Algebra Qual solutions

Tomoki Oda

1 Introduction

This document cover solution for recent problems, with other people's solution, it covers all the correct solutions except for Fall 2021 problem 7 which we couldn't figure out if Noetherian or not. For the solution part, I would like to appreciate Spencer Martin and Jung Joo Suh for the countless of discussions.
I would like to credit all the people who attribute for making credit Emil Geisler, Emmy Van Rooy, Harahm Park, Matthew Tyler, Robert Miranda Thomas Martinez and William Chang.
I would like especially thanks to **Ariana Chin** and **Stepan Malkov**.

2 Spring 2024

I think only problems need to argue on here for this year are 3, 6 and 9. I can explain briefly how to solve others, 1.it is almost identical to Fall 2022 problem 2
2. It is just a Nullstellensatz
4. Basic property of Tor functor, quite similar to Spring 2022 Problem 3
5. Asked so many times
7. Basic properties of Nilpotent group
8. This is nontrivial but I gave as an alternative solution as 2022 Fall 6
10. construction of the colimit

Spring 2024 Question 3 Find all positive integers n such that $cos(\frac{2\pi i}{n})$ is rational

Solution sketch When $n = 1, 2$ this is rational and omit those cases.
Assume $n \neq 1, 2$ so that $e^{\frac{2\pi i}{n}} \notin \mathbb{R}$. Suppose $\mathbb{Q}(cos\frac{2\pi i}{n}) = \mathbb{Q}$, then the nontrivial extension $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}(cos\frac{2\pi i}{n})$ has degree 2, as the minimal polynomial being $x^2 - 2cos(\frac{2\pi i}{n}) + 1$, so the extension of $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ is also degree 2 extension. This is same things as calculating the degree of cyclotomic polynomial. The degree of cyclotomic polynomial can be calculate by the Euler's tortient function. Tortient function is multiplicative when prime is relatively prime. Also we can exclude all prime bigger than $2, 3$ by estimate it below. Only possibilities are $1, 2, 3, 4, 6$

Spring 2024 Question 6 Analysing the structure of the Sylow 5 group, prove finite group G of order 300 is not simple.

Solution$n_5 = 1, 6$ when $n_5 = 1$ this is not simple, so assume $n_5 = 6$. In this case, by the conjugation action of G to the set of Sylow 5 subgroup, you can map G into the S_6. This is indeed embedding if we say G is simple. However $|S_6| = 720, |G| = 300$ we can not realize it via embedding due to the Lagrange theorem.

Spring 2024 Quedtion 9 A is finite dimensional algebra over $k = \overline{k}$. Prove following statement is equivalent.
(1)A simple A module is 1dimension.
(2) $J(A)$ is set of all nilpotent element of A.

Solution (1) $\rightarrow$ (2) Fact: All simple A module appears as a submodule of $A/J(A)$, reason is simple module can be written as $A/\mathfrak{m}$ for left maximal ideal. Jacobson radical is the intersection of the all maximal ideal, so using chinese reminder theorem we get all of maximal ideals as each component. Using Artin wedderburn we have $A/J(A) \cong \prod Mat_i(k')$ where k'/k is an algebraic extension. Since $k = \overline{k}$ indeed $k' = k$, also $i = 1$ for the hypothesis. We have a multiplicative structure $A/J(A) \cong k^n$ with each component. Although this ring is not reduced, no elements are nilpotent, so $J(A)$ contains all nilpotent elements. Furthermore, A is finite dimensional algbra, so Artinian. In general the Jacobson radical of the Artinian ring is Nilpotent, so $J(A)$ is the set of nilpotent elements.

Conversely if some $i \geqslant 2$ then there is a nonzero nilpotent element in $A/J(A)$. If we lift to A, then that gives a nilpotent element of A which is not in $J(A)$.

