Problem 1. Let G be a group. Use G to define a category $\underline{G}$ with a single object as we did with monoids. Show that in this (small) category all morphisms are isomorphisms. [We then define a *groupoid* to be a small category in which all morphisms are isomorphisms.]

Proof. We form the category $\underline{G}$ by setting one object (say, $\mathrm{Ob}(\underline{G}) = \{A\}$), and by setting $\mathrm{Hom}(A, A) = G$, 1_A the identity of G, and xy for $x, y \in \mathrm{Hom}(A, A)$ the product of x and y as given in G. We define $f \in \mathrm{Hom}(A, A)$ to be an *isomorphism* if there exists a $g \in \mathrm{Hom}(A, A)$ such that $fg = gf = 1_A$. Since G is a group, we have that for every $f \in \mathrm{Hom}(A, A) = G$, there exists a $g \in \mathrm{Hom}(A, A) = G$ so that $gf = fg = 1 = 1_A$, i.e. its inverse. Hence, every morphism is an isomorphism. □

Problem 2. An object A of a category $\mathcal{C}$ is called an *initial* object if for every $X \in \mathrm{Ob}(\mathcal{C})$, the set $\mathrm{Hom}(A, X)$ consists of a single element (in other words, there is a unique morphism from the object to every other object in the category). An object A of a category $\mathcal{C}$ is called a *terminal* object if, for every object $X \in \mathrm{Ob}(\mathcal{C})$, the set $\mathrm{Hom}(X, A)$ has a single element (in other words, every object in $\mathcal{C}$ has a unique morphism to A). An object that is both an initial and terminal object is called a *zero* object of $\mathcal{C}$.

(a) If A and A' are both initial objects in a category $\mathcal{C}$, then show that there is a unique isomorphism in $\mathrm{Hom}(A, A')$, and similarly for terminal objects. Hence, these objects are "unique up to isomorphism".

(b) Show that there exist zero objects in **R-mod** and **Grp**.

Proof. (a) Let A, A' be initial objects in a category $\mathcal{C}$. We first remark that, by the category axioms, $1_A \in \mathrm{Hom}(A, A)$, and that the property of being initial dictates that $\mathrm{Hom}(A, A) = \{1_A\}$. Now, since A and A' are initial, we have that $\mathrm{Hom}(A, A') = \{f\}$ and $\mathrm{Hom}(A', A) = \{g\}$; in other words, there exists a unique morphism $f : A \to A'$ and a unique morphism $g : A' \to A$. By the composition axiom, we get that $g \circ f : A \to A \in \mathrm{Hom}(A, A)$. However, the only element in $\mathrm{Hom}(A, A)$ is 1_A, so we must have $g \circ f = 1_A$. Likewise, we have that $f \circ g : A' \to A' \in \mathrm{Hom}(A', A')$, and by uniqueness this forces $f \circ g = 1_{A'}$. Hence, we have that f is an isomorphism, and so A and A' are isomorphic. Furthermore, we notice that this is a unique isomorphism, since the morphisms must be unique by definition.

The same argument applies for when A, A' are terminal. The properties dictate that $\mathrm{Hom}(A, A) = \{1_A\}$, $\mathrm{Hom}(A', A') = \{1_{A'}\}$, and we have that $\mathrm{Hom}(A, A') = \{f\}$, $\mathrm{Hom}(A', A) = \{g\}$, so composition gives us that $g \circ f : A \to A = 1_A \in \mathrm{Hom}(A, A)$, $f \circ g : A' \to A' = 1_{A'} \in \mathrm{Hom}(A', A')$, so f is an isomorphism. Thus, these objects are unique up to isomorphism. Again, the isomorphism is unique by definition.

(b) Let 0 denote the trivial module; i.e., the module consisting of only an identity element. We first show that this is an initial object. Let $A \in \mathrm{Ob}(\mathbf{R\text{-}mod})$ be another object. Define $f : 0 \to A$ via $f(0) = 0_A$. This clearly satisfies the properties of being a module homomorphism; we have $f(0 + 0) = f(0) = 0_A$, and $f(0) + f(0) = 0_A$, so $f(0 + 0) = f(0) + f(0)$, and for all $r \in R$ we have $f(r0) = f(0) = 0_A = rf(0)$. This is unique, since a property of module homomorphisms (moreover group homomorphisms) is that they must map the identity to the identity. Hence, we get $\mathrm{Hom}(0, A) = \{\mathbf{0}\}$, and this applies for all $A \in \mathrm{Ob}(\mathbf{R\text{-}mod})$. Thus, 0 is initial.

We now want to show that 0 is terminal in **R-mod**. Let $A \in \mathrm{Ob}(\mathbf{R\text{-}mod})$, and consider $f : A \to 0$ which maps everything to 0. We check that this is a module homomorphism. For $x, y \in A$, we see $f(x + y) = 0 = 0 + 0 = f(x) + f(y)$. For $x \in A$, $r \in R$, we see that $f(rx) = 0 = r0 = rf(x)$. So this is indeed a module homomorphism. Moreover, this is the only such module homomorphism to 0, since 0 consists of only one element. Thus, now denoting the

0 map as $\mathbf{0}$, we have that $\mathrm{Hom}(A, 0) = \{\mathbf{0}\}$, as desired. Since 0 is both initial and terminal, we have established the existence of a zero object.

The argument is similar for the case of **Grp**. Letting 1 now denote the group consisting of only the identity element, we wish to show that this is an initial object. Taking arbitrary $A \in \mathrm{Ob}(\mathbf{Grp})$, we define $f : 1 \to A$ by $f(1) = 1_A$. We see that this defines a group homomorphism, since $f(1 \cdot 1) = 1_A = 1_A \cdot 1_A = f(1) \cdot f(1)$. Furthermore, we see that this is unique, since group homomorphisms must send the identity to the identity. So we have that $\mathrm{Hom}(1, A) = \{f\}$ for all $A \in \mathrm{Ob}(\mathbf{Grp})$, as desired.

To see that 1 is terminal, take any $A \in \mathrm{Ob}(\mathbf{Grp})$ and consider the map $\mathbf{1} : A \to 1$ defined by $\mathbf{1}(x) = 1$. This is a morphism, since for all $x, y \in A$ we have $\mathbf{1}(xy) = 1 = 1 \cdot 1 = \mathbf{1}(x) \cdot \mathbf{1}(y)$, and this is clearly unique since we only have one element to map to. In other words, we have that $\mathrm{Hom}(A, 1) = \{\mathbf{1}\}$ as desired, and so 1 is a zero object as well.

□

Problem 3. Let $\mathcal{C}$ and $\mathcal{D}$ be categories, and $F : \mathcal{C} \to \mathcal{D}$ be a (covariant) functor that is faithful and full. For any $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, show that if $F(f)$ is monic (resp. epic) then so is f.

Proof. We first do the monic case. Let $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. Then we have that $F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$. Consider $g_1, g_2 \in \mathrm{Hom}_C(C, A)$, we wish to show that $f \circ g_1 = f \circ g_2 \implies g_1 = g_2$. Notice that $f \circ g_1 = f \circ g_2$ implies $F(f \circ g_1) = F(f \circ g_2)$, and by the axioms of functors this gives $F(f) \circ F(g_1) = F(f) \circ F(g_2)$. Since $F(f)$ is monic, we have that this implies $F(g_1) = F(g_2)$, and since our functor is faithful this implies that $g_1 = g_2$. Hence, f is monic.

Next, assume that $F(f)$ is epic, $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. Then we wish to show that if $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ are such that $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$. Notice that $g_1 \circ f = g_2 \circ f$ implies that $F(g_1 \circ f) = F(g_2 \circ f)$, and the functor axioms give $F(g_1) \circ F(f) = F(g_2) \circ F(f)$. Since $F(f)$ is epic, we have $F(g_1) = F(g_2)$, and since F is faithful we have $g_1 = g_2$. So f is epic.

Remark. In other words, we have that F reflects monics and epics.

□

Problem 4. Let M and N be monoids, and associate to each category $\underline{M}$ and $\underline{N}$ with a single object. Show that with this identification, a (covariant) functor $F : \underline{M} \to \underline{N}$ is simply a homomorphism $F : M \to N$. Show that a natural transformation $\eta : F \to G$ for two functors F and G corresponds to an element $b \in N$ such that $b \cdot F(x) = G(x) \cdot b$ for all $x \in M$.

Proof. Let $\mathrm{Ob}(\underline{M}) = \{A\}$, $\mathrm{Ob}(\underline{N}) = \{B\}$ for some A, B. Since functors send objects to objects, it's clear that we have $F(A) = B$. Furthermore, we have that $F : M = \mathrm{Hom}_{\underline{M}}(A, A) \to \mathrm{Hom}_{\underline{N}}(B, B) = N$, and we have that it satisfies $F(1_M) = 1_N$, $F(xy) = F(x)F(y)$ by the functor axioms. So in essence, we have that F is just a homomorphism of the monoids M and N. Likewise, we can take a homomorphism of monoids $F : M \to N$ and create a functor $F : \underline{M} \to \underline{N}$ via assigning $F(A) = B$ and $F : M = \mathrm{Hom}_{\underline{M}}(A, A) \to \mathrm{Hom}_{\underline{N}}(B, B) = N$ to be the homomorphism itself. This satisfies all of the properties of being a functor due to the monoid homomorphism axioms. So a functor between these categories really is just a homomorphism of the monoids M and N.

Recall that a natural transformation $\eta : F \to G$ is a map that assigns to the object $A \in \mathrm{Ob}(\underline{M})$ a morphism $\eta_A \in \mathrm{Hom}_{\underline{N}}(B, B) = N$ such that we have

$$\eta_A \circ F(f) = G(f) \circ \eta_A.$$

Since $f \in M$, we can rewrite this as x, and since the only object is A we have that $\eta_A = b \in N$ is the only morphism we need to consider. Furthermore, the product in this case is just the product in N, and so we have that a natural transformation corresponds to $b \in N$ with $b \cdot F(x) = G(x) \cdot b$ for all $x \in M$. □

Problem 5. Use the previous exercise to construct a functor F and a monomorphism f such that $F(f)$ is not a monomorphism and an epimorphism g such that $F(g)$ is not an epimorphism.

Proof. Consider the monoids $M = \mathbb{N} \setminus \{0\}$ equipped with multiplication, $N = \{0, 1\}$ equipped with multiplication. We see that M is cancellative; i.e. for $a \in \mathbb{N}$ we have that $ab = ac \implies b = c$, and likewise $ba = ca \implies b = c$ (to see this, simply divide out by a). We note, however, that the only unit in M is 1. Construct a morphism $F : M \to N$ defined by

$$F(x) = \begin{cases} 1 \text{ if } x \text{ is invertible,} \\ 0 \text{ otherwise.} \end{cases}$$

We check that this is a monoid homomorphism. We have that $F(1) = 1$ is satisfied clearly. We then consider the following cases:

Case 1: ($x = 1$, $y \neq 1$) Here, we have $F(xy) = F(y) = 0$, and $F(x)F(y) = 1 \cdot 0 = 0$, so $F(xy) = F(x)F(y)$.

Case 2: ($x \neq 1$, $y = 1$) Analogous to the last case.

Case 3: ($x = 1$, $y = 1$) We have $F(xy) = F(1) = 1$, $F(x)F(y) = 1 \cdot 1 = 1$. So $F(xy) = F(x)F(y)$.

Case 4: ($x \neq 1$, $y \neq 1$) Since no element in M is invertible, we do not need to worry about the case where $xy = 1$. Hence, we have $F(xy) = 0$, and $F(x)F(y) = 0 \cdot 0 = 0$.

It is indeed a monoid homomorphism, then. We then note that 0 is not left or right cancellative in N, since we have that $0 \cdot 1 = 0 \cdot 0 = 1 \cdot 0 = 0$, but $1 \neq 0$. By the remark above, F corresponds to a functor $F : \underline{M} \to \underline{N}$ via $F(A) = B$ and $F : \mathrm{Hom}_{\underline{M}}(A, A) \to \mathrm{Hom}_{\underline{N}}(B, B)$ is the morphism we just described. Taking $y \in M$ such that $y \neq 1$, we have that y is left and right cancellative, so it corresponds to both a monomorphism and an epimorphism. However, $F(y) = 0$ is neither a monomorphism nor an epimorphism. Thus, we have the desired properties. $\square$

Remark. Thomas O'Hare was a collaborator.

Problem 6. Define the *center* of a category $\mathcal{C}$ to be the class of natural transformations of the identity functor $1_{\mathcal{C}}$ to itself. Let $\mathcal{C} = \mathbf{R\text{-}mod}$ and let c be an element of the center of R. For any $M \in \mathrm{Ob}(\mathbf{R\text{-}mod})$, let $\eta(c)_M : M \to M$ denote the map $x \mapsto cx$ for $x \in M$. Show that the map $\eta(c) : M \mapsto \eta(c)_M$ is a natural transformation in the center of **R-mod**, and every element of the center of **R-mod** is of this form. Show that $c \mapsto \eta(c)$ is a bijection of the center of R with the center of **R-mod**, and hence the center of **R-mod** is a set.

Proof. We first show that the map $\eta(c) : M \to \eta(c)_M$ is a natural transformation in the center of **R-mod**. That is to say, it is a natural transformation of the identity functor to itself. The existence of a morphism for every object follows by construction; since we are in **R-mod**, the morphisms are module homomorphisms, and we see that the map $\eta(c)_M(x + y) = c(x + y) = cx + cy = \eta(c)_M(x) + \eta(c)_M(y)$, and $\eta(c)_M(rx) = c(rx) = r(cx) = r\eta(c)_M(x)$, since c is in the center. We then need to show that the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{\eta(c)_M} & M \\ {\scriptstyle 1_{\mathbf{R\text{-}mod}}(f)}\downarrow & & \downarrow{\scriptstyle 1_{\mathbf{R\text{-}mod}}(f)} \\ N & \xrightarrow[\eta(c)_N]{} & N \end{array}$$

In other words, for any module homomorphism $f : M \to N$, we have that

$$\eta(c)_N(f(x)) = f(\eta(c)_M(x)).$$

Writing things out more explicitly, this is equivalent to

$$cf(x) = f(cx),$$

which follows since f is a module homomorphism. Hence, we have that this is a natural transformation of the identity functor to itself.

Now, let η be some natural transformation of the identity functor to itself; i.e., for every $M \in \mathrm{Ob}(\mathbf{R\text{-}mod})$, we have a morphism $\eta_M : M \to M$, and furthermore this morphism commutes with any morphism $f : M \to N$. In other words, we have that

$$\eta_N(f(x)) = f(\eta_M(x)).$$

Consider $f : R \to R$ which is the identity. Examine that $\eta_R(1) \in R$ is such that

$$\eta_R(1)r = \eta_R(r) = r\eta_R(1)$$

for all $r \in R$, and hence we have that $\eta_R(1)$ is in the center of R. Denote $\eta_R(1) = c$. Now, we have a module homomorphism $f : R \to M$ which is given by $f(1) = m$, and using the commutativity of the diagram we get that

$$\eta_M(m) = \eta_M(f(1)) = f(\eta_R(1)) = f(c) = cf(1) = cm.$$

This holds for all $m \in M$, our module, so we have the desired result. That is to say, any natural transformation satisfying these properties is of the form $\eta(c)$ for some $c \in Z(R)$.

The first step in this showed that, for all $c \in Z(R)$, we can establish a natural transformation $\eta(c)$, thus giving us a map. It follows that this map from the center of the ring to the center of **R-mod** is well-defined; if $c = d$ in the center, we have that $\eta(c) = \eta(d)$, since we have the morphisms are the same for each $M \in \mathrm{Ob}(\mathbf{R\text{-}mod})$. The second step showed that, for all η a natural transformation in the center of **R-mod**, we have that η is of the form $\eta(c)$ for some c. Hence, we have established

surjectivity. The final step is to show injectivity; i.e. if $\eta(c) = \eta(d)$, then $c = d$ as elements. To see this, notice that we have $\eta(c)_R = \eta(d)_R$, which implies that $\eta(c)_R(1) = c = d = \eta(d)_R(1)$, as desired. So we indeed have a bijection, establishing the fact that the center of **R-mod** is a set. □

Problem 7. Let $\mathcal{C}$ and $\mathcal{D}$ be categories, and let $F : \mathcal{C} \to \mathcal{D}$ and $G : D \to \mathcal{C}$ define an equivalence of categories. Let $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. Show that any of the following properties of f implies the same property for $F(f)$:

(a) f is monic;
(b) f is epic;
(c) f has a right (or left) inverse;
(d) f is an isomorphism.

Proof. Since we have an equivalence of categories, we have that F is a fully faithful functor which is "essentially surjective". We use this fact below.

(a) Assume that f is monic. Then for any $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(D, A)$, we have that $f \circ g_1 = f \circ g_2 \implies g_1 = g_2$. We wish to show this for $F(f)$ as well. That is, if we have $g_1, g_2 \in \mathrm{Hom}_{\mathcal{D}}(D, F(A))$, then $F(f) \circ g_1 = F(f) \circ g_2$ implies $g_1 = g_2$. Since F essentially surjective, we have that there exists some object $D' \in \mathcal{C}$ and an isomorphism $g' : F(D') \to D$ so that $g_1 g'$, $g_2 g' : F(D') \to F(A)$, and so since F is full we can find h_1, h_2 such that $F(h_1) = g_1 g'$, $F(h_2) = g_2 g'$, so $F(f) \circ F(h_1) = F(f \circ h_1) = F(f \circ h_2) = F(f) \circ F(h_2)$. Notice that faithful implies $f \circ h_1 = f \circ h_2$, which tells us that $h_1 = h_2$. Using that g' is an isomorphism, Thus, we have that $F(h_1) = g_1 g' = g_2 g' = F(h_2) \implies g_1 = g_2$.
(b) Assume that f is epic. Then for any $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(B, D)$, we have that $g_1 \circ f = g_2 \circ f \implies g_1 = g_2$. We wish to show this for $F(f)$ as well. That is, if we have $g_1, g_2 \in \mathrm{Hom}_{\mathcal{D}}(F(B), D)$, then $g_1 \circ F(f) = g_2 \circ F(f)$ implies $g_1 = g_2$. Since F is essentially surjective, we have that there exists a D' and an isomorphism g' with $g' : D \to F(D')$, so that $g' g_1$, $g' g_2 : F(B) \to F(D')$. Hence since F is full, we can find morphisms h_1, h_2 such that $F(h_1) = g' g_1$, $F(h_2) = g' g_2$, so $F(h_1) \circ F(f) = F(h_1 \circ f) = F(h_2 \circ f) = F(h_2) \circ F(f)$. Notice that faithful implies $h_1 \circ f = h_2 \circ f$, which tells us that $h_1 = h_2$. Thus, we have that $F(h_1) = g' g_1 = g' g_2 = F(h_2)$, and since g' is an isomorphism we have that $g_1 = g_2$, as desired.
(c) Assume that $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ has a section; i.e., a $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ with $f \circ g = 1_A$. We wish to show that $F(f)$ has a section. Notice that $F(f \circ g) = F(1_A) = 1_{F(A)}$, and we have $F(f \circ g) = F(f) \circ F(g)$. So $F(f)$ has a section. By the same argument, if f is a retraction, there exists a g with $g \circ f = 1_A$, and so the functor takes this to a retraction.
(d) Notice that if f is an isomorphism, we have a g such that $f \circ g = 1_A$, $g \circ f = 1_B$. Thus, we have that $F(g)$ is such that $F(f) \circ F(g) = F(f \circ g) = 1_{F(A)}$, $F(g) \circ F(F) = F(g \circ f) = 1_{F(B)}$. So $F(f)$ is an isomorphism.

□

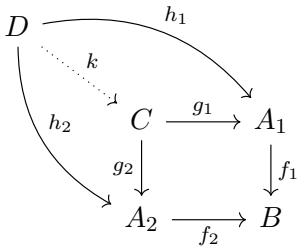
Let $\mathcal{C}$ be a category and $f_i : A_i \to B$ be two morphisms in $\mathcal{C}$. A *pullback* of $\{f_1, f_2\}$ or a *fibered product* of A_1 and A_2 is a triple (C, g_1, g_2) consisting of an object C of $\mathcal{C}$ and morphisms $g_i : C \to A_I$ such that the following diagram commutes:

$$\begin{array}{ccc} C & \xrightarrow{g_1} & A_1 \\ {\scriptstyle g_2}\downarrow & & \downarrow{\scriptstyle f_1} \\ A_2 & \xrightarrow[f_2]{} & B \end{array}$$

and such that if

$$\begin{array}{ccc} D & \xrightarrow{h_1} & A_1 \\ {\scriptstyle h_2}\downarrow & & \downarrow{\scriptstyle f_1} \\ A_2 & \xrightarrow[f_2]{} & B \end{array}$$

is any commutative diagram containing f_1 and f_2, then there is a unique $k : D \to C$ such that



is commutative. We usually denote C by $A_1 \times_B A_2$. As in the above exercise, if a pull back exists, it is unique up to isomorphism. [The dual notion to a pull back is a *push out* and can be defined by reversing all the arrows above.]

Problem 8. Now take $\mathcal{C} = \mathbf{Grp}$ and $f_i : G_i \to H$ in $\mathbf{Grp}$. Let M be the subgroup of the product $G_1 \times G_2$ defined by

$$M := \{(g_1, g_2) \in G_1 \times G_2 \ : \ f_1(g_1) = f_2(g_2)\}.$$

Let $m_i = p_i|_M$, where the p_i are the projection of $G_1 \times G_2$ onto G_i. Show that (M, m_1, m_2) is a pull back of $\{f_1, f_2\}$, i.e., $M = G_1 \times_H G_2$.

Proof. We must first establish that M is indeed a group. To do so, it suffices to show that it is a subgroup of $G_1 \times G_2$. Let $(g_1, g_2), (h_1, h_2) \in M$, then we have that

$$(g_1, g_2) \cdot (h_1, h_2)^{-1} = (g_1, g_2) \cdot (h_1^{-1}, h_2^{-1}) = (g_1 h_1^{-1}, g_2 h_2^{-1}).$$

We now check that this is still in the group M. Since the f_i are group homomorphisms, we have that

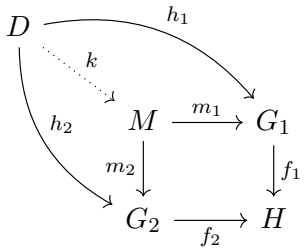
$$f_1(g_1 h_1^{-1}) = f_1(g_1) f_1(h_1)^{-1} = f_2(g_2) f_2(h_2)^{-1} = f_2(g_2 h_2^{-1}).$$

So $(g_1 h_1^{-1}, g_2 h_2^{-1}) \in M$, and it is indeed a group.

Let D be a group such that we have the following commutative diagram:

$$\begin{array}{ccc} D & \xrightarrow{h_1} & G_1 \\ {\scriptstyle h_2}\downarrow & & \downarrow{\scriptstyle f_1} \\ G_2 & \xrightarrow[f_2]{} & H \end{array}$$

We need to show then that D factors through M. That is, we have a unique group homomorphism $k : D \to M$ such that we have the commutative diagram. We first establish the existence of such a group homomorphism. Define $k : D \to M$ by $k(g) = (h_1(g), h_2(g))$. We first notice that this is a map from D into M. That is, $k(g) = (h_1(g), h_2(g))$ is such that $f_1(h_1(g)) = f_2(h_2(g))$. However, this follows by the commutativity of the above diagram. We now notice this is a group homomorphism, since if $g, h \in D$, we have $k(gh) = (h_1(gh), h_2(gh)) = (h_1(g)h_1(h), h_2(g)h_2(h)) = (h_1(g), h_2(g))(h_1(h), h_2(h)) = k(g)k(h)$. Finally, we check that the following diagram



is commutative. However, this is clear by how we've constructed k; taking $g \in D$, we have that $m_2(k(g)) = m_2((h_1(g), h_2(g)) = h_2(g)$, and likewise $m_1(k(g)) = h_1(g)$. Hence, the diagram commutes, and so we have the existence of such a morphism.

We next need to check the uniqueness of such a morphism. Let k' be another morphism which makes the following diagram commute. We wish to show that $k'(g) = k(g)$ for all $g \in D$. Since they both make the diagrams commute, we get that $m_1(k'(g)) = h_1(g) = m_1(k(g))$ so that $m_1(k'(g))m_1(k(g))^{-1} = m_1(k'(g)k(g)^{-1}) = e_{G_1}$, and likewise we have that $m_2(k'(g))m_2(k(g)^{-1}) = m_2(k'(g)k(g)^{-1}) = e_{G_2}$. Thus, we have that $k'(g)k(g)^{-1} = (e_{G_1}, e_{G_2})$, so that $k'(g) = k(g)$ for all $g \in D$. Hence, we have uniqueness. Since we have a unique morphism $k : D \to M$ for any D which makes the diagram commute, we have that M is the pull back. □

Problem 9. Let p be a prime number and let $I = \{1, 2, 3, \ldots\}$ be the directed set of positive integers with their usual order. For each $n \in I$, let $\mathbb{Z}/p^n\mathbb{Z}$ be the ring of integers mod p^n. If $m \leq n$, we have the projections $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$. The *ring of p-adic integers* is the inverse limit ring $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

(i) Show that $\mathbb{Z}_p$ can be constructed as sequences of residue classes

$$a = (a_1 \pmod p), a_2 \pmod{p^2}, \ldots),$$

where the a_i are integers and for $l \geq k$ we have that $a_k \equiv a_l \pmod{p^k}$ with componentwise addition and multiplication. The maps $\eta_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ are given by $a \mapsto a_n \pmod{p^n}$.

(ii) Show that every element of $\mathbb{Z}_p$ can be represented by a representative of the form

$$(r_0, r_0 + r_1 p, r_0 + r_1 p + r_2 p^2, \ldots)$$

with $0 \leq r_i < p$.

(iii) Show that if we associate to

$$(r_0, r_0 + r_1 p, r_0 + r_1 p + r_2 p^2, \ldots)$$

the formal sum

$$r_0 + r_1 p + r_2 p^2 + \cdots = \sum r_i p^i,$$

called a p-adic number, then the addition and multiplication in $\mathbb{Z}_p$ corresponds to the usual sum and product of series with the usual rules of "carrying".

Proof. (i) Let

$$K := \{a = (a_1 \pmod p), a_2 \pmod{p^2}, \ldots) \ : \ a_i \in \mathbb{Z}, a_k \equiv a_l \pmod{p^k} \text{ for } l \geq k\};$$

i.e., the set of sequences of residue classes which satisfies the desired property, and such that it is a ring under componentwise addition and componentwise multiplication (which form this into a ring with identity). We wish to show that this satisfies the property of the inverse limit, which will tell us that $\mathbb{Z}_p \cong K$. That is, we can construct $\mathbb{Z}_p$ as we have constructed K.

We first check that the projections commute. Our projections in this case are $\eta_n : K \to \mathbb{Z}/p^n\mathbb{Z}$ given by $a \mapsto a_n \pmod{p^n}$. Let $m \leq n$. Then we wish to show that $\varphi_{mn} \circ \eta_n = \eta_m$. Taking $a \in K$, we have

$$\varphi_{mn} \circ \eta_n(a) = \varphi_{mn}(a_n \pmod{p^n}) = a_n \pmod{p^m},$$

but by construction we have

$$a_n \pmod{p^m} = a_m = \eta_m(a).$$

Hence, the maps commute for all $m \leq n$.

Next, we need to check the universal property. Let V be another ring such that, for all $m \leq n$, we have maps $\psi_k : V \to \mathbb{Z}/p^k\mathbb{Z}$ with $\varphi_{mn} \circ \psi_n = \psi_m$. We wish to construct a unique morphism $u : V \to K$ which commutes with all the maps. That is, for all m, we want that $\psi_m = \eta_m \circ u$. Define $u : V \to K$ via $u(v) = (\psi_1(v), \psi_2(v), \ldots)$. We check that this is a ring morphism. Notice that if $1 \in V$ is the identity, we have that $\psi_m(1) = 1 \in \mathbb{Z}/p^m/\mathbb{Z}$, so we get that $u(1) = (1, 1, \ldots)$, which is the identity in K, since we have componentwise multiplication. If $v, w \in V$, then we have

$$\begin{aligned} u(v+w) &= (\psi_1(u+v), \psi_2(u+v), \ldots) \\ &= (\psi_1(u) + \psi_1(v), \ldots) = u(v) + u(w), \end{aligned}$$

again since we have componentwise addition. Finally, we have

$$u(vw) = (\psi_1(vw), \ldots) = (\psi_1(v)\psi_1(w), \ldots) = u(v)u(w),$$

since we have componentwise multiplication. So this is indeed a morphism. To check uniqueness, let $u' : V \to K$ be another such morphism. Then by the commutativity of the diagrams, we see that $\eta_m(u'(v) - u(v)) = \psi_m(v) - \psi_m(v) = 0$ for all $v \in V$ and for all m. We get then that $u'(v) - u(v)$ is the 0 map, which forces $u'(v) = u(v)$ for all $v \in V$. Thus, this is a unique morphism, and K is the inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$ up to isomorphism. So we can construct $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ as these residue classes, as desired. We will denote K as $\mathbb{Z}_p$ for the remainder of the problem.

(ii) Letting a_i be the smallest positive representative in the class $a_i \pmod{p}$, we have that

$$a_1 \equiv a_2 \pmod{p},$$

implies that (after assigning $a_1 = r_0$) there is a r_1 with $0 \leq r_1 < p$ with

$$a_2 = r_0 + r_1 p.$$

To see this, notice that $a_2 - a_1 \equiv 0 \pmod{p}$, so there is an integer k so that $a_2 = kp + a_1$. Since we have a_2 is the smallest representative in mod p^2, we must have $0 \leq a_2 < p^2$, thus forcing $0 \leq k < p$.

We then have

$$r_0 + r_1 p \equiv a_3 \pmod{p^2},$$

so we must have that

$$r_0 + r_1 p + r_2 p^2 = a_3$$

by the same procedure above. Notice here that we must have $0 \leq r_2 < p$ again, since a_3 is the smallest representative of its class in p^3. Continuing inductively, we have that $a_{n+1} = a_n + p^n r_n$, with $0 \leq r_n < p$, so we have that we can represent elements as

$$a = (r_0, r_0 + r_1 p, r_0 + r_1 p + r_2 p^2, \ldots),$$

where $0 \leq r_i < p$.

(iii) Taking $a, b \in \mathbb{Z}_p$, we have from (ii) that

$$\begin{aligned} a &= (r_0, r_0 + r_1 p, r_0 + r_1 p + r_2 p^2, \ldots), \\ b &= (q_0, q_0 + q_1 p, q_0 + q_1 p + q_2 p^2, \ldots), \end{aligned}$$

both with $0 \leq r_i, q_i < p$. Hence, we get that

$$a+b = (r_0+q_0 \pmod{p}, r_0+q_0+(r_1+q_1)p \pmod{p^2}, r_0+q_0+(r_1+q_1)p+(r_2+q_2)p^2 \pmod{p^3}, \ldots),$$

which matches that if we represent these as sums, i.e.

$$a = \sum r_i p^i, \quad b = \sum q_i p^i,$$

then

$$a + b = \sum (r_i + q_i) p^i,$$

where we note we may have to carry if $r_i + q_i \geq p$. For multiplication, we have componentwise multiplication, so we see that

$$ab = (r_0 q_0, (r_0 + r_1 p)(q_0 + q_1 p), \ldots),$$

which after expanding and taking mod p^n, we have

$$ab = (r_0 q_0, r_0 q_0 + r_0 q_1 p + r_1 q_0 p, \ldots),$$

which matches up with

$$ab = \left(\sum r_i p^i\right)\left(\sum q_i p^i\right) = \sum c_i p^i,$$

where c_i is defined to be

$$c_i = \sum_{k+j=i} r_i q_j.$$

So we have that this is indeed an alternate representation of numbers.

□

Remark. Thomas O'Hare was a collaborator.

Problem 10. As an application of Yoneda's Lemma, show that there is a bijection between:

- The class of natural transformations between the functors $\mathrm{Hom}_{\mathcal{C}}(A,\cdot)$ and $\mathrm{Hom}_{\mathcal{C}}(A',\cdot)$ for two objects A, A' of $\mathcal{C}$.
- The set $\mathrm{Hom}_{\mathcal{C}}(A,A')$.

Proof. Recall Yoneda's Lemma.

Theorem 1 (Yoneda's Lemma)**.** Let F be a functor from $\mathcal{C}$ to **Set**, $A \in \mathrm{Ob}(\mathcal{C})$, a an element of the set $F(A)$. For any $B \in \mathrm{Ob}(\mathcal{C})$, let a_B be the map of $\mathrm{Hom}_{\mathcal{C}}(A,B)$ into $F(B)$ such that $k \mapsto F(k)(a)$ (i.e., the evaluation map). Then $B \mapsto a_B$ is a natural transformation $\eta(a)$ of $\mathrm{Hom}_{\mathcal{C}}(A,\cdot)$ into F. Moreover, $a \mapsto \eta(a)$ is a bijection of the set $F(A)$ onto the class of natural transformations of $\mathrm{Hom}_{\mathcal{C}}(A,\cdot)$ to F. The inverse of $a \mapsto \eta(a)$ is the map $\eta \mapsto \eta_A(1_A) \in F(A)$.

