CALCULATING $\mathbf{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$

The purpose of this note is to provide my Math 830 class with a proof that, as $\mathbb{Z}$-modules, i.e., abelian groups, $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) \cong \mathbb{R}$. There are more detailed descriptions of $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ in terms of the *Pontryagin dual* and the p-adic numbers $\mathbb{Q}_p$, but on the face of it, the description at hand has a certain appeal. The overall strategy of the proof is as follows: We will show that $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ is a torsion-free, divisible $\mathbb{Z}$-module. This will give $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ the structure of a vector space over $\mathbb{Q}$. We will then observe: (i) The cardinality of $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ is the same as the cardinality of $\mathbb{R}$ and (ii) Any vector space over $\mathbb{Q}$ whose cardinality is the same as the cardinality of $\mathbb{R}$ is isomorphic to $\mathbb{R}$ as $\mathbb{Z}$-modules.

We proceed with a sequence of lemmas.

Lemma A. For a commutative ring R and an exact sequence of R-modules $0 \to A \to B \to C \to 0$, for any R-module D, there is a long exact sequence

$$0 \to \text{Hom}_R(D,A) \to \text{Hom}_R(D,B) \to \text{Hom}_R(D,C) \to \text{Ext}^1_R(D,A) \to \text{Ext}^1_R(D,B) \to \text{Ext}^1_R(D,C) \to \text{Ext}^2_R(D,A) \to \cdots .$$

Moreover, if the map from A to B is multiplication by $r \in R$, then the map from $\text{Ext}^n_R(D,A) \to \text{Ext}^n_R(D,B)$ is multiplication by r, for all $n \geq 0$.

Proof. To be presented later in the semester. □

Lemma B. For any integer $n \geq 1$, $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_n) = 0 = \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$.

Proof. Let $f : \mathbb{Q} \to \mathbb{Z}_n$ be a $\mathbb{Z}$-module homomorphism. For $x \in \mathbb{Q}$, we have $f(x) = f(n \cdot \frac{x}{n}) = n \cdot f(\frac{x}{n}) = 0$, which gives the first equality. Now suppose $f : \mathbb{Q} \to \mathbb{Z}$ and take $x \in \mathbb{Q}$. Suppose $f(x) = t \neq 0$. Then we have $t = f(x) = f(xt \cdot \frac{1}{t}) = tf(\frac{x}{t})$, which implies that $f(\frac{x}{t}) = 1$. Thus, $1 = f(\frac{2x}{2t}) = 2f(\frac{x}{2t})$, which is a contradiction. Thus, $f(x) = 0$. Since x was arbitrary, $f = 0$, which gives the second equality. □

Lemma C. For a prime p and $e \geq 1$, the map $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty}) \xrightarrow{\cdot p^e} \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty})$ is surjective.

Proof. Let $f \in \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty})$. Define $g : \mathbb{Q} \to \mathbb{Z}_{p^\infty}$ by $g(x) := f(p^{-e}x)$, for all $x \in \mathbb{Q}$. Then it is easy to check that $g \in \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty})$ and for all $x \in \mathbb{Q}$, $(p^e g)(x) = p^e f(p^{-e}x) = f(p^e p^{-e} x) = f(x)$. □

Lemma D. For $n \geq 1$, $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_n) = 0$.

Proof. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n, so that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{e_r}}$. Then it is easy to check that $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_n) \cong \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p_1^{e_1}}) \oplus \cdots \oplus \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p_r^{e_r}})$. Thus, it suffices to show that if p is prime and $e \geq 1$, then $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^e}) = 0$. For this, we let K denote the elements $x \in \mathbb{Z}_{p^\infty}$ such that $p^e x = 0$. Then $K \cong \mathbb{Z}_{p^e}$. Moreover, since $\mathbb{Z}_{p^\infty}$ is a divisible $\mathbb{Z}$-module, multiplication by p^e is surjective. Thus, from the exact sequence

$$0 \to K \to \mathbb{Z}_{p^\infty} \xrightarrow{\cdot p^e} \mathbb{Z}_{p^\infty} \to 0,$$

and the long exact sequence in Ext, we have

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty}) \xrightarrow{\cdot p^e} \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty}) \to \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},K) \to \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty}) = 0,$$

where the 0 on the right comes from the fact that $\mathbb{Z}_{p^\infty}$ is injective. By Lemma C, the map from $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^\infty})$ to $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},K)$ is the zero map, so we have $0 = \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},K) = \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}_{p^e})$. □

Proposition E. $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ is both torsion-free and divisible.

