrow \mathrm{Tor}_k(M, X/X') \longrightarrow \cdots$$

But for any $k \geq 1$, since both X/X' and X' are generated by fewer than n elements, we may assume by induction that $\mathrm{Tor}_k(M, X') = 0$, $\mathrm{Tor}_k(M, X/X') = 0$, so this reads:

$$\cdots \longrightarrow 0 \longrightarrow \mathrm{Tor}_k(M, X) \longrightarrow 0 \longrightarrow \cdots$$

Thus, $\mathrm{Tor}_k(M, X) = 0$ for all $k \geq 1$.

Question 7. Deduce from Q6, *or* from Q6′, *or* prove directly: for any torsion-free M,

$$\mathrm{Tor}_k(M, X) = 0 \qquad \text{for all } k > 0 \qquad \text{and any } X.$$

[If you give a self-contained direct proof for Q7, you will automatically get credit for Q6.]

Solution. Both deductions from Q6, Q6' are similar. Let's show Q6 $\Longrightarrow$ Q7 first.

Let M be an arbitrary torsion-free module. We want to show that $\mathrm{Tor}_k(M, X) = 0$ for all R-modules X, which is equivalent to showing that M is flat. We will show directly that if $\varphi\colon X \to Y$ is an injective homomorphism, then $\mathrm{id}_M \otimes_R \varphi\colon M \otimes_R X \to M \otimes_R Y$ is injective. Now, let $\beta = \sum_{i=1}^n m_i \otimes x_i$ be an arbitrary element of $M \otimes_R X$ and suppose that $\varphi(\beta) = 0$. We want to show that $(\mathrm{id}_M \otimes_R \varphi)\big(\sum_i m_i \otimes x_i\big) = \sum_i m_i \otimes \varphi(x_i)$ is non-zero. Since only finitely many elements of M appear in this sum, there is a finitely generated submodule $M' \subseteq M$ which contains $m_1, \dots, m_n$. Since submodules of torsion-free modules are torsion-free, we know that M' is torsion-free and finitely generated. By Q6, this implies that $\mathrm{Tor}_k(M', X) = 0$ for any R-module X, i.e. that M' is flat. We have a commutative diagram:

$$\begin{array}{ccc} M' \otimes_R X & \xrightarrow{\mathrm{id}_{M'} \otimes \varphi} & M' \otimes_R Y \\ \big\downarrow{\scriptstyle \iota \otimes \mathrm{id}_X} & & \big\downarrow{\scriptstyle \iota \otimes \mathrm{id}_Y} \\ M \otimes_R X & \xrightarrow{\mathrm{id}_M \otimes \varphi} & M \otimes_R Y \end{array}$$

Applying this to $\alpha = \sum_i m_i \otimes x_i \in M' \otimes_R X$, we get that

$$(\iota \otimes \mathrm{id}_Y)\big((\mathrm{id}_{M'} \otimes \varphi)(\alpha)\big) = (\mathrm{id}_M \otimes \varphi)\big((\iota \otimes \mathrm{id}_X)(\alpha)\big) = (\mathrm{id}_M \otimes \varphi)(\beta) = 0$$

Since we do not know if Y is flat, we cannot conclude immediately that $\gamma := (\mathrm{id}_{M'} \otimes \varphi)(\alpha) = 0$. However, we know that *any* finitely generated submodule of M is flat. Let M'' be a finitely generated submodule of M containing M'. Then we can extend the above commutative diagram to:

$$\begin{array}{ccc} M' \otimes_R X & \xrightarrow{\mathrm{id}_{M'} \otimes \varphi} & M' \otimes_R Y \\ \big\downarrow{\scriptstyle \iota_1 \otimes \mathrm{id}_X} & & \big\downarrow{\scriptstyle \iota_1 \otimes \mathrm{id}_Y} \\ M'' \otimes_R X & \xrightarrow{\mathrm{id}_{M''} \otimes \varphi} & M'' \otimes_R Y \\ \big\downarrow{\scriptstyle \iota_2 \otimes \mathrm{id}_X} & & \big\downarrow{\scriptstyle \iota_2 \otimes \mathrm{id}_Y} \\ M \otimes_R X & \xrightarrow{\mathrm{id}_M \otimes \varphi} & M \otimes_R Y \end{array}$$