Let η be a natural transformation between $\mathrm{Hom}_{\mathcal{C}}(A,\cdot)$ and $\mathrm{Hom}_{\mathcal{C}}(A',\cdot)$, where $A, A' \in \mathrm{Ob}(\mathcal{C})$. Notice that the statement of Yoneda's lemma above tells us that, if we assign our functor $F = \mathrm{Hom}_{\mathcal{C}}(A,\cdot)$ and $A' \in \mathrm{Ob}(\mathcal{C})$ to be our object, there is a bijection between the class of natural transformation of $\mathrm{Hom}_{\mathcal{C}}(A',\cdot)$ and $\mathrm{Hom}_{\mathcal{C}}(A,\cdot)$ and the set $F(A') = \mathrm{Hom}_{\mathcal{C}}(A,A')$, which is given through the evaluation map. □

Problem 11. Let G be a group and $\underline{G}$ the associated category as in **Problem 1.1**, so the category with a single object, call it $*$, and such that $\mathrm{Hom}_{\underline{G}}(*,*) = G$.

(a) Show that a covariant functor $F : \underline{G} \to \mathbf{Set}$ is determined by a set $X = F(*)$, and a left action of G on X. Call this functor F_X.

(b) Show that a natural transformation $\eta : F_X \to F_Y$ determines a G-equivariant map $\eta : X \to Y$, i.e., $\eta(g \cdot x) = g \cdot \eta(x)$ for all $g \in G$, $x \in X$.

(c) Show that Yoneda's Lemma for the functor $F = \mathrm{Hom}_{\underline{G}}(*,\cdot)$ from $\underline{G}$ to **Set** gives Cayley's Theorem: G is isomorphic to a subgroup of $\mathrm{Sym}(G)$, the permutations of G as a set.

We will need a claim for this.

Claim 1. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor, let $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ be an isomorphism. Then $F(f)$ is also an isomorphism.

Proof. If $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ is an isomorphism, we have that there is a $g \in \mathrm{Hom}_{\mathcal{C}}(B,A)$ so that $fg = \mathrm{id}_B$, $gf = \mathrm{id}_A$. Hence, we have $F(fg) = \mathrm{id}_{F(B)} = F(f)F(g)$, $F(gf) = \mathrm{id}_{F(A)} = F(g)F(f)$, so $F(f)$ is an isomorphism as well. □

Proof. (a) We have that a covariant functor $F : \underline{G} \to \mathbf{Set}$ assigns to the object $*$ a set, call it $F(*) = X \in \mathrm{Ob}(\mathbf{Set})$. We wish to show that this functor determines a left action of G on X. Recall that one can see this action as a group morphism $G \to \mathrm{Sym}(X)$. We have that $F : \mathrm{Hom}_{\underline{G}}(*,*) = G \to \mathrm{Hom}_{\mathbf{Set}}(X,X) = \mathrm{Sym}(X)$ is defined by $F(1_G) = 1$ (the identity permutation) and $F(xy) = F(x)F(y)$. We remark that it *is* $\mathrm{Sym}(X)$ and not $\mathrm{Fun}(X)$, since the elements in $\mathrm{Hom}_{\underline{G}}(*,*)$ are isomorphisms, and functors take isomorphisms to isomorphisms; moreover, isomorphisms in **Set** are bijections, giving us $\mathrm{Sym}(X)$. Hence, this functor is really a group morphism from G to $\mathrm{Sym}(X)$, and so really is a group action of G on X. Moreover, we see that this information goes both ways; if we know what set G is acting on, we set $F(*) = X$, and we have that there is a group morphism $f : G \to \mathrm{Sym}(X)$, and so we define the functor to act on elements of G via this group morphism; i.e. we have that $F : \mathrm{Hom}_{\underline{G}}(*,*) \to \mathrm{Hom}_{\mathbf{Set}}(X,X)$ is defined by $F(x) = f(x)$. So a contravariant functor is completely determined by the set and the left group action of G on the set.

(b) Recall that a *G-equivariant map* is a map between two sets X and Y, say $f : X \to Y$, such that if G acts on X and on Y, we have that $f(gx) = gf(x)$. In other words, the action commutes with the map.

Let $\eta : F_X \to F_Y$ be a natural transformation of these functors. Recall from (a) that these functors are completely determined by the action of G on the sets X and Y. So, using the commutativity of the following diagram

$$\begin{array}{ccc} X & \xrightarrow{\eta_*} & Y \\ {\scriptstyle F_X(g)}\downarrow & & \downarrow{\scriptstyle F_Y(g)} \\ X & \xrightarrow[\eta_*]{} & Y \end{array}$$

we have that $\eta_*(F_X(g)(x)) = F_Y(g)(\eta_*(x))$. Since $\eta_* =: \eta$ is a map of sets, we can rewrite this as

$$\eta(F_X(g)(x)) = F_Y(g)(\eta(x)),$$

and furthermore using the fact that F_X, F_Y determine actions, we have

$$\eta(gx) = g\eta(x),$$

in other words, the natural transformation is just a G-equivariant map from X to Y.

(c) Our goal is to show that G is isomorphic to a subgroup of $\mathrm{Sym}(G)$. Using **Theorem 1**, letting $F = \mathrm{Hom}_{\underline{G}}(*, \cdot)$, we get that the class of natural transformations from F to $\mathrm{Hom}_{\underline{G}}(*, \cdot)$ is in bijection with $F(*) = \mathrm{Hom}_{\underline{G}}(*, *) = G$. First, we remark that by (a) this F determines an action of G on itself, which by the properties of covariant Hom determines that we will have G acting on itself via left multiplication. So throughout, unless otherwise stated, the action will be left multiplication.

Now the class of natural transformations from $\mathrm{Hom}_{\underline{G}}(*, \cdot)$ to $\mathrm{Hom}_{\underline{G}}(*, \cdot)$ is the collection of G-equivariant maps from G to itself by (b), which we claim is a subgroup of $\mathrm{Sym}(G)$. To see this, we need to show that G-equivariant maps from G to itself are bijective. Let f be a G-equivariant map from G to G. Then we have that

$$f(e) = h \in G,$$

and

$$f(g) = f(ge) = gf(e) = gh$$

for all $g \in G$. Hence, we have that G-equivariant maps can be described as multiplication on the right; i.e. $f = R_h : G \to G$. This is clearly bijective, since we have that

$$R_{h^{-1}} \circ R_h(g) = (gh)h^{-1} = g(hh^{-1}) = g,$$

$$R_h \circ R_{h^{-1}}(g) = (gh^{-1})h = g(h^{-1}h) = g$$

for all $g \in G$. Hence, the set of all G-equivariant maps is inside of $\mathrm{Sym}(G)$.

Next, we claim that this is a subgroup, with the induced structure being composition. Let H denote the set of G-equivariant maps. We have $1 = R_e \in H$, for $f \in H$, we describe it as $f = R_g$, so $f^{-1} = R_{g^{-1}} \in H$, and we have that if $f, h, \in H$, then we can write them as $f = R_a$, $h = R_b$, and so

$$f \circ h = R_a \circ R_b = R_{ba} \in H.$$

So this is indeed a subgroup.

Finally, we note that we have a bijection between H and G, and so showing this is an isomorphism (or, at least, induces an isomorphism) gives us the desired result. Denote this bijection as η, then we have that $\eta : G \to H$ is given by $\eta(g) = R_g$ by Yoneda's lemma. To see this explicitly, we have that $\eta(g)$ is a natural transformation from $\mathrm{Hom}_{\underline{G}}(*, \cdot)$ to itself, and so

$$\begin{array}{ccc} G & \xrightarrow{\eta(g)} & G \\ {\scriptstyle \mathrm{Hom}_{\underline{G}}(*,h)}\downarrow & & \downarrow{\scriptstyle \mathrm{Hom}_{\underline{G}}(*,h)} \\ G & \xrightarrow{\eta(g)} & G \end{array}$$

commutes for all $h \in G$. That is, we have

$$\eta(g)\left(\mathrm{Hom}_{\underline{G}}(*,h)\right) = \mathrm{Hom}_{\underline{G}}(*,h)(\eta(g))$$

for all $h \in H$. Examining at the point $e \in G$, we get

$$\eta(g)\left(\mathrm{Hom}_{\underline{G}}(*,h)(e)\right) = \eta(g)(h) = \mathrm{Hom}_{\underline{G}}(*,h)(\eta(g)(e)) = \mathrm{Hom}_{\underline{G}}(*,h)(\mathrm{Hom}_{\underline{G}}(*,e)(g)) = hg,$$

where the second to last inequality is derived from the construction in Yoneda's Lemma. That is, Yoneda says

$$\eta(g)(k) = \mathrm{Hom}_{\underline{G}}(*,k)(g),$$

so

$$\eta(g)(e) = \mathrm{Hom}_{\underline{G}}(*,e)(g).$$

Thus, for all $h \in G$, we have $\eta(g)(h) = hg = R_g(h)$, so $\eta(g) = R_g$. Now, using this, we check whether η is a homomorphism. We have

$$\eta(gh) = R_{gh} = R_h \circ R_g = \eta(h) \circ \eta(g).$$

So we see that this, in fact, gives us a bijective *anti-homomorphism*. We can use this to then construct an actual isomorphism by noting that the map $\theta : H \to H$ given by $R_g \mapsto (R_g)^{-1} = R_{g^{-1}}$ is an anti-isomorphism, and so we get that defining $\gamma = \theta \circ \eta$ that

$$\gamma(gh) = (\theta \circ \eta)(gh) = \theta(\eta(h)\eta(g)) = \theta(R_h \circ R_g) = R_{g^{-1}} \circ R_{h^{-1}} = \gamma(g)\gamma(h).$$

We have γ is a composition of bijections, so a bijection, and so γ is an isomorphism. Thus, Cayley's theorem is satisfied.

□

Problem 12. Dualize Yoneda's Lemma to show that if F is a contravariant functor from $\mathcal{C}$ to **Set** and $A \in \mathrm{Ob}(\mathcal{C})$, then any natural transformation of $\mathrm{Hom}_{\mathcal{C}}(\cdot, A)$ to F has the form $B \mapsto a_B$, where a_B is a map from $\mathrm{Hom}_{\mathcal{C}}(B, A)$ to $F(B)$ determined by an element $a \in F(A)$ as $a_B : g \mapsto F(g)(a)$. Show that this gives a bijection of the set $F(A)$ with the class of natural transformations of $\mathrm{Hom}_{\mathcal{C}}(\cdot, A)$ to F.

Proof. We work through the proof of Yoneda's Lemma in the dual version.

We wish to determine the natural transformations from a contravariant functor $F : \mathcal{C} \to \mathbf{Set}$ to the functor $\mathrm{Hom}_{\mathcal{C}}(\cdot, A)$. Let $A \in \mathrm{Ob}(\mathcal{C})$ be arbitrary, and let $a \in F(A)$, $k \in \mathrm{Hom}_{\mathcal{C}}(B, A)$. Then we have

$$\begin{array}{ccc} A & & F(A) \\ {\scriptstyle k}\uparrow & & \downarrow{\scriptstyle F(k)} \\ B & & F(B) \end{array}$$

and hence we have that for $a \in A$, $F(k)(a) \in F(B)$. So in general, for $B \in \mathrm{Ob}(\mathcal{C})$, we have a map

$$a_B : \mathrm{Hom}_{\mathcal{C}}(B, A) \to F(B), \quad a_B(k) = F(k)(a).$$

Let $g : B \to C$. Then we see that

$$F(g)a_C(k) = F(g)F(k)(a) = F(kg)(a),$$
$$a_B(\mathrm{Hom}_{\mathcal{C}}(g, A)(k)) = a_B(kg) = F(kg)(a),$$

so that

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(C,A) & \xrightarrow{a_C} & F(C) \\ {\scriptstyle \mathrm{Hom}_{\mathcal{C}}(g,A)}\downarrow & & \downarrow{\scriptstyle F(g)} \\ \mathrm{Hom}_{\mathcal{C}}(B,A) & \xrightarrow[a_B]{} & F(B) \end{array}$$

commutes. So $\eta(a) : B \mapsto a_B$ is a natural transformation of $\mathrm{Hom}_{\mathcal{C}}(\cdot, A)$ into F.

Now, we wish to show that every natural transformation is of this form. Let η be any natural transformation of $\mathrm{Hom}_{\mathcal{C}}(\cdot, A)$ into F. Let $f \in \mathrm{Hom}_{\mathcal{C}}(B, A)$. Then we have

$$\begin{array}{ccc} A & & \mathrm{Hom}_{\mathcal{C}}(A,A) \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle \mathrm{Hom}_{\mathcal{C}}(f,A)} \\ B & & \mathrm{Hom}_{\mathcal{C}}(B,A) \end{array}$$

and since η is a natural transformation, we the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(A,A) & \xrightarrow{\eta_A} & F(A) \\ {\scriptstyle \mathrm{Hom}_{\mathcal{C}}(f,A)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ \mathrm{Hom}_{\mathcal{C}}(B,A) & \xrightarrow[\eta_B]{} & F(B) \end{array}$$

This tells us that $\eta_B(f) = \eta_B(1_A f) = \eta_B(\mathrm{Hom}_{\mathcal{C}}(f, A)(1_A)) = F(f)(\eta_A(1_A)) = F(f)(a)$, where $a = \eta_A(1_A) \in F(A)$. This tells us that $\eta = \eta(a)$, as defined before. So we have our desired bijection. □

The next two exercises investigate the definition of kernels and cokernels in a categorical context. Let $\mathcal{C}$ be a category with a zero object, which we denote by $0_{\mathcal{C}}$. Let $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.

We call a morphism $k \in \mathrm{Hom}_{\mathcal{C}}(K, A)$ a *kernel of* f if

(1) k is monic.
(2) $fk = 0$ where $0 \in \mathrm{Hom}_{\mathcal{C}}(K, B)$ is defined by the composition $K \to 0_{\mathcal{C}} \to B$.
(3) For any $g \in \mathrm{Hom}_{\mathcal{C}}(G, A)$ such that $fg = 0$, there exists a $g' \in \mathrm{Hom}_{\mathcal{C}}(G, K)$ such that $g = kg'$. [Remark: Since k is monic, such a g' is unique.]

Dually, we call a morphism $c \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ a *cokernel of* f if

(1) c is epic.
(2) $cf = 0$ where $0 \in \mathrm{Hom}_{\mathcal{C}}(A, C)$ is defined by the composition $A \to 0_{\mathcal{C}} \to C$.
(3) For any $h \in \mathrm{Hom}_{\mathcal{C}}(B, H)$ such that $hf = 0$, there exists a $h' \in \mathrm{Hom}_{\mathcal{C}}(C, H)$ such that $h = h'c$. [Remark: Since c is monic, such a h' is unique.]

Lemma 1. Categorical kernels and cokernels are unique up to isomorphism.

Proof. Note that property (3) for kernels tells us that for any $g \in \mathrm{Hom}_{\mathcal{C}}(G, A)$ such that $fg = 0$, there exists a (unique) $g' \in \mathrm{Hom}_{\mathcal{C}}(G, K)$ such that $g = kg'$. Let k and k' both be kernels; i.e., we have $k \in \mathrm{Hom}_{\mathcal{C}}(K, A)$, $k' \in \mathrm{Hom}_{\mathcal{C}}(K', A)$ satisfies the above desired properties. Using property (3), we get a (unique) morphism g such that $k' = kg$ and a (unique) morphism g' such that $k = k'g'$. Moreover, this tells us that $k' = k'g'g$, and so we have $g'g = 1$ (since the morphism must be unique, and we have $k' = k'1$). A similar argument gives $gg' = 1$, so we get that g is an isomorphism. The same argument applies to give that cokernels are unique up to isomorphism. □

Problem 13. In **R-mod**, show that this recovers the usual notion of kernel and cokernel; that is,

(i) If $f \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(A, B)$ and we let $K = \mathrm{Ker}(f) \subset A$ and $k : K \hookrightarrow A$ is the embedding of K into A, then $k \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(K, A)$ is a kernel of f in the categorical sense for **R-mod**.

(ii) If $f \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(A, B)$ and we let $C = B/f(A)$ and $c : B \to C$ the canonical quotient map, then $c \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(B, C)$ is a cokernel of f in the categorical sense in **R-mod**.

Proof. (i) To show that k is the kernel in the categorical sense, we need to show that the three properties hold.

(1) We would like to show that k is monic. Recall that a map is monic in **R-mod** iff it is injective. Since k is an embedding, we have that $\mathrm{Ker}(k) = 0$, so that k is injective.

(2) Recall that the zero object of **R-mod** is just the 0 module. We have then that $f \circ k = 0$ by definition of kernel, and furthermore this matches the map $K \to 0_{\mathbf{R\text{-}mod}} \to B$, since the map from K to $0_{\mathbf{R\text{-}mod}}$ is the 0 map and the map from $0_{\mathbf{R\text{-}mod}}$ to B is again the map which sends 0 to 0. [Remark: This also tells us that the 0 map is what you would guess; i.e., it is the map that sends everything to 0.]

(3) Let $g \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(G, A)$ be such that $fg = 0$. Then we have that $f(g(x)) = 0$ for all $g \in G$, or in other words $\mathrm{Im}(g) \subset \mathrm{Ker}(f) = K$. We define then the map $g' : G \to \mathrm{Im}(g) \subset K$, and we see that $k(g'(x)) = g(x)$ for all $x \in G$.

(ii) Again we need to show the three properties hold.

(a) We have that a map is epic iff it is surjective in **R-mod**. Since c is the canonical quotient map, we have naturally that it is surjective.

(b) We need to show that $cf = 0$, where here we again note that this is the 0 map. Let $x \in A$, we have that $f(x) \in f(A)$, so that we have $c(f(x)) = 0$.

(c) Finally, let $h \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(B, H)$ be such that $hf = 0$. We need to show there is a map $h' \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(C, H)$ so that $h = h'c$. Since $hf = 0$, we have that $f(A) \subset \mathrm{Ker}(h)$. In other words, all of the elements in f are mapped to zero under h. Hence, we can define $h'(x + f(A)) = h(x + f(A)) = h(x) + h(f(A)) = h(x)$, and we see that this is well-defined since if $x - y \in f(A)$, we get

$$h'(x - y + f(A)) = h(x - y) = h(x) - h(y) = h'(x + f(A)) - h'(y + f(A)) = 0,$$

and it is indeed a module homomorphism since

$$h'(x + y + f(A)) = h(x + y) = h(x) + h(y) = h'(x + f(A)) + h'(y + f(A)),$$

$$h'(r(x + f(A)) = h'(rx + rf(A)) = h(rx) = rh(x) = rh'(x + f(A)).$$

Moreover, we get that $h'(c(x)) = h(x)$.

□

Problem 14. In **R-mod** show that

(i) If $f \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(A, B)$ is monic, then it is a kernel of its cokernel.

(ii) If $f \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(A, B)$ is epic, then it is a cokernel of its kernel.

Proof. (i) We determined from the last problem that one of the cokernels of f is the map $c : B \to B/f(A)$. We will show that f is a kernel of this map, and then deduce that f is a kernel of *any* of its cokernels.

(1) By assumption, we have that f is monic.

(2) We have by construction that, for all $x \in A$, $c(f(x)) = f(x) + f(A) = f(A)$ (i.e. it is 0), so that $cf = 0$.

(3) Let g be any map $g \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(G, B)$ such that $cg = 0$. We need to find a map $g' \in \mathrm{Hom}_{\mathbf{R\text{-}mod}}(G, A)$ such that $g = fg'$. Since $cg = 0$ this implies that $g(G) \subset f(A)$, i.e. for every $x \in G$, there is a $y \in A$ with $g(x) = f(y)$. Define $g'(x) = y$ for some y which satisfies this. Since f is monic, it is well-defined. We see that this is a module homomorphism, since

$$f(g'(x + z)) = g(x + y) = g(x) + g(y),$$

$$f(g'(x)+g'(z)) = f(g'(x)) + f(g'(z)) = g(x)+g(z),$$

and so by injectivity we have $g'(x+z) = g'(x)+g'(z)$. Likewise,

$$f(g'(rx)) = g(rx) = rg(x)f(rg'(x)) = rf(g'(x)) = rg(x),$$

and so injectivity again gives $g'(rx) = rg'(x)$. By construction, this is a map such that $fg' = g$.

Now, assume $c' : B \to C$ is any cokernel of f. From prior, we have that this is isomorphic to $B/f(A)$, so we have that there is some isomorphism $\varphi : C \to B/f(A)$. We then show that f is still a kernel of this.

(1) We have f is still monic.

(2) Now, we want to show that $c'f = 0$. We have that

$$cf = \varphi c'f = 0,$$

so applying φ^{-1} to both sides, we still get a zero map on the right, and so we have

$$c'f = 0,$$

as desired.

(3) Let $g : G \to B$ be some map so that $c'g = 0$. The final property comes from noting that $c'g = 0$ implies $\varphi c'g = \varphi 0 = 0$, so that we have $cg = 0$. From the canonical map, we get an induced map g' so that $fg' = g$.

(ii) We have that a kernel of $f : A \to B$ is the map $k : \mathrm{Ker}(f) \hookrightarrow A$, the natural embedding of $\mathrm{Ker}(f)$ into A. We again will show that f is a cokernel of k, and then deduce that f is a cokernel of *any* of its kernels.

(1) By construction, f is epic.

(2) We have that $fk = 0$ again by construction (for all $x \in K$, $k(x) \in \mathrm{Ker}(f)$ so that $f(k(x)) = 0$).

(3) Let $h : A \to H$ be such that $hk = 0$. We need to find a morphism $h' : B \to H$ such that $h = h'f$. That is, for all $a \in A$, we wish to find h' so that $h(a) = h'(f(a))$. With f being surjective, we get that $A/\mathrm{Ker}(f) \cong B$. Since $\mathrm{Ker}(f) \subset \mathrm{Ker}(h)$, we can define a map $\hat{h} : A/\mathrm{Ker}(f) \to H$ via $\hat{h}(a + \mathrm{Ker}(f)) = h(a) + h(\mathrm{Ker}(f)) = h(a)$. It is well-defined, since if $a - b \in \mathrm{Ker}(f)$, we get

$$\hat{h}(a-b+\mathrm{Ker}(f)) = h(a-b) = h(a) - h(b) = \hat{h}(a+\mathrm{Ker}(f)) - \hat{h}(b+\mathrm{Ker}(f)) = 0,$$

so that $\hat{h}(a+\mathrm{Ker}(f)) = \hat{h}(b+\mathrm{Ker}(f))$. Notice this is a homomorphism, since

$$\hat{h}(a+b+\mathrm{Ker}(f)) = h(a+b) = h(a)+h(b) = \hat{h}(a+\mathrm{Ker}(f)) + \hat{h}(b+\mathrm{Ker}(f)),$$

and

$$\hat{h}(r(a+\mathrm{Ker}(f))) = \hat{h}(ra+\mathrm{Ker}(f)) = h(ra) = rh(a) = r\hat{h}(a+\mathrm{Ker}(f)).$$

Define then $h' : B \to H$ to be the map so that $h'(b) = \hat{h}(a+\mathrm{Ker}(f))$; i.e., we use the isomorphism given by $A \to A/\mathrm{Ker}(f) \cong B$. Everything is a module homomorphism, and furthermore by construction we get that $h(a) = h'(f(a))$ for all $a \in A$. Hence, we have a morphism so that $h = h'f$.

We now show this holds for any kernel $k' : K' \to A$. From prior, we have an isomorphism $\varphi : \mathrm{Ker}(f) \to K'$.

(1) We have f is still epic.

(2) We wish to show that $fk' = 0$. Notice that composing with the isomorphisms inverse on the right, we have that

$$fk = 0 \implies fk'\varphi = 0\varphi \implies fk' = 0.$$

(3) Finally, let $h : A \to H$ be such that $hk' = 0$. We have that $fk' = 0$ implies that $fk'\varphi = fk = 0\varphi = 0$, so that $fk = 0$. Using what we've just shown, we get a map h' such that $h = h'f$.

□

Remark. Thomas O'Hare was a collaborator.

Problem 15. Show that the contravariant Hom functor $\mathrm{Hom}_R(\cdot, N)$ from **R-mod** to $\mathbb{Z}$**-mod** is left exact.

Proof. Recall that a contravariant functor F is said to be left exact if it sends the exact sequence

$$M' \xrightarrow{g} M \xrightarrow{f} M'' \to 0$$

to the exact sequence

$$0 \to F(M'') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M').$$

In terms of the contravariant Hom functor, we wish to show that the following sequence is exact:

$$0 \to \mathrm{Hom}_R(M'', N) \xrightarrow{\mathrm{Hom}_R(f,N)} \mathrm{Hom}_R(M, N) \xrightarrow{\mathrm{Hom}_R(g,N)} \mathrm{Hom}_R(M', N),$$

So we need to show three things:

(1) First, we wish to show $\mathrm{Hom}_R(f, N)$ is injective. Let $h \in \mathrm{Ker}(\mathrm{Hom}_R(f, N))$. Then we have $\mathrm{Hom}_R(f, N)(h) = 0$. Recall that $\mathrm{Hom}_R(f, N)(h) = h \circ f$, so that $h \circ f = 0$. Notice as well that the exactness above implies that f is surjective, so for all $x \in M''$, there exists a $y \in M$ such that $f(y) = x$. Hence, we have $h(x) = g(f(y)) = 0$, so that $h(x) = 0$ for all $x \in M''$. This then forces $h = 0$, so that $\mathrm{Ker}(\mathrm{Hom}_R(f, N)) = 0$.

(2) Next, we wish to show $\mathrm{Im}(\mathrm{Hom}_R(f, N)) \subset \mathrm{Ker}(\mathrm{Hom}_R(g, N))$. Notice that $\mathrm{Im}(g) = \mathrm{Ker}(f)$ by the exactness above. Let $\psi \in \mathrm{Im}(\mathrm{Hom}_R(f, N))$. Then this implies that $\psi = \mathrm{Hom}_R(f, N)(h)$ for some $h \in \mathrm{Hom}_R(M'', N)$, or in other words $\psi = h \circ f$. Now, we wish to show that $\psi \in \mathrm{Ker}(\mathrm{Hom}_R(g, N))$, so examine $\mathrm{Hom}_R(g, N)(\psi) = \psi \circ g$. Writing things out, this is the same thing as $h \circ f \circ g$, and since $\mathrm{Im}(g) = \mathrm{Ker}(f)$ we get that this is 0. Hence, $\psi \in \mathrm{Ker}(\mathrm{Hom}_R(g, N))$. Since this holds for all ψ we have $\mathrm{Im}(\mathrm{Hom}_R(f, N)) \subset \mathrm{Ker}(\mathrm{Hom}_R(g, N))$.

(3) Finally, we wish to show $\mathrm{Ker}(\mathrm{Hom}_R(g, N)) \subset \mathrm{Im}(\mathrm{Hom}_R(f, N))$. Let $\psi \in \mathrm{Ker}(\mathrm{Hom}_R(g, N))$, i.e. $\psi : M \to N$ is such that $\psi \circ g = 0$. Our goal is to write $\psi = \mathrm{Hom}_R(f, N)(\varphi) = \varphi \circ f$ for some $\varphi \in \mathrm{Hom}_R(M'', N)$. Since $\psi \in \mathrm{Ker}(\mathrm{Hom}_R(g, N))$, we have that $\mathrm{Hom}_R(g, N)(\psi) = \psi \circ g = 0$, or in other words, for all $x \in M'$, $\psi \circ g(x) = 0$. Since $\mathrm{Im}(g) = \mathrm{Ker}(f)$, we have that $\psi(g(x)) = \psi(y) = 0$ for all $y \in \mathrm{Ker}(f)$; that is, $\mathrm{Ker}(f) \subset \mathrm{Ker}(\psi)$. Since f is surjective, we have that $M/\mathrm{Ker}(f) \cong M''$. Denote the induced isomorphism by $\hat{f} : M'' \to M/\mathrm{Ker}(f)$. We can then define $\hat{\psi} : M/\mathrm{Ker}(f) \to N$ via $\hat{\psi}(x + \mathrm{Ker}(f)) = \psi(x + \mathrm{Ker}(f)) = \psi(x)$. This is well-defined, since if $x - y \in \mathrm{Ker}(f)$ we have

$$\hat{\psi}(x - y + \mathrm{Ker}(f)) = \psi(x - y) = \psi(x) - \psi(y) = \hat{\psi}(x + \mathrm{Ker}(f)) - \hat{\psi}(y + \mathrm{Ker}(f)) = 0$$
$$\implies \hat{\psi}(x + \mathrm{Ker}(f)) = \hat{\psi}(y + \mathrm{Ker}(f)),$$

and this is a module homomorphism since

$$\hat{\psi}(x + y + \mathrm{Ker}(f)) = \psi(x + y) = \psi(x) + \psi(y) = \hat{\psi}(x + \mathrm{Ker}(f)) + \hat{\psi}(y + \mathrm{Ker}(f)),$$
$$\hat{\psi}(r(x + \mathrm{Ker}(f))) = \hat{\psi}(rx + \mathrm{Ker}(f)) = \psi(rx) = r\psi(x) = r\psi(x + \mathrm{Ker}(f))$$

for all $x, y \in M/\mathrm{Ker}(f)$, $r \in R$. Define then $\varphi : M'' \to N$ via $\hat{\psi} \circ \hat{f}$. By construction, we have

$$\varphi \circ f(x) = \hat{\psi} \circ \hat{f} \circ f(x) = \hat{\psi}(x + \mathrm{Ker}(f)) = \psi(x),$$

and since this holds for all x we have $\varphi \circ f = \psi$. We have done this for arbitrary ψ, so we get that $\mathrm{Ker}(\mathrm{Hom}_R(g, N)) \subset \mathrm{Im}(\mathrm{Hom}_R(f, N))$.

Thus, $\mathrm{Hom}_R(\cdot, N)$ is left exact. □

Problem 16. Let $M = \mathbb{Z}$, $N = \mathbb{Z}/m\mathbb{Z}$ with $m > 1$, and let $\nu \in \mathrm{Hom}_{\mathbb{Z}}(M, N)$ be the canonical homomorphism from M to N. Show that id_N cannot be written as $\nu \circ f$ for any $f \in \mathrm{Hom}_{\mathbb{Z}}(N, M)$. Hence, show that the image of the exact sequence $M \to N \to 0$ under $\mathrm{Hom}_{\mathbb{Z}}(N, \cdot)$ is not exact.

Proof. Let $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$. Notice that we must have $f(0) = 0$, and so we get that

$$0 = f(0) = f(m) = mf(1) \implies f(1) = 0.$$

Hence, the only homomorphism is the zero homomorphism, so $\mathrm{id}_N \neq \nu \circ f$ for any $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$. We then wish to show that

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \nu)} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \to 0$$

is not exact, even though

$$\mathbb{Z} \xrightarrow{\nu} \mathbb{Z}/m\mathbb{Z} \to 0$$

is exact. This, however, is clear, since if this were exact we would have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \nu)$ is surjective, and from what we've just shown this does not hold (we cannot, for example, hit the identity function). So $\mathrm{Hom}_R(M, \cdot)$ is not necessarily right exact. □

Problem 17. Let $M = \mathbb{Z}$ and $N = m\mathbb{Z}$ with $m > 1$, and let $\iota \in \mathrm{Hom}_{\mathbb{Z}}(N, M)$ be the injection of N into M. Show that the homomorphism $\rho : N \to M$ given by $\rho(mx) = x$ cannot be written as $g \circ \iota$ for any $g \in \mathrm{Hom}_{\mathbb{Z}}(M, M)$. Hence, show that the image of the exact sequence $0 \to N \to M$ under $\mathrm{Hom}_{\mathbb{Z}}(\cdot, M)$ is not exact.

Proof. We first establish that $\rho : m\mathbb{Z} \to \mathbb{Z}$ given by $\rho(mx) = x$ is a module homomorphism. Notice that it is well-defined, since if $x = y$ in $m\mathbb{Z}$ we get that we can write $x = mz$, $y = mj$, and so we have $z = j$ by dividing by m, and hence $\rho(x) = \rho(y)$. Notice that $\rho(0) = 0$, and $\rho(x + y) = \rho(mz + mj) = \rho(m(z + j)) = z + j = \rho(x) + \rho(y)$, and for all $r \in \mathbb{Z}$, we have $\rho(rx) = \rho(rmz) = \rho(m(rz)) = rz = r\rho(x)$.

Now, we have that $\iota : m\mathbb{Z} \to \mathbb{Z}$ is given by $\iota(x) = x$. So for $\rho = g \circ \iota$ for some $g \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$, we have that $\rho(mx) = g(\iota(mx)) = g(mx) = x$. Since g is a module homomorphism this implies that $mg(x) = x$ for all $x \in \mathbb{Z}$. Notice that this implies $g(m) = mg(1) = 1$, which is impossible for $m > 1$ (this implies that $g(1) = 1/m$, which is not an integer). Thus there is no g for which $\rho = g \circ \iota$.

