210B Discussion Notes

Jung Joo Suh

Winter 2023

Discussion 1 - Category Theory Review

Definition 1 (Category)**.** A (locally small) category $\mathcal{C}$ consists of the following info:

(I) A class of objects $\mathrm{Obj}(\mathcal{C})$

(II) For each $X, Y \in \mathrm{Obj}(\mathcal{C})$, a set $\mathrm{Hom}(X, Y)$ of all morphisms "arrows from X to Y"

(III) A composition map $\circ : \mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, Z) \to \mathrm{Hom}(X, Z)$ satisfying the following:

(a) (Associativity) For all f, g, h, $(h \circ g) \circ f = h \circ (g \circ f)$

(b) (Identity) For every $X \in \mathrm{Obj}(\mathcal{C})$, there exist $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ such that for all f, g, $f \circ \mathrm{id}_X = f$ and $\mathrm{id}_X \circ g = g$. It's a quick exercise that such element id_X is in fact, unique for all X.

Definition 2 (Functor)**.** Let $\mathcal{C} \to \mathcal{D}$ be categories. A functor $F : \mathcal{C} \to \mathcal{D}$ consists of a following data:

(I) $F : \mathrm{Obj}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{D})$ a function class

(II) For each objects $X, Y \in \mathcal{C}$, a function $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ satisfying

(a) For all f, g, $F(g \circ f) = F(g) \circ F(f)$

(b) $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$

Definition 3 (Natural Transformations)**.** Given two functors $F, G : \mathcal{C} \to \mathcal{D}$, a natural transformation $\eta : F \Rightarrow G$ is a data of morphisms $\eta_X : F(X) \to G(X)$ such that the following diagram commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta_X} & G(X) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\eta_Y} & G(Y) \end{array}$$

Fall 2020, Problem 10: Let $\mathcal{C}$ and $\mathcal{D}$ be categories, and suppose that every pair of morphisms in $\mathcal{C}$ admits a coequalizer. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor that preserves coequalizers: i.e., if $f, g : A \to B$ are morphisms in $\mathcal{C}$ and $\pi : B \to \mathrm{coeq}(f, g)$ is the coequalizer morphism, then $F(\pi)$ is the coequalizer morphisms for $F(f)$ and $F(g)$. Suppose also that if h is a morphism in $\mathcal{C}$ such that $F(h)$ is an isomorphism, then h is an isomorphism. Show that F is faithful.

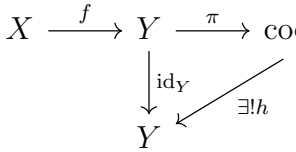
Proof. Let $f, g : X \to Y$ be such that $F(f) = F(g)$. We will show $f = g$. Consider the commutative diagram below:

$$X \underset{g}{\overset{f}{\rightrightarrows}} Y \xrightarrow{\pi} \text{coeq}(f,g) \implies F(X) \underset{F(g)}{\overset{F(f)}{\rightrightarrows}} F(Y) \xrightarrow{F(\pi)} \text{coeq}(F(f), F(g))$$

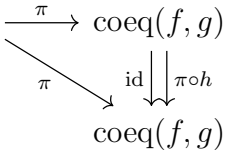
We know $F(f) = F(g)$. There's a lemma that can help us.

Lemma 1. Let $X \underset{g}{\overset{f}{\rightrightarrows}} Y \xrightarrow{\pi} \text{coeq}(f,g)$ be a commutative diagram with $\text{coeq}(f,g)$ the coequalizer of f and g. Then, π is an isomorphism if and only if $f = g$.

Proof of the lemma. ($\Leftarrow$ Part:) Since $\pi \circ f = \pi \circ g$ and π is an isomorphism, we can compose with π^{-1} to get $f = \pi^{-1} \circ \pi \circ f = \pi^{-1} \circ \pi \circ g = g$.
($\Rightarrow$ Part:) Suppose $f = g$. Then every $k : B \to C$ satisfies $k \circ f = k \circ g$. We can apply the universal property to $\text{id}_Y : Y \to Y$ and get that there exists a unique $h : \text{coeq}(f,g) \to Y$ commuting with the following diagram:



In particular, $h \circ \pi = \text{id}_Y$, so π has a left inverse. To see that $\pi \circ h = \text{id}$, first, compose it with π on the left. $\pi \circ h \circ \pi = \pi$. We rewrite it as: $(\pi \circ h) \circ \pi = \text{id} \circ \pi$.



Then, by the uniqueness in the universal property, we get $\pi \circ h = \text{id}$. □

Since $F(f) = F(g)$, we get that $F(\pi)$ is an isomorphism. But by assumption, π must also be an isomorphism. Applying the lemma again, we see that $f = g$. □

Definition 4 (Adjoints)**.** Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be two functors. We say that F and G are (left-right) adjoints if $\text{Hom}_{\mathcal{D}}(F(X), Y) \simeq \text{Hom}_{\mathcal{C}}(X, G(Y))$ and the isomorphisms are natural. Adjoint functors are often written $\begin{array}{c}\mathcal{C}\\ {\scriptstyle F}\downarrow\uparrow{\scriptstyle G}\\ \mathcal{D}\end{array}$ and F is denoted "left-adjoint" and G denoted "right-adjoint". Also, naturality means the following: we have two functors $\mathcal{C}^{\text{op}} \times \mathcal{D} \to \text{Set}$ $(X, Y) \mapsto \text{Hom}_{\mathcal{D}}(F(X), Y)$ and $(X, Y) \mapsto \text{Hom}_{\mathcal{C}}(X, G(Y))$. Naturality means that the isomorphims between the two functors are natural transformations.

Theorem 1 (Yoneda Lemma)**.** Let $\mathcal{C}$ be a small category, and consider the functor $y_{\mathcal{C}} : \mathcal{C} \to \text{Fun}(\mathcal{C}^{\text{op}}, \text{Set})$ $X \mapsto \text{Hom}(-, X)$. We call this the *Yoneda* embedding. For any functor $F : \mathcal{C}^{\text{op}} \to \text{Set}$, we have a natural isomorphism given by $\text{Nat}(\text{Hom}(-, X), F) \simeq F(X)$ $\alpha \mapsto \alpha_X(\text{id}_X)$. Moreover, if $F = \text{Hom}(-, Y)$, then the isomorphism is the inverse of the Yoneda embedding $y_{\mathcal{C}}$. It follows that the Yoneda embedding is in fact, fully faithful.

Fall 2018 Problem 7: Let $F : \mathcal{C} \to \mathcal{D}$ be a functor with a right adjoint G. Show that F is fully faithful if and only if the unit of the adjunction $\eta : \text{Id}_{\mathcal{C}} \to GF$ is an isomorphism.

Proof. Note we have the diagram

$$\mathrm{Hom}_{\mathcal{C}}(X,Y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{D}}(F(X),F(Y)) \xrightarrow{\simeq} \mathrm{Hom}_{\mathcal{C}}(X,GF(Y))$$

Lemma 2. $f \mapsto \eta_Y \circ f$ for all $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$

Proof of Lemma. Set $\alpha_{X,Z}$ the canonical isomorphism $\mathrm{Hom}_{\mathcal{D}}(F(X),Z) \to \mathrm{Hom}_{\mathcal{D}}(X,G(Z))$ so that the above isomorphism is in fact, $\alpha_{X,F(Y)}$. Consider the three functors $Y \mapsto \mathrm{Hom}_{\mathcal{C}}(-,Y), Y \mapsto \mathrm{Hom}_{\mathcal{D}}(F(-),F(Y)), Y \mapsto \mathrm{Hom}_{\mathcal{C}}(-,GF(Y))$. We label the natural transformations between them as follows:

$$\mathrm{Hom}_{\mathcal{C}}(-,Y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{D}}(F(-),F(Y)) \xrightarrow{\alpha_{-,F(Y)}} \mathrm{Hom}_{\mathcal{C}}(-,GF(Y))$$

By Yoneda lemma, the natrual transformation $\alpha_{-,F(Y)} \circ F$ corresponds to $(\alpha_{-,F(Y)} \circ F)_Y(\mathrm{id}_Y) = \alpha_{Y,F(Y)} \circ F(\mathrm{id}_Y) = \alpha_{Y,F(Y)} \circ \mathrm{id}_{F(Y)}$, which, by definition, is η_Y. Hence, the map $\mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}}(X,GF(Y))$ is given by $f \mapsto \eta_Y \circ f$. □

Proof of Lemma (Without Yoneda). Fix an f and consider the following diagram:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathcal{C}}(Y,Y) & \xrightarrow{F} & \mathrm{Hom}_{\mathcal{C}}(F(Y),F(Y)) & \xrightarrow{\simeq} & \mathrm{Hom}_{\mathcal{C}}(Y,GF(Y)) \\
\downarrow{\scriptstyle -\circ f} & & \downarrow{\scriptstyle -\circ F(f)} & & \downarrow{\scriptstyle -\circ f} \\
\mathrm{Hom}_{\mathcal{C}}(X,Y) & \xrightarrow{F} & \mathrm{Hom}_{\mathcal{C}}(F(X),F(Y)) & \xrightarrow{\simeq} & \mathrm{Hom}_{\mathcal{C}}(X,GF(Y))
\end{array}$$

Let's follow what happens to id_Y. Going down and right, it's sent to f first, and then, to something. On the other hand, if we move to the right and then, down $\mathrm{id}_Y \mapsto \mathrm{id}_{F(Y)} \mapsto \eta_Y$ by definition of η_Y, and then, is sent to $\eta_Y \circ f$. So f in $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ must be sent to $\eta_Y \circ f$ in $\mathrm{Hom}_{\mathcal{C}}(X,GF(Y))$. □

($\Rightarrow$ Part:) Suppose F is fully faithful. Then, on the above diagram, F (from hom-sets to hom-sets) is bijective. So the map $\mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}}(X,GF(Y))$ $f \mapsto \eta_Y \circ f$ is bijective for all $X \in \mathrm{Obj}(\mathcal{C})$. The conclusion follows immediately from the following lemma:

Lemma 3. Let $g : Y \to Z$ be such that for all X, the map $\mathrm{Hom}(X,Y) \xrightarrow{g\circ -} \mathrm{Hom}(X,Z)$ is bijective. Then, g is an isomorphism.

Proof of the Lemma. The Yoneda functor $Y \mapsto \mathrm{Hom}_{\mathcal{C}}(-,Y)$ is fully faithful, so an isomorphism $f \mapsto g \circ f$ pulls back to an isomorphism g. □

Proof of the Lemma (Without Yoneda). Set $X = Z$, and we get that $\mathrm{Hom}(Z,Y) \xrightarrow{g\circ -} \mathrm{Hom}(Z,Z)$ is surjective, in particular, there exists $h \in \mathrm{Hom}(Z,Y)$ such that $h \mapsto g \circ h = \mathrm{id}_Z$. So g is right-invertible. Now, we claim that $h \circ g = id_Y$. Once again, we have $g \circ h \circ g = g = g \circ id_Y$. But then, since $f \mapsto g \circ f$ is injective, we have that $h \circ g = id_Y$. □

($\Leftarrow$ Part:) Suppose η_Y is invertible. Then the composition by η_Y is bijective again (inverse given by composition with η_Y^{-1}) so we have the following diagram:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}}(X,Y) & \xrightarrow{F} & \mathrm{Hom}_{\mathcal{D}}(F(X),F(Y)) \\
& \overset{\simeq}{\searrow} & \downarrow{\scriptstyle \simeq} \\
& & \mathrm{Hom}_{\mathcal{C}}(X,GF(Y))
\end{array}$$

Hence, the inverse of F can be found by inverting the right isomorphisms. □

Discussion 2 - More Category Theory, Localizations of Rings

Fall 2017 Problem 10: Let $\mathcal{C}$ be a category with finite products, and let $\mathcal{C}^2$ be the category of pairs of objects of $\mathcal{C}$ together with morphisms $(A, A') \to (B, B')$ of pairs consisting of pairs $(A \to B, A' \to B')$ of morphisms in $\mathcal{C}$. Let $F : \mathcal{C}^2 \to \mathcal{C}$ be the direct product functor (that takes pairs of objects and morphisms to their products).

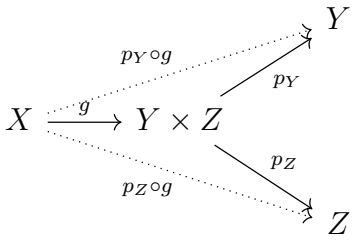
(a) Find a left adjoint of F

(b) For $\mathcal{C}$ a category of abelian groups, determine whether or not F has a right adjoint.

Proof of Part a). We want:

$$\mathrm{Hom}_{\mathcal{C}^2}(L(X), (Y, Z))) \simeq \mathrm{Hom}_{\mathcal{C}}(X, Y \times Z)$$

But observe that we have an isomorphism $\mathrm{Hom}_{\mathcal{C}}(X, Y \times Z) \xrightarrow{\simeq} \mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(X, Z)$ given by $g \mapsto (p_Y \circ g, p_Z \circ g)$ where $p_Y : Y \times Z \to Y$ and $p_Z : Y \times Z \to Z$ are projection maps. The fact that it is an isomorphism is equivalent to the universal property of the product.