3 Fall 2023

Problem 1

Let G be a group, let $H \subset G$ be a subgroup of finite index $n \geqslant 2$ let $x \in G$. Prove $[H : xHx^{-1} \cap H] \leqslant n - 1$

Solution to the problem 1

Consider

By assumption $[G : H] = n$, and each cosets of G/H can be represented by $x_1H, \dots x_nH$. Pick an element $x \in G$, we will estimate the cardinality of $[H : H \cap xHx^{-1}]$. When $x \in H$ then statement is trivially true, so we can assume $x \notin H$.
Note xHx^{-1} is a subgroup of G, and consider the left multiplication action of $h \in H$ to the left coset G/xHx^{-1}. Since $[G : H] = [G : xHx^{-1}] = n$ we can pick representative $xHx^{-1}, g_1xHx^{-1} \dots g_nxHx^{-1}$. The stabilizer of the element xHx^{-1} contains $H \cap xHx^{-1}$. So $[H : xHx^{-1} \cap H] \leqslant n$, however pick $g_i = x^{-1}$ so that there is a coset represented as Hx^{-1}. This is a stable under any action by H. So this has a orbit of length 1. This reduce the bound of previous inequality as n to $n - 1$. Thus $[H : xHx^{-1} \cap H] \leqslant n - 1$

Problem 2

Let A be a commutative Noetherian ring. Prove that every nonzero ideal I of A contains a finite product of nonzero prime ideals.

Solution to the problem 2

Suppose there is an ideal I such that I is not contain a finite product of non zero prime ideals. Then the set of ideals such that

$$\mathcal{K} = \{I | I \quad \text{is an ideal} \quad I \quad \text{is not contain a finite products of prime ideal}\} \neq \varnothing$$

. We can introduce a poset structure for K Since A is a Noetherian ring, there is a upper bound for the chain of ideals. The maximal element I'. We can prove this I' is prime itself so that contradict the hypothesis.
If I' is not prime, pick $x, y \notin I'$ but $xy \in I'$ so that $I' + xA$ and $I' + yA$ are stricktly larger than I. Note they are not trivial: if $I' + xA = A$ then $yI' + yxA = yA$ but $yI' + yxA$ is contained in I'. So $I' + xA$ and $I' + yA$ is both proper ideal.

By the maximality of $I'+xA$ and $I'+yA$ each of them must contain a product of prime ideals, but then so does $(I' + xA)(I' + yA) \subset I'$, which contradicts the choice of I'.

Comment: If I remove the Noetherian hypothesis, can I find counter examples of the ring?

Problem 2'

Find a commutative ring R that there is a ideal I of R does not contains a finite product of nonzero prime ideals.

Solution to the problem 2'

Here honestly, I didn't have idea, so copied from Stack exchanges
We can chose ring R to be $R = \{(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} | a_{n+1} = a_n \quad \text{for n sufficiently large} \quad \}$
and the ideal $I = (0)$. For all $i \in \mathbb{N}$, let $e_i \in R$ be an element such that $e_i = (a_i)_{n\in\mathbb{N}}$ with $a_i = 1$ if $i = n$ and 0 otherwise. Let P be a prime ideal, and $0 \in P$.
If there exists $i \in \mathbb{N}$ such $e_i \notin P$. Then since for $i \neq j, e_i e_j = 0$, $e_j \in P$ for all $j \neq i$. So $\oplus_{i\neq j}\mathbb{Z}e_j \subset P$.If we choose a finite number of prime ideals $P_1 \dots P_k$ with $\oplus_{m\neq j}\mathbb{Z}e_m \subset P_m$ then we have $0 \subset \oplus_{j\neq 1\dots m}\mathbb{Z}e_j \subset P_1 \dots P_m$ doesn't contained in a product of prime ideals.
As shown above, R is not an integral domain, so 0 is not a prime ideal so 0 is not prime ideal itself. Thus this shows 0 does not containing a finite product of prime ideals.

Question 3

Show that there is an isomorphism of $\mathbb{Q}$-algebra $\mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t] \cong \mathbb{Q}[x, y]/(x^2 - y^2)$.