To conclude, even though

$$0 \to m\mathbb{Z} \xrightarrow{\iota} \mathbb{Z}$$

is exact, we do not have

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(\iota, \mathbb{Z})} \mathrm{Hom}_{\mathbb{Z}}(m\mathbb{Z}, \mathbb{Z}) \to 0$$

is exact, since $\mathrm{Hom}_{\mathbb{Z}}(\iota, \mathbb{Z})$ is not surjective by the above argument. □

Problem 18. Show that if m is a positive integer, than $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$. Hence, show that

$$0 \to (m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) \xrightarrow{\iota \otimes 1} \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z})$$

is *not* exact, where ι is the canonical injection $m\mathbb{Z} \hookrightarrow \mathbb{Z}$. Use this to conclude that $M \otimes \cdot$ and $\cdot \otimes N$ need not be exact functors.

Proof. Consider $(\mathbb{Z}/m\mathbb{Z}) \times (m\mathbb{Z})$. We form a map $f : (\mathbb{Z}/m\mathbb{Z}) \times (m\mathbb{Z}) \to \mathbb{Z}/m\mathbb{Z}$ via $f(x \pmod m, my) = xy \pmod m$. This is well-defined, since if $x - x' \in m\mathbb{Z}$ and $my = my'$ (so that $y = y'$), we get

$$\begin{aligned} f(x \pmod m, my) = xy \pmod m = xy' \pmod m = xy' - (x - x')y' \pmod m \\ = x'y' \pmod m = f(x' \pmod m, my'). \end{aligned}$$

We then check that this satisfies the properties of a balanced product:

(1) We notice that

$$f((x+x') \pmod m, my) = (x+x')y \pmod m$$
$$= xy + x'y \pmod m = f(x \pmod m, my) + f(x \pmod m', my),$$

(2) We have

$$f(x \pmod m, m(y+y')) = x(y+y') \pmod m = xy + xy' \pmod m$$
$$= f(x \pmod m, my) + f(x \pmod m, my')$$

(3) Finally, we see $f(xr \pmod m, m) = xry \pmod m = f(x \pmod m, rmy)$.

Hence, we have that this is a balanced product, so the universal property gives us a unique morphism $\varphi : (\mathbb{Z}/m\mathbb{Z}) \otimes_Z (m\mathbb{Z}) \to \mathbb{Z}/m\mathbb{Z}$ which is defined by $(x \pmod m) \otimes (my) \mapsto f(x \pmod m, my) = xy \pmod m$. We check that this is an isomorphism.

Construct a map $\psi : \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \otimes_Z (m\mathbb{Z})$ via $\psi(x \pmod m) = (x \pmod m) \otimes m$. We first check that this is well-defined. If $x - x' \in m\mathbb{Z}$, then we have that

$$\psi(x \pmod m) = (x \pmod m) \otimes m = (x \pmod m) \otimes m - (x - x' \pmod m) \otimes m$$
$$= (x' \pmod m) \otimes m = \psi(x' \pmod m).$$

Next, we check that this is indeed a module homomorphism. Notice that for all $x, y \in \mathbb{Z}/m\mathbb{Z}$ we have

$$\psi((x+y) \pmod m) = ((x+y) \pmod m) \otimes m = (x \pmod m) \otimes m + (y \pmod m) \otimes m$$
$$= \psi(x \pmod m) + \psi(y \pmod m),$$

and for all $r \in \mathbb{Z}$ we have

$$\psi(rx \pmod m) = (rx \pmod m) \otimes m = r((x \pmod m) \otimes m) = r\psi(x \pmod m).$$

So this is indeed a module homomorphism. Now we wish to show that these functions are inverses of each other; doing so will give us that φ is an isomorphism. To do this, it suffices to check it on pure tensors. We see that

$$\varphi(\psi(x \pmod m)) = \varphi((x \pmod m) \otimes m) = f(x \pmod m, 1) = x,$$

and we have

$$\psi(\varphi((x \pmod m) \otimes my)) = \psi(xy \pmod m) = (xy \pmod m) \otimes m = (x \pmod m) \otimes my.$$

So φ is an isomorphism.

For the diagram

$$0 \to (m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) \xrightarrow{\iota \otimes 1} \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z})$$

to be exact, we must have that $\iota \otimes 1$ is injective. We can show this fails in two different ways. Directly, we see that

$$(\iota \otimes 1)(mx \otimes r \pmod m) = \iota(mx) \otimes 1(r \pmod m) = mx \otimes r = x \otimes mr = x \otimes 0 = 0$$

for all generators $mx \otimes r \pmod m$, so in fact the map is trivial. Alternatively, using the isomorphism we just constructed, we have that $\iota \otimes 1$ corresponds to a homomorphism $\kappa : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Using prior knowledge, we know that this homomorphism is determined entirely by where it sends 1. The isomorphism ψ (with a slight alteration since we changed sides) tells us that $\psi(1 \pmod m) = m \otimes (1 \pmod m)$. Hence, using the isomorphism $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$ given in the book/class notes, we see that we must $\kappa(1) = m \pmod m = 0 \pmod m$, so that κ must be the trivial homomorphism. In other words, $\iota \otimes 1$ is the trivial map.

We wish to use this to deduce that $\cdot \otimes N$ is not a left exact functor. Recall that the tensor is covariant in each variable. From prior work, we have that

$$0 \to m\mathbb{Z} \xrightarrow{\iota} \mathbb{Z}$$

is an exact sequence, but what we've just established is that when we apply $\cdot \otimes (\mathbb{Z}/m\mathbb{Z})$, this is no longer necessarily an exact sequence. So we do not have that $\cdot \otimes N$ is left exact. Since $\mathbb{Z}$ is a commutative ring, we get that $M \otimes_Z N \cong N \otimes_Z M$, and so we have that $M \otimes \cdot$ is not necessarily left exact either. □

Problem 19. Let I be an index set and $\{N_\alpha : \alpha \in I\}$ be a set of left R-modules. Let

$$N = \bigoplus_\alpha N_\alpha$$

be their direct sum. Show that N is flat iff each N_α is flat.

Proof. Recall that a module N is *flat* if we have that

$$0 \to K \xrightarrow{f} L \xrightarrow{g} J \to 0$$

is a short exact sequence if and only if

$$0 \to K \otimes_R N \xrightarrow{f \otimes_R \mathrm{id}_N} L \otimes_R N \xrightarrow{g \otimes_R \mathrm{id}_N} J \otimes_R N \to 0$$

is a short exact sequence. In other words, using the fact that tensors are right exact, this is equivalent to saying that a module is flat if $\cdot \otimes_R N$ sends injective maps to injective maps.

We wish to show that injective maps are sent to injective maps, as remarked. Let $f : M' \to M$ be an injective map. Since N is flat, we have that

$$0 \to M' \otimes_R N \xrightarrow{f \otimes_R \mathrm{id}_N} M \otimes_R N$$

is exact. Expanding things out, we have

$$0 \to M' \otimes_R \left(\bigoplus_\alpha N_\alpha \right) \xrightarrow{f \otimes_R (\bigoplus_\alpha \mathrm{id}_{N_\alpha})} M \otimes_R \bigoplus_\alpha N_\alpha$$

is exact.

Now, define $f_M : M \times (\bigoplus_\alpha N_\alpha) \to \bigoplus_\alpha (M \otimes N_\alpha)$ via $f_M(x, (y_\alpha)) = (x \otimes y_\alpha)$. It follows that this defines a balanced product; we have

$$f_M(x + x', (y_\alpha)) = ((x + x') \otimes y_\alpha) = (x \otimes y_\alpha) + (x' \otimes y_\alpha) = f_M(x, (y_\alpha)) + f_M(x', (y_\alpha)),$$

$$f_M(x, (y_\alpha) + (y'_\alpha)) = (x \otimes (y_\alpha + y'_\alpha)) = (x \otimes y_\alpha) + (x \otimes y'_\alpha) = f_M(x, (y_\alpha)) + f_M(x, y'_\alpha),$$

$$f_M(xr, (y_\alpha)) = (xr \otimes y_\alpha) = (x \otimes ry_\alpha) = f_M(x, r(y_\alpha)),$$

where $x, x' \in M$, $(y_\alpha), (y'_\alpha) \in \bigoplus_\alpha N_\alpha$, and $r \in R$. Hence, we have a balanced product, so we get an induced map

$$\eta_M : M \otimes \left(\bigoplus_\alpha N_\alpha \right) \to \bigoplus_\alpha (M \otimes N_\alpha),$$

which on generators is defined by

$$\eta_M(x \otimes (y_\alpha)) = (x \otimes y_\alpha).$$

Now, we use the fact that we have a canonical morphism $i_\alpha : N_\alpha \to N$, and we use this to defined a homomorphism $1_m \otimes i_\alpha : M \otimes N_\alpha \to M \otimes (\bigoplus_\alpha N_\alpha)$. Using the universal property, we get a homomorphism $\zeta_M : \bigoplus_\alpha (M \otimes N_\alpha) \to M \otimes (\bigoplus_\alpha N_\alpha)$, which on generators is defined by

$$\zeta_M((x \otimes y_\alpha)) = x \otimes (y_\alpha),$$

and so we see on generators that η and ζ are inverses. Hence, we have that they are inverses in general, and so ζ_M is an isomorphism.

Using this, then, we have the following diagram is comutative:

$$\begin{array}{ccccc} 0 & \longrightarrow & M' \otimes_R (\bigoplus_\alpha N_\alpha) & \xrightarrow{f\otimes 1_N} & M \otimes_R (\bigoplus_\alpha N_\alpha) \\ & & \downarrow{\scriptstyle \eta_{M'}} & & \downarrow{\scriptstyle \eta_M} \\ 0 & \longrightarrow & \bigoplus_\alpha (M' \otimes_R N_\alpha) & \xrightarrow{f^*} & \bigoplus_\alpha (M \otimes_R N_\alpha) \end{array}$$

where f^* is defined so that

$$f^*((x \otimes y_\alpha)) = (f(x) \otimes y_\alpha).$$

To see commutativity, notice that for $x \otimes (y_\alpha) \in M' \otimes_R (\bigoplus_\alpha N_\alpha)$, we have

$$f^*(\eta_{M'}(x \otimes (y_\alpha)) = f^*((x \otimes y_\alpha)) = (f(x) \otimes y_\alpha),$$

and

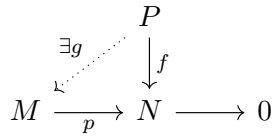
$$\eta_M(f \otimes 1_N(x \otimes (y_\alpha))) = \eta_M(f(x) \otimes (y_\alpha)) = (f(x) \otimes y_\alpha).$$

Thus, we have that $f \otimes 1_N$ is injective iff f^* is injective. It suffices to then show that f^* is injective iff $f \otimes 1_{N_\alpha}$ is injective for all α (the former being equivalent to N being a flat module, and the latter being equivalent to N_α being flat for all α). This follows by the construction of f^*: Assume there is some α for which $\mathrm{Ker}(f \otimes 1_{N_\alpha}) \neq 0$. Taking $x \in \mathrm{Ker}(f \otimes 1_{N_\alpha})$, we have that $0 \neq (0, \ldots, 0, x, 0, \ldots) \in \mathrm{Ker}(f^*)$ so that f^* is also not injective. Taking the contrapositive of this statement, we have that f^* injective implies that $f \otimes 1_{N_\alpha}$ is injective for all α. Now, assume that $\mathrm{Ker}(f \otimes 1_{N_\alpha}) = 0$ for all α. Then we have for $x = (x_\alpha) \in \bigoplus_\alpha (M' \otimes_R N_\alpha)$ that $f^*(x) = f^*((x_\alpha)) = 0$ implies $f \otimes 1_{N_\alpha}(x_\alpha) = 0$ for all α, so that $x_\alpha = 0$ for all α, and thus $x = 0$. That is, $\mathrm{Ker}(f^*) = 0$. $\square$

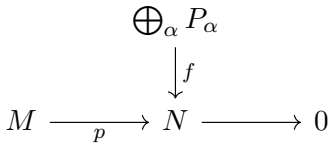
Remark. Thomas O'Hare was a collaborator.

Problem 20. Prove that the direct sum of projective modules is projective, i.e. if each P_α is projective with $\alpha \in I$, then so is $\bigoplus_{\alpha \in I} P_\alpha$.

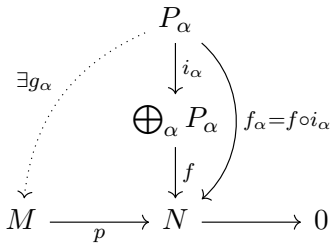
Proof. Recall that we say that a module P is *projective* if we have the following for all p epimorphisms:



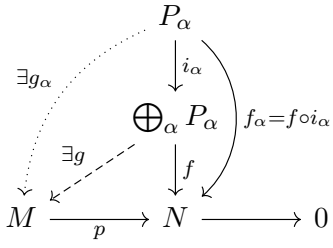
where $pg = f$. Assume then we have the following set up:



Notice that we have natural morphisms $i_\alpha : P_\alpha \to \bigoplus_\alpha P_\alpha$, so using the projective property of P_α we have the following diagram for each α:



where the g_α are such that $pg_\alpha = f_\alpha$ for each α. Thus, we can define $g : \bigoplus_\alpha P_\alpha \to M$ via $g((x_\alpha)) = \sum g_\alpha(x_\alpha)$, noting that this is fine to do since we have a direct sum. We now have the following diagram:



By construction, we see that we have $g_\alpha = g \circ i_\alpha$ for all α. It remains to show that this commutes; i.e., that we have $pg = f$. We have $gi_\alpha = g_\alpha$ for all α, and hence $fi_\alpha = f_\alpha = pg_\alpha = pgi_\alpha$ for all α. Taking $x = (x_\alpha) \in \bigoplus_\alpha P_\alpha$, we have

$$f(x) = f((x_\alpha)) = f\left(\sum_\alpha i_\alpha(x_\alpha)\right) = \sum_\alpha fi_\alpha(x_\alpha) = \sum_\alpha pgi_\alpha(x_\alpha) = pg\left(\sum_\alpha i_\alpha(x_\alpha)\right) = pg(x);$$

where we note that it's fine to use the homomorphic properties of f and pg since we are in a direct sum, and so we must have all but finitely many of the x_α are zero. Hence, the maps commute, as desired.

Alternatively, as David Green suggested, we can use a characterization of projective modules which is given by the fact that a module is projective if and only if it is a direct summand of a free module; that is, a module P is projective iff there is a free module F so that $F = P \oplus P'$ for some module P'. Hence, if each P_α is a projective module, we have that there is some free module F_α such that $F_\alpha = P_\alpha \oplus P'_\alpha$. The direct sum of free modules is a free module, and so we have

$$\bigoplus_\alpha F_\alpha = F = \bigoplus_\alpha (P_\alpha \oplus P'_\alpha) = \bigoplus_\alpha P_\alpha \oplus \bigoplus_\alpha P'_\alpha.$$

□

Problem 21. If $e \in R$ is idempotent (so $e^2 = e$) show that Re is a projective R-module.

Proof. The idea is to use the characterization that a module if projective iff it is a direct summand of a free module. The goal, then, is to get $R = Re \oplus R(1-e)$. Since R is a free module, this tells us that Re (and $R(1-e)$) are projective. Recall that we can write this as a direct sum if $Re \cap R(1-e) = 0$ and $Re + R(1-e) = R$.

(1) To see $Re \cap R(1-e) = 0$, let $x \in Re \cap R(1-e)$. Then we have that $x = r_1 e = r_2(1-e)$, $r_i \in R$ for $i = \{1, 2\}$. We can rewrite this as

$$r_1 e = r_2 - r_2 e \implies (r_1 + r_2)e = r_2,$$

and multiplying both sides on the right by e gives

$$(r_1 + r_2)e^2 = (r_1 + r_2)e = r_2 e \implies r_1 e = x = 0.$$

Hence, we have $x = 0$.

(2) It follows that $Re + R(1-e) \subset R$, since $Re \subset R$, $R(1-e) \subset R$, and $R + R \subset R$. So it suffices to show that $R \subset Re + R(1-e)$. Taking $r \in R$, we have $r = re + r(1-e) \in Re + R(1-e)$, so we have the desired result.

Hence, we have $Re \oplus R(1-e) = R$, and so Re is projective.

Alternatively, we can use a trick Daniel Packer came up with. Examine

$$R \xrightarrow{f} Re \to 0,$$

where $f(x) = xe$. This is well-defined, since if $x = x'$ then $xe = x'e$, it is surjective by design, and is a homomorphism since $f(x+y) = (x+y)e = xe + ye = f(x) + f(y)$, $f(rx) = rxe = rf(x)$ for all $x, y, r \in R$. Furthermore, we see that we have a map $g : Re \to R$ given by $g(x) = xe$. Notice that $g \circ f(x) = xe^2 = xe$, so we see that this splits. We then have

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow R \underset{f}{\overset{g}{\rightleftarrows}} Re \longrightarrow 0$$

so that $R \cong Re \oplus \mathrm{Ker}(f)$, and we reach the same conclusion as above. □

Problem 22. (Schanuel's Lemma) Suppose we have two short exact sequences:

$$0 \to N_1 \xrightarrow{g_1} P_1 \xrightarrow{f_1} M \to 0$$

and

$$0 \to N_2 \xrightarrow{g_2} P_2 \xrightarrow{f_2} M \to 0$$

with P_1, P_2 projective modules. Show that $P_1 \oplus N_2 \cong P_2 \oplus N_1$.

Proof. We follow the general idea outlined in Rotman's, "Introduction to Homological Algebra." Notice that we have

$$\begin{array}{ccccc} & & P_1 & & \\ & & \downarrow & & \\ P_2 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

so by definition of P_1 being projective, we get an induced map

$$\begin{array}{ccccc} & & P_1 & & \\ & \overset{h}{\swarrow} & \downarrow & & \\ P_2 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

In other words, we have the following diagram:

$$\begin{array}{ccccccccc} & & & & 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & P_1 \\ & & & & & & & \overset{h}{\swarrow} & \downarrow f_1 \\ 0 & \longrightarrow & N_2 & \xrightarrow{g_2} & P_2 & \xrightarrow{f_2} & M & \longrightarrow & 0 \end{array}$$

The goal is to show that $P_1 \oplus N_2 \cong N_1 \oplus P_2$. We use h to define a map $\psi : P_1 \oplus N_2 \to P_2$ with $\psi(x, y) = h(x) - g_2(y)$. Note this is well-defined, since if $x = x'$, $y = y'$, then $h(x) = h(x')$, $g_2(y) = g_2(y')$, so $h(x) - g_2(y) = h(x') - g_2(y')$, and hence $\psi(x, y) = h(x) - g_2(y) = h(x') - g_2(y') = \psi(x', y')$. Moreover, we see that it is a homomorphism, since

$$\begin{aligned} \psi((x, y) + (x', y')) = \psi(x + x', y + y') = h(x + x') - g(y + y') = h(x) - g(y) + h(x') - g(y') \\ = \psi(x, y) + \psi(x', y'), \end{aligned}$$

and

$$\psi(r(x, y)) = \psi(rx, ry) = h(rx) - g(ry) = r[h(x) - g(y)] = r\psi(x, y),$$

where $x, x' \in P_1$, $y, y' \in N_2$ and $r \in R$.

We now check that this map is surjective. Take $z \in P_2$. If $z \in \mathrm{Im}(h)$, we are done since we have $r \in P_1$ with $h(r) = z$, and so $\psi(r, 0) = h(r) - g_2(0) = h(r) = z$. Thus, assume $z \notin \mathrm{Im}(h)$. We have that h is such that $f_2 h = f_1$. Furthermore, we see that $f_2(z) \in M$ is such that there is a $k \in P_1$ with $f_1(k) = f_2(z)$ by the surjectivity of f_1. Hence, taking this k, we have $f_2(h(k) - z) = f_2(h(k)) - f_2(z) = f_1(k) - f_2(z) = 0$, and so $z - h(k)$ is in the kernel of f_2. Since $\mathrm{Ker}(f_2) = \mathrm{Im}(g_2)$, we have that there is some $y \in N_2$ with $g_2(y) = h(k) - z$; that is, we have $z = h(k) - g_2(y) = \psi(k, y)$. Thus, we have that ψ is surjective.

Before moving on, we note that the map h gives an additional map $\kappa : N_1 \to N_2$. Since we have $f_2 h = f_1$, we get that if $x \in P_1$ is such that $f_1(x) = 0$ (that is, $x = g_1(t)$ for some $t \in N_1$), then $f_2(h(x)) = 0$; that is, $h(x) \in \mathrm{Ker}(f_2) = \mathrm{Im}(g_2)$. Hence, we have some $z \in N_2$ where $g_2(z) = h(x)$. Using this, we can define $\kappa : N_1 \to N_2$ by $\kappa(x) = y \in N_2$, where $h g_1(x) = g_2(y)$. We check that this map is well-defined; if $x = x'$ in N_1, then we have $g_2(y) = h g_1(x) = h g_1(x') = g_2(y')$, and since g_2 is injective this implies that $y = y'$. So $\kappa(x) = \kappa(x')$. To see that this is a homomorphism, we have $h g_1(x) = g_2(y)$, $h g_1(x') = g_2(y')$, so $h g_1(x + x') = h g_1(x) + h g_1(x') = g_2(y) + g_2(y') = g_2(y + y')$, and hence $\kappa(x + x') = y + y' = \kappa(x) + \kappa(x')$. If $r \in R$, then $h g_1(rx) = r h g_1(x) = r g_2(y) = g_2(ry)$, so that $\kappa(rx) = ry = r\kappa(x)$.

Using this last fact, we now have the following commutative diagram:

$$\begin{array}{ccccccccc} & & 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & P_1 & & \\ & & & \overset{\kappa}{\swarrow} & & \overset{h}{\swarrow} & \downarrow{\scriptstyle f_1} & & \\ 0 & \longrightarrow & N_2 & \xrightarrow{g_2} & P_2 & \xrightarrow{f_2} & M & \longrightarrow & 0 \end{array}$$

Notice that κ is constructed so that the square in the middle commutes; i.e., we have that

$$\begin{array}{ccc} N_1 & \xrightarrow{g_1} & P_1 \\ \kappa\downarrow & & \downarrow h \\ N_2 & \xrightarrow{g_2} & P_2 \end{array}$$

commutes.

We now examine the kernel of ψ. We have

$$\mathrm{Ker}(\psi) = \{(x,y) : \psi(x,y) = h(x) - g_2(y) = 0\} = \{(x,y) : h(x) = g_2(y)\}.$$

Now using the fact that $\mathrm{Im}(g_2) = \mathrm{Ker}(f_2)$ and $f_2 h = f_1$, we get that $h(x) = g_2(y) \implies f_2(h(x)) = f_2(g_2(y)) = 0 \implies h(x) \in \mathrm{Ker}(f_2)$, and furthermore $f_2(h(x)) = f_1(x) = 0$, so we get that $x \in \mathrm{Ker}(f_1) = \mathrm{Im}(g_1)$.

Next, we wish to construct a map $\varphi : N_1 \to P_1 \oplus N_2$ which is an injection, and is such that $\mathrm{Im}(\varphi) = \mathrm{Ker}(\psi)$. We follow the illustration from the last paragraph to define $\varphi(x) = (g_1(x), \kappa(x))$. To see that this is an injection, we note that $x \in \mathrm{Ker}(\varphi)$ implies that $x \in \mathrm{Ker}(g_1) \cap \mathrm{Ker}(\kappa) = 0$, since g_1 injective, so we have that $\mathrm{Ker}(\varphi) = 0$.

Now we wish to show that $\mathrm{Im}(\varphi) = \mathrm{Ker}(\psi)$. First, we show that $\mathrm{Im}(\varphi) \subset \mathrm{Ker}(\psi)$. If $(y,z) \in \mathrm{Im}(\varphi)$, we have that there is some x so that $\varphi(x) = (g_1(x), \kappa(x)) = (y,z)$, and we get that $\psi((g_1(x), \kappa(x)) = h(g_1(x)) - g_2(\kappa(x))$. By the commutativity of the above square, we see that $h(g_1(x)) = g_2(\kappa(x))$, so $\psi(\varphi(x)) = 0$ for all x. That is, $\mathrm{Im}(\varphi) \subset \mathrm{Ker}(\psi)$.

Finally, we wish to show that $\mathrm{Ker}(\psi) \subset \mathrm{Im}(\varphi)$. Let $x = (y,z) \in \mathrm{Ker}(\psi)$; that is, (y,z) is such that $\psi((y,z)) = h(y) - g_2(z) = 0$, with $y \in P_1$ and $z \in N_2$. Notice that this implies $h(y) = g_2(z)$. Since $y \in P_1$, we get that $f_1(y) = f_2(h(y)) = f_2(g_2(z)) = 0$, so that $y \in \mathrm{Ker}(f_1) = \mathrm{Im}(g_1)$. Hence, we have there is some $r \in N_1$ so that $g_1(r) = y$. Now, using the commutativity of the above square, we see that $h(g_1(r)) = g_2(\kappa(r)) = g_2(z)$. Since g_2 is injective, we get that $\kappa(r) = z$. So we see that $x = (g_1(r), \kappa(r)) = \varphi(r)$, and thus $x \in \mathrm{Im}(\varphi)$. That is, we have $\mathrm{Ker}(\psi) \subset \mathrm{Im}(\varphi)$.

Combining all of the above gives us that

$$0 \longrightarrow N_1 \xrightarrow{\varphi} P_1 \oplus N_2 \xrightarrow{\psi} P_2 \longrightarrow 0$$

is a short exact sequence. Since P_2 is projective, we get that this splits; i.e., we have

$$0 \longrightarrow N_1 \xrightarrow{\varphi} P_1 \oplus N_2 \underset{\psi}{\overset{}{\rightleftarrows}} P_2 \longrightarrow 0$$

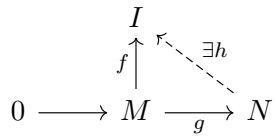
which gives

$$P_1 \oplus N_2 \cong N_1 \oplus P_2,$$

as desired. □

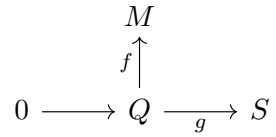
Problem 23. Show that the direct summand of injective modules is injective, i.e., if I is an injective R-module and $I = M \oplus N$, then M is injective (Remark: the same is true for N).

Proof. Recall that a module I is *injective* if we have

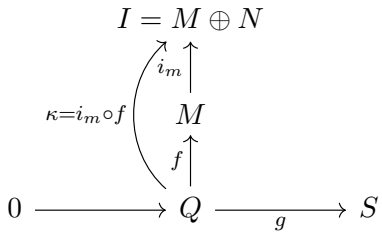


such that $hg = f$.

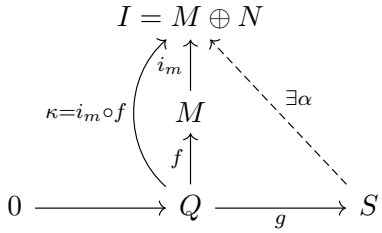
Assume then that we have the following set up:



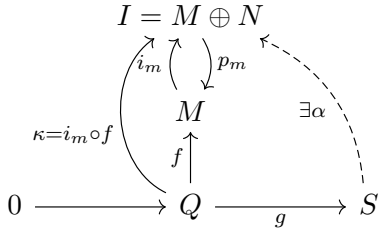
Since $I = M \oplus N$, we get that there is a map $i_M : M \to M \oplus N = I$. Hence, we can write



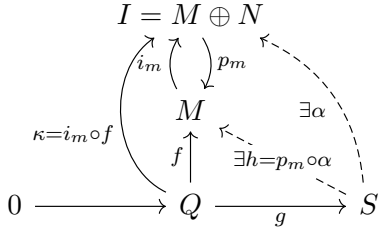
Now, since I is injective, we get that there is a map $\alpha : S \to I$ so that $\alpha g = \kappa$; i.e., we have the following



Furthermore, we can define a homomorphism $p_M : M \oplus N \to M$ which is the projection map, since this is a finite direct sum. That is, we have $p_M : M \oplus N \to M$ is such that $p_m \circ i_m = \mathrm{id}_M$. Hence, we have



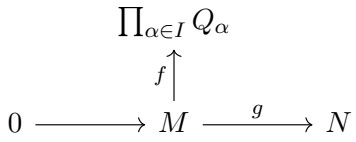
We define then $h = p_m \circ \alpha$, and this gives us a map



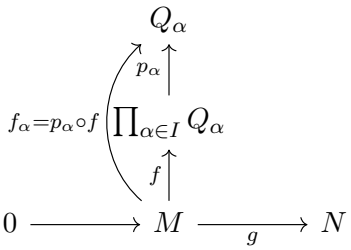
We check that this commutes; that is, we check that $hg = f$. Writing things out, this is the same as checking $p_m \alpha g = f$. From prior, we have that $\alpha g = \kappa = i_m f$, and so substituting this in we get $hg = p_m \alpha g = p_m i_m f = f$. That is, we have $hg = f$ as desired. Hence, M is injective. □

Problem 24. Prove that the direct product of injective modules is again injecive, i.e., if each Q_α with $\alpha \in I$ is injective, then so is $\prod_{\alpha \in I} Q_\alpha$.

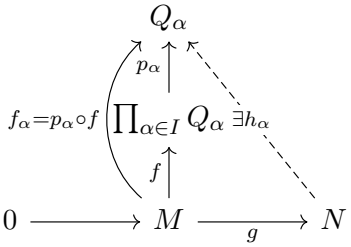
Proof. We follow a similar argument to what we did in the first proof of **Problem 1**. Using properties of direct products, we get that we have maps $p_\alpha : \prod_{\alpha \in I} Q_\alpha \to Q_\alpha$ for each α. Now, assume we have the following set up:



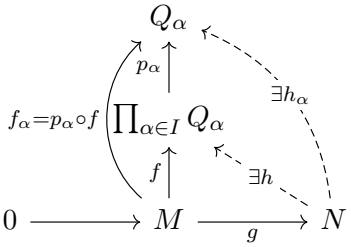
Using the p_α, we can append the Q_α to get



Since each of the Q_α are injective, we get that there is a map $h_\alpha : N \to Q_\alpha$:



The diagrams here commute; that is, we have $f_\alpha = h_\alpha g$, or $p_\alpha f = h_\alpha g$. Hence, define $h : N \to \prod_{\alpha \in I} Q_\alpha$ via $x \mapsto (h_\alpha(x))_{\alpha \in I} = (h_\alpha(x))$. This gives us the following diagram:



We check now that this actually commutes; that is, we check that $hg = f$. Taking $x \in M$, we have

$$h(g(x)) = (h_\alpha(g(x))) = (f_\alpha(x)) = (p_\alpha(f(x))) = f(x),$$

where we note that $f(x) = (p_\alpha(f(x)))$ by construction of the direct product. Thus, we have that $\prod_{\alpha \in I} Q_\alpha$ is injective, as desired. □

Remark. Thomas O'Hare was a collaborator.

Problem 25 (Baer's Criterion)**.** Prove that an R-module Q is injective iff any homomorphism of a left ideal $\mathfrak{a}$ of R into Q can be extended to a homomorphism of R into Q.

Proof. ($\implies$) : Assume that Q is injective. Assume as well that we have a homomorphism of a left ideal $\mathfrak{a}$ of R into Q, i.e. we have $f : \mathfrak{a} \to Q$. Notice that we can embed any left ideal $\mathfrak{a}$ into R via $i(x) = x$. This then gives us the following diagram:

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{i} & R \end{array}$$

Since Q is injective, this implies that we have a map $\overline{f}$ so that the diagram commutes, i.e. we have

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle \exists \overline{f}} & \\ 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{i} & R \end{array}$$

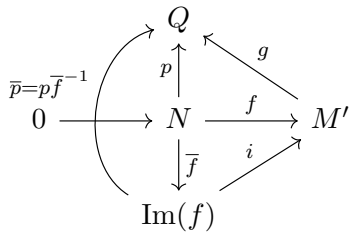
The commutativity tells us that this $\overline{f}$ extends the map from $\mathfrak{a}$ into Q; that is, $\overline{f}i = \overline{f}|_{\mathfrak{a}} = f$.
($\impliedby$): This is the more interesting direction. Assume now that we can extend any homomorphism from a left ideal to all of R. We wish to show that if we have the following diagram, we can find a $g : M \to Q$ so that this commutes:

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle p} & & \\ 0 & \longrightarrow & N & \xrightarrow{f} & M \end{array}$$

We now follow the idea put forth by Dr. Ranthony Edmonds and Kyle Binder. Note first that since f is an injection, it suffices to view N as a submodule of M. Suppose that we can prove the result for submodules of M. Then we have that $N \cong \mathrm{Im}(f)$ and denote this isomorphism by $\overline{f}$. We have the following set up, then:

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle p} & & \\ 0 & \longrightarrow & N & \xrightarrow{f} & M' \\ & & \downarrow{\scriptstyle \overline{f}} & \nearrow{\scriptstyle i} & \\ & & \mathrm{Im}(f) & & \end{array}$$

Note that $i\overline{f} = f$. Furthermore, we get a homomorphism $\overline{p} = p\overline{f}^{-1} : \mathrm{Im}(f) \to Q$. Thus, since we've assumed the result for submodules and $\mathrm{Im}(f)$ is a submodule of M, we can extend $\overline{p}$ to some homomorphism $g : M' \to Q$; i.e., we have

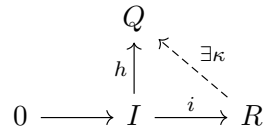


We then note that $gf = p$. We see that $gi = \overline{p} = p\overline{f}^{-1}$, so applying $\overline{f}$ to the right of both sides gives $gi\overline{f} = gf = p$. Hence, we've extended f to $g : M' \to Q$ still, and so the result holds. Thus, proving it for submodules is sufficient, and so we just consider N as a submodule of M, with f being the natural injection.