But note now that by definition, $\mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(X, Z) = \mathrm{Hom}_{\mathcal{C}^2}((X, X), (Y, Z))$. So, if we take $L : \mathcal{C} \to \mathcal{C}^2$ to be $L(X) = (X, X)$ (and with the morphisms sent to the obvious ones), we have that $\mathrm{Hom}_{\mathcal{C}}(X, Y \times Z) \simeq \mathrm{Hom}_{\mathcal{C}^2}(L(X), (Y, Z))$ naturally (we leave the naturality of the isomorphism as an exercise). □

Part b) solution. The answer is a YES. It follows from the fact that in Ab, finite coproducts and products coincide. As before, if we set $R(G) = (G, G)$, then

$$\begin{array}{ccc} \mathrm{Hom}_{\mathrm{Ab}}(G \times H, K) & \xrightarrow{=} & \mathrm{Hom}_{\mathrm{Ab}}(G \oplus H, K) \\ & & \downarrow \simeq \\ & & \mathrm{Hom}_{\mathrm{Ab}}(G, K) \times \mathrm{Hom}_{\mathrm{Ab}}(H, K) \xrightarrow{=} \mathrm{Hom}_{\mathrm{Ab}^2}((G, H), (K, K)) \end{array}$$

So R is a right adjoint of F. □

Fall 2016 Problem 8: Prove that if a functor $\mathcal{F} : \mathcal{C} \to \mathrm{Sets}$ has a left adjoint functor, then $\mathcal{F}$ is representable.

Proof. Once again, we use the fact that F has a left adjoint functor $\begin{array}{c} \mathcal{C} \\ {\scriptstyle L}\uparrow\downarrow{\scriptstyle F} \\ \mathrm{Sets} \end{array}$ so

$$\mathrm{Hom}_{\mathcal{C}}(L(X), Y) \simeq \mathrm{Hom}_{\mathrm{Sets}}(X, F(Y))$$

Conveniently, this is true for when $X = \{p\}$ for some element p. So then,

$\mathrm{Hom}_{\mathcal{C}}(L(\{p\}), Y) \simeq \mathrm{Hom}_{\mathrm{Sets}}(\{p\}, F(Y)) \simeq F(Y)$ (the last bijection can be given by $g \mapsto g(p)$ and $a \mapsto (p \mapsto a)$). So $F(Y)$ is represented by $L(\{p\})$. □

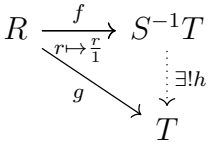
Definition 5. Let R be a commutative ring and $S \subset R$ a multiplicatively closed subset (i.e $1 \in S$ and $\forall x, y \in S, xy \in S$). Then, we can define an equivalence relation $\sim$ on $R \times S$ via $(r_1, s_1) \sim (r_2, s_2)$ iff $\exists t \in S$ such that $t(r_1 s_2 - r_2 s_1) = 0$ (the fact that $\sim$ is an equivalence relation is HW). We denote $\frac{r}{s} = [(r, s)]_\sim$ and $S^{-1}R = (R \times S)/\sim$ and define addition and multiplication as follows:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2}$$

It's again a HW that 1) these operations are well-defined (that it does not depend on the choice of the representatives) and 2) $(S^{-1}R, +, \cdot))$ is a commutative ring.

Theorem 2. The map $f : R \to S^{-1}R r \mapsto \frac{r}{1}$ is a homomorphism. Moreover, if $g : R \to T$ is a homomorphism to a commutative ring T such that $\forall s \in S, g(s) \in T^\times$, there exists a unique $h : S^{-1}R \to T$ such that $g = h \circ f$. In other words, the following diagram commutes:



Proof. HW! □

Example 1 (Examples of Multiplicative Subsets and Localizations with them)**.**

(I) $S = \{1, r, \ldots, r^n, \ldots\}$. We denote $S^{-1}R = R[r^{-1}]$. As a special case, if $R = F[X]$ for some field F, and $r = X$, then $S^{-1}R = F[X, X^{-1}]$, the set of all Laurent polynomials in F (finite sum of aX^n as $n \in \mathbb{Z}$).

(II) $S = 1 + I$ for an ideal I.

(III) For a prime ideal P, $S = R - P$. Then, we denote $S^{-1}R = R_P$. As a special case, we can take R an integral domain, and $P = (0)$, and we get $R_{(0)} = Q(R)$, the field of fractions of R.

Remark 1. In the example (III) from above, $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ if and only if $r_1 s_2 - r_2 s_1 = 0$. In general, $f : R \to S^{-1}R$ is injective iff S does not contain any non-zero divisors iff $\frac{r_1}{s_1} = \frac{r_2}{s_2} \Leftrightarrow r_1 s_2 - r_2 s_1 = 0$.

Lemma 4. Fix an ideal $I \subset R$ s.t. $I \cap S = \varnothing$, denote $I \cdot S^{-1}R$ the ideal of $S^{-1}R$ generated by $f(I) \subset S^{-1}R$.

(a) $I \cdot S^{-1}R = S^{-1}I = \{\frac{r}{s} \mid r \in I, s \in S\}$, and it's a proper ideal of $S^{-1}R$.

(b) $f^{-1}(S^{-1}I) = \{a \in R \mid S \cdot a \cap I \neq \varnothing\} (\supset I)$

(c) For any proper ideal $J \subset S^{-1}R$, $f^{-1}(J) \cap S = \varnothing$ and $S^{-1}f^{-1}(J) = J$

In other words, we can view $I \mapsto S^{-1}I$ and $J \mapsto f^{-1}(J)$ as mappings from $\{I \subset R \mid I \cap S = \varnothing, I \text{ is an ideal}\}$ to $\{J \subset S^{-1}R \mid J \text{ is a proper ideal}\}$ and $I \mapsto S^{-1}I \mapsto f^{-1}S^{-1}(I) \supset I$ and $J \mapsto f^{-1}(J) \mapsto J$.

Proof. (Part a): Clearly, $S^{-1}(I) \subset I \cdot S^{-1}$ as if $\frac{r}{s}$ is such that $r \in I$, then $\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} \in I \cdot S^{-1}R$. For the other inclusion, suppose we have $\sum_{k=1}^{n} \frac{a_k}{1} \cdot \frac{r_k}{s_k}$ with $a_k \in I$. Then, each $\frac{a_k}{r_k} s_k \in S^{-1})(I)$ so their sum must also remain in $S^{-1}(I)$ (it's not hard to check that $S^{-1}I$ is additively closed).
(Part b): If a is in the latter set, then there exists $s \in S$ such that $sa \in I$. So then, $\frac{a}{1} = \frac{sa}{s} \in S^{-1}(I)$. So $a \in f^{-1}S^{-1}(I)$. For the reverse inclusion, take $a \in f^{-1}S^{-1}(I)$. Then, $\frac{a}{1} \in S^{-1}(I)$, so $\frac{a}{1} = \frac{r}{s}$ for some $r \in I$. Then, there exists $t \in S$ such that $t(sa - r) = 0$, so $(ts)a = tr \in I$. Since $ts \in S$ (this is where we use that S is multiplicatively closed), $tr \in Sa \cap I$.
(Part c): Let $\frac{r}{s} \in J$. Then, $\frac{r}{1} = \frac{r}{s} \cdot \frac{s}{1} \in J$. So $r \in f^{-1}(J)$. So $\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} \in f(f^{-1}(J)) \cdot S^{-1}R = S^{-1}(f^{-1}(J))$. Now, suppose $\frac{r}{s} \in S^{-1}f^{-1}(J)$. Then, $\frac{r}{s} = \frac{a}{t}$ for some $a \in f^{-1}(J)$ and $t \in S$. Then, $\frac{a}{t} = \frac{a}{1} \cdot \frac{1}{t} \in J$ since by definition, $f(a) = \frac{a}{1} \in J$. □

Discussion 3 - More Ring Localizations

Theorem 3 (Given as Qual Spring 2017 Problem 5)**.** Suppose in addition, that $P \cap S = \varnothing$ is a prime ideal. Then, $S^{-1}P$ is prime, and the map $P \mapsto S^{-1}P$ and $Q \mapsto f^{-1}(Q)$ are inverse bijections between

$\{P \subset R \mid P \text{ prime and } P \cap S = \varnothing\}$ and $\{Q \subset S^{-1}R \mid Q \text{ prime}\}$

Proof. Suppose $\frac{r}{s} \cdot \frac{a}{t} \in S^{-1}P$. Then, $\frac{ra}{st} = \frac{b}{u}$ for some $u \in S$. So there exists $w \in S$ s.t. $w(ra \cdot u - b \cdot st) = 0$, or equivalently, $rauw = bstw$. The right hand side belongs to P as $b \in P$, so $rauw \in P$. But since $uw \in S$, $uw \notin P$, so $ra \in P$. So $r \in P$ or $a \in P$, hence $\frac{r}{s} \in S^{-1}P$ or $\frac{a}{t} \in S^{-1}P$.

Now, it remains to show that $\{a \in P \mid Sa \cap P \neq \varnothing\} = P$. The $\supseteq$ part is already done, so we do the other inclusion. Let a be such that there exists $s \in S$ s.t. $sa \in P$. Then, since $s \in S$, $s \notin P$, so $a \in P$ (this is where we use P is prime!). □

Remark 2. It's clear that the above maps $I \mapsto S^{-1}I$ and $J \mapsto f^{-1}(J)$ are inclusion-preserving. This leads to the following corollaries.

Corollary 1. For any P prime, R_P is a local ring with max ideal $P \cdot R_P = P_P$, hence the name "localization."

Proof. An ideal is maximal if and only if it is maximal among prime ideals (since every maximal ideal is prime). Every prime ideal of R_P is of the form $Q \cdot R_P$ for some $Q \subset P$. So $P \cdot R_P$ is the maximal prime ideal. □

Corollary 2. If R is a commutative noetherian (resp. artinian) ring, then so is $S^{-1}R$.

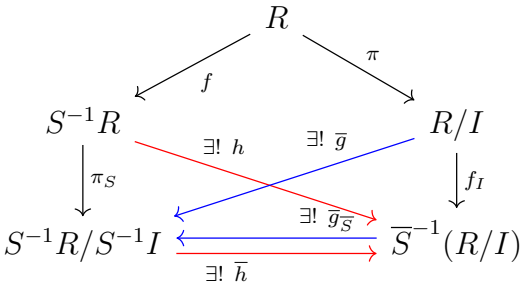
Proof. Take any X a non-empty set of ideals of $S^{-1}R$. Take $Y = \{f^{-1}(J) \mid J \in X\}$, which, since R is noetherian (resp. artinian), has a maximal (resp. minimal) element $f^{-1}(J)$. Then, $J = S^{-1}(f^{-1}(J))$ must be maximal (resp. minimal) among ideals in X as well. □

Lemma 5. Let $S \subset R$ be a multiplicative subset, and let I be an ideal. Denote $\overline{S} \subset R/I$ the image of S in R/I (i.e. $\overline{S} = \pi(S)$ where $\pi : R \twoheadrightarrow R/I$). Then, as rings,

$$S^{-1}R/S^{-1}I \cong \overline{S}^{-1}(R/I)$$

.

Proof. Of course, we want $\frac{r}{s} + S^{-1}I := \frac{\overline{r}}{s}$ matched with $\frac{r+I}{s+I} = \frac{\overline{r}}{\overline{s}}$. The problem is with well-definedness of the maps, etc. Here's how to proceed: take a commutative diagram (black arrows) below.



Observe that for all $s \in S$, $f_I \circ \pi(s) = f_I(\overline{s}) = \frac{\overline{s}}{\overline{1}}$ which is invertible (with inverse given by $\frac{\overline{1}}{\overline{s}}$). So by the universal property, there exists unique $h : S^{-1}R \to \overline{S}^{-1}(R/I)$ s.t. $h \circ f = f_I \circ \pi$. For any $\frac{r}{s} \in S^{-1}I$ (with $r \in I$), $h : \frac{r}{s} \mapsto \frac{\overline{r}}{\overline{1}} \cdot \frac{\overline{s}}{\overline{1}}^{-1} = 0 \cdot \frac{\overline{1}}{\overline{s}}$. So $S^{-1}(I) \subset \mathrm{Ker}(h)$, so h descends to the quotient $\overline{h} : S^{-1}R/S^{-1}I \to \overline{S}^{-1}(R/I)$. As desired, $h : \frac{\overline{r}}{s} \mapsto \frac{\overline{r}}{\overline{s}}$.

Similarly, if $r \in I$, $\pi_S \circ f(r) = \pi_S(\frac{r}{1}) = 0$ since $\frac{r}{1} \in S^{-1}I$. So $\pi_S \circ f$ descends to the quotient, say $\overline{g} : R/I \to S^{-1}R/S^{-1}I$. Take any $\overline{s} \in \overline{S}$ (with $s \in S$ mapping to $\overline{s}$). Then, $\overline{g}(s) = \frac{\overline{s}}{\overline{1}}$ which has an inverse $\frac{\overline{1}}{s}$ in $S^{-1}R/S^{-1}I$. So once again, by the universal property, there exists unique $\overline{g}_{\overline{S}} : \overline{S}^{-1}(R/I) \to S^{-1}R/S^{-1}I$ such that $\overline{g}_{\overline{S}} \circ f_I = \overline{g}$. We see that $\overline{g}_{\overline{S}} : \frac{\overline{r}}{\overline{s}} \mapsto \frac{\overline{r}}{s}$.