Note that we have $\iota = \iota_2 \circ \iota_1$, so we know that

$$0 = (\iota \otimes \mathrm{id}_Y)(\gamma) = (\iota_2 \otimes \mathrm{id}_Y) \circ (\iota_1 \otimes \mathrm{id}_Y)(\gamma)$$

If we can find some such M'' such that $(\iota_1 \otimes \mathrm{id}_Y)(\gamma) = 0$, then we have:

$$0 = (\iota_1 \otimes \mathrm{id}_Y)(\gamma) = (\mathrm{id}_{M''} \otimes \varphi) \circ (\iota_1 \otimes \mathrm{id}_X)(\alpha)$$

Since M'' is flat, $\mathrm{id}_{M''} \otimes \varphi$ is injective, so this means that $(\iota_1 \otimes \mathrm{id}_X)(\alpha) = 0$. But $\beta = (\iota \otimes \mathrm{id}_X)(\alpha) = (\iota_2 \otimes \mathrm{id}_X)\big((\iota_1 \otimes \mathrm{id}_X)(\alpha)\big)$, so this implies $\beta = 0$, as desired.

To see that there is a finitely generated submodule $M'' \subseteq M$ with $M' \subseteq M''$ such that $(\iota_1 \otimes \mathrm{id}_Y)(\gamma) = 0$, we recall the construction of the tensor product $M \otimes_R Y$. This is defined as the free abelian group $\mathscr{A}$ on the symbols $m \otimes y$ with $m \in M, y \in Y$, modulo relations of the form $\rho_{m_1,m_2,+} := (m_1 + m_2) \otimes y - m_1 \otimes y - m_2 \otimes y$ and $\rho_{r,m,*} := rm \otimes y = m \otimes ry$ for all $m_1, m_2, m \in M$, $y \in Y$, and $r \in R$.

We can write $\gamma = \sum_{i=1}^n m_i \otimes y_i$, and its image in $M \otimes Y$ is represented by $A = \sum_{i=1}^n m_i \otimes y_i \in \mathscr{A}$. Since it is 0 in $M \otimes Y$, this means that A is in the subgroup of $\mathscr{A}$ generated by $\rho_{m_1,m_2,+}, \rho_{r,m,*}$. Thus, there are *finitely many* m_1^i, m_2^i, r^j, m^j such that $A = \sum_{i=1}^N \rho_{m_1^i,m_2^i,+} + \sum_{j=1}^M \rho_{r^j,m^j,*}$. We can then take M'' to be the R-submodule of M generated by the m_1^i, m_2^i, m^j and the generators of M'. This is a finitely generated submodule of M. Then, $(\iota_1 \otimes \mathrm{id}_Y)(\gamma)$ is represented by $A \in \mathscr{A}'' \subseteq \mathscr{A}$, where $\mathscr{A}''$ is the free abelian group corresponding to $M'' \otimes Y$, which is clearly a subgroup of $\mathscr{A}$ (it is the free abelian group on a subset of the generators). But by construction, the $\rho_{m_1^i,m_2^i,+}$ and $\rho_{r^j,m^j,*}$ are in $\mathscr{A}''$. Then, since $\mathscr{A}'' \to \mathscr{A}$ is injective, the equation $A = \sum_i \rho_{m_1^i,m_2^i,+} + \sum_j \rho_{r^j,m^j,*}$ holds in $\mathscr{A}''$, so A is in the kernel of $\mathscr{A}'' \to M'' \otimes_R Y$. This means that $(\iota_1 \otimes \mathrm{id}_Y)(\gamma) = 0$ as desired.

The deduction that Q6' $\implies$ Q7 is very similar. We need to show that for any $\varphi \colon X \to Y$, the map $(\mathrm{id}_M \otimes \varphi) \colon M \otimes X \to M \otimes Y$ is injective. Let $\beta = \sum_i m_i \otimes x_i$ be in the kernel. Taking X' to be any finitely generated submodule of X containing the x_i, we can define $\alpha := \sum_i m_i \otimes x_i$, thought of as an element of X'. Since the homomorphic image of a finitely generated module is finitely generated, we get a map $\varphi' \colon X' \to Y'$ with $Y' \subseteq Y$ finitely generated. This gives us a commutative diagram:

$$\begin{array}{ccc} M \otimes_R X' & \xrightarrow{\mathrm{id}_M \otimes \varphi'} & M \otimes_R Y' \\ \downarrow{\scriptstyle \mathrm{id}_M \otimes \iota_{X'}} & & \downarrow{\scriptstyle \mathrm{id}_M \otimes \iota_{Y'}} \\ M \otimes_R X & \xrightarrow{\mathrm{id}_M \otimes \varphi} & M \otimes_R Y \end{array}$$