Proof. Fix $n \geq 1$. From the short exact sequence $0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}_n \to 0$, we have the part of the long exact Ext sequence

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, Z_n) \to \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \xrightarrow{\cdot n} \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \to \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}_n).$$

By Lemma B, $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}_n) = 0$ and by Proposition E, $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}_n) = 0$. This shows that multiplication by n on $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ is 1-1 and onto, which implies that $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ is both torsion-free and divisible. □

Proposition F. Let D be a $\mathbb{Z}$-module that is both torsion-free and divisible. Then D has the structure of a $\mathbb{Q}$-module that is compatible with its $\mathbb{Z}$-module structure.

Proof. Let $r := \frac{a}{b} \in \mathbb{Q}$ and $x \in D$. Then there exists $y \in D$ such that $ax = by$, since D is divisible. If $ax = by'$, for $y' \in D$, then $by = by'$, so $b(y - y') = 0$. Since D is torsion-free, $y - y' = 0$, i.e., $y = y'$. Thus, there exists a unique $y \in D$ such that $ax = by$. We define $\frac{a}{b} \cdot x := y$. It must now be verified that:

(i) $(r_1 + r_2)x = r_1x + r_2x$, for all $r_1, r_2 \in \mathbb{Q}$ and $x \in D$.
(ii) $r(x_1 + x_2) = rx_1 + rx_2$, for all $r \in \mathbb{Q}$ and $x_i \in D$.
(iii) $(rs)x = r(sx)$, for all $r, s \in \mathbb{Q}$ and $x \in D$.

The proofs of (i)-(iii) are straight forward, so we just illustrate (i). Suppose $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ and $x \in D$. Write $\frac{a}{b}x = y$ and $\frac{c}{d}x = z$, so that $ax = by$ and $cx = dz$. Then $adx = bdy$ and $bcx = bdz$. Thus, $(ad + bc)x = bd(y + z)$, which gives $(\frac{a}{b} + \frac{c}{d})x = \frac{(ad+bc)}{bd}x = y + z = \frac{a}{b}x + \frac{c}{d}x$. □

Lemma G. $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}) \cong \mathbb{Q}$.

Proof. Let $f : \mathbb{Q} \to \mathbb{Q}$ be a $\mathbb{Z}$-module homomorphism. For any $0 \neq b \in \mathbb{Z}$, $f(1) = f(b \cdot \frac{1}{b}) = bf(\frac{1}{b})$, so that $f(\frac{1}{b}) = \frac{1}{b}f(1)$. It follows that for all $\frac{a}{b} \in \mathbb{Q}$, $f(\frac{a}{b}) = \frac{a}{b}f(1)$. Thus, f is determined by $f(1)$. Thus, for each $r \in \mathbb{Q}$, we can define a map $\mathbb{Q} \to \mathbb{Q}$ by sending 1 to r. It's now easy to check that the map $\phi : \text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}) \to \mathbb{Q}$ defined by $\phi(f) = f(1)$ is a $\mathbb{Z}$-module isomorphism. □

Facts from set theory. In the proofs of Lemma H and Theorem I, we need the set-theoretic facts (i)-(iii) below. We use $|X|$ to denote the cardinality of the set X, i.e., the equivalence class of all sets Y for which there exists a 1-1, onto function from X to Y, in which case we have $|X| = |Y|$. The famous Schroeder-Bernstein Theorem states that for sets X, Y, $|X| = |Y|$ if and only if $X| \leq |Y|$ and $|Y| \leq |X|$, where by definition, $|X| \leq |Y|$ if there is a 1-1 function from X to Y.