Clearly, h and $\overline{g}_{\overline{S}}$ are inverses to one another. □

Corollary 3. For any prime P, $F(R/P) \cong R_P/P_P$ where $F(T)$ denotes a field of fractions of a given integral domain T.

Proof. Set $S = R - P$ and $I = P$. Then, $\overline{S} = R/P - \{0\}$. □

Remark 3. The above field is called the "residue field" at P.

Fall 2020 Problem 8: Consider $R = \mathbb{C}[X,Y]/(X^2, XY) := \mathbb{C}[x,y]$. Determine the prime ideals of R. Which of the localizations R_P are integral domains?

Proof. (Prime ideals of R Part:) Let $\pi : \mathbb{C}[X,Y] \twoheadrightarrow \mathbb{C}[X,Y]/(X^2, XY)$ be the quotient map. Then, $P \subset R$ corresponds one-to-one to $\pi^{-1}(P)$ a prime ideal of $\mathbb{C}[X,Y] \supset (X^2, XY)$. Given a prime $Q \subset \mathbb{C}[X,Y]$, $X^2 \in Q \Rightarrow X \in Q$ so $(X^2, XY) \subset Q$ if and only if $X \in Q$. Hence, prime ideals of $P \subset R$ corresponds to prime ideals $\pi^{-1}(P)$ of $\mathbb{C}[X,Y]$ containing X, which, by taking the surjection $q : \mathbb{C}[X,Y] \twoheadrightarrow \mathbb{C}[Y]$ sending $X \mapsto 0$, corresponds to the prime ideals of $\mathbb{C}[Y]$ (since $\mathbb{C}[X,Y]/(X) \simeq C[Y]$ via the map induced by q). The prime ideals of $\mathbb{C}[Y]$ are (0) and $(Y - z)$ (as the only irreducible $g \in \mathbb{C}[Y]$ are of the form $Y - z$). So $P \subset R$ are either $\boxed{(x)} \subset \mathbb{C}[x,y]$ or $\boxed{(x, y - z)} \subset \mathbb{C}[x,y]$ for some irreducible $z \in \mathbb{C}$.
(Which Localization R_P are integral domains Part:) Answer: $P = \boxed{(x)}$ or $\boxed{(x, y - z)}$ for $z \in \mathbb{C} - \{0\}$

Note first that $R_P = \mathbb{C}[X,Y]_P/(X^2, XY)_P$ (by abuse of notation, $\pi^{-1}(P)$ will also be denoted P). So R_P is an integral domain iff $(X^2, XY)_P$ is a prime ideal in $\mathbb{C}[X,Y]$. If $P = (X)$ or $(X, Y - z)$ for some $z \in \mathbb{C} - 0$, then $Y \notin P$ (exercise!), so in $\mathbb{C}[X,Y]_P$, Y becomes invertible. Hence, $\frac{X}{1} = \frac{XY}{Y} \in (X^2, XY)_P$, so $(X^2, XY)_P = (X)_P$. Since (X)

is already a prime ideal, so is $(X)_P$. On the other hand, if $P = (X, Y)$, then we claim that $\frac{X}{1} \notin (X^2, XY)_P$. Suppose otherwise; then $\frac{X}{1} = \frac{fX^2}{g} + \frac{kXY}{h}$ for some $f, k \in \mathbb{C}[X, Y]$ and $h, g \notin (X, Y)$. Clearing out the denominator, we have $ghX = fhX^2 + kgXY$ so $gh = fhX + kgY$ after canceling X. But $gh \notin P = (X, Y)$ whereas, $fhX + kgY \in (X, Y)$, a contradiction.

But then, we have $(\frac{X}{1})^2 = \frac{X^2}{1} \in (X^2, XY)_P$ even though $\frac{X}{1} \notin (X^2, XY)_P$, so $(X^2, XY)_P$ is not prime. □

Discussion 4 - Localization of Modules, Nakayama's Lemma

Fall 2018 Problem 5: Let R be a commutative ring. Show the following:

(a) Let S be a non-empty *saturated* multiplicative set in R, i.e. if $a, b \in R$, then $ab \in S$ if and only if $a, b \in S$. Show that $R - S$ is a union of prime ideals.

(b) (Kaplansky's Theorem for UFDs): If R is a domain, show that R is a UFD if and only if every nonzero prime ideal in R contains a non-zero principal prime ideal.

Proof. (Part a): Clearly,

$$R - S \supseteq \bigcup_{P \cap S = \varnothing} P$$

where the union is taken over all P prime not meeting S. So, it suffices to prove the other inclusion. Let $x \notin S$. We want x to be in the union - i.e. we want to find a P prime ideal not meeting S such that $x \in P$.

Now, consider $\mathcal{A} = \{I \mid x \in I \text{ and } I \cap S = \varnothing\}$, with the partial order $\subseteq$.

Lemma 6. $(x) \in \mathcal{A}$.

Proof. The only thing to check is $(x) \cap S = \varnothing$. Suppose not; let $rx \in (x)$ be such that $rx \in S$. Then, since S is saturated, $x \in S$, which contradicts that $x \notin S$. □

So $\mathcal{A} \neq \varnothing$. Now, we apply Zorn's lemma to $\mathcal{A}$ to find a maximal element. Let $\{I_\alpha\}_{\alpha \in \Lambda}$ be a chain of ideals in $\mathcal{A}$. Then, $I := \cup_{\alpha \in \Lambda} I_\alpha$ is an ideal which contains all I_α's, $x \in I$, and $I \cap S = \cup_{\alpha \in \Lambda}(I_\alpha \cap S) = \varnothing$. Hence, I is an upper bound of I_α's in $\mathcal{A}$.

Thus, by Zorn's lemma, $\mathcal{A}$ has a maximal element $M \in \mathcal{A}$. The conclusion follows by the following lemma:

Lemma 7. M is a prime ideal.

Proof. Let $a, b \notin M$. Then, $M \subsetneq M + (a), M + (b)$, so $M + (a), M + (b) \cap S \neq \varnothing$. So choose $s \in M + (a) \cap S$ and $t \in M + (b) \cap S$. Then, $st \in (M + (a))(M + (b)) \subset M + (ab)$. If $ab \in M$, then $st \in M + (ab) = M$ and $st \in S$, contradicting that $S \cap M = \varnothing$. So $ab \notin M$. □

(Part b): If R is a UFD and P is a prime containing a nonzero $r = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then at least one p_i belongs to P. So we prove the reverse implication, which is much harder.

Let $S = R^\times \cup \{p_1 p_2 \cdots p_k \mid p_i \text{ are primes}\}$. This is also the multiplicative subset generated by primes and units (Exercise!).

Lemma 8. S is a saturated multiplicative subset.

Proof. Let $st \in S$. If $st \in R^\times$, then take $u = (st)^{-1}$, then $stu = s(tu) = 1$ and $t(su) = 1$, so both s and t are invertible. So we assume st is of the form $p_1 p_2 \cdots p_k$ for some primes p_i's.

We know $p_1 \mid s$ or t. Define $s_1 = \frac{s}{p}$ if $p \mid s_1$ and $t_1 = t$; otherwise, $s_1 = s$ and $p \mid t$ so $t_1 = \frac{t}{p}$. So we have $s_1 t_1 = p_2 p_3 \cdots p_k$. Continuing in this way, we can define $s_j t_j$ such that $s_j t_j = p_{j+1} \cdots p_k$. Then, $s_k t_k = 1$, so s_k and t_k are units. But note s is s_k times a product of some p_i's, and t is t_k times a product of primes. Hence, $s, t \in S$. □

Now, clearly, $R - S \supseteq (0)$. Now, suppose $R - S$ contains an $r \neq 0$. Then, by part a), there exists a prime $P \subset R - S$ such that $r \in P$. But then, P contains a principal prime $(p) \subseteq P$. But by definition, $p \in S$, contradicting the fact that $(p) \cap S \subseteq P \cap S = \varnothing$.

Since every non-zero element has a prime factorization, R is in fact, a UFD (since factorization by primes must be unique and primes are always irreducible). □

Definition 6 (Localization of Modules)**.** Let R be a commutative ring, and M be an R-module. We can construct $S^{-1}M$, the localization of M at S, as follows: take $S \times M$ and define a relation $\sim$ by $(s, m) \sim (t, n) \Leftrightarrow \exists u \in S$ such that $u(sn - tm) = 0$. Set $\frac{m}{s} = [(s, m)]_\sim$, and $S^{-1}M = S \times M/\sim$.

Furthermore, we can define addition $+$ on $S^{-1}M$ by:

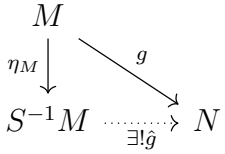
$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st}$$

which is 1) well-defined, and 2) turns $S^{-1}M$ with $+$ into an abelian group. Then, we can define scalar multiplication by $\frac{r}{s} \cdot \frac{m}{t} = \frac{r \cdot m}{st}$, which again, is well-defined and turns $S^{-1}M$ into an $S^{-1}R$-module (exercise!).

Proposition 1 (Restriction of Scalars)**.** Let $\phi : A \to B$ a ring homomorphism between two commutative rings, and M a B-module. We can turn M into an A-module by setting $r \cdot_A m = \phi(r) \cdot_B m$. Furthermore, if $f : M \to N$ is a B-module homomorphism, f is also an A-module homomorphism. So this act of taking a B-module and assigning an A-module structure as in above is functorial (from B-Mod to A-Mod), and is called *Restriction of Scalars along* $\phi : A \to B$. It's clear restriction of scalars is in fact, exact.

Proposition 2. Via restriction of scalars along $f : R \to S^{-1}R$, $r \mapsto \frac{r}{1}$, we can view $S^{-1}M$ as an R-module as well. Moreover, every R-module M such that $\forall s \in S$, $s \cdot - : M \to M$ $(m \mapsto s \cdot m)$ is invertible, can be turned into an $S^{-1}R$-module via $\frac{r}{s} \cdot m = (s \cdot -)^{-1}(r \cdot m)$. In particular, such M's form precisely the image of restriction of scalars along $f : R \to S^{-1}R$.

Proposition 3 (Universal Property of Localization)**.** Let R be a commutative ring and $g : M \to N$ be a R-module homomorphism. If N is such that $\forall s \in S$, $(s \cdot -) : N \to N$ is invertible, there exists unique $\hat{g} : S^{-1}M \to N$ such that $g = \hat{g} \circ eta_M$ (where $\eta_M : M \to S^{-1}M$, $m \mapsto \frac{m}{1}$). That is, $\hat{g}(\frac{m}{s})$ is given by $(s \cdot -)^{-1} g(m)$.



Remark 4. Given $f : M \to N$, we can apply the universal property to the R-module homomorphism $\eta_N \circ f : M \to S^{-1}N$ (where η_N and $S^{-1}N$ are now viewed as R-modules and homomorphisms under restriction of scalars). Then, we obtain a unique map, labeled $S^{-1}f : S^{-1}M \to S^{-1}N$, such that $S^{-1}f \circ \eta_M = \eta_N \circ f$. That is, the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \eta_M}\downarrow & & \downarrow{\scriptstyle \eta_N} \\ S^{-1}M & \xrightarrow[S^{-1}f]{} & S^{-1}N \end{array}$$

Moreover, $(S^{-1}f)(\frac{m}{s}) = (s \cdot -)^{-1}\eta_N \circ f(m) = (s \cdot -)^{-1}\frac{f(m)}{1} = \frac{f(m)}{s}$.

So, the localization $M \mapsto S^{-1}M$ and $f \mapsto S^{-1}f$ is functorial (exercise!). It's a homework problem that this is actually an exact functor.

Remark 5. We may similarly denote $S^{-1}M$ as $M[r^{-1}]$, M_P when $S = \{1, r, \ldots, r^n, \ldots\}, S = R - P$, respectively.

Proposition 4. Let R be a commutative ring. For an R-module, the following are equivalent:

(I) $M = 0$.

(II) $\forall P$ prime, $M_P = 0$.

(III) $\forall P$ maximal, $M_P = 0$.

Proof. (I) $\implies$ (II) $\implies$ (III) are trivial, so we prove (III) $\implies$ (I). Suppose $M \neq 0$. Then, choose $m \neq 0$ in M. Then, consider $I = \mathrm{Ann}(M) := \{r \in R \mid r \cdot m = 0\}$, which is an ideal (exercise!) not containing 1 (otherwise, $1 \cdot m = m = 0$). So I is a proper ideal, so there exists a maximal ideal P containing I. Now, consider M_P.

Claim. $M_P \neq 0$

Proof of the Claim. Consider $\frac{m}{1}$, and suppose it is 0. Then, there exists $s \notin P$ such that $s \cdot m = 0$. So then, $s \in I = \mathrm{Ann}(m) \subset P$, contradicting that $s \notin P$. So $\frac{m}{1} \neq 0$, so $M_P \neq 0$. □

So we found a prime ideal P such that $M_P \neq 0$. □

Proposition 5. Let R be a commutative ring and $f : M \to N$ an R-module homomorphism. The following are equivalent.

(I) f is injective.

(II) $\forall P$ prime, $f_P : M_P \to N_P$ is injective.

(III) $\forall P$ maximal, $f_P : M_P \to N_P$ is injective.