Thus, $\gamma := (\mathrm{id}_M \otimes \varphi')(\alpha)$ is in the kernel of $\mathrm{id}_M \otimes \iota_{Y'}$. Exactly as in the proof that Q6 $\implies$ Q7 (note that we did not use torsion-freeness for this part of the proof), we can see that there is a finitely generated submodule $Y'' \subseteq Y$ with $Y' \subseteq Y''$ such that if $\iota_1 \colon Y' \hookrightarrow Y''$ is the inclusion, $(\mathrm{id}_M \otimes \iota_1)(\gamma) = 0$. We get a map $\varphi'' \colon X' \to Y''$ defined by $\iota_1 \circ \varphi'$, and this gives a commutative diagram:

$$\begin{array}{ccc} & \overset{\mathrm{id}_M \otimes \varphi'}{\nearrow} & M \otimes_R Y' \\ & & \downarrow{\scriptstyle \mathrm{id}_M \otimes \iota_1} \\ M \otimes_R X' & \xrightarrow{\mathrm{id}_M \otimes \varphi''} & M \otimes_R Y'' \\ \downarrow{\scriptstyle \mathrm{id}_M \otimes \iota_{X'}} & & \downarrow{\scriptstyle \mathrm{id}_M \otimes \iota_{Y''}} \\ M \otimes_R X & \xrightarrow{\mathrm{id}_M \otimes \varphi} & M \otimes_R Y \end{array}$$

Thus, we see that $0 = (\mathrm{id}_M \otimes \iota_1)(\gamma) = (\mathrm{id}_M \otimes \varphi'')(\alpha) = 0$. But since $\varphi'' \colon X' \to Y''$ is the composition of the injective maps $\varphi' \colon X' \to Y'$ and $\iota_1 \colon Y' \to Y''$, it is injective.

Now, consider the exact sequence:

$$0 \to X' \to Y'' \to \operatorname{coker} \varphi'' \to 0$$

Since $\operatorname{coker} \varphi''$ is a quotient of the finitely generated module Y'', it is finitely generated, so $\operatorname{Tor}_1(M, \operatorname{coker} \varphi'') = 0$. Thus, taking the Tor long exact sequence, we get:

$$0 = \operatorname{Tor}_1(M, \operatorname{coker} \varphi'') \longrightarrow M \otimes_R X' \xrightarrow{\mathrm{id}_M \otimes \varphi''} M \otimes Y'' \longrightarrow M \otimes (\operatorname{coker} \varphi'') \longrightarrow 0$$

Thus, $\mathrm{id}_M \otimes \varphi''$ is injective, so the fact that $(\mathrm{id}_M \otimes \varphi'')(\alpha) = 0$ implies $\alpha = 0$, and thus $\beta = (\mathrm{id}_M \otimes \iota_{X'})(\alpha) = 0$.

Question 8. Deduce from the previous question that for *any* M,

$$\mathrm{Tor}_k(M, X) = 0 \qquad \text{for all } k > 1 \qquad \text{and any } X.$$

Solution. For any R-module M, there is a short exact sequence $0 \to K \to F \to M \to 0$ with F free and $K \subseteq F$. Since submodules of torsion-free modules are torsion-free, we know that K is torsion-free. Now, for any X, we can take the long exact Tor sequence. For any $k \geq 2$, we have the following piece:

$$0 = \mathrm{Tor}_k(F, X) \to \mathrm{Tor}_k(M, X) \to \mathrm{Tor}_{k-1}(K, X) = 0$$

Here, we used Q7 and the fact that $k - 1 \geq 1$ to show that $\mathrm{Tor}_{k-1}(K, X) = 0$. Certainly we know that for a free module F, $\mathrm{Tor}_k(F, X) = 0$ as soon as $k > 0$. Thus, $\mathrm{Tor}_k(M, X) = 0$ for $k > 1$.

Do at least one of the following questions. If you've seen one of these questions before, please at least try to do one of the others.

Question 9A. Compute $\mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{Q}, \mathbf{Z})$.