Consider the set $\{(L, f) \ : \ N \subset L \subset M, f : L \to Q\}$ with partial ordering given by $(L, f) \leq (L', f')$ iff $L \subset L'$ and $f'|_L = f$. The goal is to show that every chain has a supremum, use Zorn's lemma to find a maximal module, and then conclude that this module must be M. Let $\{(L_i, f_i)\}$ be a chain in this poset. Consider $K = \bigcup_i L_i$, equipped with a map $g : K \to Q$ defined by $g(x) = f_i(x)$, where $x \in L_i$ for some i. We note that g is well-defined, since if $x = x'$, then $x, x' \in L_i$ for some i, and so $g(x) = f_i(x) = f_i(x') = g(x')$. It is a module homomorphism, since for $x, y \in K$, we have that there is some i for which both $x, y \in L_i$, and so $g(x+y) = f_i(x+y) = f_i(x)+f_i(y) = g(x)+g(y)$, and for $r \in R$, $x \in K$, we get $g(rx) = f_i(rx) = rf_i(x) = rg(x)$. Since K is a union of increasing modules, we get that it is also a module, and so (K, g) is the supremum of this chain. Hence, we can apply Zorn's lemma to find a maximal (M', g) where $g : M' \to Q$.

Now, we claim that $M' = M$. Assume for contradiction $M' \neq M$. Since $M' \subset M$, we have that there is some non-trivial $x \in M/M'$. Consider now $I = \{r \in R : rx \in M'\}$. We note that I is an ideal. First, we must check that it is a subgroup under addition. We see $0 \in I$, since $0x = 0 \in M'$, and we see that if $r, s \in I$, then $r - s \in M'$, since $(r - s)x = rx - sx \in M'$. If $k \in R$ arbitrary, $r \in I$, we see that $kr \in I$, since $krx = k(rx) \in M'$. So I is a (left) ideal.

Now, we define a homomorphism $h : I \to Q$ via $h(r) = p(rx)$. This is a module homomorphism, since $h(r + s) = p((r + s)x) = p(rx + sx) = p(rx) + p(sx) = h(r) + h(s)$ for all $x, y \in I$, and for all $k \in R$ we have $h(kr) = p(krx) = kp(rx) = kh(r)$, where we utilized that p was a module homomorphism. Notice then that the assumption gives us a κ such that



commutes. Our goal from here is to define a map $g' : M'' = M' + \langle x \rangle \to Q$, where $g'|_{M'} = g$. A good guess would be $g'(y + rx) = g(y) + \kappa(r)$. We must first show that this is well-defined. If $y + rx = y' + r'x$, then we see that $y - y' = (r' - r)x$. Since $y - y' \in M'$, we have that $r' - r \in I$. Furthermore, we have

$$g(y) - g(y') = g(y - y') = g((r' - r)x) = h(r' - r) = \kappa(r' - r) = \kappa(r') - \kappa(r).$$

Hence, we see that

$$g'(y + rx) - g'(y' + r'x) = g(y) + \kappa(r) - g(y') - \kappa(r') = (g(y) - g(y')) - (\kappa(r') - \kappa(r)) = 0,$$

so that

$$g'(y + rx) = g'(y' + r'x).$$

Thus, it is well-defined. We see it is a homomorphism, since for $y + rx, z + sx \in M''$, we have

$$g'((y + rx) + (z + sx)) = g'((y + z) + (r + s)x) = g(y + z) + \kappa(r + s) = g(y) + g(z) + \kappa(r) + \kappa(s)$$
$$= [g(y) + \kappa(r)] + [g(z) + \kappa(s)] = g'(y + rx) + g'(z + sx),$$

and for all $k \in R$ we have

$$g'(k(y + rx)) = g'(ky + (kr)x) = g(ky) + \kappa(kr) = k[g(y) + \kappa(r)] = kg'(y + rx),$$

where we use that g and κ are homomorphisms. Therefore, we have extended (M', g) to $(M'+\langle x\rangle, g')$ so that $g'|_{M'} = g$. This contradicts the fact that (M', g) is maximal, and so we have that there could be no such x, implying that $M' = M$. Hence, we have

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle p} & \nwarrow{\scriptstyle g} & \\ 0 & \longrightarrow & N & \xrightarrow{f} & M \end{array}$$

Since we can do this for all such diagrams, we get that Q is injective, as desired. □

Recall that if D is an integral domain, then a D-module T is *divisible* iff for all $a \in D$, $a \neq 0$, the map $a_T : T \to T$ given by $a_T(x) = ax$ is surjective.

Problem 26. Show that any injective module over an integral domain is divisible. If, in addition, D is a PID, show that any divisible module is injective. [In particular, as an abelian group T is divisible iff it is injective as a $\mathbb{Z}$-module.]

Proof. We follow Rotman for the first step (**Lemma 3.33**). We first assume that Q is an injective module over an integral domain, say R. We wish to show that for all $a \in R$ with $a \neq 0$, the map $a_Q : Q \to Q$ given by $a_Q(x) = ax$ is surjective. Let $y \in Q$, then we wish to show that there exists some $z \in Q$ with $az = y$. Consider the left ideal $\mathfrak{a} = Ra$. We have $f : \mathfrak{a} \to Q$ given by $f(ra) = ry$ is a homomorphism. First, we note it is well-defined, since $ra = r'a$ implies $(r - r')a = 0$, and since $a \neq 0$ this implies that $r = r'$. Hence, we have $f(ra) = ry = r'y = f(r'a)$. Now, it's a homomorphism, since for all $ra, sa \in \mathfrak{a}$, we have

$$f(ra + sa) = f((r + s)a) = (r + s)y = ry + sy = f(ra) + f(sa),$$

and for all $t \in R$ we have

$$f(tra) = try = t(ry) = tf(ra).$$

Thus, by the prior problem (i.e. Baer's criterion) we can extend f to a map $\varphi : R \to Q$. That is, we have the following set up:

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle \varphi} & \\ 0 & \longrightarrow & \mathfrak{a} & \xrightarrow[i]{} & R \end{array}$$

Now, the diagram commutes. Furthermore, we see $f(a) = y$, and so we have

$$y = f(a) = \varphi(i(a)) = \varphi(a) = a\varphi(1) = az,$$

where $z = \varphi(1)$ and we use that φ is a module homomorphism. Thus, since the choice of y was arbitrary in the beginning, we have that a_Q is surjective.

Assume now that R is a PID. We wish to show that if Q is a divisible module, it is injective. Let $\mathfrak{a}$ be an arbitrary left ideal, and assume we have a homomorphism $f : \mathfrak{a} \to Q$; i.e. we have the following set up:

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & \mathfrak{a} & \xrightarrow[i]{} & R \end{array}$$

By the equivalence established in Baer's Criterion, it suffices to show that f extends to R. Since R is a PID, we get that $\mathfrak{a} = (s)$, where $s \in R$. We then rewrite this as

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & (s) & \xrightarrow[i]{} & R \end{array}$$

Now, Q is divisible, so we have that for all $r \in R$, $r_Q : Q \to Q$ is surjective. In other words, $s_Q : Q \to Q$ is surjective, where $s(x) = sx$. Thus, we have $f(s) = sz$ for some $z \in Q$ since Q is divisible, and since this is an R-module homomorphism we get $f(rs) = rf(s) = rsz$. Define $\overline{f} : R \to Q$ where $\overline{f}(r) = rz$. We see that this extends f, since we have $\overline{f}(i(rs)) = \overline{f}(rs) = rsz = f(rs)$ for all $rs \in (s)$. So $\overline{f}|_{(s)} = f$. That is, we have the following commutative diagram:

$$\begin{array}{ccccc} & & Q & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle \overline{f}} & \\ 0 & \longrightarrow & (s) & \xrightarrow[i]{} & R \end{array}$$

Since we did this for arbitrary homomorphisms f and arbitrary left ideals $\mathfrak{a}$, we get that Q must be injective by Baer's criterion.

To conclude, any abelian group T can be viewed as a $\mathbb{Z}$-module. Recall that a group T is said to be *divisible* for all positive integers n and every $g \in T$, there is a $y \in T$ so that $ny = g$. In other words, for all positive integers n, the map $n_T : T \to T$ given by $n_T(x) = nx$ is surjective. Notice that a group is divisible iff it is divisible as a $\mathbb{Z}$-module. If it is divisible as a $\mathbb{Z}$-module, it follows that for all positive integers we have that n_T is surjective. If it is a divisible group, consider $-n < 0$. We wish to show that $-n_T : T \to T$ where $-n_T(x) = -nx$ is surjective as well. Fix $y \in T$ and consider $-y$, the inverse of y. We see there is some x so that $nx = -y$, so we have $-nx = (-1)(nx) = (-1)(-y) = y$. We can do this for all $y \in T$, so the map is surjective, and hence we have that T is a divisible $\mathbb{Z}$-module as well.

If T is a divisible group, this tells us that it is a divisible $\mathbb{Z}$-module, and so since $\mathbb{Z}$ is a PID the second part implies that it is an injective $\mathbb{Z}$-module. If T is injective as a $\mathbb{Z}$-module, then since $\mathbb{Z}$ is an integral domain the first part implies that it is divisible as a $\mathbb{Z}$-module, which is equivalent to being a divisible group. So an abelian group T is divisible iff it is injective as a $\mathbb{Z}$-module. □

Problem 27. Given the Snake Diagram as in class:

$$\begin{array}{ccccccccc} & & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{h} & N & \xrightarrow{k} & N'' & & \end{array}$$

(a) Show that if d' and d'' are injective, then so is d.
(b) Show that if d' and d'' are surjective, then so is d.
(c) Show that if the rows are actually short exact sequences, so that in addition f is injective and k is surjective, then if any two of d', d and d'' are isomorphisms, then so is the third.

Proof. There are two ways of doing this; one is by diagram chasing, and the other is via the snake lemma (as Kyle pointed out). I'll first do the diagram chasing, and then follow it up with a gist of how you can deduce these from the snake lemma.

(1) If d' and d'' are injective, then we have the following commutative diagram:

$$\begin{array}{ccccccccc} & & 0 & & & & 0 & & \\ & & \downarrow & & & & \downarrow & & \\ & & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{h} & N & \xrightarrow{k} & N'' & & \end{array}$$

Let $x \in M$ so that $d(x) = 0$. We wish to show that $x = 0$; i.e., $\mathrm{Ker}(d) = 0$. Since $d(x) = 0$, we have that $k(d(x)) = 0 = d''(g(x))$, and since d'' is injective this implies $g(x) = 0$. So $x \in \mathrm{Ker}(g)$. We have that $\mathrm{Ker}(g) = \mathrm{Im}(f)$, so there is some $z \in M'$ where $f(z) = x$. Now, $d(f(z)) = d(x) = 0 = h(d'(z))$, and since h is injective we get $d'(z) = 0$. Since d' is injective, we have that $z = 0$. Since f is a homomorphism, this implies that $f(z) = x = f(0) = 0$. Hence, $\mathrm{Ker}(d) = 0$, so that d is injective.

(2) If d' and d'' are surjective, we have the following:

$$\begin{array}{ccccccccc} & & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{h} & N & \xrightarrow{k} & N'' & & \\ & & \downarrow & & & & \downarrow & & \\ & & 0 & & & & 0 & & \end{array}$$

We wish to show that d is surjective, so take $y \in N$. We wish to find $x \in M$ so that $d(x) = y$. Taking $k(y) \in N''$, we see that we must have some $z \in M''$ so that $d''(z) = k(y)$. Since g is surjective, we get that there is some $r \in M$ with $g(r) = z$, and since the diagram commutes we have $d''(g(r)) = k(d(r)) = k(y)$. So $k(d(r) - y) = 0$, and hence $d(r) - y \in \mathrm{Ker}(k)$. We have $\mathrm{Ker}(k) = \mathrm{Im}(h)$, and so there is some $e \in N'$ where $h(e) = d(r) - y$. Since d' is surjective, we get some $q \in M'$ with $d'(q) = e$, or $h(d'(q)) = d(r) - y = d(f(q))$ by commutativity. So $d(r) - d(f(q)) = y$, or $d(r - f(q)) = y$. Setting $x = r - f(q) \in M$, we have that $d(x) = y$. Since the choice of y was arbitrary, we get that d is surjective.

(3) (1) and (2) establish that if the outside morphisms (d' and d'') are isomorphisms, then we get that d must be an isomorphism as well. We first consider the case of d and d' being isomorphisms. We have the following setup:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{h} & N & \xrightarrow{k} & N'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array}$$

Let $x \in M''$ be such that $d''(x) = 0$. Since g is surjective, there is some $q \in M$ so that $g(q) = x$. Furthermore, this gives $d''(g(q)) = k(d(q)) = 0$. So $d(q) \in \mathrm{Ker}(k)$. Since $\mathrm{Ker}(k) = \mathrm{Im}(h)$, we have that there is some $z \in N'$ with $h(z) = d(q)$. Since d' is an isomorphism, we

get that there is some $r \in M'$ with $d'(r) = z$, so that $h(d'(r)) = d(f(r)) = d(q)$, so applying d^{-1} we have that $f(r) = q$, and hence $q \in \text{Im}(f) = \text{Ker}(g)$. Thus, $g(q) = 0 = x$. Since $x \in \text{Ker}(d'')$ was arbitrary, this gives $\text{Ker}(d'') = 0$.

Now, we wish to show that d'' is surjective. Let $y \in N''$. Since k is surjective, we have that there is some $r \in N$ with $k(r) = y$. Since d is an isomorphism, there is some $s \in M$ with $d(s) = r$, so $k(d(s)) = d''(g(s)) = y$. Since we can do this for all y, we have that d'' is surjective. Hence, d'' is an isomorphism, as desired.

Now, consider the case of d and d'' being isomorphisms. We have the following setup:

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{h} & N & \xrightarrow{k} & N'' & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array}$$

We want to first establish that d' is injective. Let $x \in M'$ so that $d'(x) = 0$. Notice that $d(f(x)) = h(d'(x)) = 0$, and since d is an isomorphism, we get $f(x) = 0$. Since f is injective, we get $x = 0$, which implies $\text{Ker}(d') = 0$, i.e. d' is injective.

Now, let $y \in N'$. We wish to show that that there is an $x \in M'$ with $d'(x) = y$. We have $h(y) \in N$, and since d is an isomorphism there is an $r \in M$ with $d(r) = h(y)$. Applying g, we see that $d''(g(r)) = k(d(r))$, and since $d(r) = h(y)$, we see that $d''(g(r)) = k(h(y)) = 0$. Since d'' is an isomorphism, this implies that $g(r) = 0$, and hence $r \in \text{Ker}(g) = \text{Im}(f)$. Finally, $r \in \text{Im}(f)$ implies there is an $x \in M'$ with $f(x) = r$, so we get that $h(d'(x)) = d(f(x)) = d(r) = h(y)$, and since h is injective this implies that $d'(x) = y$. So d' is surjective.

Recall that the snake lemma says that if we have the following commutative diagram

$$\begin{array}{ccccccccc} & & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{h} & N & \xrightarrow{k} & N'' & & \end{array}$$

then we get a map $\delta : \text{Ker}(d'') \to \text{Coker}(d')$ so that

$$\text{Ker}(d') \xrightarrow{\overline{f}} \text{Ker}(d) \xrightarrow{\overline{g}} \text{Ker}(d'') \xrightarrow{\delta} \text{Coker}(d') \xrightarrow{h_*} \text{Coker}(d) \xrightarrow{k_*} \text{Coker}(d'')$$

is exact.

(1) We see that by assumption we have the desired set up, except $\text{Ker}(d') = \text{Ker}(d'') = 0$. Our diagram then looks like

$$0 \xrightarrow{\overline{f}} \text{Ker}(d) \xrightarrow{\overline{g}} 0 \xrightarrow{\delta} \text{Coker}(d') \xrightarrow{h_*} \text{Coker}(d) \xrightarrow{k_*} \text{Coker}(d'')$$

Since this sequence is exact, this implies that $\text{Ker}(\overline{g}) = \text{Im}(\overline{f})$. Since $\overline{g}$ maps to 0, we have $\text{Ker}(\overline{g}) = \text{Ker}(d)$, but $\text{Im}(\overline{f}) = 0$, so we get $\text{Ker}(d) = 0$, implying that d is injective.

(2) We have d' and d'' are surjective, so $\text{Coker}(d') = \text{Coker}(d'') = 0$. Hence, our set up is

$$\text{Ker}(d') \xrightarrow{\overline{f}} \text{Ker}(d) \xrightarrow{\overline{g}} \text{Ker}(d'') \xrightarrow{\delta} 0 \xrightarrow{h_*} \text{Coker}(d) \xrightarrow{k_*} 0$$

The exactness of this sequence implies again that $\text{Coker}(d) = 0$, as before.

(3) Again, (1) and (2) tell us that if d' and d'' are isomorphisms, then d must be an isomorphism. Now consider if d and d' are isomorphisms. This implies that $\text{Ker}(d') = \text{Coker}(d') = \text{Ker}(d) = \text{Coker}(d) = 0$. Furthermore, k is surjective, so we see that this descends to a surjective function k_* on the cokernels. To see this, notice that $k_* : \text{Coker}(d) \to \text{Coker}(d'')$ is given by $k_*(x + \text{Im}(d)) = k(x) + \text{Im}(d'')$. Since k is surjective, for all $y \in N''$ there is a $x \in N$ so that $k(x) = y$. Hence, we see that $k_*(x + \text{Im}(d)) = k(x) + \text{Im}(d'') = y + \text{Im}(d'')$, and since all elements in $\text{Coker}(d'')$ are of the form $y + \text{Im}(d'')$ for $y \in N''$, we have that the map is surjective. Thus, our set up is as follows:

$$\text{Ker}(d') \xrightarrow{\overline{f}} \text{Ker}(d) \xrightarrow{\overline{g}} \text{Ker}(d'') \xrightarrow{\delta} \text{Coker}(d') \xrightarrow{h_*} \text{Coker}(d) \xrightarrow{k_*} \text{Coker}(d'') \longrightarrow 0$$

and substituting in the values which are 0, we have

$$0 \xrightarrow{\overline{f}} 0 \xrightarrow{\overline{g}} \text{Ker}(d'') \xrightarrow{\delta} 0 \xrightarrow{h_*} 0 \xrightarrow{k_*} \text{Coker}(d'') \longrightarrow 0$$

By similar reasoning to before, this forces $\text{Ker}(d'') = \text{Coker}(d'') = 0$, so that d'' is an isomorphism.

Now, notice that if f is injective, then $\overline{f}$ is also injective. This follows since $\overline{f}$ is just a restriction of f to $\text{Ker}(d') \subset M'$, so $\text{Ker}(\overline{f}) \subset \text{Ker}(f) = 0 \implies \text{Ker}(\overline{f}) = 0$. Using this, our set up is now

$$0 \longrightarrow \text{Ker}(d') \xrightarrow{\overline{f}} \text{Ker}(d) \xrightarrow{\overline{g}} \text{Ker}(d'') \xrightarrow{\delta} \text{Coker}(d') \xrightarrow{h_*} \text{Coker}(d) \xrightarrow{k_*} \text{Coker}(d'')$$

Assuming d and $''$ are isomorphisms, we have $\text{Ker}(d) = \text{Coker}(d) = \text{Ker}(d'') = \text{Coker}(d'') = 0$. Substituting these in, we have

$$0 \longrightarrow \text{Ker}(d') \xrightarrow{\overline{f}} 0 \xrightarrow{\overline{g}} 0 \xrightarrow{\delta} \text{Coker}(d') \xrightarrow{h_*} 0 \xrightarrow{k_*} 0$$

By similar reasoning to before, this gives us that $\text{Ker}(d') = \text{Coker}(d') = 0$, forcing d' to be an isomorphism as well.

□

Remark. Thomas O'Hare was a collaborator.

Problem 28 (Five Lemma)**.** Prove the **Five Lemma**: Suppose we have a commutative diagram of R-modules so that each row is exact:

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \downarrow{\scriptstyle d_4} & & \downarrow{\scriptstyle d_5} \\ N_1 & \xrightarrow[g_1]{} & N_2 & \xrightarrow[g_2]{} & N_3 & \xrightarrow[g_3]{} & N_4 & \xrightarrow[g_4]{} & N_5 \end{array}$$

Show that

(a) If d_1 is surjective and d_2, d_4 are injective, then d_3 is injective.
(b) If d_5 is injective and d_2, d_4 are surjective, then d_3 surjective.

Proof. We prove this by diagram chasing.

(a) We wish to show that d_3 is injective, so take $x \in \text{Ker}(d_3)$. We see that $g_3(d_3(x)) = d_4(f_3(x)) = 0$, so that $f_3(x) \in \text{Ker}(d_4)$. Since d_4 is injective, this implies that $f_3(x) = 0$; that is, $x \in \text{Ker}(f_3)$. We have that $\text{Ker}(f_3) = \text{Im}(f_2)$ by exactness, so this implies that there is some $y \in M_2$ so that $f_2(y) = x$. We again go around the square: $d_3(f_2(y)) = g_2(d_2(y)) = d_3(x) = 0$. Hence, $g_2(d_2(y)) = 0$, so we have $d_2(y) \in \text{Ker}(g_2) = \text{Im}(g_1)$. That is, there is some $z \in N_1$ so $g_1(z) = d_2(y)$. Since d_1 is surjective, we have some $h \in M_1$ so that $d_1(h) = z$. Hence, $g_1(d_1(h)) = g_1(z) = d_2(f_1(h)) = d_2(y)$. Since d_2 is injective, we get that $f_1(h) = y$. Finally, putting things together, we have $f_2(y) = f_2(f_1(h)) = x$, and by exactness we get that $f_2(f_1(h)) = 0$. Thus, $\text{Ker}(d_3) = 0$.

(b) We again go around the square. We wish to show that d_3 is surjective, so in other words we wish to show that for $y \in N_3$, there exists $x \in M_3$ so that $d_3(x) = y$. Applying g_3 to y, we have $g_3(y) \in N_4$. Since d_4 is surjective, there is some $z \in M_4$ with $d_4(z) = g_3(y)$. By commutativity, we see that $g_4(d_4(z)) = d_5(f_4(z)) = g_4(g_3(y)) = 0$. Hence, $f_4(z) \in \text{Ker}(d_5)$, and since d_5 is injective, this implies that $z \in \text{Ker}(f_4) = \text{Im}(f_3)$. So there is some $h \in M_3$ with $f_3(h) = z$. Going around, we have $g_3(d_3(h)) = d_4(f_3(h)) = d_4(z) = g_3(y)$. So subtracting, we have $d_3(h) - y \in \text{Ker}(g_3) = \text{Im}(g_2)$. So there is some $k \in N_2$ with $g_2(k) = d_3(h) - y$. Since d_2 is surjective, there is some $p \in M_2$ with $d_2(p) = k$. Going around, we have $g_2(d_2(p)) = d_3(f_2(p)) = g_2(k) = d_3(h) - y$. So we see that $d_3(f_2(p) - d_3(h)) = y$, and hence setting $x = f_2(p) - d_3(h)$, we have $d_3(x) = y$. We can do this for all $y \in N_3$, and so we must have that d_3 is surjective, as desired.

□

The following is the Five Lemma:

Lemma 2. If we have that

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \downarrow{\scriptstyle d_4} & & \downarrow{\scriptstyle d_5} \\ N_1 & \xrightarrow[g_1]{} & N_2 & \xrightarrow[g_2]{} & N_3 & \xrightarrow[g_3]{} & N_4 & \xrightarrow[g_4]{} & N_5 \end{array}$$

is a commutative diagram such that d_1 is surjective, d_5 is injective, and d_2 and d_4 are bijective, then d_3 is bijective.

We note that the prior problem gives us this as a corollary.

Problem 29. Let R be a commutative ring. Let F be a flat R-module and suppose that

$$0 \longrightarrow N \longrightarrow M \longrightarrow F \longrightarrow 0$$

is an exact sequence of R-modules. Show that for any R-module E, we have

$$0 \longrightarrow N \otimes E \longrightarrow M \otimes E \longrightarrow F \otimes E \longrightarrow 0$$

is exact.

Proof. We know that every module E can be written as the quotient of a free module (say L), so we have the following exact sequence:

$$0 \longrightarrow K \longrightarrow L \longrightarrow E \longrightarrow 0$$

Recall as well that a free module is flat. The hint, then, is to tensor the two sequences together. Note that this is valid to do, since the base ring R is commutative. We then get the following square, using that L is flat and tensor is right exact:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & N \otimes K & \longrightarrow & M \otimes K & \longrightarrow & F \otimes K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\
0 & \longrightarrow & N \otimes L & \longrightarrow & M \otimes L & \longrightarrow & F \otimes L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \\
 & & N \otimes E & \longrightarrow & M \otimes E & \longrightarrow & F \otimes E & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Note this is exact by definition of the tensor product. Examining just the upper square portion, we have

$$\begin{array}{ccccccc}
 & & N \otimes K & \longrightarrow & M \otimes K & \longrightarrow & F \otimes K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\
0 & \longrightarrow & N \otimes L & \longrightarrow & M \otimes L & \longrightarrow & F \otimes L & &
\end{array}$$

Recall that Snake lemma says for the following commutative diagram

$$\begin{array}{ccccccccc}
 & & \operatorname{Ker}(d_1) & \longrightarrow & \operatorname{Ker}(d_2) & \longrightarrow & \operatorname{Ker}(d_3) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N \otimes K & \longrightarrow & M \otimes K & \longrightarrow & F \otimes K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\
0 & \longrightarrow & N \otimes L & \longrightarrow & M \otimes L & \longrightarrow & F \otimes L & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{Coker}(d_1) & \longrightarrow & \operatorname{Coker}(d_2) & \longrightarrow & \operatorname{Coker}(d_3) & &
\end{array}$$

we get a map $\delta : \operatorname{Ker}(d_3) \to \operatorname{Coker}(d_1)$ so that

$$\operatorname{Ker}(d_1) \longrightarrow \operatorname{Ker}(d_2) \longrightarrow \operatorname{Ker}(d_3) \xrightarrow{\delta} \operatorname{Coker}(d_1) \longrightarrow \operatorname{Coker}(d_2) \longrightarrow \operatorname{Coker}(d_3)$$

is exact. Note that $\mathrm{Coker}(d_1) = (N \otimes L)/\mathrm{Im}(d_1)$. By the exactness above, $\mathrm{Im}(d_1) = \mathrm{Ker}(h_1)$, so $\mathrm{Coker}(d_1) = (N \otimes L)/\mathrm{Ker}(h_1)$. Since h_1 is surjective, we get that $\mathrm{Coker}(d_1) \cong N \otimes E$ by the first isomorphism theorem. We analogously get $\mathrm{Coker}(d_2) \cong M \otimes E$, $\mathrm{Coker}(d_3) \cong F \otimes E$. Fitting this into the diagram and using that $\mathrm{Ker}(d_3) = 0$, since F is a flat module, we have the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & \mathrm{Ker}(d_1) & \longrightarrow & \mathrm{Ker}(d_2) & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N \otimes K & \longrightarrow & M \otimes K & \longrightarrow & F \otimes K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\
0 & \longrightarrow & N \otimes L & \longrightarrow & M \otimes L & \longrightarrow & F \otimes L & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N \otimes E & \longrightarrow & M \otimes E & \longrightarrow & F \otimes E & \longrightarrow & 0
\end{array}$$

Thus, Snake lemma gives us a map δ so that

$$\mathrm{Ker}(d_1) \longrightarrow \mathrm{Ker}(d_2) \longrightarrow 0 \xrightarrow{\delta} N \otimes E \longrightarrow M \otimes E \longrightarrow F \otimes E \longrightarrow 0$$

is exact. Chopping off the head, we get

$$0 \xrightarrow{\delta} N \otimes E \longrightarrow M \otimes E \longrightarrow F \otimes E \longrightarrow 0$$

is exact, giving us our desired result. □

Problem 30. Use a similar technique to prove that if

$$0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$$

is exact and F'' is flat, then F is flat iff F' is flat.

Proof. We follow the hint. Take an exact sequence

$$0 \longrightarrow E' \longrightarrow E$$

We tensor it with the above sequence to get

$$\begin{array}{ccccc}
F' \otimes E' & \longrightarrow & F \otimes E' & \longrightarrow & F'' \otimes E' \\
\downarrow & & \downarrow & & \downarrow \\
F' \otimes E & \longrightarrow & F \otimes E & \longrightarrow & F'' \otimes E
\end{array}$$

By the last problem, since F'' is flat, we have

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & F' \otimes E' & \longrightarrow & F \otimes E' & \longrightarrow & F'' \otimes E' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F' \otimes E & \longrightarrow & F \otimes E & \longrightarrow & F'' \otimes E & \longrightarrow & 0
\end{array}$$

Assume now that F is flat. Then we have

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F' \otimes E' & \xrightarrow{f_1} & F \otimes E' & \xrightarrow{f_2} & F'' \otimes E' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\ 0 & \longrightarrow & F' \otimes E & \xrightarrow{g_1} & F \otimes E & \xrightarrow{g_2} & F'' \otimes E & \longrightarrow & 0 \end{array}$$

Let $x \in \mathrm{Ker}(d_1) \subset F' \otimes E'$. Then we have $d_2(f_1(x)) = g_1(d_1(x)) = 0$. Hence, $f_1(x) \in \mathrm{Ker}(d_2)$, so that $x \in \mathrm{Ker}(f_1)$. Notice that since f_1 is injective, this forces $x = 0$. Hence, $\mathrm{Ker}(d_1) = 0$, and so F' is flat.

Now, assume that F' is flat. We have then

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F' \otimes E' & \xrightarrow{f_1} & F \otimes E' & \xrightarrow{f_2} & F'' \otimes E' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\ 0 & \longrightarrow & F' \otimes E & \xrightarrow{g_1} & F \otimes E & \xrightarrow{g_2} & F'' \otimes E & \longrightarrow & 0 \end{array}$$

Invoking Snake lemma, we see that we have an exact sequence

$$0 \longrightarrow \mathrm{Ker}(d_2) \longrightarrow 0 \longrightarrow \mathrm{Coker}(d_1) \longrightarrow \mathrm{Coker}(d_2) \longrightarrow \mathrm{Coker}(d_3)$$

By the prior homework, we note that

$$0 \to \mathrm{Ker}(d_2) \to 0$$

begin exact implies that $\mathrm{Ker}(d_2) = 0$. To reiterate, adding labels to these we have

$$0 \xrightarrow{f} \mathrm{Ker}(d_2) \xrightarrow{g} 0,$$

and $\mathrm{Ker}(g) = \mathrm{Im}(f)$. Since g is the zero map, $\mathrm{Ker}(g) = \mathrm{Ker}(d_2) = \mathrm{Im}(f)$, and since $f : 0 \to \mathrm{Ker}(d_2)$, we see that $\mathrm{Im}(f) = 0$. Hence, $\mathrm{Ker}(d_2) = 0$, and thus F is flat. Thus, we have that F is flat iff F' is flat.

Alternatively, we note that the induced map f_1 on the kernels will be injective (see last homework for why), so we have

$$0 \longrightarrow \mathrm{Ker}(d_1) \longrightarrow \mathrm{Ker}(d_2) \longrightarrow 0 \longrightarrow \mathrm{Coker}(d_1) \longrightarrow \mathrm{Coker}(d_2) \longrightarrow \mathrm{Coker}(d_3)$$

is exact. Hence, if either $\mathrm{Ker}(d_1)$ or $\mathrm{Ker}(d_2)$ are 0, then we will get that the other must also be 0 by exactness. $\square$

Remark. Thomas O'Hare was a collaborator.

In all problems, let F be a covariant additive functor from **R-mod** to $\mathbb{Z}$**-mod**.

Problem 31. Let $(P_\cdot, \epsilon)$ and $(P'_\cdot, \epsilon')$ be two projective resolutions of M. Let $\alpha : P_\cdot \to P'_\cdot$ be a lift of the identity morphism $\mathrm{id}_M : M \to M$. Show that $\widetilde{F(\alpha_n)}$ is an isomorphism from $H_n(F(P_\cdot))$ to $H_n(F(P'_\cdot))$. Conclude that the left derived functor $L_n(F(M))$ is independent of the projective resolution up to isomorphism.