Proof. ((I) $\implies$ (II) Part:) We have an exact sequence $0 \longrightarrow M \xrightarrow{f} N$. Localizing at P, we obtain an exact sequence $0 \longrightarrow M_P \xrightarrow{f_P} N_P$, so f_P remains injective. ((II) $\implies$ (III) Part:) Trivial

((III) $\implies$ (I) Part:) Given any f, we get an exact sequence $0 \longrightarrow \ker(f) \longrightarrow M \xrightarrow{f} N$. Localizing at P, we get:

$0 \longrightarrow (\ker(f))_P \longrightarrow M_P \xrightarrow{f_P} N_P$ So $(\ker(f))_P \cong \ker(f_P)$ by exactness. So in particular, $(\ker(f))_P = 0$ at every P maximal. By the previous proposition, $\ker(f) = 0$, hence, f is injective. $\square$

Remark 6. We can replace the word "injective" with surjective and obtain the same equivalence in the proposition. The proof would involve analyzing the cokernel of f instead of f, but otherwise, is exactly the same.

Theorem 4 (Nakayam's Lemma, Most General Version)**.** Let R be a commutative ring and M a finitely generated R-module, and let $f : M \to M$ is an R-module homomorphism such that $f(M) = I \cdot M$ for an ideal I. Then, there exists

$$p = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in R[x]$$

with $a_i \in I$ (for $i = 0, 1, \ldots, n-1$) such that

$$p(f) = a_0\mathrm{id} + a_1 f + \cdots + a_{n-1}f^{n-1} + f^n = 0 \text{ in } \operatorname{End}_R(M)$$

Proof. Choose $x_1, x_2, \ldots, x_n \in M$ a generator. Then,

$$\begin{aligned}
f(x_1) &= \sum_{i=1}^{n} a_{1i}x_i = \sum_{i=1}^{n} (a_{1i}\mathrm{id})(x_i) \\
f(x_2) &= \sum_{i=1}^{n} a_{2i}x_i = \sum_{i=1}^{n} (a_{2i}\mathrm{id})(x_i) \\
&\vdots \\
f(x_n) &= \sum_{i=1}^{n} a_{ni}x_i = \sum_{i=1}^{n} (a_{ni}\mathrm{id})(x_i)
\end{aligned}$$

Now, consider $F : M^n \to M^n$ defined by $\begin{pmatrix} f - a_{11}\mathrm{id} & -a_{12}\mathrm{id} & \cdots & -a_{1n}\mathrm{id} \\ -a_{21}\mathrm{id} & f - a_{22}\mathrm{id} & \cdots & -a_{2n}\mathrm{id} \\ \vdots & \vdots & & \vdots \\ -a_{n1}\mathrm{id} & -a_{n2}\mathrm{id} & \cdots & f - a_{nn}\mathrm{id} \end{pmatrix}$ Now, the equations above can be rephrased as

$$F \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Observe that $F \in M_n(R[f]) \subset M_n(\operatorname{End}_R(M))$ as the coefficients are all in terms of the R-multiplications and f. More importantly, $R[f]$ is a *commutative* ring, so we can multiply by the adjoint to obtain:

$$F^{\text{adjoint}} F \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (\det F) I_n \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Setting $\phi = \det F$, we see that $\phi(x_1) = \phi(x_2) = \ldots \phi(x_n) = 0$. So $\phi = 0$. But $\phi = p(f) = a_0 + a_1 f + \cdots + a_{n-1} f^{n-1} + f^n$, for some $a_0, a_1, \ldots, a_{n-1} \in I$, so the conclusion follows. □

Discussion 5 - More Nakayama, Exact Sequences and Functors, and Tensor-Hom Adjunctions

Remark 7. When $M = R^n$ and $f : R^n \to R^n$ is represented by the matrix $A = (a_{ij})$, the above determinant is precisely $P_A(f)$, the characteristic polynomial of A evaluated at f. By the arguments from the theorem above, $P_A(f) = 0$, which is precisely the statement of the Cayley-Hamilton Theorem. This is one of the nicest proofs of the Cayley-Hamilton Theorem.

Corollary 4. Let R be a commutative ring, and M be a finitely generated R-module. If for a given ideal $I \subseteq R$, $M = I \cdot M$, then there exists $r \equiv 1 \bmod I$ such that $r \cdot M = 0$.

Proof. Take $f = \text{id}$, then $a_0 + a_1 f + \cdots + a_{n-1} f^{n-1} + f^n = (a_0 + a_1 + \cdots + a_{n-1} + 1)\text{id} = 0$ in $\text{End}_R(M)$. □

Theorem 5 (Nakayama's Lemma Local Version)**.** Let R be a commutative ring, M a finitely generated R-module, and I an ideal contained in $J(R)$, the Jacobson radical of R (e.g. this happens when R is local and I is the unique maximal ideal). If $M = I \cdot M$, then $M = 0$.

Proof. By the corollary, there exists $r \equiv 1 \bmod I$ such that $r \cdot M = 0$. But then, since $r - 1 \in J(R)$, r is actually a unit. So $M = r^{-1} \cdot (r \cdot M) = r^{-1} \cdot 0 = 0$. □

Second proof. Suppose $M \neq 0$ and $x_1, x_2, \ldots, x_n$ be the minimum number of generators. Then, $x_n \in M = I \cdot M$, so $x_n = \sum_{j=1}^{n} a_j \cdot x_j = \sum_{j=1}^{n-1} a_j \cdot x_j + a_n x_n$ for some $a_1, a_2, \ldots, a_n \in I$. So $(1 - a_n)x_n = \sum_{j=1}^{n} a_j \cdot x_j$. But since $a_n \in J(R)$, $1 - a_n$ is a unit, so $x_n = \sum_{j=1}^{n-1} (1 - a_n)^{-1} a_j x_j \in \sum_{j=1}^{n-1} R x_j$. This contradicts the assumption that $x_1, x_2, \ldots, x_n$ was a minimal generator. □

Remark 8. The second proof goes through for even when R is non-commutative.

Definition 7 (Exactness)**.** Recall we say $L \xrightarrow{f} M \xrightarrow{g} N$ is exact if $\text{Im}(f) = \ker(g)$. In general, given a sequence of modules and maps

$\ldots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \longrightarrow \ldots$ We say such a sequence is exact if $\text{Im}(f_i) = \ker(f_{i+1})$ whenever it makes sense.

Remark 9. In the definition, exactly where i ranges is made purposefully vague as to include a wide range of possible sequences.

Definition 8 (Short Exact Sequence)**.** An exact sequence of the form

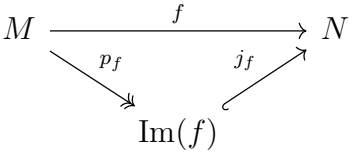
$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ is called a short exact sequence.

Definition 9 (Long Exact Sequence)**.** An exact sequence where i ranges over an unbounded set (of integers) in either directions is called a long exact sequence.

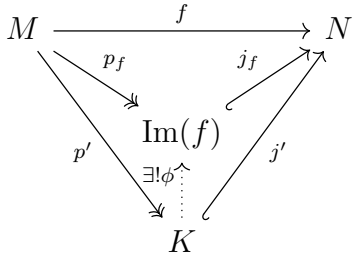
Remark 10. Any exact sequence $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} M_n$ can be extended to a long exact sequence as follows:

$$\cdots \longrightarrow 0 \longrightarrow \ker(f_1) \longrightarrow M_1 \longrightarrow \cdots \xrightarrow{f_{n-1}} M_n \longrightarrow \operatorname{coker}(f_n) \longrightarrow 0 \longrightarrow \cdots$$

Lemma 9 (Epi-Mono Factorization)**.** Let R be a ring and $f : M \to N$ an R-linear map. Then, we have the following commutative diagram

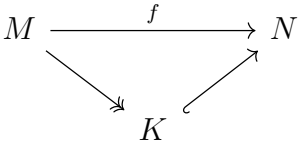


Moreover, if K is any other such decomposition, that is, if we had another K fitting as in the diagram,



there exists unique isomorphism $\phi : K \to \operatorname{Im}(f)$ such that the above diagram commutes.

Remark 11. The factorization of $f : M \to N$ as in the lemma



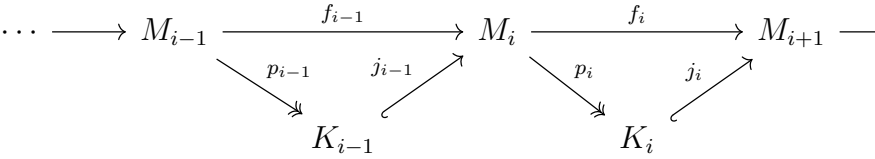
is called the Epi-mono factorization of f.

Proof of the lemma. The first part of the lemma (that $M \to \operatorname{Im}(f)$ is surjective and $\operatorname{Im}(f) \to N$ is injective) is trivial. So suppose we had another factorization of f: i.e. $p' : M \to K$ surjective and $j' : K \to N$ injective such that $j' \circ p' = f$. Then, for each $y \in K$, define $y = p'(x)$ for some $x \in M$. Then, define $\phi(y) := j'(y)$. Then, $j'(y) = j' \circ p'(x) = f(x) \in \operatorname{Im}(f)$ so $\phi : M \to \operatorname{Im}(f)$. Since ϕ is (as a function) same as j', ϕ is clearly R-linear.

Now, by definition, $j_f \circ \phi(y) = j'(y)$ so ϕ commutes with the j's. For p's, let $x \in M$, and note that $\phi \circ p'(x) = j' \circ p'(x) = f(x) = p_f(x)$. So ϕ commutes with the p's as well. As for checking ϕ is an iso, note that ϕ is injective since j' is, and ϕ is surjective since p_f is.

Finally, suppose $\psi : K \to \operatorname{Im}(f)$ was another map that commuted with the p's and the j's. Then, $\psi \circ p' = \phi \circ p'$ and p' is surjective, so $\psi = \phi$ (or similarly, we could use that $j_f \circ \psi = j_f \circ \phi$ and that j_f is injective). So uniqueness follows. □

Lemma 10. Given long sequence together with epi-mono factorizations K_i of f_i,



The following are equivalent:

(I) The above sequence is exact

(II) For each i, $0 \longrightarrow K_{i-1} \xrightarrow{j_{i-1}} M_i \xrightarrow{p_i} K_i \longrightarrow 0$ is short exact

Proof. (I) $\Rightarrow$ (II) Part: Each K_i is $\mathrm{Im}(f_i) = \ker(f_{i+1})$. So the short sequence is

$$0 \longrightarrow \ker(f_i) \longrightarrow M_i \longrightarrow \mathrm{Im}(f_i) \longrightarrow 0$$

which is exact.
(II) $\Rightarrow$ (I) Part: Note $\ker(f_i) = \ker(j_i \circ p_i)$, but since j_i is injective, $\ker(f_i) = \ker(p_i)$. Similarly, $\mathrm{Im}(f_{i-1}) = \mathrm{Im}(j_{i-1} \circ p_{i-1})$, but again, since p_{i-1} is surjective, so $\mathrm{Im}(f_{i-1}) = \mathrm{Im}(j_{i-1})$. By short-exactness, we have $\ker(p_i) = \mathrm{Im}(j_{i-1})$, which clearly implies $\ker(f_i) = \mathrm{Im}(j_{i-1})$. □

Definition 10. Given two abelian categories (e.g. R-Mod, Mod-R, R-Mod-S, etc.) $\mathcal{A}$ and $\mathcal{B}$, a functor $F : \mathcal{A} \to \mathcal{B}$ is additive if it preserves finite (co)-products. Equivalently, $F(f + g) = F(f) + F(g)$ for all f, g homomorphisms.

Lemma 11. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor between two abelian categories. The following are equivalent:

(I) F sends an exact sequence $L \xrightarrow{f} M \xrightarrow{g} N$ to an exact sequence

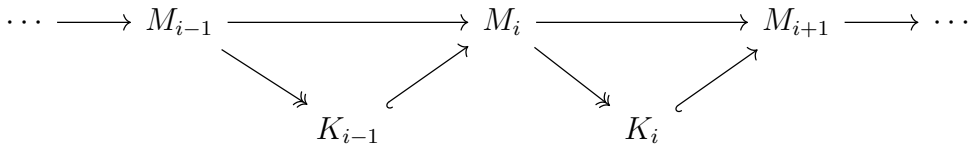
$$FL \xrightarrow{Ff} FM \xrightarrow{Fg} FN$$

(II) F sends a long exact sequence to a long exact sequence

(III) F sends a short exact sequence $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ to a short exact sequence

$$0 \longrightarrow FL \xrightarrow{Ff} FM \xrightarrow{Fg} FN \longrightarrow 0$$

Proof. (I) $\Leftrightarrow$ (II) Part: (I) $\Rightarrow$ (II) is trivial, and (II) $\Rightarrow$ (I) follows immediately from the fact that every exact sequence can be extended to a long exact seqence.
(I) $\Rightarrow$ (III) Part: Trivial
(III) $\Rightarrow$ (II) Part: Given a long exact sequence



For each i, $0 \longrightarrow K_{i-1} \longrightarrow M_i \longrightarrow K_i \longrightarrow 0$ is short exact. Now, under the image of the functor F, $0 \longrightarrow FK_{i-1} \longrightarrow FM_i \longrightarrow FK_i \longrightarrow 0$ remains short exact. But that shows the image of the long exact sequence is exact. □

Definition 11. We say that an additive functor $F : \mathcal{A} \to \mathcal{B}$ is exact if it satisfies any of the three conditions above.