(i) Let $\{A_n\}_{n\geq 1}$ be a countable collection of sets with $|A_n| = |X|$, for all n. Then $|\bigcup_{n\geq 1} A_n| = |X|$.
(ii) Let Suppose E is the disjoint union of the sets $\{A_j\}_{j\in J}$, with each A_j countable. Then $|E| = |J|$.
(iii) Let X be the set of sequences $x_1, x_2, \ldots$, where x_1 comes from a countable set, x_2 comes from a set with two elements, x_3 comes from a set with three elements, etc. Then $|X| = |\mathbb{R}|$.

Lemma H. Let V be a vector space over $\mathbb{Q}$ whose cardinality as a set equals the cardinality of $\mathbb{R}$, i.e., $|V| = |\mathbb{R}|$. Then, $V \cong \mathbb{R}$ as $\mathbb{Z}$-modules.

Proof. We first note that if V and $\mathbb{R}$ are isomorphic as vector spaces over $\mathbb{Q}$, then they are isomorphic as $\mathbb{Z}$-modules, since a vector space linear transformation is also a $\mathbb{Z}$-module homomorphism. We will show that if B is a basis for V, then $|B| = |V| = |\mathbb{R}|$. Applying this to the special case $V = \mathbb{R}$ shows that if B' is a basis for $\mathbb{R}$ as a vector space over $\mathbb{Q}$, then $|B'| = |\mathbb{R}|$. It follows that $|B| = |B'|$, so $V \cong \mathbb{R}$ as vector spaces over $\mathbb{Q}$. Showing that $|B| = |V|$ comes down to some basic set theory facts. Since every element in V is uniquely a finite linear combination of elements from B, if we let C_n denote the set of finite linear combinations (with no zero coefficients) of n elements from B, we have $V = \bigcup_{n\geq 1} C_n \cup \{0\}$, where $\bigcup_{n\geq 1} C_n$ is a disjoint union. By the set-theoretic property (i) above, for a countable union of infinite sets C_n such that $|C_1| = |C_2| = \cdots$, then $|\bigcup_{n\geq 1} C_n| = |C_1|$. Now we have $|C_1| = |\mathbb{Q} \times B| = |B|$ since B is infinite. Similarly,

$$|C_2| = |(\mathbb{Q} \times B) \times (\mathbb{Q} \times B)| = |B \times B| = |B|.$$

Induction yields, $|C_n| = |B|$ all n, so $|B| = |\bigcup_{n\geq 1} C_n| = |V| = |\mathbb{R}|$, as required. □

Theorem I. $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) \cong \mathbb{R}$ as $\mathbb{Z}$-modules.

Proof. By Proposition E, $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ is torsion-free and divisible. By Proposition F, $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ is a vector space over $\mathbb{Q}$. Thus, by Lemma H, it suffices to show that $|\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})| = |\mathbb{R}|$. For this, consider the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ and apply $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},-)$ together with the Ext Lemma to obtain

$$0 \to \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) \to \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}) \to \text{Hom}_{\mathbb{Z}}(Q,\mathbb{Q}/\mathbb{Z}) \to \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) \to 0.$$

By Lemma B, $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) = 0$, and by Lemma G, $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}) \cong \mathbb{Q}$, so the Ext Lemma sequence becomes

$$0 \to \mathbb{Q} \to \text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}/\mathbb{Z}) \to \text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) \to 0.$$

Since $\mathbb{Q}$ is countable and $\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) \cong \text{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Q}/\mathbb{Z})/\mathbb{Q}$, $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}/\mathbb{Z})$ is is a disjoint union of $|\text{Ext}^1_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}/\mathbb{Z})|$ countable cosets. By the set-theoretic fact (ii) above, the proof will be complete if we show that the cardinality of $\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}/\mathbb{Z})$ is $|\mathbb{R}|$.