Proof. Assume we have the set up of two projective resolutions; i.e., we have the following set up:

$$\begin{array}{ccccccccccccc}
\cdots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\epsilon} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \mathrm{id}_M} & & \\
\cdots & \xrightarrow{d'_3} & P'_2 & \xrightarrow{d'_2} & P'_1 & \xrightarrow{d'_1} & P'_0 & \xrightarrow{\epsilon'} & M & \longrightarrow & 0
\end{array}$$

Applying our covariant functor F, we get

$$\begin{array}{ccccccccccccc}
\cdots & \xrightarrow{F(d_3)} & F(P_2) & \xrightarrow{F(d_2)} & F(P_1) & \xrightarrow{F(d_1)} & F(P_0) & \xrightarrow{F(\epsilon)} & F(M) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle F(\alpha_2)} & & \downarrow{\scriptstyle F(\alpha_1)} & & \downarrow{\scriptstyle F(\alpha_0)} & & \downarrow{\scriptstyle \mathrm{id}_{F(M)}} & & \\
\cdots & \xrightarrow{F(d'_3)} & F(P'_2) & \xrightarrow{F(d'_2)} & F(P'_1) & \xrightarrow{F(d'_1)} & F(P'_0) & \xrightarrow{F(\epsilon')} & F(M) & \longrightarrow & 0
\end{array}$$

Notice that each of the squares commute; that is, we have that $F(\alpha_{i-1})F(d_i) = F(d'_i)F(\alpha_i)$ for $i \geq 1$ and $F(\epsilon')F(\alpha_0) = F(\epsilon)$. We check now that $\widetilde{F(\alpha_n)} : H_n(F(P_\cdot)) \to H_n(F(P'_\cdot))$ is an isomorphism (the tilde denoting the induced map on homology). To do so, we use the fact that the identity is bijective to get the following commutative diagram:

$$\begin{array}{ccccccccccccc}
\cdots & \xrightarrow{F(d_3)} & F(P_2) & \xrightarrow{F(d_2)} & F(P_1) & \xrightarrow{F(d_1)} & F(P_0) & \xrightarrow{F(\epsilon)} & F(M) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle F(\alpha_2)} & & \downarrow{\scriptstyle F(\alpha_1)} & & \downarrow{\scriptstyle F(\alpha_0)} & & \downarrow{\scriptstyle \mathrm{id}_{F(M)}} & & \\
\cdots & \xrightarrow{F(d'_3)} & F(P'_2) & \xrightarrow{F(d'_2)} & F(P'_1) & \xrightarrow{F(d'_1)} & F(P'_0) & \xrightarrow{F(\epsilon')} & F(M) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle F(\beta_2)} & & \downarrow{\scriptstyle F(\beta_1)} & & \downarrow{\scriptstyle F(\beta_0)} & & \downarrow{\scriptstyle \mathrm{id}_{F(M)}} & & \\
\cdots & \xrightarrow{F(d_3)} & F(P_2) & \xrightarrow{F(d_2)} & F(P_1) & \xrightarrow{F(d_1)} & F(P_0) & \xrightarrow{F(d_0)} & F(M) & \longrightarrow & 0
\end{array}$$

Composing, we see that $F(\alpha)F(\beta) = F(\alpha\beta)$ is a chain map from $F(P_\cdot)$ to itself. Furthermore, by the fact that this is unique up to homotopy (**Theorem 6.3** in Jacobson), we have that $F(\alpha\beta) \cong 1_{F(P_\cdot)}$ (the identity chain map); that is, they are homotopic. Since homotopic maps induce the same maps on homology (remark in Jacobson, top of page 338), we get that

$$\widetilde{F(\alpha_n)F(\beta_n)} = \widetilde{F(\alpha_n)}\widetilde{F(\beta_n)} = \widetilde{1_{F(P_n)}},$$

where here we note that

$$\widetilde{F(\alpha_n)F(\beta_n)} = \widetilde{F(\alpha_n)}\widetilde{F(\beta_n)}$$

and

$$\widetilde{1_{F(P_n)}} = \mathrm{id}_{H_n(F(P_\cdot))}.$$

To see these last facts, notice that

$$\widetilde{F(\alpha_n)F(\beta_n)}(z_n + B_n) = F(\alpha_n)F(\beta_n)(z_n) + B_n = \widetilde{F(\alpha_n)}(F(\beta_n)(z_n) + B'_n) = \widetilde{F(\alpha_n)}\widetilde{F(\beta_n)}(z_n + B_n),$$

where $B_n = \mathrm{Im}(d_{n+1})$ and $B'_n = \mathrm{Im}(d'_{n+1})$ are the appropriate boundaries, z_n a cycle. We have as well that

$$\widetilde{1_{F(P_n)}}(z + B_n) = 1_{F(P_n)}(z) + B_n = z + B_n,$$

so on homology, $\widetilde{1_{F(P_n)}} = \mathrm{id}_{H(F(P_\cdot))}$. A similar argument will give us that $\widetilde{F(\beta_n)}\widetilde{F(\alpha_n)} = \widetilde{1_{F(P'_n)}}$, and so we get that $\widetilde{F(\alpha_n)}$ is an isomorphism, as desired.

If we had two different projective resolutions which defined left derived functors, say $L_n(F(M))$ and $\overline{L_n}(F(M))$, then we see that the above argument says that says that $L_n(F(M)) = H_n(F(P_\cdot)) \cong H_n(F(P'_\cdot)) = \overline{L_n}(F(M))$, so the objects are independent up to isomorphism. □

Problem 32. Let $\mu \in \mathrm{Hom}_R(M, M')$. In the spirit of the previous problem, determine the dependence of $L_n(F(\mu))$ on the choice of projective resolutions of M and M'.

Proof. Say we have two projective resolutions of M, $(P_\cdot, \epsilon)$ and $(P_\cdot, \epsilon')$, and two projective resolutions of M', $(Q_\cdot, \eta)$ and $(Q'_\cdot, \eta')$. Let $\overline{L_n}$ denote the left derived functor with respect to the alternate projective resolutions (the resolutions with a prime). We wish to show that these functors are naturally isomorphic via $\widetilde{F(\alpha_n)} : L_n(F(M)) \to \overline{L_n}(F(M))$ and $\widetilde{F(\beta_n)} : L_n(F(M')) \to \overline{L_n}(F(M))$, where here $L_n(F(\mu))$ and $\overline{L_n}(F(\mu))$ will denote the maps between homologies. That is, we wish to show that

$$\begin{array}{ccc} L_n(F(M)) & \xrightarrow{\widetilde{F(\alpha_n)}} & \overline{L_n}(F(M)) \\ \downarrow{\scriptstyle L_n(F(\mu))} & & \downarrow{\scriptstyle \overline{L_n}(F(\mu))} \\ L_n(F(M')) & \xrightarrow[\widetilde{F(\beta_n)}]{} & \overline{L_n}(F(M')) \end{array}$$

is commutative. Then we get that the dependence of $L_n(F(\mu))$ is going to be up to composing with some isomorphisms.

This boils down to a uniqueness up to homotopy argument again (**Theorem 6.3** in Jacobson). We see that we have

$$\begin{array}{ccccccccccccc} \cdots & \xrightarrow{F(d_3)} & F(P_2) & \xrightarrow{F(d_2)} & F(P_1) & \xrightarrow{F(d_1)} & F(P_0) & \xrightarrow{F(\epsilon)} & F(M) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F(\alpha_2)} & & \downarrow{\scriptstyle F(\alpha_1)} & & \downarrow{\scriptstyle F(\alpha_0)} & & \downarrow{\scriptstyle \mathrm{id}_{F(M)}} & & \\ \cdots & \xrightarrow{F(d'_3)} & F(P'_2) & \xrightarrow{F(d'_2)} & F(P'_1) & \xrightarrow{F(d'_1)} & F(P'_0) & \xrightarrow{F(\epsilon')} & F(M) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F(\beta'_2)} & & \downarrow{\scriptstyle F(\beta'_1)} & & \downarrow{\scriptstyle F(\beta'_0)} & & \downarrow{\scriptstyle \mu} & & \\ \cdots & \xrightarrow{F(\partial'_3)} & F(Q'_2) & \xrightarrow{F(\partial'_2)} & F(Q'_1) & \xrightarrow{F(\partial'_1)} & F(Q'_0) & \xrightarrow{F(\partial'_0)} & F(M) & \longrightarrow & 0 \end{array}$$

is a commutative diagram, giving us a map on homology $\overline{L_n}(F(\mu))\widetilde{F(\alpha_n)}$, and

$$\begin{array}{ccccccccccccc} \cdots & \xrightarrow{F(d_3)} & F(P_2) & \xrightarrow{F(d_2)} & F(P_1) & \xrightarrow{F(d_1)} & F(P_0) & \xrightarrow{F(\epsilon)} & F(M) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F(\alpha'_2)} & & \downarrow{\scriptstyle F(\alpha'_1)} & & \downarrow{\scriptstyle F(\alpha'_0)} & & \downarrow{\scriptstyle F(\mu)} & & \\ \cdots & \xrightarrow{F(\partial_3)} & F(Q_2) & \xrightarrow{F(\partial_2)} & F(Q_1) & \xrightarrow{F(\partial_1)} & F(Q_0) & \xrightarrow{F(\eta)} & F(M') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F(\beta_2)} & & \downarrow{\scriptstyle F(\beta_1)} & & \downarrow{\scriptstyle F(\beta_0)} & & \downarrow{\scriptstyle \mathrm{id}_{F(M')}} & & \\ \cdots & \xrightarrow{F(\partial'_3)} & F(Q'_2) & \xrightarrow{F(\partial'_2)} & F(Q'_1) & \xrightarrow{F(\partial'_1)} & F(Q'_0) & \xrightarrow{F(\eta')} & F(M') & \longrightarrow & 0 \end{array}$$

is a commutative diagram, giving us a map on homology $L_n(F(\mu))\widetilde{F(\beta_n)}$ [Note that the α', β' are not necessarily related to the α, β, but rather are just poorly chosen map names]. Notice that these maps must be homotopic, and hence they induce the same maps on homology; in other words, we have

$$L_n(F(\mu))\widetilde{F(\beta_n)} = \widetilde{F(\alpha_n)}\overline{L_n}(F(\mu)).$$

So the relation is, in fact,

$$L_n(F(\mu)) = \widetilde{F(\alpha_n)}\overline{L_n}(F(\mu))\widetilde{F(\beta_n)}^{-1},$$

that is, the diagram above commutes. We have a natural isomorphism, then. □

Problem 33. (a) Show that L_0F is always right exact.
(b) Show that if F is right exact, then F and L_0F are naturally isomorphic.

Proof. (a) Consider an exact sequence of modules

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

The goal is to show that applying L_0F gives us

$$L_0(F(M')) \xrightarrow{L_0(F(\alpha))} L_0(F(M)) \xrightarrow{L_0(F(\beta))} L_0(F(M'')) \longrightarrow 0$$

is exact as well. Recall from the lecture notes that associated to this exact sequence is a projective resolution; i.e. we have

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P'_\cdot & \xrightarrow{i} & P_\cdot & \xrightarrow{\pi} & P''_\cdot & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

So for every $n \geq 0$, we have a short exact sequence

$$0 \longrightarrow P'_n \xrightarrow{i_n} P_n \underset{\nwarrow\!\!\cdots}{\xrightarrow{p_n}} P''_n \longrightarrow 0$$

That is, we have that $P_n \cong P'_n \oplus P''_n$. Thus, since we assume F is additive, we get that

$$0 \longrightarrow F(P'_n) \xrightarrow{F(i_n)} F(P_n) \underset{\nwarrow\!\!\cdots}{\xrightarrow{F(p_n)}} F(P''_n) \longrightarrow 0$$

remains exact; i.e., we get that $F(P_n) \cong F(P'_n) \oplus F(P''_n)$. Since this holds for all n, and the diagrams are commutative, when we chop off the head (the sequence of $F(M)$s) we get that we have an exact sequence of chains

$$0 \longrightarrow F(P'_\cdot) \xrightarrow{F(i)} F(P_\cdot) \xrightarrow{F(p)} F(P''_\cdot) \longrightarrow 0$$

Applying the long exact sequence of homology and examining just the head, we are left with

$$H_0(F(P'_\cdot)) \xrightarrow{\widetilde{F(i_0)}} H_0(F(P_\cdot)) \xrightarrow{\widetilde{F(p_0)}} H_0(F(P''_\cdot)) \longrightarrow 0$$

is exact. Notice that it ends in 0, since we have $H_{-1}(F(P'_\cdot)) = 0$, since $F(P'_{-1}) = 0$, and so $H_{-1}(F(P'_\cdot))$ is the kernel of this map to 0 quotiented by the image of $F(P'_0)$ into it, which is 0. Translating to the left-derived functor, we have

$$L_0(F(M')) \xrightarrow{L_0(F(\alpha))} L_0(F(M)) \xrightarrow{L_0(F(\beta))} L_0(F(M'')) \longrightarrow 0$$

is exact. Thus, L_0F is right exact.

(b) The goal is to show that, for all modules M, M' and all homomorphisms $\mu : M \to M'$, there exists a natural isomorphism η; i.e., a map η so that

$$\begin{array}{ccc} L_0(F(M)) & \xrightarrow{\eta_M} & F(M) \\ {\scriptstyle L_0(F(\mu))}\downarrow & & \downarrow{\scriptstyle F(\mu)} \\ L_0(F(M')) & \xrightarrow{\eta_{M'}} & F(M') \end{array}$$

commutes and η_M, $\eta_{M'}$ are isomorphisms. Choose some projective resolution of M and M', say $(P_\cdot, \epsilon)$ and $(P'_\cdot, \epsilon')$. Applying F to both of these, we get exact sequences

$$F(P_1) \xrightarrow{F(d_1)} F(P_0) \xrightarrow{F(\epsilon)} F(M) \longrightarrow 0$$

$$F(P'_1) \xrightarrow{F(d'_1)} F(P'_0) \xrightarrow{F(\epsilon')} F(M') \longrightarrow 0$$

Note that $F(M)$ is isomorphic to $F(P_0)/\mathrm{Ker}(F(\epsilon)) = F(P_0)/\mathrm{Im}(F(d_1)) = \mathrm{Coker}(F(d_1)) = H_0(F(M))$. Thus, we have an associated isomorphism $\eta_M : H_0(F(M)) = L_0(F(M)) \to F(M)$. Similarly, we have $\eta_{M'} : L_0(F(M')) \to F(M')$. It suffices then to check that these maps commute.

Let α be the induced chain map between the projective resolutions. Let $z + B_i \in H_0(F(M))$, then $F(\mu)\eta_M(z+B_i) = F(\mu)F(\epsilon)(z) = F(\mu\epsilon)(z)$. Similarly, $\eta_{M'}L_0(F(\mu))(z+B_i) = \eta_{M'}(F(\alpha_0)(z)+B'_i) = F(\epsilon')F(\alpha_0)(z) = F(\epsilon'\alpha_0)(z)$. Recall that, by construction, we have that $\mu\epsilon = \epsilon'\alpha_0$, so we see that $F(\epsilon'\alpha_0)(z) = F(\mu\epsilon)(z)$; that is, we have $F(\mu)\eta_M = \eta_{M'}L_0(F(\mu))$. Thus, the map is natural, and so we have that the functors are naturally isomorphic.

□

Problem 34. Let R be a commutative PID (such as $\mathbb{Z}$). Let $a \in R$, $a \neq 0$, and $M = R/(a)$. For any R module N, show that

$$\mathrm{Ext}^1_R(M, N) \cong N/aN.$$

In particular, show that if $N = R/(b)$, then $\mathrm{Ext}^1_R(M, N) \cong R/(a, b)$.

Proof. Consider the projective presentation of M given by

$$0 \longrightarrow R \xrightarrow{f} R \xrightarrow{\pi} M \longrightarrow 0$$

where $f : R \to R$ is given by $f(x) = xa$, and $\pi : R \to M$ is the canonical projection map. We have then the following long exact sequence:

$$0 \longrightarrow \mathrm{Ext}^0_R(M, N) \xrightarrow{\mathrm{Ext}^0_R(\pi,N)} \mathrm{Ext}^0_R(R, N) \xrightarrow{\mathrm{Ext}^0_R(f,N)} \mathrm{Ext}^0_R(M, N) \xrightarrow{\Delta_0} \mathrm{Ext}^1_R(M, N) \xrightarrow{\mathrm{Ext}^1_R(\pi,N)} \mathrm{Ext}^1_R(R, N)$$

$$\xrightarrow{\mathrm{Ext}^1_R(f,N)} \mathrm{Ext}^1_R(R, N) \longrightarrow \cdots$$

We recall that, for all modules K, $\mathrm{Ext}^0_R(K, N) \cong \mathrm{Hom}_R(K, N)$. Plugging this in gives

$$0 \longrightarrow \hom_R(M, N) \xrightarrow{\hom_R(\pi,N)} \hom_R(R, N) \xrightarrow{\hom_R(f,N)} \hom_R(R, N) \xrightarrow{\Delta'_0} \mathrm{Ext}^1_R(M, N) \xrightarrow{\mathrm{Ext}^1_R(\pi,N)} \mathrm{Ext}^1_R(R, N)$$

$$\xrightarrow{\mathrm{Ext}^1_R(f,N)} \mathrm{Ext}^1_R(R, N) \longrightarrow \cdots$$

exact, where the map Δ_0' is induced from the isomorphism. Note that $\hom_R(R,N) \cong N$. Let $\tau : \hom_R(R,N) \to N$ be defined by $\tau(f) = f(1)$, and let $\theta : N \to \hom_R(R,N)$ by $\theta(n) = f : R \to N$, where $f(r) = rn$. We see that τ is an R-module homomorphism, since $\tau(f+g) = (f+g)(1) = f(1) + g(1) = \tau(f) + \tau(g)$, and for all $r \in R$, $\tau(rf) = rf(1) = r\tau(f)$, and likewise $\theta(n+m)(r) = r(n+m) = rn + rm = \theta(n)(r) + \theta(m)(r)$, $\theta(rn)(s) = rns = r\theta(n)(s)$. Furthermore, $\tau(\theta(n)) = \theta(n)(1) = n$, $\theta(\tau(f))(r) = \theta(f(1))(r) = f(1)r = f(r)$, since f is an R-module homomorphism, so $\theta(\tau(f)) = f$. Furthermore, we see that we can induce a map $\kappa : N \to N$ by $\kappa = \tau \hom_R(f,N)\theta$, where $\kappa(n) = \tau(\hom_R(f,N)(\theta(n))) = \tau(f(\theta(n))) = \tau(a\theta(n)) = a\theta(n)(1) = an$; i.e. $\kappa(n) = an$. Notice as well that $\operatorname{Ext}^1_R(R,N) = 0$, since R is projective. Thus, we are left with

$$N \xrightarrow{\kappa} N \xrightarrow{\Delta_0''} \operatorname{Ext}^1_R(M,N) \longrightarrow 0$$

where the Δ_0'' is induced from the isomorphisms. Since this is exact, we get that

$$\operatorname{Ext}^1_R(M,N) \cong N/\operatorname{Ker}(\Delta_0'') = N/\operatorname{Im}(\kappa) = N/aN.$$

Hence,

$$\operatorname{Ext}^1_R(M,N) \cong N/aN.$$

Now, consider $N = R/(b)$. Notice that $aN = a(R/(b)) = ((a)+(b))/(b) = (d)/(b)$, where $d = (a,b)$. The third isomorphism theorem gives us that $N/aN = (R/(b))/((d)/(b))$ is isomorphic to $R/(d)$, as desired. □

Problem 35. In the category of $\mathbb{Z}$-modules, show that $\operatorname{Ext}^n_{\mathbb{Z}}(\cdot,\cdot) = 0$ for $n \geq 2$.

Proof. Fix modules M and N. The idea is to calculate $\overline{\operatorname{Ext}^n_{\mathbb{Z}}}(M,N)$ (since we'd like to use an injective resolution) and then use the fact that these are isomorphic to deduce the same result for $\operatorname{Ext}^n_{\mathbb{Z}}(M,N)$ (this is **Theorem 6.9** in Jacobson).

Notice we can embed N into an injective module, say Q; thus, we view it as a submodule of Q. Furthermore, completing the sequence, we get an exact sequence

$$0 \longrightarrow N \xrightarrow{i} Q \xrightarrow{\pi} Q/N \longrightarrow 0$$

Recall that, since we are over $\mathbb{Z}$, Q is injective iff Q is divisible. Recall that divisible means that for all $a \in \mathbb{Z}$, $a \neq 0$, we have that the map $a_Q : Q \to Q$ given by $a_Q(x) = ax$ is surjective. The goal, then, is to establish that Q/N is divisible as well. Let $y + N \in Q/N$, $a \in \mathbb{Z}$, $a \neq 0$. Since Q is divisible, we have that there exists an x so that $ax = y$. Hence, $a_{Q/N}(x) = a(x+N) = ax + aN = ax + N = y + N$. Since the choice of y was arbitrary, we get that $a_{Q/N}$ is surjective; since the choice of a was arbitrary, we get that Q/N is divisible, and hence injective.

Using this, we have that $\overline{\operatorname{Ext}^n_{\mathbb{Z}}}(M,Q) = \overline{\operatorname{Ext}^n_{Z}}(M,Q/N) = 0$ for all $n \geq 1$. Using the long exact sequence, we see that

$$\cdots \longrightarrow \overline{\operatorname{Ext}^1_{\mathbb{Z}}}(M,Q/N) \longrightarrow \overline{\operatorname{Ext}^2_{\mathbb{Z}}}(M,N) \longrightarrow \overline{\operatorname{Ext}^2_{\mathbb{Z}}}(M,Q) \longrightarrow \cdots$$

is exact. By what we've just observed, we have that

$$\cdots \longrightarrow 0 \longrightarrow \overline{\operatorname{Ext}^2_{\mathbb{Z}}}(M,N) \longrightarrow 0 \longrightarrow \cdots$$

is exact, forcing $\overline{\operatorname{Ext}^2_{\mathbb{Z}}}(M,N) = 0$. Similarly, for $n > 2$, we have

$$\cdots \longrightarrow \overline{\operatorname{Ext}^{n-1}_{\mathbb{Z}}}(M,Q/N) \longrightarrow \overline{\operatorname{Ext}^n_{\mathbb{Z}}}(M,N) \longrightarrow \overline{\operatorname{Ext}^n_{\mathbb{Z}}}(M,Q) \longrightarrow \cdots$$

is exact, and since Q/N, Q are injective, we get

$$\cdots \longrightarrow 0 \longrightarrow \overline{\mathrm{Ext}}^n_{\mathbb{Z}}(M,N) \longrightarrow 0 \longrightarrow \cdots$$

is exact, forcing $\overline{\mathrm{Ext}}^n_{\mathbb{Z}}(M,N) = 0$. Thus, for $n \geq 2$, we have $\overline{\mathrm{Ext}}^n_{\mathbb{Z}}(M,N) = 0$. Since $\mathrm{Ext}^n_{\mathbb{Z}}(M,N) \cong \overline{\mathrm{Ext}}^n_{\mathbb{Z}}(M,N)$, we get that this forces $\mathrm{Ext}^n_{\mathbb{Z}}(M,N) = 0$ as well. $\square$

Remark. Thomas O'Hare was a collaborator.

Problem 36. Let F be a field and let $E = F(u)$, where u is algebraic of odd degree over F (hence, the minimal polynomial of u has odd degree). Show that $E = F(u^2)$.

Proof. Let $p_u(x) \in F[x]$ denote the minimal polynomial of u; that is, the unique monic irreducible polynomial so that $p_u(u) = 0$. Note that, in general, $F(u^2) \subset F(u)$ – if $a \in F(u^2)$, then a is of the form

$$a = \sum_{j=0}^{k} a_j (u^2)^j = \sum_{j=0}^{k} a_j u^{2j},$$

so that $a \in F(u)$ as well. Hence, we have $F \subset F(u^2) \subset E$. The goal, then, is to show that $E \subset F(u^2)$. Assume for contradiction that $u \notin F(u^2)$. Thus, the minimal polynomial for u over $F(u^2)$ will be $x^2 - u^2$, and hence the degree of the extension will be 2. Recall that the degree of the extension $[E : F]$ is the degree of the minimal polynomial, so that this is odd. By the towers of degree theorem, we have that

$$[E : F] = [E : F(u^2)][F(u^2) : F] = 2[F(u^2) : F].$$

This, however, is impossible, since this implies that $[E : F]$ has even degree, a contradiction. Thus, we must have that $u \in F(u^2)$, so that $E = F(u)$. □

Problem 37. Let E/F be an algebraic extension. Show that any subring of E that contains F is a subfield.

Proof. Let $F \subset R \subset E$, where R is a subring of E. The goal is to show that all non-zero elements of R have multiplicative inverse in R; thus, R is a field. Since E is an algebraic extension, we have that, for all $r \in R \setminus F$, r is algebraic over F; thus, there is some minimal polynomial $p(x) \in F[x]$ so that

$$p(x) = \sum_{j=0}^{k} a_j x^j, \quad a_k = 1, \quad p(r) = 0.$$

Notice that this implies that

$$r(r^{n-1} + \cdots + a_1) + a_0 = 0,$$

so

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

We have that $a_0 \in F$, so $-a_0$ is invertible in F; hence, we have

$$r\left[(-a_0)^{-1}(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1)\right] = 1.$$

Thus,

$$r^{-1} = (-a_0)^{-1}(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1) \in R,$$

since $F \subset R$ and powers of r are in R.

Alternatively, as noted by Nick Bolle, we can do the following (clever) trick. Let $\alpha \in R$ be non-zero. Then we see that $F[\alpha] = F(\alpha)$, since α is algebraic. Notice that this implies that $F \subset F(\alpha) \subset R$, and since $\alpha^{-1} \in F(\alpha)$, we get $\alpha^{-1} \in R$. Thus, every non-zero element of R is invertible, so R is a subfield. □

Problem 38. Let p be a prime. Determine a splitting field over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of the polynomial $x^{p^e} - 1$ for $e \geq 1$.

Proof. We assume $p \neq 2$ for the moment. Notice that for $e \geq 1$, we can write

$$(x-1)^{p^e} = \sum_{j=0}^{p^e} \binom{p^e}{j} x^j (-1)^{p^e - j}.$$

Since we are viewing this in $\mathbb{Z}/p\mathbb{Z}$, we see that all but the first and last term vanish, leaving us with

$$(x-1)^{p^e} = (-1)^{p^e} + x^{p^e} = x^{p^e} - 1.$$

Now, if $p = 2$, we have that all applies except that we have

$$(x-1)^{p^e} = x^{p^e} + 1.$$

Notice that this is the same as

$$(x-1)^{p^e} = x^{p^e} - 1,$$

since we are in $\mathbb{Z}/2\mathbb{Z}$, so we have that the polynomial splits in $\mathbb{F}_p$. That is, $\mathbb{F}_p$ is the splitting field for $x^{p^e} - 1$. □

Problem 39. Let $\sigma : F \to F'$ be an isomorphism of fields. Let E/F be an extension of F and E'/F' be an extension of F'. Let $\alpha \in E$ be algebraic over F with minimal polynomial $f_\alpha \in F[x]$, and let $f'_\alpha = \sigma(f_\alpha) \in F'[x]$. Show that σ can be extended to an embedding $\sigma_1 : F(\alpha) \hookrightarrow E'$ iff f'_α has a root in E', and that the number of possible extensions equals the number of distinct roots of f'_α in E'.

Proof. Assume that σ can be extended to an embedding $\sigma_1 : F(\alpha) \hookrightarrow E'$. The goal is to show that $\sigma(f_\alpha)$ has a root in E'. If we write

$$f_\alpha(x) = a_0 + a_1 x + \cdots + x^n,$$

then we see that

$$f_\alpha(\alpha) = a_0 + a_1\alpha + \cdots + \alpha^n = 0,$$

and

$$\begin{aligned} \sigma_1(f_\alpha(\alpha)) &= \sigma_1(a_0 + a_1\alpha + \cdots + \alpha^n) \\ &= \sigma_1(a_0) + \sigma_1(a_1)\sigma_1(\alpha) + \cdots + (\sigma_1(\alpha))^n \\ &= \sigma(a_0) + \sigma(a_1)\sigma_1(\alpha) + \cdots + (\sigma_1(\alpha))^n \\ &= f'_\alpha(\sigma_1(\alpha)) = 0. \end{aligned}$$

Hence, we see that f'_α admits a root $\sigma_1(\alpha) \in E'$. This tells us the number of embeddings is at least the number of roots of f'_α in E'.

Assume that f'_α has a root in E', say β. We can define a homomorphism $\gamma : F[x] \to E'$ via $\gamma(p(x)) = \sigma(p)(\beta)$. Notice that $(f_\alpha(x)) \subset \mathrm{Ker}(\gamma)$, since

$$\gamma(f_\alpha(x)) = f'_\alpha(\beta) = 0.$$

Thus, we get an induced injective homomorphism $\overline{\gamma} : F[x]/(f_\alpha(x)) \to E'$. Finally, $F[x]/(f_\alpha(x)) \cong F(\alpha)$, so we get an injective map $\sigma_1 : F(\alpha) \to E'$ taking the inverse of the isomorphism and applying $\overline{\gamma}$. We have that $F(\alpha)$ is generated by α, and this is defined via setting $\sigma_1(\alpha) = \beta$ and $\sigma_1|_F = \sigma$ and extending linearly, so this is the unique extension sending α to β. Thus, this tells the number of embeddings is at most the number of roots of f'_α in E'. Coupling this with the last result, we have that the number of embeddings is exactly the number of roots of f'_α in E'. □

Problem 40. Let E be a finite extension of F with $(E : F) = n$. Let K be any extension of F. Show that the number of embeddings $\sigma : E \hookrightarrow K$ which are the identity on F does not exceed n.

Proof. Assume that it did exceed n; that is, we have $\sigma_1, \ldots, \sigma_k : E \hookrightarrow K$ for $k > n$, all distinct, and all are such that they are the identity on F; that is, $F \subset R$, where R is the fixed field of the σ_j. Then we have that $(E : F) = (E : R)(R : F)$, and since there are k extensions, this tells us that $n = (E : F) \geq (E : R) \geq k > n$ (by the theorem from the lecture notes, **Week 10, page 18**), which is a contradiction. Hence, we must have $k \leq n$. $\square$

Remark. Thomas O'Hare was a collaborator.

Problem 41. Let E/F be a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(E/F)$. Let K_1, K_2 be two intermediate fields with Galois groups $H_i = \mathrm{Gal}(E/K_i)$ respectively. Show that

(a) $\mathrm{Gal}(E/K_1K_2) = H_1 \cap H_2$.
(b) $\mathrm{Gal}(E/(K_1 \cap K_2))$ is the subgroup of G generated by H_1 and H_2.
(c) $K_1 \subset K_2$ iff $H_2 \subset H_1$.

Claim 2. If E/F is a finite Galois extension, then there is an order reversing bijection between intermediate fields $F \subset K \subset E$ and subgroups of $G = \mathrm{Gal}(E/F)$.

Proof. Given an intermediate field, we can map

$$K \mapsto H_K = \mathrm{Gal}(E/K) = \{\sigma \in \mathrm{Aut}(E) : \sigma|_K = \mathrm{id}_K\}.$$

Given a subgroup $H \leq \mathrm{Gal}(E/K)$, we can map

$$H \mapsto E^H = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

The fact that these maps are well-defined and inverses follows from from part (1) of the Fundamental Theorem of Finite Galois Theory (see **Week 11, page 34**). To see the order reversing property, suppose $F \subset K_1 \subset K_2 \subset E$. We wish to show that if

$$H_{K_i} = \{\sigma \in \mathrm{Aut}(E) : \sigma|_{K_i} = \mathrm{id}_{K_i}\} = \mathrm{Gal}(E/K_i),$$

then $H_{K_2} \subset H_{K_1}$. Let $\sigma \in H_{K_2}$, then by definition $\sigma|_{K_2} = \mathrm{id}_{K_2}$ – so for all $\alpha \in K_2$, $\sigma(\alpha) = \alpha$. In particular, since $K_1 \subset K_2$, we have that for all $\alpha \in K_1$, $\sigma(\alpha) = \alpha$, so $\sigma|_{K_1} = \mathrm{id}_{K_1}$. Thus, $\sigma \in H_{K_1}$. The choice of σ was arbitrary, so we have $H_{K_2} \subset H_{K_1}$.