Definition 12. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor between additive categories. We say F is left exact if it sends a short exact sequence $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ to an exact sequence $0 \longrightarrow FL \xrightarrow{Ff} FM \xrightarrow{Fg} FN$ Similarly, we say F is right exact if it sends a short exact sequence to an exact sequence $FL \xrightarrow{Ff} FM \xrightarrow{Fg} FN \longrightarrow 0$

Lemma 12. Let F be a left-exact functor. Then, F sends every exact sequence of the form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N$ to an exact sequence

$0 \longrightarrow FL \xrightarrow{Ff} FM \xrightarrow{Fg} FN$ Similarly, if F is a right-exact functor, then F sends every exact sequence of the form $L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ to an exact sequence $FL \xrightarrow{Ff} FM \xrightarrow{Fg} FN \longrightarrow 0$

Proof. Take an epi-mono factorization of g of the exact sequence:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & & \\ & & & & & \searrow^{p_g} & \uparrow{\scriptstyle j} & & \\ & & & & & & \mathrm{Im}(g) & & \end{array}$$

Now, the sequence $0 \longrightarrow L \longrightarrow M \longrightarrow \mathrm{Im}(g) \longrightarrow 0$ is exact. So by left-exactness of F, $0 \longrightarrow FL \xrightarrow{Ff} FM \xrightarrow{Fp_g} F\mathrm{Im}(g)$ is exact. So we have a sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & FL & \xrightarrow{Ff} & FM & \xrightarrow{Fg} & FN & & \\ & & & & & \searrow^{Fp_g} & \uparrow{\scriptstyle Fj} & & \\ & & & & & & F\mathrm{Im}(g) & & \end{array}$$

Notice Fp_g is no longer surjective, but it doesn't matter (though Fj still remains injective by left-exactness of F). First, on the far left, the map Ff still remains injective. And in them middle, $\ker(Fg) = \ker(Fj \circ Fp_g) = \ker(Fp_g)$ since Fj is injective. So then, $\ker(Fg) = \ker(Fp_g) = \mathrm{Im}(Ff)$, as desired.

For the right exactness part of the lemma, take the epi-mono factorization of f instead of g:

$$\begin{array}{ccccccccc} L & & \xrightarrow{f} & & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ \downarrow{\scriptstyle p_f} & \nearrow_{j} & & & & & & & \\ \ker(g) & & & & & & & & \end{array}$$

The rest of the details are left as an exercise. □

Exercise 1. An additive functor F is left exact if and only if F sends kernels to kernels. That is, if for $f : M \to N$, $j : \ker(f) \to M$ is the inclusion map, then $Fj : F\ker(f) \to \ker(Ff)$ is an isomorphism. Similarly, F is right exact if and only if F sends cokernels to cokernels.

Remark 12 (Tensor product as a bimodule)**.** Let A be a ring. Given A-mod (left A-module) N and mod-A (right A-module) M, we have an abelian group $M \otimes_A N$. If in addition, M is a B-mod or N a mod-C for some rings B and C, then $M \otimes_A N$ has the structure of B-mod or mod-C via:

$$b \cdot_B (m \otimes_A n) = (bm) \otimes_A n$$

and

$$(m \otimes_A n) \cdot_C c = m \otimes_A nc$$

Moreover, if M is a B-mod and N is a mod-C, then $M \otimes_A N$ has the structure of $B - C$ bimodule (denoted B-mod-C).

Moreover, in that case, we have, for M a B-mod-A, and N a A-mod-C, tensor producting with M or N are additive functors:

$$M \otimes_A (-) : A - \text{Mod} - C \to B - \text{Mod} - C$$

and

$$(-) \otimes_A N : B - \text{Mod} - A \to B - \text{Mod} - C$$

Remark 13 (Hom-set as a bimodule)**.** Similarly, given two A-mods M and N, $\text{Hom}_A(M, N)$ is an abelian group. If in addition, M has a structure of mod-B and N a mod-C, then $\text{Hom}_A(M, N)$ is B-C bimodule via:

$$(b \cdot_B f) : x \mapsto f(xb)$$

and

$$(f \cdot_C c) : x \mapsto f(x)c$$

Note that the side flips when B acts on the input! (the hom set is now a *left* B-module). Moreover, once again, we have additive functors

$$\text{Hom}_A(M, (-)) : A - \text{Mod} - C \to B - \text{Mod} - C$$

and

$$\text{Hom}_A((-), N) : (A - \text{Mod} - B)^{\text{op}} \to B - \text{Mod} - C$$

We're now ready to state Tensor-Hom adjunctions in full-generality:

Theorem 6. Given a $B - A$ bimodule X, the following functors are adjunctions:

$$\begin{array}{c} B - \text{Mod} - C \\ {\scriptstyle X \otimes_A (-)}\uparrow\downarrow{\scriptstyle \text{Hom}_B(X,(-))} \\ A - \text{Mod} - C \end{array}$$

Proof. $\text{Hom}_{B-C}(X \otimes_A M, N) \cong \text{Bil}(X \times M, N)$ where here, the set Bil denotes the set of all B-C bilinear AND A-balanced maps from $X \times N$ to N. Now, $\text{Bil}(X \times M, N) \cong \text{Hom}_{A-C}(M, \text{Hom}_B(X, N))$, so the conclusion follows. □

Exercise 2. Formulate and prove the Tensor-Hom adjunctions for the right-A modules (i.e. find adjunctions of $(-) \otimes_A X$).

Theorem 7 (Hom-Hom adjunctions)**.** Given a A-mod-C X, the following are adjunctions:

$$\begin{array}{c} (A - \text{Mod} - B)^{\text{op}} \\ {\scriptstyle \text{Hom}_{\text{Mod}-C}((-),X)^{\text{op}}}\uparrow\downarrow{\scriptstyle \text{Hom}_A((-),X)} \\ B - \text{Mod} - C \end{array}$$

where $\text{Hom}_{\text{Mod}-C}((-), X)$ indicates the right C-module hom set.

Proof. Exercise! □

Remark 14. It follows that $\mathrm{Hom}((-), X), \mathrm{Hom}(X, (-))$ are left exact (as right-adjoints) and $X \otimes_A (-)$ is right exact (as a left-adjoint).

Corollary 5. Recall that given two rings A and B, and a homomorphism $\phi : A \to B$, we have the restriction of scalars from B-Mod to A-Mod via taking M and setting $a \cdot_A m = \phi(a) \cdot_B m$. The two functors $B \otimes_A (-)$ and $\mathrm{Hom}_A(B, (-))$ are left and right adjoints to the restriction of scalar functors.

Proof. Apply Tensor-Hom adjunctions to B: $B \otimes_A (-)$ is left adjoint to $\mathrm{Hom}_B(B, (-))$ when B is viewed as a B-Mod-A and $B \otimes_B (-)$ is left adjoint to $\mathrm{Hom}_A(B, (-))$ when B is viewed as A-Mod-B. Note $\mathrm{Hom}_B(B, (-))$ and $B \otimes_B (-)$ are precisely the restriction of scalars (why?). □

Proposition 6. Given a commutative ring R, $S^{-1}R \otimes_R M$ is naturally isomorphic to $S^{-1}M$ (as $S^{-1}R$-modules). And given a ring R (not necessarily commutative) and a (two-sided) ideal I, $R/I \otimes_R M$ is naturally isomorphic to $M/I \cdot M$ (as R/I-modules).

Proof. We define an R-bilinear map $S^{-1}R \times M \to S^{-1}M$ via $(\frac{r}{s}, m) \mapsto \frac{rm}{s}$, which induces an R-linear map $S^{-1} \otimes_R M \to S^{-1}M$, with $\frac{r}{s} \otimes_R m \mapsto \frac{rm}{s}$. Now, we define a map $M \to S^{-1}R \otimes_R M$ via $m \to \frac{1}{1} \otimes m$, which is clearly R-linear. Then, since $S^{-1}R \otimes_R M$ is an $S^{-1}R$-module (every element of S acts as an automorphism), this descends to a map $S^{-1}M \to S^{-1}R \otimes_R M$ with $\frac{m}{s} \mapsto (s \cdot -)^{-1}(\frac{1}{1} \otimes_R m) = \frac{1}{s} \otimes_R m$. It's not hard to check that the two maps are inverses.

Similarly, for R/I, we have a bilinear map $R/I \times M \to M/I \cdot M$ via $(\overline{r}, m) \mapsto rm + IM$. We can check that this does not depend on the representative of $\overline{r} = r + I$. So we have an induced R-linear map $R/I \otimes_R M \to M/I \cdot M$ via $\overline{r} \otimes_R m \mapsto rm + IM$. Now, we also define a map $M \to R/I \otimes_R M$ via $m \mapsto \overline{1} \otimes_R m$, whose kernel contains IM (check!). So this descends to the R-linear map $M/I \cdot M \to R/I \otimes_R M$ via $m + IM \mapsto \overline{1} \otimes_R m$. It's not hard to check again, that the two maps are inverses of one another. □

Corollary 6. $S^{-1}R$ is flat, and the functor $M \to M/I \cdot M$ is right-exact.

Discussion 6 - Rings and Modules Qual Problems

Spring 2020 Problem 10: Let R be a commutative ring and M a left R-module. Let $f : M \to M$ be a surjective R-linear endomorphism. [Hint: Let $R[X]$ act on M via f.]

(a) Suppose that M is finitely generated. Show that f is an isomorphism and that f^{-1} can be described as a polynomial in f.

(b) Show that this fails if M is not finitely generated.

Proof. (b): Take $M = R^{(\mathbb{N})}$ and $f : M \to M(r_1, r_2, \dots, r_n, \dots) \mapsto (r_2, r_3, \dots, r_n, \dots)$. This is clearly surjective (and R-linear) but not injective.
(a): As given in the hints, turn M into an $R[X]$-module via $X \cdot m = f(m)$. More formally, we have $R \to \mathrm{End}_R(M)$ via $r \mapsto (m \mapsto rm)$ and $X \mapsto f \in \mathrm{End}_R(M)$. By the universal property, we have the map $R[X] \to \mathrm{End}_R(M)$. Now, M still remains finitely

generated, and by surjectivity of f, $M = (X)M$. So by Nakayama's lemma, there exists $q \cong 1 \bmod (X)$ such that $q(X)M = 0$. Set $q(X) = 1 + p(X)X$.

Let's look at $\ker(f)$. Let m be such that $f(m) = X \cdot m = 0$. Then, $p(X)X \cdot m = 0$. So $0 = q(X)m = m + p(X)Xm = m$. Hence, it follows $\ker(f) = 0$, and f is injective. For the inverse of f, consider $m = Xn$. Then, $p(X)m = p(X)Xn = -n$. So $n = -p(X)m$, so $f^{-1} = -p(f)$. □

Spring 2021 Problem 6: Let A be a commutative ring, and P a flat A-module and let I be an injective A-module. Show that $\mathrm{Hom}_A(P, I)$ is an injective A-module.

Proof. Let $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ be a short exact sequence. We want $\mathrm{Hom}_A((-), \mathrm{Hom}_A(P, I))$ to be an exact functor. First, since P is flat, we have a short exact sequence $0 \longrightarrow P \otimes_A L \longrightarrow P \otimes_A M \longrightarrow P \otimes_A N \longrightarrow 0$

Next, we use that I is an injective to an exact sequence:

$$0 \longrightarrow \mathrm{Hom}_A(P \otimes_A N, I) \longrightarrow \mathrm{Hom}_A(P \otimes_A M, I) \longrightarrow \mathrm{Hom}_A(P \otimes_A L, I) \longrightarrow 0$$

But by Tensor-Hom adjunction, this is precisely naturally isomorphic to an exact sequence:

$$0 \longrightarrow \mathrm{Hom}_A(N, \mathrm{Hom}_A(P, I)) \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(P, I)) \longrightarrow \mathrm{Hom}_A(L, \mathrm{Hom}_A(P, I)) \longrightarrow 0$$

So we have that $\mathrm{Hom}_A((-), \mathrm{Hom}_A(P, I))$ is exact, as desired. □

Spring 2020 Problem 9: Let R be a commutative ring and $S \subset R$ a multiplicative subset. Construct a natural transformation (in either direction) between the functors $\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ and $S^{-1}\mathrm{Hom}_R(M, N)$, considered as functors of R-modules M and N, and prove that it is an isomorphism if M is finitely presented.

Proof. Observe that we have a R-linear map from $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ given by $f \mapsto S^{-1}f$ (the localization functor map). Since the latter is an $S^{-1}R$-module (where S acts invertibly), this descends to an $S^{-1}R$-linear map $S^{-1}\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ via $\frac{f}{s} \mapsto \frac{S^{-1}f}{s} : \frac{m}{t} \mapsto (s\cdot(-))^{-1}S^{-1}f(\frac{m}{t}) = (s\cdot(-))^{-1}\frac{f(m)}{t} = \frac{f(m)}{st}$. We live it as an exercise to check that this is natural in both M and N.