Solution to the problem 3

Construct the $\mathbb{Q}-$algebra morphism $\pi : \mathbb{Q}[x, y] \to \mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t]$ by $x \to t \otimes 1$ and $y \to 1 \otimes t$. The kernel contains $(x^2 - y^2)$ because $\pi(x^2 - y^2) = t^2 \otimes 1 - 1 \otimes t^2 = t^2(1 \otimes 1 - 1 \otimes 1) = 0$. Hence this morphism factor through $\pi' : \mathbb{Q}[x, y]/(x^2 - y^2) \to \mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t]$
We will construct the inverse morphism of π' so that two ring are isomorphic with each other. Construct morphisms $f : \mathbb{Q}[t] \to \mathbb{Q}[x, y]/(x^2 - y^2)$ by $f(t) = x$ and $g : \mathbb{Q}[t] \to \mathbb{Q}[x, y]/(x^2 - y^2)$ by $g(t) = y$. Since $f(t^2) = x^2 = y^2 = g(t^2)$, by the universal properties of tensor product, there is an morphism $h : \mathbb{Q}[t] \otimes_{\mathbb{Q}[t^2]} \mathbb{Q}[t] \to \mathbb{Q}[x, y]/(x^2 - y^2)$ such that $h(t\otimes 1) = f(t)$ and $h(1\otimes t) = g(t)$. This in an inverse morphism of π'. Since $h \circ \pi'(x) = h(t \otimes 1) = x, h \circ \pi'(y) = h(1 \otimes t) = y$. As a $\mathbb{Q}-$ algebra, x, y are generators, so this is enough to show the isomorphism of $\mathbb{Q}-$algebra.

Question 4

Let K/F be the finite Galois extensions, pick $\alpha \in K/F$. Let E be a subfield of K containing F of a largest degree over F such that $\alpha \notin E$. Prove $E(\alpha)/E$ be a Galois extension of a prime degree.

The first Solution to 4

First step: Prove $E(\alpha)/E$ is a Galois extension.

$E(\alpha)/E$ is separable extension because K/F is a separable extension, and any intermidiate extension of separable extension is separable.

Show the normality, since K/E is Galois, the minimal polynomial of α over E, m_α split completely on K. We will show that minimal polynomial m_α splite in $E(\alpha)$. Let β be an other roots for m_α. If $\beta \in E(\alpha)$ then nothing to prove. Hence without loss of generalities we can assume that is not contained in $E(\alpha)$. By the maximality of E, $E(\beta)$ contains α. This can be written as $\sum c_i\beta^i = \alpha$ for $c_i \in E$. Let N be a normal closure of $E(\alpha)$ over E. By the assumption of Galois, $N \subset K$ and there is a $\sigma \in Gal(N/E)$ such that $\sigma(\beta) = \alpha$. Let the order of σ be n. Then since $\sum c_i\alpha^i = \sigma(\alpha)$. This means $\sigma(\alpha) \in E(\alpha)$, and by keep doing this argument we have $\sigma^i(\alpha) \in E(\alpha)$. But $\sigma^{n-1}(\alpha) = \sigma^n(\beta) = \beta$ so $\beta \in E(\alpha)$. Thus m_α splite completely on E_α.
Second Step: Prove $E(\alpha)/E$ is a prime degree. Let G be a Galois group of $E(\alpha)/E$. If the extension is not prime degree, due to the Cauchy theorem, there is a order p-cyclic subgroup of G. then there is a nontrivial proper subgroup generated by some element $\sigma \in G$ such that $< \sigma > \neq G$. By the Galois correspondence, $E(\alpha)^{<\sigma>}$ correspond to the field containing E. Since σ is nontrivial generator, α was not fixed by σ. This means $E(\alpha)^\sigma$ but not a containing α. It contradict to the maximality of the E.

The second Solution to 4

Use Galois correspondence. Let E/F be the largest field not containing α. Then, $Gal(K/E)$ is the smallest subgroup of $Gal(K/F)$ that does not fix α. There is an element σ in $Gal(K/E)$ not fixing α, and the subgroup $< \sigma >$ does not fix α. However if there is any proper subgroup, this proper subgroup fixes α. By the minimality of $Gal(K/E)$ this has to be a cyclic group.

Consider $Gal(K/E(\alpha))$. If $Gal(K/E(\alpha)) = \{e\}$ then $E(\alpha)$ is normal, so by the second step on the first solution this is prime index. This reduce cases, suppose now that $Gal(K/E(\alpha))$ is a proper nontrivial subgroup of $Gal(K/E)$ that fixes α.

If there are any intermediate subgroups $1 \subset Gal(K/E(\alpha)) \subset G' \subset Gal(K/E)$, they correspond to a nontrivial field extension of E not containing α, which contradicts the maximality of E. Thus, there are no intermediate subgroup, which means that $Gal(K/E(\alpha))$ is the maximal subgroup of cyclic group, $Gal(K/E(\alpha))$ has prime index in $Gal(K/E)$. Notice $Gal(K/E)$ is a cyclic group as we showed

above, in particular abelian. By the Galois correspondence every abelian subgroup is realizeable by the subfield of K. Using the Galois correspondence, $E(\alpha)/E$ is Galois with Galois group $Gal(K/E)/Gal(K/E(\alpha))$ which is index p.