Solution. Consider the short exact sequence:

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

We can take the long exact $\mathrm{Ext}(\mathbf{Q}, \cdot)$ sequence:

$$0 \to \mathrm{Hom}(\mathbf{Q}, \mathbf{Z}) \to \mathrm{Hom}(\mathbf{Q}, \mathbf{Q}) \to \mathrm{Hom}(\mathbf{Q}, \mathbf{Q}/\mathbf{Z}) \to \mathrm{Ext}^1(\mathbf{Q}, \mathbf{Z}) \to \mathrm{Ext}^1(\mathbf{Q}, \mathbf{Q}) = 0$$

We know that $\mathrm{Ext}^1(\mathbf{Q}, \mathbf{Q}) = 0$, since $\mathbf{Q}$ is an injective $\mathbf{Z}$-module. Now, $\mathrm{Hom}(\mathbf{Q}, \mathbf{Z}) = 0$: if $q \in \mathbf{Q}$, we can write $q = nq'$ for any n, so if $f \in \mathrm{Hom}(\mathbf{Q}, \mathbf{Z})$ then $f(q) = nf(q')$, i.e. $f(q)$ is divisible by n for all n, which is clearly impossible unless $f(q) = 0$. We also know that $\mathrm{Hom}(\mathbf{Q}, \mathbf{Q}) \simeq \mathbf{Q}$, since any $\mathbf{Z}$-linear map f from $\mathbf{Q}$ to $\mathbf{Q}$ is just multiplication by an element of $\mathbf{Q}$. So we have:

$$\mathrm{Ext}^1(\mathbf{Q}, \mathbf{Z}) \simeq \mathrm{Hom}(\mathbf{Q}, \mathbf{Q}/\mathbf{Z})/\mathbf{Q}$$

Thus, it suffices to describe the group $\mathrm{Hom}(\mathbf{Q}, \mathbf{Q}/\mathbf{Z})$.

Let's start by describing the structure of $\mathbf{Q}/\mathbf{Z}$. For any prime p, there is the subgroup $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$, consisting of elements of the form $\frac{a}{p^k}$ with $p \nmid a$ and $0 \leq a < p^k$. Putting all of these subgroups together, we get a map from $\bigoplus_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z} = \bigoplus_p (\mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$ to $\mathbf{Q}/\mathbf{Z}$. This map is injective: if $\frac{a}{m} + \frac{b}{n} = \frac{an+bm}{nm} = 0$ in $\mathbf{Q}/\mathbf{Z}$ with n, m coprime, then $\frac{an+bm}{nm} \in \mathbf{Z}$, i.e. $nm \mid an + bm$, so $n \mid bm$ and $m \mid an$. But since n, m are coprime, this means that $m \mid a$ and $n \mid b$. Thus, $\frac{a}{m}$ and $\frac{b}{n}$ are in $\mathbf{Z}$, so they are 0 in $\mathbf{Q}/\mathbf{Z}$. Now, we can write an element of $\bigoplus_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ as:

$$\frac{a_1}{p_1^{k_1}} + \cdots + \frac{a_n}{p_n^{k_n}} = \frac{N}{p_1^{k_1} \cdots p_{n-1}^{k_{n-1}}} + \frac{a_n}{p_n^{k_n}}$$

Thus, the above argument shows that $\frac{a_n}{p_n^{k_n}} \in \mathbf{Z}$, so we may induct on n to show that the whole sum is in $\mathbf{Z}$, and therefore 0 in $\bigoplus_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$.

Now, we will show that $\bigoplus_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ is actually an isomorphism. To do this, let $\frac{a}{q} \in \mathbf{Q}$ with $q = q_1 q_2$ coprime. Then we may write $1 = aq_1 + bq_2$ for some $a, b \in \mathbf{Z}$ (e.g. by the Chinese Remainder

Theorem, or by the fact that $\mathbf{Z}$ is a PID, so the ideal (q_1, q_2) is $(\gcd(q_1, q_2)) = (1)$). Then we can take the "partial fraction" decomposition:

$$\frac{1}{q_1 q_2} = \frac{aq_1 + bq_2}{q_1 q_2} = \frac{a}{q_2} + \frac{b}{q_1}$$

By breaking q into its prime factorization and repeatedly using this identity, we may write q as an element in the image of $\bigoplus_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$.