Now, recall M is finitely presented if there exists an exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

For a fixed M, denote the map $S^{-1}\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ via $\frac{f}{s} \mapsto \frac{S^{-1}f}{s}$ as η_M. We show that η_M is an isomorphism in stages:

<u>$M = R$ case</u>: we have the following commutative diagram:

$$\begin{array}{ccc} S^{-1}\mathrm{Hom}_R(R, N) & \xrightarrow{\eta_R} & \mathrm{Hom}_{S^{-1}R}(S^{-1}R, S^{-1}N) \\ \downarrow & & \downarrow \\ S^{-1}N & \xrightarrow{\quad\mathrm{id}\quad} & S^{-1}N \end{array}$$

To check that this is commutative, the top map (η_R) takes $\frac{f}{s}$ to $\frac{S^{-1}f}{s}$. The right map takes $\frac{S^{-1}f}{s}$ to $\frac{S^{-1}f}{s}(\frac{1}{1}) = \frac{f(1)}{s}$. The left map takes $\frac{f}{s}$ to $\frac{f(1)}{s}$, which gets sent to itself by the identity map on the bottom. So the above diagram is commutative. Since all three other maps are isomorphisms, so is η_R.

$\underline{M = R^n \text{ case}}$: We have that $\eta_{R^n} : S^{-1}\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ is given by $\frac{1}{s}\begin{pmatrix} f_1 & f_2 & \cdots & f_n \end{pmatrix} \mapsto \begin{pmatrix} \frac{S^{-1}f_1}{s} & \frac{S^{-1}f_2}{s} & \cdots & \frac{S^{-1}f_n}{s} \end{pmatrix}$. Injectivity is clear from injectivity in each entry. For surjectivity, suppose we had $\begin{pmatrix} h_1 & h_2 & \cdots & h_n \end{pmatrix}$ given by $h_i = \frac{S^{-1}f_i}{t_i}$ for some f_i and $t_i \in S$. Then, set $\hat{t}_i = t_1 t_2 \cdots t_{i-1} t_{i+1} \cdots t_n$ and $t = t_1 t_2 \cdots t_n$. Then, the above map is the image of the map $\frac{1}{t}\begin{pmatrix} \hat{t}_1 f_1 & \hat{t}_2 f_2 & \cdots & \hat{t}_n f_n \end{pmatrix}$

$\underline{\text{General case}}$: We have an exact sequence $R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$. By left exactness of the functors

$$S^{-1}\mathrm{Hom}_R((-), N)(= S^{-1}(-) \circ \mathrm{Hom}_R((-), N))$$

and

$$\mathrm{Hom}_{S^{-1}R}(S^{-1}(-), S^{-1}N)(= \mathrm{Hom}_{S^{-1}R}((-), S^{-1}N) \circ S^{-1}(-))$$

we have a natural transformation between the exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & S^{-1}\mathrm{Hom}_R(M,N) & \longrightarrow & S^{-1}\mathrm{Hom}_R(R^n,N) & \longrightarrow & S^{-1}\mathrm{Hom}_R(R^m,N) \\
\downarrow \simeq & & \downarrow \simeq & & \downarrow \eta_M & & \downarrow \eta_{R^n} \simeq & & \downarrow \eta_{R^m} \simeq \\
0 & \longrightarrow & 0 & \longrightarrow & \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) & \longrightarrow & \mathrm{Hom}_{S^{-1}R}(S^{-1}R^n, N) & \longrightarrow & \mathrm{Hom}_{S^{-1}R}(S^{-1}R^m, N)
\end{array}$$

We know from the $M = R^n$ case that the last two columns are isomorphisms, and the first two columns are clearly isomorphisms. By the five lemma, the middle column map η_M is also an isomorphism. □

Fall 2018 Problem 9: Let $f : M \to N$ and $g : N \to M$ be two R-linear homomorphisms of R-modules such that $\mathrm{id}_M - gf$ is invertible. Show that $\mathrm{id}_N - fg$ is invertible as well and give a formula for its inverse. [Hint: You may use Analysis to make a guess.]

Proof. As given in the hints, we use analysis to make a guess: if we had an operator $A : L \to L$ from a $\mathbb{R}$-vector space with $||A|| < 1$, then $(I - A)^{-1} = I + A + A^2 + \cdots$. So this is how we make a guess:

$$\begin{aligned}
(\mathrm{id}_N - fg)^{-1} &= \mathrm{id} + fg + fgfg + fgfgfgfg + \cdots + (fg)^{m+1} + \cdots \\
&= \mathrm{id} + f[\mathrm{id}_M + gf + gfgf + \cdots + (gf)^m + \cdots]g \\
&= \mathrm{id} + f(\mathrm{id}_M - gf)^{-1}g
\end{aligned}$$

Now that we made a guess, it remains to check that the guess is in fact the desired inverse.

$$\begin{aligned}
(\mathrm{id}_N - fg)(\mathrm{id}_N + f(\mathrm{id}_M - gf)^{-1}g) &= \mathrm{id}_N - fg + f(\mathrm{id}_M - gf)^{-1}g - fgf(\mathrm{id}_M - gf)^{-1}g \\
&= \mathrm{id}_N - fg + f\cancel{[\mathrm{id}_M - gf](\mathrm{id}_M - gf)^{-1}}g \\
&= \mathrm{id}_N - fg + f\mathrm{id}_M g \\
&= \mathrm{id}_N
\end{aligned}$$

And

$$\begin{aligned}(\mathrm{id}_N + f(\mathrm{id}_M - gf)^{-1}g)(\mathrm{id}_N - fg) &= \mathrm{id}_N - fg + f(\mathrm{id}_M - gf)^{-1}g - f(\mathrm{id}_M - gf)^{-1}gfg \\ &= \mathrm{id}_N - fg + f\cancel{(\mathrm{id}_M - gf)^{-1}[\mathrm{id}_M - gf]}g \\ &= \mathrm{id}_N - fg + f\mathrm{id}_M g \\ &= \mathrm{id}_N\end{aligned}$$

□

Discussion 7 - Rings and Modules Qual Problems Part 2

Spring 2019 Problem 4: Let R be a commutative local ring and P a finitely generated projective R-module. Prove that P is R-free.

Proof. Let $\mathfrak{m}$ be the unique maximal module $\mathfrak{m} = R - R^\times$, and $K = R/\mathfrak{m}$. Then, consider $K \otimes_R P \simeq P/\mathfrak{m}P$. It is a finitely generated $R/\mathfrak{m} = K$-module (vector space!), so it has a finite basis: $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}$. Then, consider the elements $x_1, x_2, \ldots, x_n \in P$ mapping to the basis.

We can now define a map $f : R^n \to P$ by $e_i \mapsto x_i$ (which, by the universal property of the coproduct, extends to the unique R-linear homomorphism). This f will be our desired isomorphism. The conclusion follows immediately from the next two claims:

Claim. f is surjective

Proof of the Claim. We have an exact sequence $R^n \xrightarrow{f} P \twoheadrightarrow \mathrm{coker}(f) \longrightarrow 0$

Tensoring $(K \otimes_R (-))$ is right-exact, so we have a new exact sequence:

$$\begin{array}{ccccccc} K \otimes_R R^n & \xrightarrow{\mathrm{id}\otimes_R f} & K \otimes_R P & \twoheadrightarrow & K \otimes_R \mathrm{coker}(f) & \longrightarrow & 0 \\ \downarrow\simeq & & \downarrow\simeq & & \downarrow\simeq & & \downarrow\simeq \\ K^n & \longrightarrow & P/\mathfrak{m}P & \twoheadrightarrow & \mathrm{coker}(f)/\mathfrak{m}\mathrm{coker}(f) & \longrightarrow & 0 \end{array}$$

But note that $\mathrm{id}\otimes_R f$ sends $1_K \otimes_R e_i$ to $1_K \otimes_R x_i$, so in the corresponding bottom exact sequence, the new map sends $e_i \in K^n$ to $\overline{x_i}$, so this is in fact, an isomorphism. Hence, the map from $P/\mathfrak{m}P$ to $\mathrm{coker}(f)/\mathfrak{m}\mathrm{coker}(f)$ is in fact, the zero map, so $\mathrm{coker}(f)/\mathfrak{m}\mathrm{coker}(f) = 0$. But that implies $\mathrm{coker}(f) = \mathfrak{m}\mathrm{coker}(f)$. Since $\mathrm{coker}(f)$ is finitely generated (as a quotient of a finitely generated module), by Nakayama's lemma, $\mathrm{coker}(f) = 0$. So f is in fact, surjective. □

Claim. f is injective.

Proof of the Claim. This time, we have a short exact sequence:

$$0 \longrightarrow \ker(f) \longrightarrow R^n \xrightarrow{f} P \longrightarrow 0$$

Since P is projective, the sequence is split, so we have $R^n \simeq \ker(f) \oplus P$, so by tensoring, we get $K \otimes_R R^n \simeq K^n \simeq (K \otimes_R \ker(f)) \oplus (K \otimes_R P) \simeq \ker(f)/\mathfrak{m}\ker(f) \oplus P/\mathfrak{m}P$. Note, by construction, $\dim_K(P/\mathfrak{m}P) = n = \dim_K(K^n)$. So in particular, $\dim_K(\ker(f)/\mathfrak{m}\ker(f)) = 0$, so $\ker(f)/\mathfrak{m}\ker(f) = 0$, i.e. $\ker(f) = \mathfrak{m}\ker(f)$.

Once again, $\ker(f)$ is finitely generated as a direct summand (hence a quotient) of R^n. So by Nakayama's lemma, $\ker(f) = 0$. □

□

Fall 2020 Problem 4: Let R be a ring and M be a left R-module. Show that M is a projective R-module if and only if there is an index set I and $m_i \in M$ and $f_i : M \to R$ R-linear satisfying:

(a) For all $m \in M$, $f_i(m) = 0$ for all but finitely many $i \in I$.

(b) For all $m \in M$, $m = \sum_{i \in I} f_i(m) m_i$

Proof. ($\Rightarrow$ Part:) Let M be a projective R-module. Then, $M \oplus N = R^{(I)}$ for some index set I (i.e. M is a direct summand of a free-module $R^{(I)}$). Define $\pi : R^{(I)} \to M$ the projection onto M. For each $i \in I$, define $g_i : R^{(I)} \to R$ by $g_i(e_j) = 1$ if $j = i$ and 0 else. Take $m_i = \pi(e_i)$ and $f_i = g_i \restriction M$ which is really $g_i \circ k$ where $k : M \to R^{(I)}$ is the embedding.

Now, we check these m_i's and f_i's satisfy (a) and (b). For (a), note for all $m \in M$, $m = \sum_{j \in I} a_j e_j$ for $a_j \in R$ where $a_j = 0$ for all but finitely many $j \in J$. Then, $f_i(m) = \sum_{j \in I} a_j f_i(e_j) = a_i$. So $a_i = f_i(m) = 0$ for all but finitely many $i \in I$. For (b), we now have:

$$\begin{aligned} m = \pi(m) &= \pi(\sum_{i \in I} a_i e_i) \\ &= \sum_{i \in I} a_i \pi(e_i) \\ &= \sum_{i \in I} f_i(m) m_i \end{aligned}$$

as desired.
($\Leftarrow$ Part): Suppose we're given such $m_i \in M$ and $f_i : M \to R$. Now, define $f : M \to R^I$ via $f(m) = (f_i(m))_{i \in I}$ (this f is the unique R-linear map satisfying the universal property of the product). Note by condition (a), $f(m) \in R^{(I)}$.

Now, define $\pi : R^{(I)} \to M$ via $e_i \mapsto m_i \in M$ (so that $(r_i)_{i \in I} \mapsto \sum_{i \in I} r_i m_i$). Now, we check $\pi \circ f = \mathrm{id}_M$:

$$\pi \circ f(m) = \pi((f_i(m))_{i \in I}) = \sum_{i \in I} f_i(m) m_i \underbrace{=}_{\text{by (b)}} m$$

Hence, $f : M \to R^{(I)}$ is an embedding of M into a free module which splits: so M is a direct summand of a free-module, hence projective. □

Spring 2018 Problem 7: Let B be a commutative noetherian ring, and let A be a noetherian subring of B. Let I be the nilradical of B. If B/I is finitely generated as an A-module, show that B is finitely generated as an A-module.

Proof. Observe that since B is noetherian, I is finitely generated: $I = (b_1, b_2, \ldots, b_k)$ for some k. Choose $n_1, n_2, \ldots, n_k$ such that $b_i^{n_i} = 0$. Then, if we set $N = n_1 + n_2 + \cdots + n_k + 1$, $I^N \subseteq (b_1^{n_1}, b_2^{n_2}, \ldots, b_k^{n_k}) = 0$, so $I^N = 0$.

Consider the ring B/I^2. Since $I \supset I^2$, I/I^2 is an ideal of B/I^2. Moreover, the quotient $B/I^2 \big/ I/I^2 \simeq B/I$. So we have a short exact sequence:

$$0 \longrightarrow I/I^2 \longrightarrow B/I^2 \longrightarrow B/I \longrightarrow 0$$

Note $I \cdot (I/I^2) = I^2/I^2 = 0$ (take any $r, s \in I$, and $r \cdot s \in I^2$, so $r \cdot \overline{s} = 0$). So both B/I and I/I^2 are B-modules that vanish when multiplied by I, hence B/I-modules. Moreover, since I/I^2 is finitely generated B-module, it remains finitely generated as a B/I-module. But since B/I is finitely generated as an A-module, I/I^2 and B/I remain finitely generated as an A-module. This is an exercise!