Question 5

Let F be a field, and let $f(x) = \sum_{i=1}^{n} a_i x^i$ be a polynomial of degree $n > 1$ with coefficients $a_i \in F$. Show that the splitting field of $f(x^2)$ over F contains a square root of $(-1)^n a_0 a_n^{-1}$

Solution to Question 5

Consider the spliting field of $f(x^2)$, which we will denote it as K. Without loss of generality by dividing a_n so that we can replace the polynomial into the monic $f(x^2) = x^{2n} + a'_{n-1}x^{2n-2} + \dots a'_0$ where $a'_i = \frac{a_i}{a_0}$ and prove $\sqrt{(-1^n a_0)}$ is contained in the splitting field.
We can factor $f(x)$ into $f(x) = \prod(x - \alpha_i)$. Using the relation of root and coefficient, we have $\prod(-\alpha_i) = a_0 \Rightarrow \prod(\alpha_i) = (-1)^n a_0$. Notice $\sqrt{\alpha_i} \in K$ as $f(\sqrt{\alpha_i}^2) = f(\alpha) = 0$. So $\prod \sqrt{\alpha_i} = \sqrt{-1 a_0}$ that prove the statement.

Question 6

For a positive integer n, let C_n be the category with objects $[1, n] := \{1, 2, \dots, n\}$ and morphisms $Mor(i, j)$ an empty set if $i > j$ and a singleton otherwise. For positive integers m and n, a nonstrictly increasing function $f : [1, n][1, m]$ can be viewed as a functor $C_n \to C_m$. Prove that this functor fhas right adjoint if and only if $f(1) = 1$.

Solution 6

1 is a initial object of this category, if there is a right adjoint g, then pick $i \in C_n$ and $j \in C_m$ so that $Hom(i, g(j)) = Hom(f(i), j)$. Notice i is initial object so the morphism exist for all j. This means we must have $f(i) < j$ for all j. Notice j can be 2 so $f(1) = 1$.

Conversely suppose $f(1) = 1$, f is increasing function. Let $\{1, f(i_2) \dots f(i_a)\} \subset \{1, \dots, m\}$ such that $f([1, n]) = \{f(1) \dots f(i_a)\}$ and $1 < f(i_2) < f(i_3) < \dots f(i_a) = f(n)$. Let $f(i_2) = f(i_3 - 1) = k_2$ and $f(i_3) = k_3$, so that $Hom(f(i_2), j) \neq \varnothing, j \geqslant k_2 + 1$. To construct an right adjoint we need to have $Hom(i_2, g(j)) = Hom(i_2, g(j)) = \{*\}$. Thus we need to construct $g(1) = \dots = g(k_2) = 2$ and $g(k_2 + 1) = g(k_3) = i_3 + 1$. We can keep this construction so that we can construct a adjoint
Comment: I am pretty sure mathematically this is correct construction, but I

am not sure my writing is good enough, I just did the case i=2, but how should I write for the general cases?

Question 7

Let R be a PID and $n \geqslant 1$. Let M be a finitely generated R^n module, show that there is a exact sequence

$$0 \to P \to Q \to M \to 0$$

with P, Q finitely generated projective R^n module.

Proof. Since M is finitely generated, there exists $m_1, m_2, \ldots, m_k \in M$ such that $\{m_i\}$ generate M as an R^n module. Let $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$ be idempotents of R^n. Consider the submodule e_iM of M for $1 \leqslant i \leqslant n$. I claim that e_iM has a natural R module structure by $rm = (re_i)m$ for $r \in R$ (where R^n is an R-module in the usual way). This gives an R module structure because $e_im = m$ for all $m \in e_i$, since e_i is idempotent:

$$e_i(e_im) = e_i^2m = e_im$$

Furthermore, e_iM is finitely generated as an R-module by $e_im_1, e_im_2, \ldots, e_im_k$. Therefore, we have a short exact sequence of R-modules (for each $1 \leqslant i \leqslant n$):

$$0 \longrightarrow \ker \psi_i \longrightarrow R^k \xrightarrow{\psi_i} e_iM \longrightarrow 0$$