Remember that for any modules M_i, $i \in I$ for some set I, the direct sum $\bigoplus_i M_i$ embeds into the direct product $\prod_i M_i$ as the set of elements such that all but finitely many factors are 0. So we will start by describing $\mathrm{Hom}\left(\mathbf{Q}, \prod_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}\right)$. By the universal property of products, a map to the product is the same as a tuple of maps to each factor, i.e. we have:

$$\mathrm{Hom}\left(\mathbf{Q},\ \prod_p \mathbf{Z}\left[\tfrac{1}{p}\right]/\mathbf{Z}\right) \simeq \prod_p \mathrm{Hom}\left(\mathbf{Q},\ \mathbf{Z}\left[\tfrac{1}{p}\right]/\mathbf{Z}\right)$$

Now, we've broken the problem up one problem for each prime p. Now, we want to characterize homomorphisms from $\mathbf{Q}$ to $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$. Such homomorphisms of course restrict to homomorphisms from $\mathbf{Z}[\frac{1}{p}]$ to $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$, and in fact any such homomorphism f extends *uniquely* to $\mathbf{Q}$. To see this, we will use the following:

Claim 1. The group $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ is *uniquely divisible* by numbers coprime to p: for any $\alpha \in \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ and $n \in \mathbf{N}$ with $p \nmid n$, there is a unique $\alpha' \in \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ such that $n \cdot \alpha' = \alpha$.

Proof. We can write $\alpha = \frac{a}{p^k} + \mathbf{Z}$ with $p \nmid a$, $0 \le a < p^k$. Since, $p \nmid n$, n and p^k are coprime, so there are $b, c \in \mathbf{Z}$ with $bp^k + cn = 1$, so $abp^k + acn = a$. Thus, we can write α as:

$$\alpha = \frac{a}{p^k} + \mathbf{Z} = \frac{abp^k}{p^k} + \frac{acn}{p^k} + \mathbf{Z} = n \cdot \frac{ac}{p^k} + \mathbf{Z}$$

Thus, we may take $\alpha' = \frac{ac}{p^k} + \mathbf{Z}$. We want to show that α' is unique, so let β' be an element of $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ with $n\beta' = \alpha$. Then $n(\beta' - \alpha') = 0$, so it suffices to show multiplication by n is injective. Now, let $\gamma = \frac{m}{p^\ell} + \mathbf{Z} \in \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$. If $n\gamma = 0$, then $\frac{nm}{p^\ell} \in \mathbf{Z}$, so $p^\ell \mid nm$. Since $p \nmid n$, this means that $p^\ell \mid m$, so $\gamma = 0$. □

Now, let $f \in \mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$. We want to show it extends uniquely to $\widetilde{f} \in \mathrm{Hom}(\mathbf{Q}, \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$. Write any element of $\mathbf{Q}$ uniquely as $\frac{a}{p^k m}$ with $p \nmid m$, $(p^k m, a) = 1$, and $m > 0$. Let $\alpha = f(\frac{a}{p^k})$, which is defined since $a \in \mathbf{Z}[\frac{1}{p}]$. We can define $\widetilde{f}(\frac{a}{p^k m})$ as the unique element α' such that $m \cdot \alpha' = \alpha$. This gives a well-defined function from $\mathbf{Q}$ to $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$, and it is easy to see that it is additive and extends f. Moreover, it is unique since we need $m \cdot \widetilde{f}\left(\frac{a}{p^k m}\right) = f\left(\frac{a}{p^k}\right)$.

Thus, we need to determine $\mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$. Let f_0 be such a homomorphism and consider $\alpha = f_0(1) \in \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$. We have $\alpha = \frac{a}{p^n}$ for some $n \ge 0$ with $p \nmid a$, so $p^n \cdot \alpha = a = 0$ and $p^m a \ne 0$ for $m < n$. Define $f = p^n f_0$, so $f(1) = 0$. Then, we define a sequence $(m_n) := (f\left(\frac{1}{p^n}\right))_n$ for $n \ge 1$. We have $p \cdot m_n = m_{n-1}$, and $p^n m_n = f(1) = 0$ for all n. On the other hand, given such a sequence (m_n) with $m_n \in \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ such that $p \cdot m_n = m_{n-1}$ and $p^n m_n = 0$ for all n, we can define a homomorphism $f\colon \mathbf{Z}[\frac{1}{p}] \to \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ with $m_n = f\left(\frac{1}{p^n}\right)$ and $f(1) = 0$. To do this, we define $f\left(\frac{a}{p^n}\right) = am_n$ with $a \in \mathbf{Z}$. If we rewrite $\frac{a}{p^n}$ as $\frac{ap}{p^{n+1}}$, then since $apm_{n+1} = am_n$, these definitions agree. This allows us to check that f is additive: if we have $x = \frac{a}{p^n}$ and $y = \frac{b}{p^k}$, then