Next, if $\{e\} \subset H_1 \subset H_2 \subset G$, then we wish to show that $E^{H_2} \subset E^{H_1}$. Recall

$$E^{H_i} = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H_i\}.$$

Let $\alpha \in E^{H_2}$. Then for all $\sigma \in H_2$, we have $\sigma(\alpha) = \alpha$. Since $H_1 \subset H_2$, we have that for all $\sigma \in H_1 \subset H_2$, $\sigma(\alpha) = \alpha$. Thus, we see that $\alpha \in E^{H_1}$. The choice of α was arbitrary, so we get that $E^{H_1} \subset E^{H_2}$. Hence, the maps are order reversing. □

Proof. (a) Recall that the composite of two fields K_1 and K_2 is the smallest subfield containing both K_1 and K_2. Hence, by the order reversing bijection, we have that $\mathrm{Gal}(E/K_1K_2)$ corresponds to the largest subgroup contained in $H_1 = \mathrm{Gal}(E/K_1)$ and $H_2 = \mathrm{Gal}(E/K_2)$. So the claim reduces to showing that the largest subgroup contained in H_1 and H_2, say H, is the intersection. If $H \subset H_1, H_2$, then we have that $H \subset H_1 \cap H_2$, and since $H_1 \cap H_2 \subset H_1, H_2$, we get that $H_1 \cap H_2 \subset H$, so $H = H_1 \cap H_2$. Thus, $\mathrm{Gal}(E/K_1K_2) = H_1 \cap H_2$.

(b) Again, we abuse the order preserving bijection. Note that $K_1 \cap K_2$ is the largest subfield contained in both K_1 and K_2, so the order reversing bijection sends $\mathrm{Gal}(E/(K_1 \cap K_2))$ to H, which is the smallest subgroup containing H_1 and H_2. This is, by definition, the subgroup of G generated by H_1 and H_2.

(c) This is a consequence of the order reversing bijection; we have $K_1 \subset K_2$ implies that $\mathrm{Gal}(E/K_2) \subset \mathrm{Gal}(E/K_1)$ and $H_2 \subset H_1$ implies that $E^{H_1} \subset E^{H_2}$, and the fundamental theorem of finite Galois theory tells us that $E^{H_1} = K_1$, $E^{H_2} = K_2$, $\mathrm{Gal}(E/K_1) = H_1$, and $\mathrm{Gal}(E/K_2) = H_2$. Thus, $K_1 \subset K_2$ iff $H_2 \subset H_1$.

□

Problem 42. Let E/F be a finite Galois extension of fields, with $G = \mathrm{Gal}(E/F)$. Suppose that K and L are intermediate fields such that $E = KL$ and $F = K \cap L$. Let $N = \mathrm{Gal}(E/L)$ and $H = \mathrm{Gal}(E/K)$.

(a) If L/F is a normal extension, show that $G = H \rtimes N$, the semi-direct product of H and N.
(b) If both L/F and K/F are normal, show that $G = H \times N$, the direct product of H and N.

Proof. (a) Recall that a normal extension is one where every irreducible polynomial in $F[x]$ which has a root in E is a product of linear factors in $E[x]$. We first wish to establish that N is a normal group in G. Let $a \in L$, $f_a \in F[x]$ the minimal polynomial of a over F. Then since the extension is normal, $f_a(x) = (x-a)\cdot(x-a_1)\cdots(x-a_r)$ in $L[x]$. Let $\theta \in G = \mathrm{Gal}(E/F)$. Then we have that $f_a(\theta(a)) = 0$, so $\theta(a) = a_i$ for some i, and so $\theta(a) \in K$. Thus, $\theta(L) \subset L$. Letting $\eta \in N = \mathrm{Gal}(E/L)$, we wish to show that $\theta\eta\theta^{-1} \in N$. Taking $x \in L$, we have $\theta\eta\theta^{-1}(x) = \theta\theta^{-1}(x) = x$ (since $\theta^{-1}(x) \in K$, we have $\eta(\theta^{-1}(x)) = \theta^{-1}(x)$), so $\theta\eta\theta^{-1}|_K = \mathrm{Id}$, and hence $\theta\eta\theta^{-1} \in N$. This holds for all $\eta \in N$, so we have that $\theta N\theta^{-1} \subset N$. Since the choice of θ was arbitrary we have that N is normal. Next, we wish to show that $H \cap N = 1$. By **Problem 1**, we see that $H \cap N = \mathrm{Gal}(E/KL) = \mathrm{Gal}(E/E) = 1$. Finally, we wish to show that $HN = G$. Again, **Problem 1** tells us that $G = \mathrm{Gal}(E/F) = \mathrm{Gal}(E/(K\cap L)) = \langle H, N\rangle = HN$ since $H \cap N = 1$ and N is normal. Thus, G is the semidirect product of N and H; that is, $G = H \rtimes N$.

(b) By the argument above, K/F and L/F normal implies that N and H are normal. Note that the semidirect product of two normal groups is the direct product of the normal groups. The goal is to show that $G = H \rtimes N = H \times N$. Construct a map $\theta : N \times H \to G$, $\theta(n,h) = nh$. The goal is to show that this is an isomorphism. First, we establish it is a homomorphism. Notice that

$$nh = hn,$$

we see this by observing that

$$nhn^{-1}h^{-1} = 1.$$

This follows since N and H are normal, so

$$nhn^{-1} \in H,$$

and

$$hn^{-1}h^{-1} \in N,$$

so

$$nhn^{-1}h^{-1} \in N \cap H = 1.$$

Hence, θ is a homomorphism;

$$\theta((n,h)(a,b)) = \theta(na, hb) = nahb = nhab = \theta(n,h)\theta(a,b).$$

Notice that

$$\theta(n,h) = nh = 1 \implies n \in N \cap H,\ h \in N \cap H, n = e = h.$$

So $\mathrm{Ker}(\theta) = e$. Next, since $G = NH$ from (a), we have that it is onto. Hence, its an isomorphism, so $N \times H \cong G$, and hence we can view G as $G = N \times H$.

□

Problem 43. Let $F = \mathbb{F}_q$ be a finite field with $q = p^\nu$ elements. Let E/F be a finite extension of degree m. The purpose of this exercise is to show that E/F is Galois, and the Galois group $\mathrm{Gal}(E/F)$ is cyclic.

(a) Let $\phi_q : E \to E$ be given by $\phi_q(\alpha) = \alpha^q$. Show that $\phi_q \in \mathrm{Gal}(E/F)$.
(b) If $(E : F) = m$, show that the order of ϕ_q is $\leq m$.
(c) Show that ϕ_q has order precisely m.

(d) If $F' = E^{\langle \phi_q \rangle}$, show that $F' = F$, so E/F is Galois with $\mathrm{Gal}(E/F) = \langle \phi_q \rangle$. ϕ_q is called the Frobenius automorphism of E/F.

Proof. (a) We need to show that ϕ_q is an automorphism of E and that it fixes F. First, we recall from the lecture notes that $\mathrm{Char}(F) = p$. We need to show that ϕ_q is an automorphism of E to itself. Notice that $\phi_q(ab) = (ab)^q = a^q b^q = \phi_q(a)\phi_q(b)$, and

$$\phi_q(a+b) = \sum_{j=0}^{q} \binom{q}{j} a^j b^{q-j} = a^q + b^q$$

since the characteristic is p. Next, we show that ϕ_q fixes F. We note that $F^\times$ is a finite group of order $q-1$, and so for all $x \in F^\times$ we have $\phi_q(x) = x^q = x^{q-1}x = x$. If $x = 0$, we have $\phi_q(0) = 0^q = 0$, so that ϕ_q fixes F. Next, we claim that ϕ_q is injective. We prove it by viewing ϕ_q as an F-linear endomorphism on E. Injectivity follows then, since if $\phi_q(a) = a^q = 0$, we must have that $a = 0$, since we are in a field. Finally, viewing E/F as a finite dimensional vector space, we see that the prior remarks show that $\phi_q : E \to E$ is an injective F-linear map between finite dimensional vector spaces of the same dimension, which forces it to be an isomorphism. In other words, we have that $\phi_q : E \to E$ is an automorphism. Thus, $\phi_q \in \mathrm{Gal}(E/F)$.

(b) Consider the set $\{\phi_q, \phi_q^2, \ldots\}$, where ϕ_q^n is defined by $\phi_q^n = \phi_q \circ \phi_q \circ \cdots \circ \phi_q$ n-times. Notice that, if these are all distinct maps, then we have that $(E : F) = \infty$, a contradiction, so we must have repeats. That is, there is some $n \neq k$ so that $\phi_q^n = \phi_q^k$. Since ϕ_q is an automorphism by (a) (so ϕ_q^{-1} is well-defined and behaves like we want), we see that this implies that there is some n so that $\phi_q^n = \mathrm{id}$. Let r be the smallest integer so that $\phi_q^r = \mathrm{id}$. We claim that $\{\phi_q, \ldots, \phi_q^{r-1}, \phi_q^r = \mathrm{id}\}$ are all distinct. If not, we have that $\phi_q^n = \phi_q^k$ for $n \neq k$, $1 \leq n, k \leq r$. Assuming $n > k$ and using the fact that ϕ_q is an automorphism, we see that $\phi_q^{n-k} = \mathrm{id}$, $n - k < r$, contradicting the minimality of our choice of r. Since these are r distinct maps, and r is the order of ϕ_q, we have that $r \leq (E : F) = m$.

(c) Since ϕ_q has order r, we get that $\phi_q^r(x) = x^{q^r} = x$ for all $x \in E$. Notice that $m = r$, since we have that m is the smallest integer so that $x^{q^m} - x$ splits over $\mathbb{F}_q$ in E, so $m \leq r$.

(d) We already have $F \subset F'$, so it suffices to show that $F' \subset F$. E/F' is a Galois extension, so we have that $(E : F') = |\langle \phi_q \rangle| = m$. Hence, we see that

$$(E : F) = (E : F')(F' : F) \implies (F' : F) = 1,$$

so $F' = F$. Thus, E/F is Galois.

□

Problem 44. Let F be the field of characteristic $p > 0$. The purpose of this exercise is to show that F is perfect iff $F = F^p$, and then show that every finite field is perfect.

(a) Show that if $F^p = \{\alpha^p : \alpha \in F\}$ then F^p is a subfield of F.
(b) If $a \in F$ but $a \notin F^p$, show that $x^p - a$ is irreducible but not separable, so F is not perfect.
(c) If F is not perfect and $f(x) \in F[x]$ is irreducible and not separable, show that one of the coefficients must not be a pth power, so $F \neq F^p$.
(d) Deduce that finite fields are perfect.

Proof. (a) Note that $F^p \subset F$, since F is closed under multiplication, so we just need to show that F^p is a subfield. If $\alpha^p, \beta^p \in F^p$, then we have that $\alpha^p \beta^p = (\alpha\beta)^p \in F^p$, so it's closed under multiplication. Notice that $\alpha^p + \beta^p = (\alpha + \beta)^p$ using the binomial theorem and the fact that the field has characteristic $p > 0$, so its closed under addition. Consequently, $0^p - \alpha^p = -\alpha^p = (0 - \alpha)^p = (-\alpha)^p$, so its closed under additive inverses, and $(\alpha^{-1})^p = \alpha^{-p} = (\alpha^p)^{-1}$, so its closed under multiplicative inverses. $0^p = 0$, $1^p = 1$, so $0, 1 \in F^p$. Thus, F^p is a subfield.

(b) Let E be the splitting field for $x^p - a$, then we have that it splits as $(x-t)^p$ for some t so that $t^p = a$. If it is not irreducible, we have that there is some monic factor $(x-t)^m \in F[x]$, where $1 \leq m \leq p-1$. Expanding this, we get

$$(x-t)^m = \sum_{j=0}^{m} \binom{m}{j} x^j (-t)^{m-j}.$$

If this were in $F[x]$, we would have that $\binom{m}{j}(-t)^{m-j} \in F$ for $0 \leq j \leq m$. Examining the case where $j = 1$, we see that this implies that $-mt^{m-1} \in F$. Since $m \neq 0$, we have that $m \in \mathbb{F}_p^\times \subset F^\times$, and so we have that this forces $t \in F$, which is a contradiction, since this would imply $t^p = a \in F^p$. Thus, the polynomial is irreducible and not separable.

(c) Assume now that F is not perfect and $f(x) \in F[x]$ is irreducible but not separable. Letting D be the formal derivative map, we note that we have $\gcd(f(x), D(f(x))) \neq 1$. Note this can only happen when $D(f(x)) = 0$. This follows, since if $\gcd(f(x), D(f(x))) = h(x) \neq 1$ and $f(x)$ is irreducible, we have that $h(x) = rf(x)$ for some element r, and $rf(x) \mid D(f(x))$ so $f(x) \mid D(f(x))$. However, the degree of $D(f(x))$ is strictly smaller than $f(x)$, so the only way this can happen is if $D(f(x))$ is 0. Thus, writing

$$f(x) = \sum_{j=0}^{n} a_j x^j,$$

we have

$$D(f(x)) = \sum_{j=1}^{n} j a_j x^{j-1} = 0.$$

Thus, $p \mid j a_j$ for $1 \leq j \leq n$. Since p is prime, we have that this implies $p \mid j$ or $p \mid a_i$. If $p \mid a_i$, this implies that the coefficient was 0 all along, so we must have $p \mid j$, and hence

$$f(x) = \sum_{j=0}^{n} a_j (x^p)^j.$$

Now, if all of the coefficients were a pth power, then we would have

$$f(x) = \sum_{j=0}^{n} (b_j x^j)^p,$$

where $b_j^p = a_j$, and so the binomial theorem gives us

$$f(x) = \left(\sum_{j=0}^{n} b_j x^j \right)^p,$$

which contradicts the fact that $f(x)$ is irreducible. Hence, we must have that one of the coefficients must not be a pth power, so $F \neq F^p$.

(d) To recollect, assuming that the field is finite, we've shown that if F is perfect, then $F = F^p$ (by part (b)), and we've shown that $F = F^p$ implies that F is perfect (by part (c)), so we have that F is perfect iff $F = F^p$. Consider the map $\phi : F \to F^p$ given by $\phi(x) = x^p$. Note that this is the Frobenius automorphism, so by the last problem we have that this is an isomorphism. Hence, we have $F = F^p$.

□

For E/F a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(E/F)$, $\alpha \in E$, we define the norm to be

$$N_{E/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Problem 45. Let E/F be a Galois extension such that $\mathrm{Gal}(E/F)$ is cyclic, and let $\mathrm{Gal}(E/F) = \langle \sigma \rangle$. For $\alpha \in E$, show that $N_{E/F}(\alpha) = 1$ iff we can write $\alpha = \beta/\sigma(\beta)$ for some $\beta \in E$.

Proof. ($\implies$): Assume $\alpha \in E$, $N_{E/F}(\alpha) = 1$ (so that $\alpha \in E^\times$). Define the map

$$\sigma^i \mapsto \alpha_{\sigma^i} = \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{i-1}(\alpha).$$

Since $\alpha \in E^\times$, we note that the map is such that $G \to E^\times$. The goal is to show that the set $\{\alpha_{\sigma^i} : \sigma^i \in G\}$ satisfies Noether's equations. Hence, we need to show that for all $\sigma^i, \sigma^j \in G$, we have

$$\alpha_{\sigma^i}\sigma^i(\alpha_{\sigma^j}) = \alpha_{\sigma^i\sigma^j}.$$

Writing this out, we have

$$\alpha_{\sigma^i} = \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha),$$
$$\alpha_{\sigma^j} = \alpha\sigma(\alpha)\cdots\sigma^{j-1}(\alpha),$$

and

$$\sigma^i(\alpha_{\sigma^j}) = \sigma^i(\alpha)\sigma^{i+1}(\alpha)\cdots\sigma^{i+j-1}(\alpha),$$

so

$$\alpha_{\sigma^i}\sigma^i(\alpha_{\sigma^j}) = \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha)\sigma^i(\alpha)\sigma^{i+1}(\alpha)\cdots\sigma^{i+j-1}(\alpha) = \alpha_{\sigma^{i+j}} = \alpha_{\sigma^i\sigma^j}.$$

We then use Speiser's theorem which says that this set is a solution to Noether's equations iff there is a $\beta \in E$ so that

$$\alpha_{\sigma^i} = \frac{\beta}{\sigma^i(\beta)}.$$

Hence, we see that

$$\alpha_\sigma = \alpha_{\sigma^1} = \alpha = \frac{\beta}{\sigma(\beta)}.$$

($\impliedby$) : Assume that $\alpha = \beta/\sigma(\beta)$ for some $\beta \in E$. Then we have

$$N_{E/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha),$$

where $|G| = \mathrm{ord}(\sigma) = n$. Notice that

$$\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha) = \frac{\beta}{\sigma(\beta)}\frac{\sigma(\beta)}{\sigma^2(\beta)}\cdots\frac{\sigma^{n-2}(\beta)}{\sigma^{n-1}(\beta)}\frac{\sigma^{n-1}(\beta)}{\beta} = 1.$$

So $N_{E/F}(\alpha) = 1$. □

Remark. Thomas O'Hare was a collaborator.

Problem 46. Let E/F be a finite extension of finite fields. Show that the norm map

$$N_{E/F} : E^\times \to F^\times, \quad N_{E/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\alpha)$$

is surjective.

Proof. We remark that E and F are finite fields, so let $F = \mathbb{F}_q$ as in the last homework. From **Problem 43** off the last homework, we know that $\mathrm{Gal}(E/F) = \langle \phi_q \rangle$; i.e., it is cyclic of order $(E : F) = m < \infty$ via the Frobenius automorphism, $\phi_q(\alpha) = \alpha^q$. So

$$\begin{aligned} N_{E/F}(\alpha) &= \alpha \phi_q(\alpha) \cdots \phi_q^{m-1}(\alpha) \\ &= \alpha \alpha^q \alpha^{q^2} \cdots \alpha^{q^{m-1}} = \alpha^{1+q+\cdots+q^{m-1}}. \end{aligned}$$

Note that we have

$$1 + q + q^2 + \cdots + q^{m-1} = \frac{1-q^m}{1-q},$$

so

$$N_{E/F}(\alpha) = \alpha^{\frac{1-q^m}{1-q}}.$$

In addition, we assume these are finite fields, so $E^\times, F^\times$ are cyclic as well from the lecture notes, with $|F^\times| = q-1$, $|E^\times| = q^m - 1$. Assume without loss of generality that α generates $E^\times$. We then need to show that $N_{E/F}(\alpha)$ generates $F^\times$; that is, of $o(\cdot)$ denotes the order of an element, we need to show that

$$o(N_{E/F}(\alpha)) = q - 1.$$

Let $k = \frac{1-q^m}{1-q}$, so $N_{E/F}(\alpha) = \alpha^k \in F^\times \leq E^\times$. We have that $o(\alpha) = q^m - 1$, so using a result on cyclic groups we get that $o(\alpha^k) = \frac{q^m-1}{(q^m-1,k)}$. Now, we note that $\left(q^m - 1, \frac{1-q^m}{1-q}\right) = \frac{1-q^m}{1-q}$, and so

$$o(\alpha^k) = \frac{q^m - 1}{\frac{1-q^m}{1-q}} = q - 1.$$

Thus, α^k generates $F^\times$, so the map is surjective. □

Problem 47. Let F contain n distinct nth roots of 1, and let E/F be a cyclic extension of degree n, so $E = F(\alpha)$ with $\alpha^n \in F$. Show that $\beta \in E$ satisfies an equation of the form $x^n - b = 0$ with $b \in F$ iff β is of the form $\beta = c\alpha^k$ for some $c \in F$, $1 \leq k \leq n$.

Proof. ($\implies$): Note that elements in $E = F(\alpha)$ are of the form

$$\beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

where $c_i \in F$. It suffices to show that if $\beta^n \in F$, then all at most one of the c_j are non-zero. Notice that if all of the c_j are non-zero, then we have that $\beta = 0$, so clearly $\beta = 0\alpha$. If exactly one of the c_j are non-zero, then we have $\beta = c_j\alpha^j$, $0 \leq j \leq n-1$, so $(c_j\alpha^j)^n = c_j^n\alpha^{nj}$ which is in F. Now consider the case where exactly two c_j are non-zero. We have

$$\beta = c_k\alpha^k + c_j\alpha^j, \quad j < k.$$

Taking this to the nth power, we see that

$$\beta^n = (c_k\alpha^k + c_j\alpha^j)^n = \sum_{s=0}^{n} \binom{n}{s} (c_k\alpha^k)^s (c_j\alpha^j)^{n-s}.$$

Letting

$$d_s = \binom{n}{s} c_k^s c_j^{n-s} \in F,$$

we can rewrite this as

$$\sum_{s=0}^{n} d_s \alpha^{(k-j)s+nj}.$$

Since $j < k < n$, taking for example $s = 1$ we see that this implies that $\alpha^{k-j} \in F$ for $k - j < n$. Notice this contradicts the fact that the degree of the extension is n, so this results in a contradiction. Hence, it is impossible to have exactly two coefficients which are non-zero.

We now proceed inductively; assume that we have shown it is impossible to have between two and $k-1$ c_j coefficients non-zero, where $k - 1 < n$. We will establish that it is impossible to have between two and k c_j coefficients non-zero, where $k \leq n$. Assume for contradiction that it is possible. We have

$$\beta = c_{j_1}\alpha^{j_1} + \cdots + c_{j_k}\alpha^{j_k}.$$

Taking this to the nth power, we have

$$\beta^n = \sum_{s=0}^{n} \binom{n}{s} \left[c_{j_1}\alpha^{j_1} + \cdots + c_{j_{k-1}}\alpha^{j_{k-1}}\right]^s (c_{j_k}\alpha^{j_k})^{n-s} \in F.$$

Notice that, examining the nth coefficient, this implies that

$$\left[c_{j_1}\alpha^{j_1} + \cdots + c_{j_{k-1}}\alpha^{j_{k-1}}\right]^n \in F,$$

which we note contradicts the induction hypothesis. Therefore, we cannot have between two and k non-zero coefficients. Moreover, this implies that we cannot have more than two non-zero coefficients; that is, we must have that β is of the form

$$\beta = c\alpha^k, \quad c \in F, 1 \leq k \leq n,$$

remarking that for $k = n$, $\alpha^n \in F$, so it's the same as saying that

$$\beta = c\alpha^k, \quad c \in F, 0 \leq k \leq n-1.$$

($\Longleftarrow$): If $\beta = c\alpha^k$, $1 \leq k \leq n$, then we have $\beta^n = (c\alpha^k) = c^n\alpha^{kn}$. Since $\alpha^n \in F$, we see that this is equal to some $b \in F$.

Alternatively we follow Alexander Goldman's solution. Again, we note that the statement trivially holds for $\beta = 0$ and $c = 0$, so it suffices to consider $c \in F^\times$ and $\beta \in E^\times$. Notice that β satisfies the polynomial iff $\beta^n \in F$, so in other words we have β satisfies $x^n - b = 0$ iff $\beta \in A$, where we define A as

$$A = \{\alpha \in E^\times : \alpha^n \in F\}.$$

So we reframe the question to be $\beta \in A$ iff $\beta = c\alpha^k$ for $c \in F^\times$, $1 \leq k \leq n$. However, notice that this is the same as A being generated by α and $F^\times$ multiplicatively; i.e., $\langle \alpha F^\times \rangle = A$. To get this, since $E = F(\alpha)$ and $[E : F] = n$, the smallest integer k such that $\alpha^k \in F^\times$ is $k = n$. Notice that this implies that the order of $\alpha F^\times$ in $A/F^\times$ must be n. Notice as well that we have $\mathrm{Gal}(E/F) \cong A/F^\times$, and since the extension has degree n we get that $|\mathrm{Gal}(E/F)| = n$, so that $\langle \alpha F^\times \rangle = A/F^\times$. This gives the problem. □

Problem 48. Let F be the field containing n distinct nth roots of 1. Let N be a subgroup of $F^\times$ such that $F^{\times,n} \subset N \subset F^\times$, recalling that

$$F^{\times,n} = \{\alpha^m : \alpha \in F^\times\}.$$

Show that there is a Kummer extension E/F such that if

$$A = A_n(E) = \{\alpha \in E^\times : \alpha^n \in F^\times\}$$

and

$$A^n = \{\alpha \in F^\times : a = \alpha^n \text{ with } \alpha \in A\},$$

then $A^n = N$ and the exponent m of $G = \mathrm{Gal}(E/F)$ divides n.

Proof. Consider the group $F^\times/F^{\times,m}$. Since $F^{\times,n} \subset N \subset F^\times$, we have that $N/F^{\times,m}$ is a subgroup of $F^\times/F^{\times,m}$. Let $\alpha_1, \ldots, \alpha_t$ be the coset representatives for $N/F^{\times,m}$. Consider the field

$$E = F(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_t}).$$

The first claim is that this is a Kummer extension. By construction, we see that E is a splitting field of

$$f(x) = (x^n - \alpha_1) \cdots (x^n - \alpha_r),$$

since $x^n - \alpha_k = \prod_j (x - z_j\alpha_k)$ and $\{z_1, \ldots, \ldots z_n\}$ denote the n nth roots. Hence, E is a splitting field over F of a separable polynomial, so E/F is a finite Galois extension.

We now need to show that the Galois group is abelian. Let $\sigma, \tau \in \mathrm{Gal}(E/F)$, $a_i^n = \alpha_i$. We see that $\sigma(a_i) = z_{\sigma(i)}a_i$ and $\tau(a_i) = z_{\tau(i)}a_i$ (these must send a_i to another root, which will be $z_{\sigma(i)}$ depending on the automorphism σ). Hence, we see that

$$\sigma\tau(a_i) = z_{\tau(i)}z_{\sigma(i)}a_i = \tau\sigma(a_i).$$

Since these are linearly extended based on these elements, we see that this implies that these commute as functions, so $\mathrm{Gal}(E/F)$ is abelian.

Finally, let m be the exponent of $\mathrm{Gal}(E/F)$. Notice that

$$\sigma^m(a_i) = z_{\sigma(i)}^m a_i = a_i.$$

So the exponent divides n. Furthermore, this is a Kummer extension of F.

Now, we need to show that $A^n = N$. We have $a_i = \sqrt[n]{\alpha_i} \in A$. Since we have $E = F(a_1, \ldots, a_t)$, we get that the cosets $a_iF^\times$ generate $A/F^\times \cong \hat{G} \cong G$ via **Claim 2** from the lecture notes. So this implies that $A^n/F^{\times,n} \cong A/F^\times \cong N/F^{\times,n}$, and we see that the generators for $A^n/F^{\times,n}$ generate $N/F^{\times,n}$ and vice versa. Thus, $N = A^n$, as desired.

□

Problem 49. Let F be a field containing n distinct nth roots of 1. Show that there exists an order preserving bijection

$$\left\{\begin{matrix}\text{subgroups } N \\ F^{\times,n} \subset N \subset F^\times \\ N/F^{\times,n} \text{ finite}\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{abelian extensions } E/F \\ \text{of exponent } m \mid n\end{matrix}\right\}$$

where $N \mapsto E(N) = F(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_t})$, $b_1, \ldots, b_t$ are coset representatives for $N/F^{\times,n}$ and $E \mapsto A_n(E)^n$.

Proof. In the prior problem, we established that subgroups N correspond to abelian extension E/F of exponent $m \mid n$. Furthermore, in the latter half of the proof, we established that $A_n(E)^n = A^n = N$, establishing that this is a bijection. We need to check that this is order preserving; i.e. we have $F^{\times,n} \subset N \subset M \subset F^\times$ iff $F \subset E \subset E'$, where E and E' are the unique fields corresponding to N and M respectively.

Assume that $N \subset M$, then $N/F^{\times,n} \subset M/F^{\times,n}$, so we can choose coset representatives $b_1, \ldots, b_t$, $b_{t+1}, \ldots, b_s$ so that $b_1, \ldots, b_t$ are representatives for $N/F^{\times,n}$ and $b_1, \ldots, b_s$ are representatives for $M/F^{\times,n}$. Hence, we get that we have corresponding field extensions $E = E(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_t})$, $E' = (\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_s})$, and we get that $E \subset E'$.

Similarly, if $E \subset E'$, where $E' = (\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_s})$, then we get that E is of the form $E = (\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_t})$ (after maybe relabeling), so the coset representatives for $N/F^{\times,n}$ are contained in the set of coset representatives for $M/F^{\times,m}$, so we get that

$$N = b_1F^{\times,n} \cup \cdots \cup b_tF^{\times,n} \subset b_1F^{\times,n} \cup \cdots \cup b_sF^{\times,n} = M.$$

Hence, we have that the bijection is order preserving. □

Problem 50. Let F be a field of characteristic $p \neq 0$. Let $E = F(\gamma_1, \ldots, \gamma_t)$, where each γ_i satisfies an Artin-Schreier equation of the form $x^p - x - c_i$ with $c_i \in F$. Show that E is an abelian extension of F of exponent p.

Proof. Recall that an extension is abelian if the Galois group is abelian. The goal, then, is to show that $\mathrm{Gal}(E/F)$ is abelian, and the exponent of the group is p. Consider

$$p_{\gamma_i}(x) = x^p - x - c_i.$$

Notice that if γ_i is a root of this polynomial, then so is $\gamma_i + k$ for $1 \leq k \leq p-1$, since

$$p_{\gamma_i}(x) = (\gamma_i + k)^p - (\gamma_i + k) - c_i = p_{\gamma_i}(\gamma_i) + k^p - k = 0.$$

So we have p roots for p_{γ_i}, and all of these are in E. Hence, in E we have that this splits as

$$p_{\gamma_i}(x) = \prod_{k=0}^{p}(x - \gamma_i - k).$$

Notice that $p_{\gamma_i}(x)$ is irreducible in $F[x]$, since if it weren't then we would have

$$\prod_{k=0}^{j}(x - \gamma_i - k) \in F[x],$$

and expanding with the binomial theorem, we see that $(-\gamma_i - k)^t \in F$ for $0 \leq t \leq j$, which gives a contradiction assuming that $\gamma_i \notin F$ (taking, for example, $t = 1$). Hence, we see that

$$p(x) = \prod_{i=1}^{t} p_{\gamma_i}(x)$$

is a polynomial such that it splits entirely in E and E contains all of its roots, and it does not have repeat roots, so E/F is Galois. Notice that we can find $\sigma \in G = \mathrm{Gal}(E/F)$ so that $\sigma(\gamma_i) = \gamma_i + 1$, since this is also a root, and so we have that all of the $\sigma \in G$ are of the form σ_i^k, where $\sigma_i^k(\gamma_i) = \gamma_i + k$, $0 \leq k \leq p-1$, and $\sigma_i^k(\gamma_j) = \gamma_j$ for $j \neq i$. From this, we see that the exponent of G is p, and we see that it is abelian, since for γ_i we have either

$$\sigma_i^k\sigma_i^l(\gamma_i) = \gamma_i + k + l \pmod p = \sigma_i^l\sigma_i^k(\gamma_i),$$

or

$$\sigma_i^k\sigma_j^l(\gamma_i) = \sigma_i + k = \sigma_j^l\sigma_i^k(\gamma_i),$$

where $j \neq i$, or

$$\sigma_r^k\sigma_j^l(\gamma_i) = \gamma_i = \sigma_j^l\sigma_r^k(\gamma_i),$$

where $r, j \neq i$. In either case, we see that the elements commute, so the extension is abelian. □

Remark. Thomas O'Hare was a collaborator.

Problem 51. Let $E = \mathbb{F}_p(x, y)$ be the field of rational functions in two variables over the field with p elements (so E is the field of fractions of the polynomial ring $\mathbb{F}_p[x, y]$.) Let $F = \mathbb{F}_p(x^p, y^p)$ be the subfield of rational functions in x^p and y^p.

(a) Show that $(E : F) = p^2$.
(b) Show that E cannot have a primitive element over F.
(c) Exhibit an infinite number of intermediate fields between F and E.

Proof. (a) The goal is to show that

$$(\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y^p)) = p^2.$$

We wish to do this via towers; that is, the goal is to show

$$(\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y)) = p, \quad (\mathbb{F}_p(x^p, y) : \mathbb{F}_p(x^p, y^p)) = p,$$

and then use the fact that

$$(\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y^p)) = (\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y)) \cdot (\mathbb{F}_p(x^p, y) : \mathbb{F}_p(x^p, y^p)).$$

Examining $\mathbb{F}_p(x^p, y)[z]$, we have that $z^p - x^p$ admits root x and is irreducible; furthermore, it is the minimal polynomial for x by an argument like in 44 (b). Thus, we have that $(\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y)) = p$. Analogously, we see that $z^p - y^p$ is a polynomial in $\mathbb{F}_p(x^p, y^p)[z]$, admits root y, and is irreducible/minimal. Hence, the index for this field extension is p, and so we get the desired result.

(b) If α is the primitive element, then we have that $F(\alpha) = E$ and $\alpha \in E$ is such that it has degree p^2. Notice that $\alpha \in E$ is of the form

$$\alpha = \sum_{i,j=0}^{n} a_{i,j} x^i y^j,$$

and so

$$\alpha^p = \left(\sum_{i,j=0}^{n} a_{i,j} x^i y^j \right)^p = \sum_{i,j=0}^{n} a_{i,j} x^{ip} y^{jp} \in \mathbb{F}_p(x^p, y^p)$$

using the fact that the underlying field has p elements. Thus, it is impossible for α to have degree p^2, so there cannot be a primitive element.