Exercise 3. Show that if $f : R \to S$ a ring homomorphism between commutative rings and M is a finitely generated S-module, and S a finitely generated R module via restriction of scalars, then M is finitely generated as an R-module as well.

Now, we I/I^2 and B/I finitely generated as A-modules, so the middle term in the exact sequence B/I^2 (which is an A-module) is also finitely generated A-module. Again, this is an exercise!

Exercise 4. Show if $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence of A-modules and L and N are finitely generated, then M is finitely generated as well.

Now, by induction on m, we'll show that B/I^m is A-finitely generated. We already did $m = 1$ and illustrated the idea for $m \to m + 1$ inductive step for $m = 1$.

Take the exact sequence $0 \longrightarrow I^m/I^{m+1} \longrightarrow B/I^{m+1} \longrightarrow B/I^m \longrightarrow 0$

Once again, I^m/I^{m+1} is a finitely generated B/I-module, hence is finitely generated as an A-module. By the inductive hypothesis, B/I^m is A-finitely generated. So B/I^{m+1} is a finitely generated A-module as well.

Taking $m = N$, we get $B/I^N = B$ is a finitely generated A-module, as desired. □

Discussion 8 - Field Theory Basics

Proposition 7. Let $f : A \to B$ and $g : A \to C$ be homomorphisms between commutative rings. Then, $B \otimes_A C$ is an A-module. But we can turn $B \otimes_A C$ into a ring as well as by defining multiplication as follows:

$$(b \otimes_A c) \cdot (r \otimes_A s) = br \otimes_A cs$$

and extending linearly. It's not hard to check that $B \otimes_A C$ is a commutative ring with homomorphisms $B \to B \otimes_A C, b \mapsto b \otimes_A 1$ and $C \to B \otimes_A C, c \mapsto 1 \otimes_A c$. In fact, we have a pushout diagram in Commutative Rings:

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ \downarrow{\scriptstyle f} & & \downarrow \\ B & \longrightarrow & B \otimes_A C \end{array}$$

In particular, if $A = \mathbb{Z}$, then $B \otimes_A C$ is a coproduct in the category of commutative rings (which is related to a homework problem).

Remark 15. There is a problem with the above definition of multiplication and "extending linearly." It's not clear that the multiplication is well-defined: if $\sum_{i=1}^{n} b_i \otimes_A c_i = \sum_{j=1}^{m} b'_j \otimes_A c'_j$ and $\sum_{k=1}^{u} r_k \otimes_A s_k = \sum_{l=1}^{v} r'_l \otimes_A s'_k$ in $B \otimes_A C$, it's not clear that the corresponding products $\sum_{i,k} b_i r_k \otimes_A c_i s_k$ and $\sum_{j,l} b'_j r'_l \otimes_A c'_j s'_l$ are equal in $B \otimes_A C$. In fact, checking this manually (using Tensor product construction) is very tedious.

Here is how we get around to this issue: given $b \in B$ and $c \in C$, we have $b\cdot(-) : B \to B$ and $c \cdot (-) : C \to C$ multiplication by the corresponding elements, which are also A-module homomorphisms when B and C are viewed as such. The maps $b \cdot (-)$ and $c \cdot (-)$ lie in $\mathrm{End}_A(B)$ and $\mathrm{End}_A(C)$, and the assignment $b \mapsto b \cdot (-)$ and $c \mapsto c \cdot (-)$ are A-linear from $B \to \mathrm{End}_A(B)$ and $C \to \mathrm{End}_A(C)$. Moreover, we know that given any $\phi : B \to B$ and $\psi : C \to C$ A-linear, we can define $\phi \otimes_A \psi : B \otimes_A C \to B \otimes_A C, A$-linear, and the assignment $\mathrm{End}_A(B) \times \mathrm{End}_A(C) \to \mathrm{End}_A(B \otimes_A C)$ is A-bilinear.

Hence, the composition $B \times C \to \mathrm{End}_A(B) \times \mathrm{End}_A(C) \to \mathrm{End}_A(B \otimes_A C)$ is A-bilinear. So in particular, this induces the unique A-linear $B \otimes_A C \to \mathrm{End}_A(B \otimes C)$. We want the image of x in $\mathrm{End}_A(B \otimes C)$ to define a multiplication by x: define $x \cdot y =$ to be the evaluation of image of x in $\mathrm{End}_A(B \otimes_A C)$ at y. It's not hard to check that this turns $B \otimes_A C$ into a commutative ring. Moreover, $(b \otimes_A c) \cdot (r \otimes_A s) = br \otimes_A cs$ so this agrees with our desired definition from the proposition.

Spring 2018 Problem 8: Let F be a field that contains the real numbers $\mathbb{R}$ as a subfield. Show that the tensor product $F \otimes_R \mathbb{C}$ is either a field or isomorphic to the product of two copies of F, $F \times F$.

Proof. Observe that $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$, so $F \otimes_R \mathbb{C} \simeq F \otimes_R \mathbb{R}[X]/(X^2+1)$. It'd be nice if $F \otimes_R \mathbb{R}[X]/(X^2+1)$ is isomorphic to $F[X]/(X^2+1)$. And it is indeed true:

Claim. In general, given two commutative rings A and B and $f : A \to B$, $A[X] \otimes_A B = B[X]$.

Proof of the Claim. Define the A-linear map from $A[X] \otimes_A B \to B[X]$ by $p(X) \otimes_A b \mapsto bf(p)(X)$ (here, given $p(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, $f(p)(X) = f(a_0) + f(a_1)X + \cdots + f(a_n)X^n$). This is the A-linear map induced from the bilinear map $A[X] \times B \to B[X], (p(X), b) \mapsto bf(p)(X)$. It's not hard to check that this map is also a ring homomorphism (or, as we'll see now, it is the inverse of the map we'll construct which we know is a ring homomorphism).

Next, define the ring homomorphism by $B[X] \to A[X] \otimes_A B, b \mapsto 1 \otimes_A b$ and $X \mapsto X \otimes_A 1$ (the universal property guarantees there is exactly one such ring homomorphism with this property). It's not hard to check that these two maps are inverses of one another. □

Claim. $L \subset F$ be a field extension, and $p \in L[X]$. Then, $F \otimes_L L[X]/(p) \simeq F[X]/(p)$.

Proof of the Claim. We have an exact sequence

$$0 \longrightarrow pL[X] \longrightarrow L[X] \longrightarrow L[X]/pL[X] \longrightarrow 0$$

Then, tensoring with F, the L-free vector space, gives you the exact sequence:

$$0 \longrightarrow F \otimes_L pL[X] \longrightarrow F \otimes_L L[X] \longrightarrow F \otimes_L L[X]/pL[X] \longrightarrow 0$$

By the claim, $F \otimes_L L[X] \simeq F[X]$ as rings. Now, $F \otimes_L pL[X]$ gets sent to $pF[X]$ in $F[X]$ (exercise!). So it follows that $F \otimes_L L[X]/pL[X] \simeq F[X]/pF[X]$. □

Now, it follows that $F \otimes_{\mathbb{R}} \mathbb{C} \simeq F \otimes_{\mathbb{R}} \mathbb{R}[X]/(X^2+1) \simeq F[X]/(X^2+1)$. We can divide into cases when F contains the root of X^2+1 or not.

Case i): F does not contain an element i such that $i^2+1 = 0$. Then, X^2+1 is a quadratic polynomial with no roots, so it is irreducible. Hence, $F[X]/(X^2+1)$ is a field.

Case ii: F contains an element i such that $i^2+1=0$. Then, $X^2+1=(X-i)(X+i)$, so by the Chinese Remainder Theorem, $F[X]/(X-i)(X+i) \simeq F[X]/(X-i) \times F[X]/(X+i) \simeq F \times F$. □

Spring 2018 Problem 1: Let $\alpha \in \mathbb{C}$. Suppose that $[\mathbb{Q}(\alpha):\mathbb{Q}]$ is finite and prime to $n!$ for an integer $n > 1$. Show that $\mathbb{Q}(\alpha^n) = \mathbb{Q}(\alpha)$.

Proof. Call $[\mathbb{Q}(\alpha):\mathbb{Q}] = m$. Then, the assumption is that $\gcd(m, n!) = 1$. Now, we have $\mathbb{Q}(\alpha^n) \subset \mathbb{Q}$ so $[\mathbb{Q}(\alpha):\mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^n)]}_{k} \cdot [\mathbb{Q}(\alpha^n):\mathbb{Q}] = k[\mathbb{Q}(\alpha^n):\mathbb{Q}]$. So k divides m.

Moreover, we know that $X^n - \alpha^n \in \mathbb{Q}(\alpha^n)[X]$ is a polynomial with root α. So $m \leq n$, so m divides $n!$. Since $\gcd(m, n!) = 1$, k must be 1. □

Fall 2021 Problem 1: Let $a \in \mathbb{Q}$ and $b, d \in \mathbb{Q}^\times$, and suppose that d is not a cube in $\mathbb{Q}^\times$. Find the minimal polynomial of $a + b\sqrt[3]{d}$ over $\mathbb{Q}$.

Proof. Let $\alpha = a + b\sqrt[3]{d}$. Then, $\alpha - a = b\sqrt[3]{d}$, so cubing both sides, we get $(\alpha - a)^3 = b^3 d$. So clearly, $(X-a)^3 - b^3 d \in \mathbb{Q}[X]$ is a polynomial with α as a root. We claim that it is actually the minimal polynomial.

First, observe that in $Y^3 - b^3 d \in \mathbb{Q}[Y]$ has no root since $b^3 d$ is not a cube (otherwise, d would be a cube!). Since it is a polynomial of degree ≤ 3, it is actually irreducible. So now, the ring homomorphism $\mathbb{Q}[Y] \to \mathbb{Q}[X]$ given by $Y \mapsto X - a$ is an isomorphism with inverse $X \mapsto Y + a$. Then, $(X-a)^3 - b^3 d$ is an image of the irreducible $Y^3 - b^3 d$, so $(X-a)^3 - b^3 d$ is monic irreducible as well. It follows that this must be the minimal polynomial. □

Spring 2019 Problem 6: Let F be a field of characteristic $p > 0$ and $a \in F^\times$. Prove that if the polynomial $f = X^p - a$ has no root in F, then f is irreducible over F.

Proof. Choose any root α and an extension $F(\alpha) \supset F$. Then, in $F(\alpha)[X]$, $f = X^p - a = X^p - \alpha^p = (X-\alpha)^p$.
Suppose $g \mid f$ in $F[X]$ with $\deg(g) > 0$ (i.e. g is a polynomial IN $F[X]$ dividing f). In, $F(\alpha)[X]$, $g = (X-a)^k$ for some $k = 1, 2, \ldots, p$. If $k < p$, then g has the form $X^k - k\alpha X^{k-1} + \text{Junk}$. $-k\alpha \in F$ and $-k \in F^\times$ since $k < p$. So $\alpha \in F$ contradicting that $X^p - a$ did not have a root in F. So it follows $k = p$ and $g = (X-\alpha)^p = f$. □

Discussion 9 - Galois Theory

Fall 2019 Problem 2: Let L be a Galois extension of field K inside an algebraic closure $\overline{K}$ of K. Let M be a finite extension K in $\overline{K}$. Show that the following are equivalent:

(i) $L \cap M = K$,

(ii) $[LM:K] = [L:K][M:K]$,

(iii) Every K-linearly independent subset of L is M-linearly independent.

Proof. (I) $\Leftrightarrow$ (II) Part: Note, since L/K is Galois, LM/M is Galois, and we have an isomorphism $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/L\cap M)$ given by $\sigma \mapsto \sigma\mid_L$. So $[LM : M] = [L : L \cap M]$. Since $[LM : K] = [LM : M][L : K] = [L : L\cap M][L : K]$. Now, the second condition is clearly equivalent to $[L : L \cap M] = [L : K]$ but since $[L : K] = [L : L \cap M][L \cap M : K]$, this is equivalent to $[L \cap M : K] = 1$, the first condition.
(III) $\Rightarrow$ (I) Part: Choose a K-basis $x_1, x_2, \ldots, x_n \in L$. Then, by assumption, this is M-linearly independent in LM. So $[LM : M] \geq n = [L : K]$. But again, by the isomorphism, $[L : L \cap M] \geq [L : K]$, and the only way this can happen is if $L \cap M = K$.
(I) $\Rightarrow$ (III) Part: Since L/K is separable, there exists an $\alpha \in L$ such that $L = K[\alpha]$. Then, $LM = M[\alpha]$. Now, let $p \in K[X]$ be the minimal polynomial of α. Since $[K[\alpha] : K] = [L : K] = [LM : M] = [M[\alpha] : M]$, it follows that p must remain irreducible in $M[X]$ as well (otherwise, we'd have a minimal polynomial of small degree, making $[M[\alpha] : M]$ smaller.