Since $\ker \psi_i$ is a submodule of the finitely generated free module R^k, it is a torsion free and finitely generated module over a PID, and thus is free. Therefore, there exist nonnegative integers $0 \leqslant b_1, \ldots, b_n \leqslant k$ such that the following sequence is short exact:

$$0 \longrightarrow R^{b_i} \xrightarrow{\rho_i} R^k \xrightarrow{\psi_i} e_iM \longrightarrow 0$$

Suppose that $A_1, \ldots, A_n$ are R-modules. Then $\bigoplus_{i=1}^n A_i$ has a natural R^n-module structure by

$$(r_1, \ldots, r_n)(a_1, \ldots, a_n) = (r_1a_1, \ldots, r_na_n)$$

Let us show that with this induced action of R^n, $M \cong \bigoplus_{i=1}^n e_iM$. Let $\psi : M \to \bigoplus_{i=1}^n e_iM$ by $\psi(m) = (e_1m, \ldots, e_nm)$, which is clearly an R^n-module homomorphism. ψ is injective since if $\psi(m) = \psi(n)$, then $e_im = e_in$ for all e_i, and thus $\sum_{i=1}^n e_im = 1 \cdot m = 1 \cdot n$. Also, it is clearly surjective onto each coordinate and thus surjective. Therefore, we have a short exact sequence of R^n modules by:

$$0 \longrightarrow \bigoplus_{i=1}^n R^{b_i} \xrightarrow{\rho} \bigoplus_{i=1}^n R^k \xrightarrow{\psi} M \longrightarrow 0$$

The R^n module $\bigoplus_{i=1}^n R^k$ is the same as $(R^n)^k$. Furthermore, we have a congruence of R-modules:

$$\bigoplus_{i=1}^{n} R^{b_i} \oplus \bigoplus_{i=1}^{n} R^{k-b_i} \cong (R^n)^k$$

and therefore $\bigoplus_{i=1}^n R^{b_i}$ is a sub R^n-module of a free module, and is thus projective. Therefore, we have an exact sequence of the desired form, since $(R^n)^k$ is free and thus projective. □

4 Spring 2023

2023S #1 Let $F, F' : C \to D$ and $G, G' : D \to C$ be four functors F is a left adjoint to G and F' be a left adjoint of G'. Establish a bijection between the natural transformations $\alpha : F \to F'$ and the natural transformations $\beta : G' \to G$

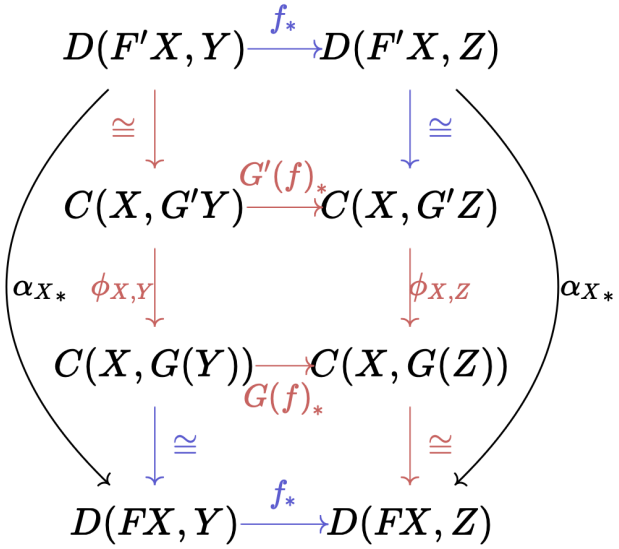
Solution. Consider the commutative diagram

$$\begin{array}{ccc} D(F'X, Y) & \xrightarrow[\cong]{} & C(X, G'Y) \\ \downarrow{\scriptstyle \alpha_X *} & & {\scriptstyle \phi_{X,Y}}\downarrow \\ D(FX, Y) & \xrightarrow{\cong} & C(X, GY) \end{array}$$