$$f(x+y) = f\left(\frac{ap^k + bp^n}{p^{n+k}}\right) = ap^k m_{k+n} + bp^n m_{k+n} = am_n + bm_k = f(x) + f(y)$$

Now, we can describe the set of sequences $(m_n)_n$ with $p \cdot m_n = m_{n-1}$ and $p^n m_n = 0$ for all n a bit differently. The second condition says exactly that $m_n = \frac{a}{p^n}$ for some a (perhaps not coprime to p). Since a is only defined mod p^n, we can think of m_n as living in $\mathbf{Z}/p^n\mathbf{Z}$ instead. Then $pm_n = \frac{pa}{p^n} = \frac{a}{p^{n-1}}$, so the condition that $pm_n = m_{n-1}$ can be rephrased as saying that $m_n \in \mathbf{Z}/p^n$ is equal to m_{n-1} mod p^{n-1}. Thus, the subgroup of $\mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$ with $f(1) = 0$ is isomorphic to the group of sequences (m_n) with $m_n \in \mathbf{Z}/p^n\mathbf{Z}$ such that $\pi_{n,n-1}(m_n) = m_{n-1}$, where $\pi_{n,n-1}$ is the map from $\mathbf{Z}/p^n\mathbf{Z}$ to $\mathbf{Z}/p^{n-1}\mathbf{Z}$ given by reducing mod p^{n-1}. Another name for this group is $\mathbf{Z}_p$, the *p-adic integers*. Note that this is $consist(\mathbf{Z}[\frac{1}{p}])$, since $p^k m \cdot \mathbf{Z}[\frac{1}{p}] = p^k\mathbf{Z}[\frac{1}{p}]$ for $p \nmid m$.

Now, for any element $f \in \mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$ and any n, there is a *unique* $f_0 \in \mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$ with $p^n f_0 = f$: we can take $f_0(x) = f(\frac{x}{p^n})$, and this is unique since multiplication by p^n on $\mathbf{Z}[\frac{1}{p}]$ is injective. Thus, $\mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$ has a unique structure of a $\mathbf{Z}[\frac{1}{p}]$-module. Since for any $f \in \mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$, there is some n such that $p^n f(1) = 0$, we can write f as $\frac{f_1}{p^n}$ with $f_1(1) = 0$. This shows that $\mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}) \simeq \mathbf{Z}_p[\frac{1}{p}] = \mathbf{Q}_p$, the *p-adic numbers* as an abelian group.

Thus, we see that $\mathrm{Hom}(\mathbf{Q}, \prod_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}) \simeq \prod_p \mathbf{Q}_p$. The submodule $\mathrm{Hom}(\mathbf{Q}, \mathbf{Q}/\mathbf{Z}) \simeq \mathrm{Hom}(\mathbf{Q}, \bigoplus_p \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$ is given by elements (f_p) such that for each $x \in \mathbf{Q}$, $f_p(x) = 0$ for all but finitely many p. This is the subgroup of $(a_p) \in \prod_p \mathbf{Q}_p$ such that for all but finitely many p, $a_p \in \mathbf{Z}_p$. To see this, let $x = \frac{m}{n}$. For all $p \nmid nm$, $f_p(x) = a \cdot f_p(1)$ for some $a \in \mathbf{Z}$ with $(a,p) = 1$, by the definition of the isomorphism from $\mathrm{Hom}(\mathbf{Z}[\frac{1}{p}], \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}) \xrightarrow{\sim} \mathrm{Hom}(\mathbf{Q}, \mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$ and the proof of Claim 1. Thus, $f_p(x) = 0$ iff $f_p(1) = 0$. Thus, we see that a sequence (f_p) satisfies the condition that for all x, $(f_p)(x) = 0$ for all but finitely many x iff $f_p(1) = 0$ for all but finitely many x, iff the corresponding element $(a_p) \in \prod_p \mathbf{Q}_p$ is in $\mathbf{Z}_p$ for all but finitely many p.