(c) Let $\alpha \in F$. Note that $F \subset F(\alpha x + y) \subset E$. We now show that for distinct elements in F, we get distinct field extensions. Consider $\alpha \neq \beta \in E$. If $F(\alpha x + y) = F(\beta x + y)$, then we see that $(\alpha x + y) - (\beta x + y) = (\alpha - \beta)x \in F(\alpha x + y)$. Thus, since $\alpha, \beta \in F$, we get that $x \in F(\alpha x + y)$, and from this we can deduce $y \in F(\alpha x + y)$ as well. So $F(\alpha x + y) = \mathbb{F}_p(x, y)$, contradicting (b). So for distinct $\alpha, \beta \in F$, we get distinct intermediate fields, and since F is an infinite field we have infinitely many intermediate fields.

□

Problem 52. Let F be a field and $\overline{F}$ be an algebraic closure of F. Let

$$\overline{F}^s = \{\alpha \in \overline{F} : \alpha \text{ is separable over } F\}.$$

(a) If $\Gamma_{\text{sep}} = \{f(x) \in F[x] : f(x) \text{ is separable and monic}\}$, show that $\overline{F}^s$ is the splitting field of Γ_{sep}.
(b) If $\alpha \in \overline{F}$ is separable over $\overline{F}^s$, show that $\alpha \in \overline{F}^s$.

Proof. (a) Let K denote the splitting field of Γ_{sep}. The monic polynomials associated to the separable elements $\alpha \in \overline{F}$ are going to be separable and monic, and hence contained in Γ_{sep}, so by definition we have that $\overline{F}^s \subset K$. For the other direction, let $\alpha \in K$. Then we have that α is the root of a separable and monic polynomial, so its associated minimal polynomial must divide this; hence, will be separable and monic. Thus, we get that $\alpha \in \overline{F}^s$. We can then identify $\overline{F}^s$ as the splitting field of all separable monic polynomials.

(b) Let $\alpha \in \overline{F}$ be separable over $\overline{F}^s$. Consider $m_\alpha(x) \in \overline{F}^s[x]$ to be its minimal polynomial. By (a), we note that $\overline{F}^s$ is a normal, separable extension, hence it is a Galois extension. Applying $G = \text{Gal}(\overline{F}^s/F)$ to m_α, we get a finite number of polynomials $f_i(x)$, $1 \leq i \leq r$ (where r is the size of the orbit), and with $f_1(x) = m_\alpha(x)$ (without loss of generality). We note that $(f_i(x), f_j(x)) = 1$ as well if $i \neq j$. We can then form $g(x) = \prod_1^r f_j(x)$ to get a polynomial in $f(x)$ which is separable and with α as a root, so we get that α is separable over F. Hence, we have that $\alpha \in \overline{F}^s$, as desired.

□

We call $\overline{F}^s$ the separable closure of F. If F is perfect or if $\text{Char}(F) = 0$, then $\overline{F}^s = \overline{F}$.

Problem 53. If E is an algebraic extension of F, show that the subset of elements of E that are separable over F form a subfield of E, call it E^s. Show that any element of E that is separable over E^s is actually contained in E^s.

Proof. By (a) of the last problem, we have that $\overline{F}^s$ is the splitting field of a set of polynomials, and moreover it is actually a field. Hence the set of elements of E that are separable over F is the set $\overline{F}^s \cap E$. The intersection of two fields is a field, so $E^s \subset E$ is a subfield.

Next, if $\alpha \in E$ is separable over E^s, then it is separable over $\overline{F}^s$, so it is in $\overline{F}^s$. Hence, $\alpha \in E \cap \overline{F}^s = E^s$. □

An algebraic extension E of F is called purely inseparable over F if $E^s = F$. An element $\alpha \in E$ is purely inseparable over F if $F(\alpha)^s = F$. Note that the above problem says that E is a purely inseparable extension of E^s.

Problem 54. If E is a finite dimensional extension of F and E^s is the subfield of separable elements of E, set $(E : F)_s = (E^s : F)$ and $(E : F)_i = (E : E^s)$. These are called the separability degree and inseparability degree of E/F respectively.

(a) If K is a finite separable extension of E, show that $(K : F)_s = (K : E)_s(E : F)_s$.

(b) If K is a finite purely inseparable extension of E, show that $(K : F)_s = (K : E)_s(E : F)_s$.

(c) If K is any finite extension of E, show that $(K : F)_s = (K : E)_s(E : F)_s$.

Proof. (a) To remove confusion, we introduce some notation. Let K_F^s be the collection of elements of K which are separable over F. Let K_E^s be the collection of elements of K which are separable over E. Let E^s be the collection of elements of E which are separable over F. Since K is a separable extension, we have that

$$(K : E) = (K_F^s : E^s),$$

by assumption. Hence, we see that

$$(K : F)_s = (K_F^s : F) = (K_F^s : E^s)(E^s : F) = (K_F^s : E^s)(E : F)_s.$$

By the remark, we have

$$(K_F^s : E^s) = (K : E) = (K_E^s : E) = (K : E)_s,$$

since K is a separable extension so $K_E^s = K$. Hence, we have that

$$(K : F)_s = (K : E)_s(E : F)_s.$$

(b) The extension is purely inseparable, so we have that $K_E^s = E$. We can write

$$(K : F)_s = (K_F^s : F) = (K_F^s : E^s)(E^s : F) = (K_F^s : E^s)(E : F)_s.$$

Now, if $\alpha \in K_F^s$, then it is separable over E as well, so $\alpha \in K_E^s$. Hence, we note that $K_F^s \subset K_E^s = E$. By **Problem 2**, we can take the separable closure with respect to F, which will preserve containment, to get that $K_F^s \subset E^s$. Notice that if $\alpha \in E^s$, then $\alpha \in K_F^s$ by extension of the fact that $E \subset K$, so we get that $E^s = K_F^s$. So $(K_F^s : E^s) = 1$, and we get

$$(K : F)_s = (E : F)_s.$$

Finally, since E/F is an inseparable extension, we get that $(K_E^s : E) = (K : E)_s = 1$, so

$$(K : F)_s = (K : E)_s(E : F)_s.$$

(c) We have that K_E^s is a finite separable extension of E. By (a), this gives us

$$(K_E^s : F)_s = (K_E^s : E)_s(E : F)_s.$$

By definition, we have $(K_E^s : E)_s = ((K_E^s)_E^s : E) = (K_E^s : E) = (K : E)_s$, so

$$(K_E^s : F)_s = (K : E)_s(E : F)_s.$$

Now, K is an inseparable extension of K_E^s by **Problem 3**, so by (b) and noting that inseparability implies that $(K : K_E^s)_s = 1$, we have

$$(K : F)_s = (K : K_E^s)_s(K_E^s : F)_s = (K : K_E^s)_s(K : E)_s(E : F)_s = (K : E)_s(E : F)_s.$$

In other words, we have the desired result.

□

Remark. Thomas O'Hare was a collaborator.

In this last set of problems, we think about the absolute Galois group of a finite field,

$$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$$

for a prime p.

Problem 55. Verify that the map ϕ_p defined by $\phi_p(x) = x^p$ is an automorphism of $\overline{\mathbb{F}}_p$ that pointwise fixes $\overline{\mathbb{F}}_p$. In other words, $\phi_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

Proof. The fact that ϕ_p fixes $\mathbb{F}_p$ is just a consequence of Fermat's little theorem (or Lagrange's theorem); if $x \in \mathbb{F}_p$ such that $x \neq 0_{\mathbb{F}_p} = 0$, then $x \in \mathbb{F}_p^\times$ (the multiplicative group), so $x^p = x$. If $x = 0$, then $0^p = 0$ still. So ϕ_p fixes $\mathbb{F}_p$.

Next, we need to establish that $\phi_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is an automorphism. We have that, for $a, b \in \overline{\mathbb{F}}_p$, $\phi_p(ab) = \phi_p(a)\phi_p(b)$, so it is a homomorphism under multiplication. Now, let $a, b \in \overline{\mathbb{F}}_p$, then we wish to show that $\phi_p(a+b) = \phi_p(a)+\phi_p(b)$. In other words, we wish to show that the characteristic of $\overline{\mathbb{F}}_p$ is p. Since $\overline{\mathbb{F}}_p$ is a extension of $\mathbb{F}_p$, we see that this forces the characteristic to be p. Hence, using the binomial theorem, we get that

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p,$$

so it is a homomorphism. Now, notice that $\phi_p(a) = 0$ implies $a^p = 0$, which forces $a = 0$, so ϕ_p is injective. For surjectivity, we fix $b \in \overline{\mathbb{F}}_p$. Notice that $x^p - b \in \overline{\mathbb{F}}_p[x]$ is a polynomial with degree ≥ 1, so it admits some root since the field is algebraically closed. Denote the root by $a \in \overline{\mathbb{F}}_p$. Hence we have that $a^p - b = 0$, or $\phi_p(a) = b$. The choice of b was arbitrary, so the map is surjective. Thus, ϕ_p is an automorphism of $\overline{\mathbb{F}}_p$ which pointwise fixes $\mathbb{F}_p$. □

Problem 56. We know that if $\mathbb{F}_{p^n}$ is a finite Galois extension of $\mathbb{F}_p$, then any $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a power of ϕ_p. From this, conclude that for any element $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p, \mathbb{F}_p)$, $\sigma|_{\mathbb{F}_{p^n}}$ coincides with a suitable power of ϕ_p restricted to ϕ_{p^n}. Show that this implies that $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \overline{\langle \phi_p \rangle}$.

Proof. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Then we have that $\sigma : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is an automorphism which fixes $\mathbb{F}_p$. Since $x^{p^n} - x \in \overline{\mathbb{F}}_p[x]$, and so all of its roots are in $\overline{\mathbb{F}}_p$, we get that $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$. Restricting σ to $\mathbb{F}_{p^n}$, we see that we get $\sigma|_{\mathbb{F}_{p^n}} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is still an automorphism, so $\sigma|_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, and by prior problems this means that $\sigma|_{\mathbb{F}_{p^n}} \in \{\phi_p^0|_{\mathbb{F}_{p^n}}, \ldots, \phi_p^{n-1}|_{\mathbb{F}_{p^n}}\}$; thus, $\sigma|_{\mathbb{F}_{p^n}} = \phi_p^k|_{\mathbb{F}_{p^n}}$ for some suitable power k. Thus, consider an open neighborhood U of σ. The goal is to show that for every open neighborhood U of σ, we have $U \setminus \{\sigma\} \cap \langle \phi_p \rangle \neq \varnothing$. Since $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ receives its topology from the restriction of $\prod_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, and the basic open sets in $\prod_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ are

$$U = \left(\prod_{\substack{n\geq 1 \\ n\neq k}} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \right) \times \overline{\sigma}_k,$$

$\overline{\sigma}_k = \sigma|_{F_{p^k}}$. Restricting U to $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, we see that this forms a basis for the topology of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. So it suffices to check it on these open sets containing σ. But we note that what we've shown establishes that for any basic open set containing σ, $U \setminus \{\sigma\} \cap \langle \phi_p \rangle \neq \varnothing$. Hence, we have that $\langle \phi_p \rangle$ is dense. □

Problem 57. We now construct an element of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ which is not in $\langle\phi_p\rangle$ by the following steps.

(a) Define a sequence $\{a_n\}_{n\in\mathbb{N}}$ by $a_n = n'x_n$, where we write $n = n'p^{\nu_n}$ with $\gcd(n', p) = 1$ and $1 = n'x_n + p^{\nu_n}y_n$. Show that $a_n \equiv a_m \pmod{m}$ whenever $m \mid n$, but there is no $a \in \mathbb{Z}$ such that $a \equiv a_n \pmod{n}$ for all n. (Note: we require $0 \leq a_n < n$, otherwise things will not be unique. This inequality makes sense in the context of the next two problems.)

(b) Let $\psi_n = \phi_p^{a_n}|_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Show that $\psi_n|_{\mathbb{F}_{p^m}} = \psi_m$ and that the ψ_n define an automorphism of ψ of $\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^n}$.

(c) Show that $\psi \notin \langle\phi_p\rangle$ by construction.

Proof. (a) If $m \mid n$, then we have that $p^{\nu_m} \mid p^{\nu_n}$, or in other words, $\nu_n \geq \nu_m$. Furthermore, since $\gcd(n', p) = \gcd(m', p) = 1$, we deduce that $m' \mid n'$. Hence, we have that $m' \mid a_m - a_n$. Now, notice that

$$a_m + y_m p^{\nu_m} = 1 = a_n + y_n p^{\nu_n}.$$

Subtracting we have that

$$a_n - a_m = y_m p^{\nu_m} - y_n p^{\nu_n}.$$

Since $\nu_m \leq \nu_n$, we can factor to get

$$a_n - a_m = p^{\nu_m}(y_m - y_n p^{\nu_n - \nu_m}).$$

Thus, $p^{\nu_m} \mid a_n - a_m$. Now, $\gcd(m', p) = 1$, so $\gcd(m', p^{\nu_m}) = 1$, and hence $m'p^{\nu_m} \mid a_n - a_m$, or $m \mid a_n - a_m$. Thus, we have that $a_n \equiv a_m \pmod{m}$.

Notice if $p \nmid n$, then $a_n = 0$. So for there to be an integer a such that $a \equiv a_n \pmod{n}$, we would have to have that a_n is a non-zero integer (since $a_p \neq 0$) divisible by infinitely many primes (since $a \equiv 0 \pmod{q}$ for all $q \neq p$ prime), which is impossible.

(b) I'm not sure if this is true as stated. Given $\psi_n := \phi_p^{a_n}|_{\mathbb{F}_{p^n}}$, the idea is to examine $\psi_n|_{\mathbb{F}_{p^m}}$. First, we need to assume that $n \geq m$, since otherwise we're not restricting down anywhere (this may be implicit in the notation). Second, it's not true that for $n \geq m$, we have $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ when viewing it all in $\overline{\mathbb{F}}_p$. Every intermediate field between $\mathbb{F}_p$ and $\mathbb{F}_{p^n}$ needs to have order p^d, where $d \mid n$. This also, however, may be implicit in the notation. In this case, we assume that $\mathbb{F}_p \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$ so that $m \mid n$. In this case, $\psi_n|_{\mathbb{F}_p^m} = \phi_p^{a_n}|_{\mathbb{F}_p^m}$. We have $\phi_p^{a_n} \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, so by restricting it down we note that $\phi_p^{a_n} \in \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$. This is cyclic and generated by $\langle\phi_p\rangle$, so we must have that $\phi_p^{a_n} = \phi_p^k$, where $a_n \equiv k \pmod{m}$ and $0 \leq k < m$ (this is just how cyclic groups work). From (a), we know that $a_n \equiv a_m \pmod{m}$, and we assumed (for uniqueness) that $0 \leq a_m < m$, so we get that $\phi_p^{a_n} = \phi_p^{a_m}$ when restricted down to $\mathbb{F}_{p^m}$, so $\psi_n|_{\mathbb{F}_{p^m}} = \psi_m$ under these assumptions. The assumptions seem reasonable, since we just want the maps to be cohesive on subfields.

We then define $\psi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ via $\psi|_{\mathbb{F}_{p^n}} = \psi_n$, recognizing that $\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^n}$. The maps are cohesive by the prior paragraph, so for any $x \in \overline{\mathbb{F}}_p$, we get that $x \in \mathbb{F}_{p^n}$ for some n, and hence $\psi(x) = \psi_n(x)$ is well-defined. It is a homomorphism by the same reason; if $x, y \in \overline{\mathbb{F}}_p$, there is some n so that $x, y \in \mathbb{F}_{p^n}$, and then ψ_n is an automorphism on $\mathbb{F}_{p^n}$, so

$$\psi(x + y) = \psi_n(x + y) = \psi_n(x) + \psi_n(y) = \psi(x) + \psi(y),$$

$$\psi(xy) = \psi_n(xy) = \psi_n(x)\psi_n(y) = \psi(x)\psi(y).$$

Finally, the kernel of ψ is trivial, since if $x \in \mathrm{Ker}(\psi)$, $x \in \mathrm{Ker}(\psi_n)$ for some n, and $\mathrm{Ker}(\psi_n) = 0$ for all n. For surjectivity, fix $y \in \overline{\mathbb{F}}_p$. We have that $y \in \mathbb{F}_{p^n}$ for some n sufficiently large, and since ψ_n is an automorphism there exists an $x \in \mathbb{F}_{p^n}$ so that $\psi_n(x) = y$, hence $\psi(x) = y$. The choice of y was arbitrary, so the map is surjective, and hence an automorphism.

(c) This just follows from an application of (a). If $\psi \in \langle \phi_p \rangle$, then $\psi = \phi_p^a$ for some integer a, but this implies that $a \equiv a_n \pmod{n}$ for all n, and we saw this was impossible. Thus, $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \setminus \langle \phi_p \rangle$.

□

Problem 58. Let $\mathcal{C}$, $\mathcal{D}$ be categories. Define the product category, and prove that it is indeed a category.

Proof. The product category, denoted $\mathcal{C} \times \mathcal{D}$, is the category with objects $\text{Ob}(\mathcal{C} \times \mathcal{D}) = \text{Ob}(\mathcal{C}) \times \text{Ob}(\mathcal{D})$ and for (A, B), $(A', B') \in \text{Ob}(\mathcal{C} \times \mathcal{D})$, we have $\text{Hom}((A, A'), (B, B')) = \text{Hom}(A, B) \times \text{Hom}(A', B')$, where here $A, A' \in \mathcal{C}$, $B, B' \in \mathcal{D}$. We need to show that this satisfies the axioms of being a category.

- It's clear that the product of classes is a class[1] so we have that $\text{Ob}(\mathcal{C} \times \mathcal{D})$ is a class.
- The product of sets is a set, so we have that $\text{Hom}((A, A'), (B, B'))$ is a set.
- We have composition: for each triple of objects $((A, A'), (B, B'), (C, C'))$ there is a map $\text{Hom}((A, A'), (B, B')) \times \text{Hom}((B, B'), (C, C')) \to \text{Hom}((A, A'), (C, C'))$ given by $((f, f'), (g, g')) \mapsto (gf, g'f')$ (inherited from the original categories).
- We check that the product given by $(f, f') \cdot (g, g') = (f \cdot g, f' \cdot g')$ (where the products here are in the underlying categories) satisfy the desired three axioms:
  (1) (Associative) We have that $(f, f') \cdot ((g, g') \cdot (h, h')) = (f, f') \cdot (g \cdot h, g' \cdot h') = (f \cdot (g \cdot h), f' \cdot (g' \cdot h')) = ((f \cdot g) \cdot h, (f' \cdot g') \cdot h') = ((f \cdot g), (f' \cdot g')) \cdot (h, h') = ((f, f') \cdot (g, g')) \cdot (h, h')$.
  (2) (Identity) We have that for $\text{Hom}((A, A'), (A, A'))$ there is an identity $1_{(A,A')}$ given by $1_{(A,A')} = (1_A, 1'_A)$. We check that this satisfies the desired properties:
  For $(f, f') \in \text{Hom}((A, A'), (B, B'))$ we have that $1_{(A,A')} \cdot (f, f') = (f, f')$ by construction.
  Similar other direction.
  (3) (Disjoint) Clear from construction.

□

Problem 59 (Section 1.1, Exercise 1)**.** Show that the following data define a category **Ring***: $\text{Ob}(\textbf{Ring}^*)$ is the class of rings; if R and S are rings, then $\text{Hom}_{\textbf{Ring}^*}(R, S)$ is the set of homomorphisms and anti-homomorphisms of R into S; gf for morphisms is the composite g following f for the maps f and g, and 1_R is the identity map on R.

Proof. To show it's a category, we go through the axioms.

- By construction, $\text{Ob}(\textbf{Ring}^*)$ is a class.
- The collection of homomorphims between two rings is a set, and the collection of anti-homomorphisms between two rings is a set. The union of two sets is a set, so we have that $\text{Hom}_{\textbf{Ring}^*}(R, S)$ is a set.
- Since the product is defined by composition, we have that the composition map property is satisfied: for the triple of objects R, S, and T, we have that there is a map $\text{Hom}_{\textbf{Ring}^*}(R, S) \times \text{Hom}_{\textbf{Ring}^*}(S, T) \to \text{Hom}_{\textbf{Ring}^*}(R, T)$ defined by $(f, g) \mapsto g \circ f$. Notice that if g and f are both homomorphisms, this is a homomorphism, and if g and f are both anti-homomorphisms, then this is an anti-homomorphism. If f is a homomorphism, g is an anti-homomorphism, then $g \circ f(xy) = g(f(x)f(y)) = g(f(y))g(f(x))$, so $g \circ f$ is an anti-homomorphism, and if f is an anti-homomorphism and g is a homomorphism then $g \circ f$ is an anti-homomorphism. So this is indeed a map.
- We check that the product satisfies the three axioms:
  (1) (Associative) It follows that $f \circ (g \circ h) = (f \circ g) \circ h$ from prior examples.

[1] Or is it?

(2) (Identity) The identity morphism $1_R \in \mathrm{Hom}_{\mathbf{Ring}^*}(R,R)$ is an identity morphism. To see this, if $f \in \mathrm{Hom}_{\mathbf{Ring}^*}(R,S)$, then we have $f \circ 1_R = f$, and if $g \in \mathrm{Hom}_{\mathbf{Ring}^*}(S,R)$, then $1_R \circ f = f$.
(3) (Disjoint) If $(A,B) \neq (R,S)$, then we have $\mathrm{Hom}_{\mathbf{Ring}^*}(A,B) \neq \mathrm{Hom}_{\mathbf{Ring}^*}(R,S)$, since $\mathrm{Hom}_{\mathbf{Ring}}(A,B) \neq \mathrm{Hom}_{\mathbf{Ring}}(R,S)$.

So we get that it's a category. □

Problem 60 (Section 1.1, Exercise 2)**.** By a *ring with involution* we mean a pair (R,j) where R is a ring (with unit) and j is an involution in R; that is, if $j(a) = a^*$, then $(a+b)^* = a^* + b^*$, $(ab)^* = b^*a^*$, $1^* = 1$, $(a^*)^* = a$. (Give some examples.) By a *homomorphism* of a ring with involution (R,j) into a second one (S,k) we mean a map η of R into S such that η is a homomorphism of R into S (sending 1 to 1) such that $\eta(j(a)) = k(\eta(a))$ for all $a \in R$. Show that the following data defines a category **Rinv**: Ob(**Rinv**) is the class of rings with involution; if (R,j) and (S,k) are rings with involution, then $\mathrm{Hom}_{\mathbf{Rinv}}((R,j),(S,k))$ is the set of homomorphisms of (R,j) into (S,k); gf for morphisms is the composite of maps; $1_{(R,j)} = 1_R$.

Proof. We skim over some of the details here (see prior two problems for the details). We check that the composition of homomorphisms is still a homomorphism; that is, if $\eta \in \mathrm{Hom}_{\mathbf{Rinv}}(R,S)$, $\gamma \in \mathrm{Hom}_{\mathbf{Rinv}}(S,T)$, then we need to show that $\gamma \circ \eta$ is a homomorphism still. It's still a homomorphism, so it suffices to show that it satisfies the involution property; $\gamma \circ \eta(j(a)) = \gamma(\eta(j(a)) = \gamma(j(\eta(a))) = j(\gamma(\eta(a)))$ (could also do this by commutativity of diagrams). The identity and associativity and everything is the same. □

Problem 61. Prove the following claims:

(1) If $f : A \to B$ and $g : B \to c$ and f and g are monic (epic), then gf is monic (epic).
(2) If $f : A \to B$ and $g : B \to C$ and gf is monic (epic), then f is monic (g is epic).
(3) If f has a section then f is epic, and if f has a retraction then f is monic.

Proof. (1) Recall that monic means left cancellation. Let $g_1, g_2 \in \mathrm{Hom}(D,A)$, then we wish to show that $(gf) \circ g_1 = (gf) \circ g_2$ implies $g_1 = g_2$. Since g is monic, we have that $fg_1 = fg_2$, and since f is monic, we have that $g_1 = g_2$. Hence, gf is monic.

Assume now that these are all epic. Let $g_1, g_2 \in \mathrm{Hom}(C,D)$. Then we want to show that $g_1(gf) = g_2(gf)$ implies $g_1 = g_2$. Since f is epic, we get that $g_1 g = g_2 g$, and since g is epic, we get that $g_1 = g_2$. Hence, gf is epic.

(2) Assume gf is monic. Let $g_1, g_2 \in \mathrm{Hom}(D,A)$. Then we have that $(gf)g_1 = (gf)g_2$ implies $g_1 = g_2$. We wish to show that $fg_1 = fg_2$ implies $g_1 = g_2$. All we have to do here is apply g to both sides to get $gfg_1 = gfg_2$ which gives $g_1 = g_2$.

Assume gf is epic. Let $g_1, g_2 \in \mathrm{Hom}(C,D)$. We wish to show that g is epic; i.e. if $g_1 g = g_2 g$ implies $g_1 = g_2$. Applying f to the right of both sides gives $g_1 gf = g_2 gf$, and since gf is epic we get that $g_1 = g_2$, as desired.

(3) If $f \in \mathrm{Hom}(A,B)$ has a section, then this means that there exists a $g \in \mathrm{Hom}(B,A)$ so that $fg = 1_B$. We wish to show that f is epic; that is, if $g_1, g_2 \in \mathrm{Hom}(B,A)$, and $g_1 f = g_2 f$, then $g_1 = g_2$. Applying g to the right hand side of both gives $g_1 fg = g_2 fg$, and since $fg = 1_B$, we get $g_1 = g_2$. Same idea for monic.

□

Problem 62. Show that a morphism in **R-mod** is monic (epic) if and only if the map of the underlying set is injective (surjective).

Proof. We show that f is injective if and only if it is monic.
($\implies$) : If f is injective, we have that it is monic on the level of **Set**, which then gives us that it is monic on the level of **R-mod**.

($\Longleftarrow$) : We proceed by the contrapositive. Assume that $f : A \to B$ is not injective. Then we have that $\mathrm{Ker}(f) \neq 0$. We can form a map $g : \mathrm{Ker}(f) \hookrightarrow A$ which is the canonical injection; i.e., $g(x) = x$. We have that $f \circ g = 0$. We can also form the zero map $h : \mathrm{Ker}(f) \to A$ such that $h(x) = 0$, and we have $f \circ h = 0$. So $f \circ g = f \circ h$, but $g \neq h$.

We now show that f is surjective if and only if it is epic.
($\Longrightarrow$) : If f is surjective, we have that it is epic on the level of **Set**, which then extends to epic on the level of **R-mod**.
($\Longleftarrow$) : We proceed by the contrapositive. Assume that $f : A \to B$ is not surjective. We want to show that it is not epic. We construct the *cokernel*, $C = B/f(A)$. There is a canonical map $g : B \to B/f(A)$ via $g(x) = x + f(A)$. Notice that $g \circ f = 0$. We construct $h : B \to B/f(A)$ to be the zero map, and we notice that $h \circ f = 0$. Notice that $g \circ f = h \circ f$ but $g \neq h$. □

Problem 63. Show that a morphism in **Grp** is monic (epic) if and only if the map of the underlying set is injective (surjective).

Proof. The proof of this is almost analogous □

Problem 64. Let R be a ring, $M_n(R)$ a ring. Show that **mod-R** and **mod-M_n(R)** are equivalent.

$$a = ((a_1' e_{11})e_{11}, (a_1' e_{11})e_{21}, \ldots, (a_1' e_{11})e_{n1}) + \cdots + ((a_n' e_{1n})e_{11}, \ldots, (a_n' e_{1n})e_{n1})$$

Proof. Recall that we have the following theorem:

Theorem 2. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor. Then there exists a functor $G : \mathcal{D} \to \mathcal{C}$ such that (F, G) determines an equivalence of categories iff

(1) F is faithful.
(2) F is full.
(3) F is "essentially surjective" - in other words, given any object $A \in \mathrm{Ob}(\mathcal{D})$, there exists an object $A' \in \mathrm{Ob}(\mathcal{C})$ such that $\mathrm{Hom}_{\mathcal{D}}(A, F(A'))$ contains an isomorphism.

So to show these two categories are equivalent, it suffices to construct a functor satisfying the last three properties. Let $F :$ **mod-R** $\to$ **mod-M_n(R)** be defined on objects by $F(M) = M^{(n)} = M \oplus \cdots \oplus M$, and defined on morphisms by $F(f) = f^{(n)} : M^{(n)} \to N^{(n)}$ where $f^{(n)}(a_1, \ldots, a_n) = (f(a_1), \ldots, f(a_n))$. We check that this satisfies the properties of being a functor. We've seen the first two axioms are required, so we need only check the last two.

(1) Let $g \circ f$ be defined in **mod-R**. We wish to show that $F(g \circ f) = F(g) \circ F(f)$. We have initially that $F(g \circ f) = (g \circ f)^{(n)}$, which is defined on elements via

$$(g \circ f)^{(n)}(a_1, \ldots, a_n) = ((g \circ f)(a_1), \ldots, (g \circ f)(a_n)).$$

Element-wise, we have

$$(g \circ f)(x) = g(f(x)),$$

so we rewrite this accordingly;

$$(g \circ f)^{(n)}(a_1, \ldots, a_n) = (g(f(a_1)), \ldots, g(f(a_n))) = g^{(n)}(f(a_1), \ldots, f(a_n)) = (g^{(n)} \circ f^{(n)})(a_1, \ldots, a_n).$$

This holds for all elements, so we win.

(2) We wish to show that $F(1_A) = 1_{F(A)}$. Notice that

$$F(1_A) = (1_A)^{(n)},$$

and checking this on elements, we have

$$(1_A)^{(n)}(a_1, \ldots, a_n) = (1_A(a_1), \ldots, 1_A(a_n)) = (a_1, \ldots, a_n) = 1_{F(A)}(a_1, \ldots, a_n).$$

Hence, we have equality.

So this is indeed a functor. We now need to show that this induces an equivalence of categories. We go through the three properties.

(1) (Faithful) We wish to show that it is faithful. In other words, we wish to show that $F : \mathrm{Hom}_{\mathbf{mod\text{-}R}}(A, B) \to \mathrm{Hom}_{\mathbf{mod}\text{-}M_n(\mathbf{R})}(F(A), F(B))$ is injective. Assume that $f^{(n)} = g^{(n)}$, we get that $f = g$ on all elements, so $f = g$.

(2) (Full) We wish to show that it is full. In other words, we wish to show that $F : \mathrm{Hom}_{\mathbf{mod\text{-}R}}(A, B) \to \mathrm{Hom}_{\mathbf{mod}\text{-}M_n(\mathbf{R})}(F(A), F(B))$ is surjective. Let $g \in \mathrm{Hom}_{\mathbf{mod}\text{-}M_n(\mathbf{R})}(F(A), F(B))$. Define $f \in \mathrm{Hom}_{\mathbf{mod\text{-}R}}(A, B)$ to be g in the first component. We wish to show that $F(f) = f^{(n)} = g$. Notice that we have $(x, 0, \ldots, 0)e_{1i} = (0, \ldots, x, \ldots, 0)$, so $g((x, 0, \ldots, 0)e_{1i}) = g((x, 0, \ldots, 0))e_{1i} = f(x)e_{1i} = (0, \ldots, f(x), \ldots, 0)$. Thus, we have that $g = f^{(n)}$.

(3) (Essentially surjective) Take $M' \in \mathrm{Ob}(\mathbf{mod}\text{-}M_n(\mathbf{R}))$. We wish to show there is a $M \in \mathrm{mod}\ (\mathbf{mod\text{-}R})$ so that $F(M) \cong M'$. Given $M' \in \mathrm{Ob}(\mathbf{mod}\text{-}M_n(\mathbf{R}))$, we can make it into a right R-module via the action $M'a = M'a'$, where a' is the diagonal matrix with a's along the diagonal. Set $M = M'e_{11}$. This is an R-submodule of M', since it's a closed subgroup and it is clearly closed under the action (we have $Ma = M'e_{11}a = M'ae_{11} \subset M'e_{11} = M$). We construct a map

$$f : M' \to FM = M^{(n)}$$

via

$$f(x) = (xe_{11}, xe_{21}, \ldots, xe_{n1}).$$

We check that this is a $M_n(R)$-homomorphism: If $x, y \in M'$, we have

$$f(x + y) = ((x + y)e_{11}, \ldots, (x + y)e_{n1}) = (xe_{11}, \ldots, xe_{n1}) + (ye_{11}, \ldots, ye_{n1}) = f(x) + f(y).$$

If $r \in R$, we have

$$f(xr) = (xe_{11}, \ldots, xe_{n1})r = f(x)r.$$

So this is indeed a module homomorphism. We then check that this is bijective. For injectivity, we note that $\mathrm{Ker}(f) = \{x \in M' : f(x) = 0\} = \{x \in M' : xe_{i1} = 0 \text{ for all } 1 \leq i \leq n\}$. Then $x' = \sum x'e_{ii} = \sum x'e_{i1}e_{1i} = \sum 0 = 0$, so the only element in the kernel is the trivial element. For surjectivity, take $a \in F(M) = M^{(n)}$. We have $a = (a_1, \ldots, a_n)$, $a_i \in M'e_{11}$, so we can write

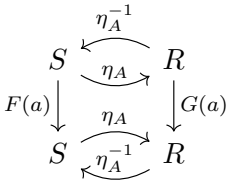
$$a = ((a'_1e_{11})e_{11}, (a'_1e_{11})e_{21}, \ldots, (a'_1e_{11})e_{n1}) + \cdots + ((a'_ne_{1n})e_{11}, \ldots, (a'_ne_{1n})e_{n1})$$

□

Problem 65 (Section 1.3, Exercise 4)**.** Let G be a group, $\underline{G}$ the one object category determined by G. Show that a functor from $\underline{G}$ to **Set** is the same thing as a homomorphism of G into the group $\mathrm{Sym}(S)$ of permutations of a set S, or, equivalently, as an action of G on S. Show that two such functors are naturally isomorphic if and only if the actions of G are equivalent.