We now, have the following commutative diagram:

$$\begin{array}{ccc} M[\alpha] & \xrightarrow{\simeq} & M[X]/(p) \\ \uparrow & & \uparrow \\ K[\alpha] & \xrightarrow{\simeq} & K[X]/(p) \end{array}$$

But note $M[X]/(p) \simeq M \otimes_K K[X]/(p)$. If $f_1, f_2, \ldots, f_n \in K[X]/(p)$ is K-linearly independent, we have an exact sequence $0 \longrightarrow K^n \longrightarrow K[X]/(p)$ where $e_i \in K^n$ is sent to f_i. Since M is a flat (and in fact, free) K-vector space, so tensoring with M, we get: $0 \longrightarrow M^n \longrightarrow M[X]/(p)$ where $e_i \in M^n$ is still send to f_i. So the f_i's remain M-linearly independent. □

Fall 2020 Problem 5: Let F be a field and $f(X) = x^6 + 3$. Determine the splitting field K of $f(X)$ over F and determine $[K : F]$ and $\mathrm{Gal}(K/F)$ for each of the following fields: $F = \mathbb{Q}, \mathbb{F}_5, \mathbb{F}_7$.

Soln: The $\mathbb{Q}$ case is left as a homework!
$\underline{\mathbb{F}_5 \text{ case}}$: Let a be a root (in a large enough finite extension) of X^6+3. Then, $a^6 = -3 = 2$, so $(a^6)^4 = a^{24} = 2^4 = 1$ by Fermat's little theorem. But then, we know that $a^{25} = a$. Hence, it follows that every root a is contained in $\mathbb{F}_{5^2}$. Now, note no root a is contained in $\mathbb{F}_{5^2}$: since for every $k \in \mathbb{F}_5$, $k^4 = 1$, $k^2 = \pm 1$, so 2 is not a square. So $K = \mathbb{F}_{5^2}$ and the $\mathrm{Gal}(K/F) = \mathbb{Z}/2Z$.
$\underline{\mathbb{F}_7 \text{ case}}$: Once again, for every root a of $X^6 + 3$, we have $a^6 = -3 = 4 = 2^2$. So $(a^6)^3 = a^18 = 2^6 = 1$ by Fermat's little theorem. So we look for n such that $18 \mid 7^n - 1$, so that $a^{7^n-1} = 1$. We can try $n = 1, 2, 3, \ldots$ and see that $n = 3$ is the smallest such n. So $K \subset \mathbb{F}_{7^3}$. Since $\mathbb{F}_{7^3}$ has degree 3 (prime), over $\mathbb{F}_7$, either $K = \mathbb{F}_7$ or $K = \mathbb{F}_{7^3}$. Once again, we know that since $b^6 = 1$ for every $b \in \mathbb{F}_7$, $b^3 = \pm 1$, which 4 is not equal to. So no root of $x^6 + 3$ can be in $\mathbb{F}_7$, so $K = \mathbb{F}_{7^3}$. □

Spring 2021 Problem 4: Prove that the field extension $\mathbb{Q}(\sqrt{-3} + \sqrt[6]{2})$ over $\mathbb{Q}$ is Galois and determine its Galois group.

Proof. Observe first that given a field extension $\mathbb{Q} \subset F$, $\sqrt{-3} \in F$ if and only if $\zeta_6 \in F$ where ζ_6 is the principal 6th root of unity. To see this, we can see that $X^6 - 1 =$

$(X^3-1)(X^3+1) = (X-1)(X+1)(X^2+X+1)(X^2-X+1)$, and ζ_6 is the root of X^2-X+1.

So then, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_6)$. Hence, $\mathbb{Q}(\sqrt{-3}+\sqrt[6]{2}) \subseteq \mathbb{Q}(\sqrt{-3}, \sqrt[6]{2})$. Set $F = \mathbb{Q}(\sqrt{-3}+\sqrt[6]{2})$ and $K = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$, and set $G = \mathrm{Gal}(K/\mathbb{Q})$ and $N = \mathrm{Gal}(K/F)$ so that $F = K^N$. Note clearly, $K/\mathbb{Q}$ is Galois since it is the splitting field of $X^6-2 \in \mathbb{Q}[X]$, so it suffices to find G and N, and show that $N \trianglelefteq G$ so that $F/\mathbb{Q}$ is normal (and hence Galois), and that $\mathrm{Gal}(\mathbb{Q}(\sqrt{-3}+\sqrt[6]{2}/\mathbb{Q}) \cong G/N$.

First, consider any element $\sigma \in G$. Then, it is determined uniquely by the values of $\sigma(\zeta_6)$ and $\sigma(\sqrt[6]{2})$, since K is generated as a field by $\mathbb{Q}$ and $\zeta_6, \sqrt[6]{2}$. Now, $\sigma(\sqrt[6]{2}) = \sqrt[6]{2}\zeta_6^a$ for some (unique) $a \in \mathbb{Z}/6\mathbb{Z}$ and $\sigma(\zeta_6) = \zeta_6^b$ for some $b \in (\mathbb{Z}/6\mathbb{Z})^\times$. So this gives us the embedding $G \to \mathbb{Z}/6\mathbb{Z} \rtimes (\mathbb{Z}/6\mathbb{Z})^\times$ for some appropriate semidirect product. Let us analyze it: suppose $\tau \mapsto (a_1, b_1)$ and $\sigma \mapsto (a_2, b_2)$. Then, $\tau \circ \sigma(\zeta_6) = \tau(\zeta_6^{b_2}) = (\zeta^{b_1})_6^{b_2} = \zeta_6^{b_1 b_2}$, and $\tau \circ \sigma(\sqrt[6]{2}) = \tau(\sqrt[6]{2}\zeta_6^{a_2}) = \tau(\sqrt[6]{2})\tau(\zeta_6^{a_2}) = \sqrt[6]{2}\zeta_6^{a_1}\zeta_6^{b_1 a_2} = \sqrt[6]{2}\zeta_6^{a_1+b_1 a_2}$. So, a semidirect product structure where the mapping $\sigma \mapsto (a, b)$ is a homomorphism is given by $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + b_1 a_2, b_1 b_2)$, which is the semidirect product structure induced by $(\mathbb{Z}/6\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/6\mathbb{Z})$, $k \mapsto (k \cdot (-))$.

We will next show that this embedding is actually surjective, so that $G \cong \mathbb{Z}/6\mathbb{Z} \rtimes (\mathbb{Z}/6\mathbb{Z})^\times$. To do this, we need some tools:

Claim. The fields $\mathbb{Q}(\zeta_6)$ and $\mathbb{Q}(\sqrt[6]{2})$ are linearly disjoint, i.e. $\mathbb{Q}(\zeta_6) \cap \mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}$.

Proof of the Claim. Note $\mathbb{Q}(\zeta_6 \cap \mathbb{Q}(\sqrt[6]{2})$ is a subfield of $\mathbb{Q}(\zeta_6)$, so since $[\mathbb{Q}(\zeta_6) : Q] = 2$, it is either $\mathbb{Q}$ or $\mathbb{Q}(\zeta_6)$. But that field is contained in $\mathbb{Q}(\sqrt[6]{2}) \subset \mathbb{R}$, so since $\mathbb{Q}(\zeta_6) \not\subset \mathbb{R}$, it has to be $\mathbb{Q}$. □

Since $\mathbb{Q}(\zeta_6)/\mathbb{Q}$ is Galois, so is the extension $\mathbb{Q}(\zeta_6, \sqrt[6]{2})/\mathbb{Q}(\sqrt[6]{2}$, and they have the same degree, 2. In particular, $[\mathbb{Q}(\zeta_6, \sqrt[6]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_6, \sqrt[6]{2}) : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 2 \times 6 = 12$, so $|G| = 6$. But the semidirect product also has order $6 \times 2 = 12$, so in fact, the embedding $G \to \mathbb{Z}/6\mathbb{Z} \rtimes (\mathbb{Z}/6\mathbb{Z})^\times$ must also be surjective.

Now, let's look at N. Suppose $\sigma \in N$ so that σ fixes all of F. It suffices to fix the elements $\sqrt{-3} = 2\zeta_6 + 1$ and $\sqrt[6]{2}$. So $\sigma(2\zeta_6 + 1) = 2\zeta_6^i + 1 = 2\zeta_6 + 1$ and $\sigma(\sqrt[6]{2}) = \sqrt[6]{2}\zeta_6^j = \sqrt[6]{2}$. Note, $\zeta_6^i = \zeta_6$ so $i = 1$, and $\zeta_6^j = 1$, so $j = 0$. But then, that gives us that $\sigma = \mathrm{id}$, so $N = \{\mathrm{id}\}$. Hence, $F = K \supset \mathbb{Q}$ is Galois and $\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) = G \cong \mathbb{Z}/6\mathbb{Z} \rtimes (\mathbb{Z}/6\mathbb{Z})^\times$.

□

Discussion 10 - Galois Theory Part 2

Spring 2018 Problem 2: Let $\zeta^9 = 1$ and $\zeta^3 \neq 1$ with $\zeta \notin \mathbb{C}$.

(a) Show that $\sqrt[3]{3} \notin \mathbb{Q}(\zeta)$,

(b) If $\alpha^3 = 3$, show that α is not a cube in $\mathbb{Q}(\zeta, \alpha)$.

Proof for Part (a). Suppose $\sqrt[3]{3} \in \mathbb{Q}(\zeta)$. Then, note $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/9\mathbb{Z})^\times$, which is abelian. In particular, every subgroup is normal. So it follows that the subgroup $N = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt[3]{3})$ must be normal as well. But then, the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{3})$ must be normal, but it's not (for instance, take the polynomial $X^3 - 3 \in \mathbb{Q}[X]$, which does not split in $\mathbb{Q}(\sqrt[3]{3})[X]$). □

Proof for Part (b). Once again, suppose α is a cube in $\mathbb{Q}(\zeta, \alpha)$. Then, after multiplying by an appropriate power of ζ, it follows that $\sqrt[9]{3} \in \mathbb{Q}(\zeta, \alpha)$. Also, by similar reasoning, $\mathbb{Q}(\zeta, \alpha) = \mathbb{Q}(\zeta, \sqrt[3]{3})$.

Note, by part (a), $\mathbb{Q}(\sqrt[3]{3}) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ since it is a subfield of $\mathbb{Q}(\sqrt[3]{3})$ not equal to $\mathbb{Q}(\sqrt[3]{3})$ and $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ is prime. So since $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{3})$ is Galois, so is $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{Q}(\sqrt[3]{3}, \zeta)$, and $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{3}, \zeta)/\mathbb{Q}(\sqrt[3]{3})) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$. In particular, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{3}, \zeta)/\mathbb{Q}(\sqrt[3]{3}))$ is abelian, so every subgroup is normal. But then, $\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{Q}(\sqrt[9]{3})$ is a normal extension, but it is not (as before, we can take $X^3 - \sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{3})[X]$ which does not split in $\mathbb{Q}(\sqrt[9]{3})[X]$). □

Fall 2016 Problem 5: Let $f \in F[X]$ be an irreducible separable polynomial of prime degree over a field F, and let K/F be a splitting field of f. Prove that there is an element in the Galois group of K/F permuting cyclically all roots of f in K.

Proof. Let $p = \deg(f)$ and $\alpha_1, \alpha_2, \ldots, \alpha_p$ be the p distinct roots of f in K, so that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_p)$. Now, set $G = \mathrm{Gal}(K/F)$ and we have an embedding $G \to S_p$ $\sigma \mapsto \sigma\,|_{\{\alpha_1, \alpha_2, \ldots, \alpha_p\}}$. Moreover, since K/F is Galois, and f has degree p, $p \mid [K : F] = [K : F(\alpha_1)][F(\alpha_1) : F] = [K : F(\alpha_1)]p$. So $p \mid |G|$.

By Cauchy's theorem, there exists an element σ of order p. But an element of order p in S_p must be a p-cycle, permuting all roots $\alpha_1, \alpha_2, \ldots, \alpha_p$ cyclically. □

Fall 2018 Problem 4: Let K be a subfield of real numbers and f an irreducible degree 4 polynomial over K. Suppose that f has exactly two real roots. Show that the Galois group of f is either S_4 or of order 8.

Proof. Let r_1, r_2 be the two distinct real roots of f, and $z_1, z_2 (= \overline{z_1})$ be the two distinct non-real complex roots. Now, consider the extensions $K \subset K(r_1) \subseteq K(r_1, r_2) \subseteq K(r_1, r_2, z_1, \overline{z_1})$.

Clearly, $[K(r_1) : K] = 4$ as f is irreducible in $K[X]$. Now, note $f = (X - r_1)(X - r_2)(X - z_1)(X - \overline{z_1}) \in K(r_1)[X]$ and $(X - r_2)(X - \overline{z_1})(X - z_1) \in K(r_1)[X]$. And similarly, $(X - z_1)(X - \overline{z_1}) \in K(r_1, r_2)[X]$ and it is irreducible in $K(r_1, r_2)[X]$ as it is irreducible in $\mathbb{R}[X]$. Hence, clearly, $[K(r_1, r_2, z_1, \overline{z_1}) : K(r_1, r_2)] = 2$. So it remains to check $[K(r_1, r_2) : K(r_1)]$. But $(X - r_2)(X - z_1)(X - \overline{z_1}) \in K(r_1)[X]$ is a degree 3 polynomial with r_2 as a root. So if $r_2 \in K(r_1)$ already, then $K(r_1, r_2) : K(r_1)] = 1$ and otherwise, the degree 3 polynomial won't have a linear factor, so is irreducible, so $[K(r_1, r_2) : K(r_1)] = 3$. Hence, either $|G| = 8$ or $|G| = 24$, the latter case, being embedded to S_4, must actually be S_4. □