We call the resulting group $\mathbf{A}^f_{\mathbf{Q}} := \prod'_{\mathbf{Z}_p} \mathbf{Q}_p$, where the $\prod'_{\mathbf{Z}_p}$ stands for "restricted product" and it means the subset of the product where all but finitely many entries are in $\mathbf{Z}_p$. This group has a natural ring structure given by component-wise multiplication, and is called the *finite adele ring of* $\mathbf{Q}$, and is studied widely in number theory.[4]

Finally, we see that $\mathrm{Ext}^1(\mathbf{Q}, \mathbf{Z}) \simeq \mathbf{A}^f_{\mathbf{Q}}/\mathbf{Q}$, where the map $\mathbf{Q} \to \mathbf{F}$ is given by sending $q \in \mathbf{Q}$ to the map $(f_p)\colon \mathbf{Q} \to \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ with f_p multiplication by q for each p. This corresponds to the element $(\iota_p(q)) \in \mathbf{A}^f_{\mathbf{Q}}$, with $\iota_p \mid \mathbf{Q} \to \mathbf{Q}_p$ defined by sending $\frac{a}{p^k m}$ with $p \nmid a, m$ to $\frac{1}{p^k}\left(m^{-1} \cdot a \pmod{p)^n}\right)_n$ (where m^{-1} is an inverse to a mod p^n, which exists for each n but depends on n). Since the denominator of q is only divisible by finitely many primes, we see that $\iota_p(q) \in \mathbf{Z}_p$ for all but finitely many p, so this in fact lands in $\mathbf{A}^f_{\mathbf{Q}}$.

If M is a $\mathbb{Z}$-module, note that $d|n$ implies $nM \subset dM$, so there is a quotient map $\pi^d_n\colon M/nM \to M/dM$ (it descends from the identity $M \to M$, so in symbols it's just $\overline{m} \mapsto \overline{m}$).

Define $consist(M)$ to be the submodule of $\prod_{n\in\mathbb{N}} M/nM$ defined by

$$consist(M) :- \left\{ (m_n \in M/nM)_{n\in\mathbb{N}} \;\middle|\; d|n \implies \pi^d_n(m_n) = m_d \right\}$$

[4]The full adele ring $\mathbf{A}_{\mathbf{Q}}$ is $\mathbf{A}^f_{\mathbf{Q}} \times \mathbf{R}$: sometimes it is useful to think of $\mathbf{R}$ as being "the prime at infinity". This ring has a locally compact topology coming from the locally compact topologies on $\mathbf{R}$ and $\mathbf{Q}_p$, and many important results in number theory can be reformulated in terms of this topological ring.

This makes $consist$ an additive functor from $\mathbb{Z}$-modules to $\mathbb{Z}$-modules (you do not have to prove this).

Question 9B. Is $consist$ an exact functor? Prove your answer is correct.

Solution. Since $\mathbf{Q}/n\mathbf{Q} = 0$ for all $n \in \mathbb{N}$, $consist(\mathbf{Q}) \subseteq \prod_{n\in\mathbf{N}} \mathbf{Q}/n\mathbf{Q} = 0$, so consistent$(\mathbf{Q}) = 0$. Since $\mathbf{Z} \to \mathbf{Q}$ is injective, in order to show that $consist$ is not an exact functor, it suffices to show that $consist(\mathbf{Z}) \neq 0$. This will be clear from the description in Question 9C, but for now note that there is an injective map $\mathbf{Z} \to consist(\mathbf{Z})$ defined by sending $m \in \mathbf{Z}$ to $(m \pmod n)_{n\in\mathbf{N}}$. Certainly, if $d \mid n$, then $\pi_n^d(m \pmod n) = m \pmod d$, so the image of this map is contained in $consist(\mathbf{Z})$. The map is injective since if $m \pmod n = 0$ for all $n \in \mathbf{N}$, then $n = 0$.

Question 9C. $consist(\mathbf{Z})$ has a natural ring structure (for example, it is a subring of $\prod_{n\in\mathbf{N}} \mathbf{Z}/n\mathbf{Z}$); you do not have to prove this.

Describe the commutative ring $\mathbf{Q} \otimes_{\mathbf{Z}} consist(\mathbf{Z})$.

(You have some flexibility here in what your "description" should be, but don't just rephrase the definition.)