Proof. We first show that a functor from $\underline{G}$ to **Set** is the same thing as a homomorphism of G into the group $\mathrm{Sym}(S)$. Notice that we must have our functor send objects to objects, so we have that $F(A) = S$ for some set S. Next, we note that homomorphisms are sent to homomorphisms, so we have that $F : G = \mathrm{Hom}_{\underline{G}}(A, A) \to \mathrm{Hom}_{\mathbf{Set}}(S, S) = \mathrm{Sym}(S)$. Notice that this map satisfies the property that $F(1_G) = 1$, the identity function from S to S, and that we have $F(ab) = F(a)F(b)$ for all $a, b \in G$. Thus, this is a homomorphism of G into $\mathrm{Sym}(S)$. Recall that this is equivalent to an action of G on S.

Let $F, G : \underline{G} \to \mathbf{Set}$ be two functors such that $F \cong G$; i.e., they are naturally isomorphic. Then we have that the natural transformation corresponds to an isomorphism $\eta_A \in \mathrm{Hom}(S, R)$, where $F(A) = S$, $G(A) = R$. That is to say, we have that the following diagram is commutative;



Since there is a bijection of R and S, we have that there is an isomorphism, and since this respects the structure of F and G (by commutativity), we get that

$$F(a) \circ \eta_A = \eta_A \circ G(a).$$

In terms of actions, we have that

$$F(a)(\eta_A(x)) = \eta_A(G(a)(x)),$$

i.e. the actions commute with the bijection.

Assuming that we have an equivalence of actions, we have a bijection $\psi : S \to R$ such that $\psi(gx) = g\psi(x)$. Notice that the actions give us functors $F, G : \underline{G} \to \mathbf{Set}$, and this commutativity of the action tells us that

$$\psi(F(g)(x)) = G(g)(\psi(x)).$$

In other words, we have that the diagram commutes. So we get a natural isomorphism between functors. □

Problem 66 (Section 1.4, Exercise 1)**.** Let (F, G) be an equivalence of $\mathcal{C}$ into $\mathcal{D}$, and let $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. Show that any one of the following properties of f implies the same property for $F(f)$: f is monic, epic, has a section, has a retraction, is an isomorphism.

Proof. We go through the properties. By the theorem, we have that an equivalence of categories corresponds to F being fully faithful and essentially surjective.

(1) (Monic) Assume that f is monic. Then for any $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(B, D)$, we have that $f \circ g_1 = f \circ g_2 \implies g_1 = g_2$. We wish to show this for $F(f)$ as well. That is, if we have $g_1, g_2 \in \mathrm{Hom}_{\mathcal{D}}(F(B), D)$, then $F(f) \circ g_1 = F(f) \circ g_2$ implies $g_1 = g_2$. Since F is full and essentially surjective, we have that there exists h_1, h_2 such that $F(h_1) = g_1$, $F(h_2) = g_2$, so $F(f) \circ F(h_1) = F(f \circ h_1) = F(f \circ h_2) = F(f) \circ F(h_2)$. Notice that faithful implies $f \circ h_1 = f \circ h_2$, which tells us that $h_1 = h_2$. Thus, we have that $F(h_1) = g_1 = g_2 = F(h_2)$.

(2) (Epic) Assume that f is epic. Then for any $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(B, D)$, we have that $g_1 \circ f = g_2 \circ f \implies g_1 = g_2$. We wish to show this for $F(f)$ as well. That is, if we have $g_1, g_2 \in \mathrm{Hom}_{\mathcal{D}}(F(B), D)$, then $g_1 \circ F(f) = g_2 \circ F(f)$ implies $g_1 = g_2$. Since F is full and essentially surjective, we have that there exists h_1, h_2 such that $F(h_1) = g_1$, $F(h_2) = g_2$, so $F(h_1) \circ F(f) = F(h_1 \circ f) = F(h_2 \circ f) = F(h_2) \circ F(f)$. Notice that faithful implies $h_1 \circ f = h_2 \circ f$, which tells us that $h_1 = h_2$. Thus, we have that $F(h_1) = g_1 = g_2 = F(h_2)$.

(3) Assume that $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ has a section; i.e., a $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ with $f \circ g = 1_A$. We wish to show that $F(f)$ has a section. Notice that $F(f \circ g) = F(1_A) = 1_{F(A)}$, and we have $F(f \circ g) = F(f) \circ F(g)$. So $F(f)$ has a section.

(4) By the same argument, if f is a retraction, there exists a g with $g \circ f = 1_A$, and so the functor takes this to a retraction.

(5) Let $f : A \to B$ be an isomorphism, then there is a unique $g : B \to A$ so that $fg = 1_B$, $gf = 1_A$. Then we have that $F(f)$ has inverse $F(g)$; to see this, we note that $F(fg) = F(f)F(g) = 1_{F(B)}$, and $F(gf) = F(g)F(f) = 1_{F(A)}$. Hence, $F(f)$ is also an isomorphism.

□

Problem 67 (Section 1.5, Exercise 1)**.** Let S be a POSET and $\underline{S}$ the associated category; i.e., let $\underline{S}$ be such that $\mathrm{Ob}(\underline{S})$ are the elements in S, and we have

$$\mathrm{Hom}_{\underline{S}}(a,b) = \begin{cases} i_{ab} \text{ if } a \leq b \\ 0 \text{ if } a > b. \end{cases}$$

Let $\{a_i : i \in I\}$ be an indexed set of elements of S. Give a condition on $\{a_i\}$ that the corresponding set of objects in $\underline{S}$ has a product (coproduct). Use this to construct an example of a category in which every finite subset of objects has a product (coproduct) but in which there are infinite sets of objects that do not have a product (coproduct).

Proof. We will focus on products – coproducts will have the same kind of argument. Recall that the categorical definition of product for $\{a_i\}$ in $\underline{S}$ is that there exists a $b \in \mathrm{Ob}(\underline{S})$ so that there are a family of homomorphisms $f_{ba_i} : b \to a_i$ where if c is any object so that c has a family of morphisms $g_{ca_i} : c \to a_i$, then there exists a unique morphism $f_{cb} : c \to b$. Notice that in the context of the partially ordered set, this is saying that there exists an element $b \in S$ so that $b \leq a_i$ for all i, and for which if c is any other object such that $c \leq a_i$ for all i, then $c \leq b$. So a product exists if the $\{a_i\}$ admit an infimum. Likewise, coproducts exist if the $\{a_i\}$ admit a supremum.

Consider $S = \mathbb{Z}$. Then every finite collection of objects will have a supremum or infimum, but taking an infinite collection of objects, we see that it does not necessarily need to admit either. □

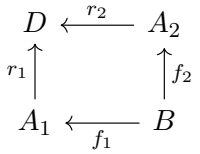
Problem 68 (Section 1.5, Exercise 2)**.** A category $\mathcal{C}$ is called a category with a product (coproduct) if any pair of objects in $\mathcal{C}$ has a product (coproduct) in $\mathcal{C}$. Show that if $\mathcal{C}$ is a category with a product, then any finitely indexed set of objects in $\mathcal{C}$ has a product (coproduct).

Proof. We will just do products, since the argument is the same. In essence, this is asking that we can induct products in this category $\mathcal{C}$. Assume, then, that we can do this for a collection of $n-1$ objects. We wish to show that we can do this for a collection of n objects; say, $A_1, \ldots, A_n$. Notice that, since we can do it for $n-1$ objects, we see that there is a product B for $A_1, \ldots, A_{n-1}$. Furthermore, we take the product of B and A_n to get a product C. We claim that this satisfies the criteria; we have a family of maps $\pi_i : C \to A_i$, where the π_i are defined appropriately if $1 \leq i \leq n-1$ through B and we have π_n defined through the product of two things. Let D be an object with a family of morphisms $f_i : D \to A_i$, $1 \leq i \leq n$. Since B is a product, we define $f : D \to C$ via $f = g \times h$, where g is the map so that D factors through B and h is the map where D factors through A_n. This is defined, since we have products for two objects, and furthermore we see that the g agrees with the maps on $A_1, \ldots, A_n$. Hence, we have that we can extend this to n objects. By induction, we can do this for all finite collections of objects. □

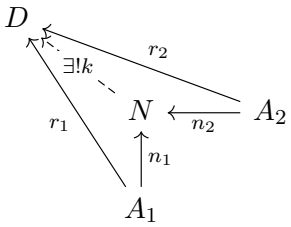
Problem 69 (Section 1.5, Exercise 8)**.** Define a pushout by dualizing pullback. Let $f_i : B \to A_i$, $i = 1, 2$ in **R-mod**. Form $A_1 \oplus A_2$. Define the map $f : B \to A_1 \oplus A_2$ via $f(b) = (-f_1(b), f_2(b))$. Let $I = \mathrm{Im}(f)$, and put $N = (A_1 \oplus A_2)/I$. Define $n_i : A_i \to N$ by $n_1(a_1) = (a_1, 0) + I$, $n_2(a_2) = (0, a_2) + I$. Verify that $\{n_1, n_2\}$ defines a pushout diagram for f_1 and f_2.

Proof. We first check that the n_i are well-defined. It suffices to do it for n_1, since they are essentially the same. Consider $a_1 = a_1'$, then $n_1(a_1) = (a_1, 0) + I = (a_1', 0) + I = n_1(a_1')$. So the maps are well-defined. They are clearly morphisms, since $n_1(a_1 + a_1') = (a_1 + a_1', 0) = (a_1, 0) + I + (a_1', 0) + I = n_1(a_1) + n_1(a_1')$, and $n_1(ra_1) = (ra_1, 0) + I = r(a_1, 0) + I$. Notice that $rI \subset I$. To see this, let $y \in \mathrm{Im}(f)$. We wish to check that $ry \in \mathrm{Im}(f)$ (establishing that $rI \subset I$). If $y \in \mathrm{Im}(f)$, there exists an x so that $f(x) = y$. Hence, $f(rx) = rf(x) = ry \in \mathrm{Im}(f)$, since f is a module homomorphism. Thus, we have that we can write $n_1(ra_1) = r[(a_1, 0) + I] = rn_1(a_1)$. So this is indeed a module homomorphism.

The goal, then, is to check that this defines a pushout diagram. Let $\{D, r_1, r_2\}$ be such that



is a commutative diagram. We wish to show that there exists a unique morphism $k : N \to D$ so that we have



commutes. Define $k((a_1, a_2) + I) = r_1(a_1) + r_2(a_2)$. We first check that this is well-defined. If $(a_1, a_2) - (a_1', a_2') \in I$, then this implies that $(a_1 - a_1', a_2 - a_2') \in \mathrm{Im}(f)$, so that there is some $b \in B$ with $f(b) = (a_1 - a_1', a_2 - a_2')$. Since $f(b) = (-f_1(b), f_2(b))$, we have that $f_1(b) = a_1' - a_1$, $f_2(b) = a_2 - a_2'$. Hence, $k((a_1 - a_1', a_2 - a_2') + I) = r_1(a_1 - a_1') + r_2(a_2 - a_2') = r_1(-f(b)) + r_2(f(b)) = -r_1(f_1(b)) + r_2(f_2(b))$. Since the diagram commutes, we have that $r_1 f_1(b)) = r_2(f_2(b))$, so we get that the above is 0. Hence, we have that k is well-defined.

It should be clear that k is a homomorphism by the fact that the r_i are homomorphisms. So we have the existence of such a map. Let $\tau : N \to D$ be another such map. Then we have that $\tau(n_2(a_2)) = r_2(a_2)$, $\tau(n_1(a_1)) = r_1(a_1)$. So for all $(a_1, a_2) + I \in N$, we get that

$$\begin{aligned} k((a_1, a_2) + I) = r_1(a_1) + r_2(a_2) = \tau(n_1(a_1)) + \tau(n_2(a_2)) = \tau(n_1(a_1) + n_2(a_2)) \\ = \tau((a_1, 0) + I + (0, a_2) + I) = \tau((a_1, a_2) + I). \end{aligned}$$

So the functions are equal, and hence we have that the function k must be unique. Thus, we have that N is the pushout of $\{B, f_1, f_2\}$. □

Problem 70 (Section 3.10, Exercise 6)**.** Show that the additive group of $\mathbb{Q}$ regarded as a $\mathbb{Z}$-module is flat.

Proof. Let $f : M \to M'$ be an injective morphism between $\mathbb{Z}$-modules. We wish to show that $\mathrm{id}_{\mathbb{Q}} \otimes f : \mathbb{Q} \otimes M \to \mathbb{Q} \otimes M'$ is injective as well. This establishes that $\mathbb{Q}$ is flat.

Recall that elements in $\mathbb{Q} \otimes M$ are of the form $\sum_1^n x_i \otimes m_i$, where $x_i \in \mathbb{Q}$ and $m_i \in M$. We can find d so that $x_i = a_i/d$ for all $1 \leq i \leq n$. We can then write this as

$$\sum_1^n x_i \otimes m_i = \sum_1^n \frac{a_i}{d} \otimes m_i = \sum_1^n \frac{1}{d} \otimes a_i m_i = \frac{1}{d} \otimes \left(\sum_1^n a_i m_i \right).$$

Assume this element is so that

$$\mathrm{id}_{\mathbb{Q}} \otimes f \left(\frac{1}{d} \otimes \left(\sum_1^n a_i m_i \right) \right) = 0,$$

then this implies that

$$\frac{1}{d} \otimes f \left(\sum_1^n a_i m_i \right) = 0.$$

Hence, this implies that $f\left(\sum_1^n a_i m_i\right)$ is a torsion element of M'; i.e., there exists a $n \in \mathbb{Z} - \{0\}$ so that

$$nf\left(\sum_1^n a_i m_i\right) = 0.$$

Using the fact that f is a $\mathbb{Z}$-module homomorphism, we have

$$f\left(\sum_1^n n a_i m_i\right) = 0,$$

and by injectivity, this implies

$$\sum_1^n n a_i m_i = 0.$$

Hence, we have

$$0 = \frac{1}{d} \otimes n \sum_1^n a_i m_i = n \sum_1^n x_i \otimes m_i,$$

so $\sum_1^n x_i \otimes m_i$ is a torsion element; i.e., it is 0. Thus, $\mathrm{Ker}(\mathrm{id}_{\mathbb{Q}} \otimes f) = 0$, and we have that it is injective, so $\mathbb{Q}$ is flat. □

For the next problem and definitions, R will be a commutative ring.

Definition. Let R be a ring, S a subset of R. We say S is a multiplicative subset of R if $1 \in S$ and S is closed under multiplication; i.e., $s, s' \in S$ implies $ss' \in S$.

Definition. Let R be a ring, S a multiplicative subset of R. We define an equivalence relation on $R \times S$ via

$$(x, s) \sim (y, t) \iff \exists u \in S \text{ such that } (xt - ys)u = 0.$$

We define x/s to be the equivalence class of (x, s), $S^{-1}R$ is the set of all equivalence classes. Define addition and multiplication in the obvious fashion;

$$x/s + y/t = (xt + ys)/st, \quad x/s \cdot y/t = (xy)/(st).$$

The ring $S^{-1}R$ is called the localization of R. We similarly define the localization of modules.

Problem 71. Let M be an R-module. Then we have that $S^{-1}R \otimes_R M \cong S^{-1}M$.

Proof. Consider the map

$$f : S^{-1}R \otimes_R M \to S^{-1}M$$

defined on pure tensors via

$$f(x/s \otimes m) = mx/s.$$

We define then

$$g : S^{-1}M \to S^{-1}R \otimes_R M$$

via

$$g(m/s) = (1/s \otimes m).$$

We check that these maps are inverses, thus giving us the isomorphism. Notice that on generators, we have

$$f(g(m/s)) = f(1/s \otimes m) = m/s,$$

and

$$g(f(x/s \otimes m)) = g(mx/s) = 1/s \otimes mx = x/s \otimes m,$$

so these are inverses. □

Problem 72. Prove that localization is exact; i.e., if we have

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

is exact, then

$$0 \to S^{-1}M' \xrightarrow{f'} S^{-1}M \xrightarrow{g'} S^{-1}M'' \to 0$$

is exact, where $f' = S^{-1}f$ is defined via $f'(x/s) = f(x)/s$.

Proof. The first thing to establish is that for a fixed multiplicative subset S, $S^{-1}\cdot : \mathbf{R\text{-}mod} \to \mathbf{S^{-1}R\text{-}mod}$. We know how it acts on objects and morphisms, so it suffices to show that $S^{-1}(fg) = S^{-1}(f)S^{-1}(g)$ and $S^{-1}(\mathrm{id}_M)$ is the identity on $S^{-1}M$. Notice that $S^{-1}(fg)(m/s) = fg(m)/s = S^{-1}(f)(g(m)/s) = S^{-1}(f)S^{-1}(g)(m/s)$, so the maps are equal. Notice that $S^{-1}(\mathrm{id}_M)(m/s) = m/s$, so the identity is mapped to the identity. Hence, localization is functorial. One can check that the construction is, in fact, an additive functor, but we choose to not do this.

We have that $S^{-1}M \cong S^{-1}R \otimes_R M$, so we can use this to get right exactness. Thus, it suffices to show injectivity. So consider $f : M \to N$ injective, it suffices to show that $S^{-1}f = f'$ is injective. This follows, since if $x/s \in \mathrm{Ker}(f')$, we have $f'(x/s) = f(x)/s = 0$, so there is some t so that $tf(x) = f(tx) = 0$. Thus, since f is injective, this implies that $tx = 0$, which tells us that $x/s = tx/ts = 0/ts = 0$, so x/s was 0 all along. Hence, the kernel is trivial, and so we have that localization is exact. □

Remark. Using this, we have that $\mathbb{Q}$ is flat by viewing it as localization!

Problem 73 (Section 3.10, Exercise 7)**.** Let R and S be rings. Let P be a finitely generated projective left R-module, M an $R - S$ bimodule, N a left S-module. Show that there is a group isomorphism

$$\eta : \mathrm{Hom}_R(P, M) \otimes_S N \to \mathrm{Hom}_S(P, M \otimes_S N)$$

such that for $f \in \mathrm{Hom}_R(P, M)$ and $y \in N$, $\eta(f \otimes y)$ is the homomorphism $\eta(f \otimes y)(x) = f(x) \otimes y$ of P into $M \otimes_S N$.

TODO. □

Problem 74. If R is a domain and R is an injective R-module, then R is a field.

Proof. We wish to show that, for all $r \in R - \{0\}$, there is some b so that $rb = 1$. Let $f : R \to R$ be an R-module homomorphism defined by $f(x) = rx$. Notice that f is injective, since $f(x) = rx = ry = f(y)$ implies that $r(x - y) = 0$, and since $r \neq 0$ this implies that $x - y = 0$, or $x = y$. We also consider $\mathrm{id}_R : R \to R$. This gives us the following diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & R & \xrightarrow{f} & R \\ & & {\scriptstyle \mathrm{id}_R}\downarrow & & \\ & & R & & \end{array}$$

Since R is an injective R-module, we see that this induces a map $h : R \to R$ so that we have the following commutative diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & R & \xrightarrow{f} & R \\ & & {\scriptstyle \mathrm{id}_R}\downarrow & \swarrow_{h} & \\ & & R & & \end{array}$$

That is, $hf = \mathrm{id}_R$. Fixing some $x \neq 0$, we see that

$$h(f(x)) = h(rx) = rxh(1) = \mathrm{id}_R(x) = x.$$

Rearranging this gives

$$x(rh(1) - 1) = 0.$$

Since $x \neq 0$, this forces

$$rh(1) = 1,$$

that is, r is invertible. The choice of r was arbitrary, so we have that this holds for all r; i.e., R is a field. □

Problem 75. If R is a domain, K its field of fractions, then K is an injective R-module.

Proof. The goal is to use Baer's criterion (see **Homework 6.1**). Let I be some left ideal. Then K is injective if we can extend any module homomorphism $f : I \to K$ to $\overline{f} : R \to K$. Fix $x \neq 0$. Since K is divisible, we have that $f(x) = xa$ for some $a \in K$. Notice that for all $r \in I$, we have

$$xf(r) = f(xr) = rf(x) = rxa,$$

and so since this is in K, we divide both sides by r to get

$$f(x) = xa.$$

We can then extend f via $\overline{f} : R \to K$ via $\overline{f}(x) = xa$. Since we've extended arbitrary f, we get that K is injective. □

Problem 76. Suppose we have a diagram of homomorphisms of complexes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C'_\cdot & \xrightarrow{\alpha} & C_\cdot & \xrightarrow{\beta} & C''_\cdot & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & D'_\cdot & \xrightarrow{\gamma} & D_\cdot & \xrightarrow{\delta} & D''_\cdot & \longrightarrow & 0 \end{array}$$

which is commutative and has exact rows. Then

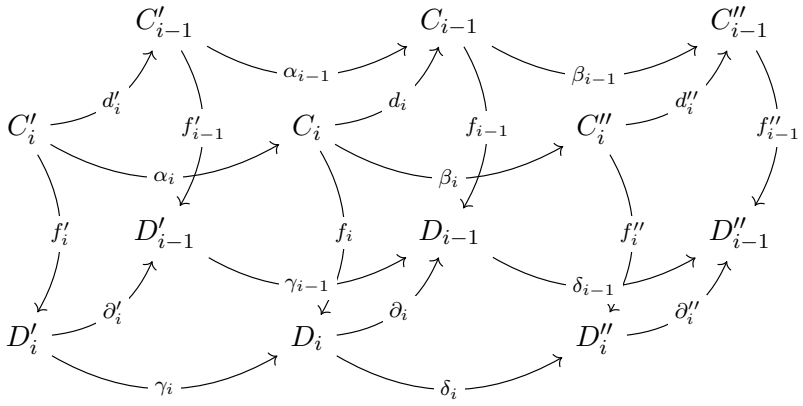
$$\begin{array}{ccc} H_i(C''_\cdot) & \xrightarrow{\Delta_i} & H_{i-1}(C'_\cdot) \\ \downarrow{\scriptstyle \widetilde{f''_i}} & & \downarrow{\scriptstyle \widetilde{f'_{i-1}}} \\ H_i(D''_\cdot) & \xrightarrow{\overline{\Delta_i}} & H_{i-1}(D'_\cdot) \end{array}$$

is commutative. That is, the connecting homomorphism is a natural transformation.

Proof. By the commutativity of the first diagram, notice that this means that

$$\begin{array}{ccccc} C'_i & \xrightarrow{\alpha_i} & C_i & \xrightarrow{\beta_i} & C''_i \\ \downarrow{\scriptstyle f'_i} & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f''_i} \\ D'_i & \xrightarrow{\gamma_i} & D_i & \xrightarrow{\delta_i} & D''_i \end{array}$$

is commutativty for all i. Let $z''_i + B''_i \in H_i(C''_\cdot)$. Then we see that $\Delta_i(z''_i + B''_i) = z'_{i-1} + B'_i$, where we have $\alpha_{i-1}(z'_{i-1}) = d(z_i)$ for some z_i with $\beta(z_i) = z''_i$. We will use this observation, along with the following commutative diagram:



With this diagram and the above observation, we see that

$$f''_i(z''_i) = f''_i(\beta_i(z_i)) = \delta_i(f_i(z_i))$$
$$= f_{i-1}(d_i(z_i)) = f_{i-1}(\alpha_{i-1}(z'_{i-1}) = \gamma_{i-1}(f'_{i-1}(z'_{i-1})).$$

So

$$\overline{\Delta_i}(\widetilde{f''_i}(z''_i + B''_i)) = \overline{\Delta_i}(f''_i(z''_i) + B''_i) = f'_{i-1}(z'_{i-1}) + B'_i$$
$$= \widetilde{f'_{i-1}}(z'_{i-1} + B'_i) = \widetilde{f'_{i-1}}(\Delta_i(z''_i + B''_i)).$$

Hence, the diagram commutes! Thus, we have the naturality of the connecting homomorphism. □

Problem 77. Let $(Q^{\cdot}, \eta)$ be an injective complex under M, $(D^{\cdot}, \eta')$ a coresolution of M', $\lambda : M' \to M$. Then there exists a homomorphism g of the complex $D^{\cdot}$ into the complex $Q^{\cdot}$ such that $\eta\lambda = g^0\eta'$. Moreover, any two such homomorphisms are homotopic.

Proof. We dualize the projective version. We inductively build the homomorphism g. First, consider

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & D^0 \\ & & \downarrow{\scriptstyle \lambda} & & \\ 0 & \longrightarrow & M & \longrightarrow & Q^0 \end{array}$$

With composition, we get an induced map

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & D^0 \\ & & \downarrow{\scriptstyle \lambda} & \swarrow & \\ 0 & \longrightarrow & M & \longrightarrow & Q^0 \end{array}$$

Now, since Q^0 is injective, we get another induced map so that

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & D^0 \\ & & \downarrow{\scriptstyle \lambda} & \swarrow & \downarrow \\ 0 & \longrightarrow & M & \longrightarrow & Q^0 \end{array}$$

is commutative. Call this new map g^0. We have that this is such that $\eta\lambda = g^0\eta'$, as desired.

Now, assume that we have $g^0, \ldots, g^{n-1}$, and we wish to build g^n. Thus, we have the following set up:

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & D^{n-2} & \xrightarrow{\partial^{n-2}} & D^{n-1} & \xrightarrow{\partial^{n-1}} & D^n & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle g^{n-2}} & & \downarrow{\scriptstyle g^{n-1}} & & & & \\ \cdots & \longrightarrow & Q^{n-2} & \xrightarrow{d^{n-2}} & Q^{n-1} & \xrightarrow{d^{n-1}} & Q^n & \longrightarrow & \cdots \end{array}$$

Consider the map $h = d^{n-1}g^{n-1}$; then we have

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & D^{n-2} & \xrightarrow{\partial^{n-2}} & D^{n-1} & \xrightarrow{\partial^{n-1}} & D^n & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle g^{n-2}} & & \downarrow{\scriptstyle g^{n-1}} \searrow^{h} & & & & \\ \cdots & \longrightarrow & Q^{n-2} & \xrightarrow{d^{n-2}} & Q^{n-1} & \xrightarrow{d^{n-1}} & Q^n & \longrightarrow & \cdots \end{array}$$

We need $\mathrm{Ker}(\partial^{n-1}) \subset \mathrm{Ker}(h)$. Doing so, we can get an induced map

$$\begin{array}{ccccc} 0 & \longrightarrow & D^{n-1}/\mathrm{Ker}(\partial^{n-1}) & \xrightarrow{\widetilde{\partial^{n-1}}} & D^n \\ & & \downarrow{\scriptstyle \widetilde{h}} & & \\ & & Q^n & & \end{array}$$

where $\widetilde{h}(x + \mathrm{Ker}(\partial^{n-1})) = h(x)$. Let $x \in \mathrm{Ker}(\partial^{n-1})$, then $\partial^{n-1}(x) = 0$. Thus, by exactness, there exists a y so that $\partial^{n-2}(y) = x$. Taking g^{n-1} of both sides, we have

$$g^{n-1}(x) = g^{n-1}(\partial^{n-2}(y)) = d^{n-2}(g^{n-2}(y)),$$

and thus applying d^{n-1} we get

$$h(x) = d^{n-1}(d^{n-2}(g^{n-2}(y))) = 0,$$

so $x \in \mathrm{Ker}(h)$, as desired. Thus, we get the induced map, and since Q^n is injective, we get an induced map

$$\begin{array}{ccccc} 0 & \longrightarrow & D^{n-1}/\mathrm{Ker}(\partial^{n-1}) & \xrightarrow{\widetilde{\partial^{n-1}}} & D^n \\ & & \downarrow{\scriptstyle \widetilde{h}} & \swarrow_{g^n} & \\ & & Q^n & & \end{array}$$

where $g^n\widetilde{\partial^{n-1}} = \widetilde{h}$. We check then that this makes

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & D^{n-2} & \xrightarrow{\partial^{n-2}} & D^{n-1} & \xrightarrow{\partial^{n-1}} & D^n & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle g^{n-2}} & & \downarrow{\scriptstyle g^{n-1}} & & \downarrow{\scriptstyle g^n} & & \\ \cdots & \longrightarrow & Q^{n-2} & \xrightarrow{d^{n-2}} & Q^{n-1} & \xrightarrow{d^{n-1}} & Q^n & \longrightarrow & \cdots \end{array}$$

commutes. Let $x \in D^{n-1}$. If $x \in \mathrm{Ker}(\partial^{n-1})$, then $g^n(\partial^{n-1}(x)) = 0 = d^{n-1}(g^{n-1}(x))$, as desired. Next, if $x \notin \mathrm{Ker}(\partial^{n-1})$, we see that $\widetilde{\partial^{n-1}}(x + \mathrm{Ker}(\partial^{n-1})) = \partial^{n-1}(x)$, $\widetilde{h}(x + \mathrm{Ker}(\partial^{n-1})) = h(x)$,, so

$$g^n(\widetilde{\partial^{n-1}}(x)) = g^n(\partial^{n-1}(x)) = h(x) = d^{n-1}(g^{n-1}(x)),$$

as desired. So it commutes!

We now check the homotopy property. Let $\alpha, \beta : D^{\cdot} \to Q^{\cdot}$ such that $\eta\lambda = \alpha^0\eta'$, $\eta\lambda = \beta^0\eta'$. We wish to check that $\gamma^n = \alpha^n - \beta^n$ is such that $\gamma^n \sim 0$. That is, we wish to construct a family of maps $\{s_i\}$ so that $\gamma^i = d^{i+1}s_i + s_{i-1}d^i$. Consider the initial set up. We have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\eta'} & D^0 & \xrightarrow{\partial^0} & D^1 & \xrightarrow{\partial^1} & \cdots \\ & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \gamma^0} & & \downarrow{\scriptstyle \gamma^1} & & \\ 0 & \longrightarrow & M & \xrightarrow{\eta} & Q^0 & \xrightarrow{d^0} & Q^1 & \xrightarrow{d^1} & \cdots \end{array}$$

We want a map $s_0 : D^1 \to Q^0$ so that $\partial^0 s_0 = \gamma^0$. Notice that $\mathrm{Ker}(\partial^0) \subset \mathrm{Ker}(\gamma^0)$, again a commutativity argument, so again we get an s_0 from this induced so that everything commutes. That is, we have our desired set up.

Assume we have found $s_0, \ldots, s_{n-1}$. Then we have

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & D^{n-2} & \xrightarrow{\partial^{n-2}} & D^{n-1} & \xrightarrow{\partial^{n-1}} & D^n & \xrightarrow{\partial^n} & D^{n+1} \\ & & {\scriptstyle \gamma^{n-2}}\downarrow & \swarrow{\scriptstyle s_{n-2}} & {\scriptstyle \gamma^{n-1}}\downarrow & \swarrow{\scriptstyle s_{n-1}} & {\scriptstyle \gamma^n}\downarrow & & \\ \cdots & \longrightarrow & Q^{n-2} & \xrightarrow[d^{n-2}]{} & Q^{n-1} & \xrightarrow[d^{n-1}]{} & Q^n & & \end{array}$$

is a commutative diagram. We wish to find s_n so that

$$\gamma^n = \partial^n s_n + d^{n-1} s_{n-1}.$$

Examine the map

$$h := \gamma^n - d^{n-1} s_{n-1} : D^n \to Q^n.$$

If $x \in \mathrm{Ker}(\partial^n)$, then $\partial^n(x) = 0$, so there is a y so that $\partial^{n-1}(y) = x$. Thus,

$$h(\partial^{n-1}(y)) = \gamma^n(\partial^{n-1}(y)) - d^{n-1}(s_{n-1}(\partial^{n-1}(y))).$$

By commutativity, $\gamma^n(\partial^{n-1}(y)) = d^{n-1}(\gamma^{n-1}(y))$, so we have

$$d^{n-1}(\gamma^{n-1}(y) - s_{n-1}(\partial^{n-1}(y))) = d^{n-1}(d^{n-2}(s_{n-2}(y)) = 0,$$

so $x \in \mathrm{Ker}(h)$. Hence, we get an induced map $s_n : D^{n+1} \to Q^n$ so that $\partial^n s_n = h = \gamma^n - d^{n-1} s_{n-1}$, so $\gamma^n = \partial^n s_n + d^{n-1} s_{n-1}$, as desired. Thus, this is a homotopy, and so we get that $\gamma \sim 0$, or $\alpha \sim \beta$. $\square$