To continue, we first make the following claim. Suppose $r \in \mathbb{Q}$ and $n \geq 1$. Then the equation $r \equiv nx$ has n distinct solutions in $\mathbb{Q}/\mathbb{Z}$. Assuming the claim holds, we set $A_n := \mathbb{Z} \cdot \frac{1}{n!}$, a free $\mathbb{Z}$-module of rank one, so that a $\mathbb{Z}$-module homomorphism from A_n to $\mathbb{Q}/\mathbb{Z}$ is determined by sending $\frac{1}{n}$ to an element of $\mathbb{Q}/\mathbb{Z}$. Then $A_1 \subsetneq A_2 \subsetneq A_2 \subsetneq \cdots$ and $\mathbb{Q} = \bigcup_{n\geq 1} A_n$. We clearly have countably many $\mathbb{Z}$-module maps from A_1 to $\mathbb{Q}/\mathbb{Z}$. Let $f : A_1 \to \mathbb{Q}/\mathbb{Z}$ be one such map. How many ways can f be extended to a $\mathbb{Z}$-module map from $A_2 \to \mathbb{Q}$? Let f_2 be such a map. Then $f(1) = f_2(1) = 2f_2(\frac{1}{2})$. Thus $f_2(\frac{1}{2})$ must satisfy the equation $f(1) \equiv 2x$ in $\mathbb{Q}/\mathbb{Z}$. By the claim, there are two solutions to this equation in $\mathbb{Q}/\mathbb{Z}$, so we may define $f_2 : A_2 \to \mathbb{Q}/\mathbb{Z}$ by sending $\frac{1}{2}$ to any one of these two solutions. In other words, there are two ways to extend f to a a $\mathbb{Z}$-module homomorphism $f_2 : A_2 \to \mathbb{Q}/\mathbb{Z}$. For a given $f_2 : A_2 \to \mathbb{Q}/\mathbb{Z}$, how many ways can we extend f_2 to a $\mathbb{Z}$-module map $f_3 : A_3 \to \mathbb{Q}/\mathbb{Z}$? Suppose f_3 is such an extension. Then $f_2(\frac{1}{2}) = f_3(\frac{1}{2}) = 3f_3(\frac{1}{6}) = 3f_3(\frac{1}{3!})$. In other words, $f_3(\frac{1}{6})$ must satisfy the equation $f_2(\frac{1}{2}) \equiv 3x$ in $\mathbb{Q}/\mathbb{Z}$. Since this equation has three solutions, it follows that for a given f_2, there are three ways to extend it to a $\mathbb{Z}$-module map $f_3 : A_3 \to \mathbb{Q}/\mathbb{Z}$.

Continuing in this way, we see that given any $\mathbb{Z}$-module map $f_n : A_n \to \mathbb{Q}/\mathbb{Z}$, there are n ways of extending it to a $\mathbb{Z}$-module map from A_{n+1} to $\mathbb{Q}/\mathbb{Z}$. Taking a union over the A_n we construct maps from $\mathbb{Q}$ to $\mathbb{Q}/\mathbb{Z}$. Each map constructed in this way corresponds to a countably infinite sequence whose first term comes from a countable set and whose subsequent nth terms comes from a set with n element. By the third set-theoretic fact above, there are $|\mathbb{R}|$ such sequences, so that $|\mathbb{R}| \leq |\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}/\mathbb{Z})|$. However, since there are $|\mathbb{R}|$ set maps from one countable set to another, we have $|\mathbb{R}| \leq |\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}/\mathbb{Z})| \leq |\mathbb{R}|$, so $|\mathbb{R}| = |\text{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}/\mathbb{Z})|$, as required.

For the claim, suppose we have $r \in \mathbb{Q}$, $n \geq 1$. We want to see that there are n solutions in $\mathbb{Q}/\mathbb{Z}$ to the equation $r \equiv nx$. The classes of $\frac{r}{n}, \frac{r}{n} + \frac{1}{n}, \ldots, \frac{r}{n} + \frac{n-1}{n}$ are clearly n distinct solutions. Suppose r_0 is such that $r \equiv nr_0$ in $\mathbb{Q}/\mathbb{Z}$. Then $n(r_0 - \frac{r}{n}) \equiv 0$ in $\mathbb{Q}/\mathbb{Z}$. But in $\mathbb{Q}/\mathbb{Z}$, the equation $rz \equiv 0$ if and only if $z \equiv \frac{i}{n}$, for some $0 \leq i \leq n-1$, which shows that $r_0 \equiv \frac{r}{n} + \frac{i}{n}$ in $\mathbb{Q}/\mathbb{Z}$, for some $0 \leq i \leq n-1$. ☐