Solution. First, we will use the Chinese remainder theorem: $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p_1^{k_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_m^{k_m}\mathbf{Z}$ for $n = p_1^{k_1} \cdots p_m^{k_m}$ its prime factorization. Let $d_i = p_i^{k_i}$. Then the maps $\pi_n^{d_i} : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/p_i^{k_i}\mathbf{Z}$ correspond to the i-th projection maps in the product decomposition $\mathbf{Z}/p_1^{k_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_m^{k_m}\mathbf{Z}$. So if $(m_n) \in consist(\mathbf{Z})$, then $m_n = (m_{p_1^{k_1}}, \ldots, m_{p_m^{k_m}})$ in this product description, so the collection of m_{p^ℓ} for p a prime and $\ell > 0$ completely determine (m_n), and conversely, any collection of the m_{p^ℓ} which are consistent with respect to the π_n^d where n, d are both powers of the same prime define an element of $consist(\mathbf{Z})$.

In other words, $consist(\mathbf{Z}) \simeq \prod_p consist_p(\mathbf{Z})$, where we define $consist_p(\mathbf{Z})$ to be the set of sequences (m_{p^n}) with $m_{p^n} \in \mathbf{Z}/p^n\mathbf{Z}$ such that $\pi_{p^n}^{p^k}(m_{p^n}) = p^k$ for all $k \leq n$. This is even an isomorphism *of rings*, since the ring structure on $consist(\mathbf{Z})$ is defined by component-wise multiplication (i.e. $(m_n) \cdot (m'_n) = (m_n m'_n)$, and it's easy to check this preserves consistency, since the π_n^d are ring homomorphisms), and the Chinese remainder theorem gives an isomorphism of rings. Note that it is equivalent in the definition of $consist_p(\mathbf{Z})$ to require that $\pi_{p^n}^{p^{n-1}}(m_{p^n}) = m_{p^{n-1}}$ for all n, since the p^n are linearly ordered by divisibility. Now, $consist_p(\mathbf{Z})$ is usually referred to as $\mathbf{Z}_p$, the *p-adic integers*.

Thus, we see that $consist(\mathbf{Z}) \simeq \prod_p \mathbf{Z}_p$ as rings. Let's see that $consist(\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Q} \simeq \mathbf{A}_{\mathbf{Q}}^f$, the finite adele ring defined in the solution to Question 9A. Essentially, this is true because tensoring with $\mathbf{Q}$ is the same thing as adjoining $\frac{1}{n}$ for all $n \in \mathbf{N}$, and n has only finitely many prime divisors. More precisely, we define a homomorphism $consist(\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathbf{A}_{\mathbf{Q}}^f$ by sending $(a_p) \otimes q$ to $(\iota_p(q)a_p)$, with $\iota_p : \mathbf{Q} \to \mathbf{Q}_p$ the embedding defined in Question 9A. Since $(a_p) \in \prod_p \mathbf{Z}_p$ and for all but finitely many p, $\iota_p(q) \in \mathbf{Z}_p$, we see that the image of this map lands in $\mathbf{A}_{\mathbf{Q}}^f$.

To see that it is an isomorphism, note that if we have a tensor of the form $(a_p) \otimes \frac{m}{n} + (b_p) \otimes \frac{m'}{n'}$, we can rewrite this as

$$(mn'a_p) \otimes \frac{1}{nn'} + (nm'b_p) \otimes \frac{1}{nn'} = (mn'a_p + nm'b_p) \otimes \frac{1}{nn'}$$

Thus, any element of $\prod_p \mathbf{Z}_p \otimes \mathbf{Q}$ may be written as $(a_p) \otimes \frac{1}{n}$. Then the map is certainly injective, since $\iota_p(\frac{1}{n})a_p$ is only 0 when a_p is 0. It is also surjective: given a finite adele $(a_p) \in \mathbf{A}_{\mathbf{Q}}^f$, let $p_1, \ldots, p_m$ be the finitely many primes p with $a_p \notin \mathbf{Z}_p$, and assume $p_i^{k_i} a_{p_i} \in \mathbf{Z}_p$ for each i. Then let $n := \prod_i p_i^{k_i}$, and let $(b_p) := n \cdot (a_p) \in \prod_p \mathbf{Z}_p$. Thus, we map $(b_p) \otimes \frac{1}{n}$ to (a_p).