construct $\phi_{X,Y}$ as composition of the isomorphism $\eta_{X,Y} : D(FX, Y) \cong C(X, GY)$ and $\eta'_{X,Y} : D(F'X, G) \cong C(X, G'Y)$ as $\phi_{X,Y} = \eta_{X,Y} \circ \alpha_X \circ {\eta'_{X,Y}}^{-1}$. We want to show that this $\phi_{X,Y}$ is natural transformation of representable functor when fixing X. Namely, we will show, given $f : Y \to Z$ then the diagram

$$\begin{array}{ccc} C(X, G'Y) & \xrightarrow{G'(f)*} & C(X, G'Z) \\ {\scriptstyle \phi_{X,Y}}\downarrow & & \downarrow{\scriptstyle \phi_{X,Z}} \\ C(X, G(Y)) & \xrightarrow[G(f)*]{} & C(X, G(Z)) \end{array}$$

commute. This can be shown by using the commutativity of



Note the outer rectangle involve α_{X*} and f_* is commutative because α_X is natural transformation by Yoneda's lemma. Upper square and bottom square is commutative because of the adjoint. Using the commutativity of small squares, composition of blue arrows in a square is same as composition of red arrows in the small square. It means the commutativity of outer rectangle implies commutativity of the red arrows. The last red arrow is isomorphism, in parituclar this is monic, so

$$\eta_{X,Y} \circ \phi_{X,Z} \circ G(f) \circ \eta'_{X,Y} = \eta_{X,Y} \circ G(f) \circ \phi_{X,Y} \circ \eta'_{X,Y}$$

implies

$$\phi_{X,Z} \circ G(f) \circ \eta'_{X,Y} = G(f) \circ \phi_{X,Y} \circ \eta'_{X,Y}$$

. The $\eta_{X,Y}$ is also isomorphism so epi morphism. This means

$$\phi_{X,Z} \circ G(f) = G(f) \circ \phi_{X,Y}$$

so $\phi_{X,Y}$ is a natural transformation of representable functor.
This result is not depend on the choice of X, so it make sense to write $\phi_{-,Y} \in \mathrm{Nat}(C(-,G'(Y)), C(-,G(Y)))$. By the fullness part of Yoneda embedding, this natural transformation is coming from the morphism $\beta_Y \in C(G'(Y), G(Y))$. With this construction, we can define an morphism β_Y for any $Y \in D$. This defines collection of morphisms β.

We already saw $G(f)_* \circ (\beta_Y)_* = (\beta_Z)_* \circ G(f)_*$. These are two same natural transformation $Nat(C(-,G'Y), C(-,GZ))$. The faithfulness part of Yoneda's lemma claims, as the morphism of $C(GY', GZ)$, they have to be same. Due to the functoriality we have the commutative diagram.

$$\begin{array}{ccc} G'Y & \xrightarrow{\beta_Y} & GY \\ \downarrow{\scriptstyle G'f} & & \downarrow{\scriptstyle Gf} \\ G'Z & \xrightarrow{\beta_z} & GZ \end{array}$$

commute. This shows β is indeed a natural transformation.
Now we will show that α and β are bijective each other. If $\alpha \in Nat(F, F')$ is given, then $\beta \in Nat(G', G)$ can be construct. Then apply the same argument for β, then we can construct a natural transformation $\tilde{\alpha} \in Nat(F, F')$. We need to show $\alpha = \tilde{\alpha}$.

Consider maps

$$\begin{aligned} (\alpha_X)_* : D(F'(X), Y) &\to Hom(F(X), Y) \\ f &\mapsto f\alpha_X \\ (\tilde{\alpha}_X)_* : D(F'(X), Y) &\to Hom(F(X), Y) \\ f &\mapsto f \circ \tilde{\alpha_X} \end{aligned}$$

We can define this for any object $Y \in D$, and these define two natural transformations in $Nat(C(F'(X), -), C(F(X), -)$.

By construction, $(\alpha_X)_*, (\tilde{\alpha}_X)_*$ both make the following diagram commute respect to the β_Y

$$\begin{array}{ccc} C(X, G'Y) & \xrightarrow{(\beta_Y)^*} & C(X, GY) \\ \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong} \\ D(F'X, Y) & \longrightarrow & D(FX, Y) \end{array}$$

Thus, $(\alpha_x)^*$ and $(\tilde{\alpha}_X)^*$ are the same map. By Yoneda's Lemma, there is a corresponding map $\alpha_X \in C(FX, F'X)$ that correspond both $\alpha_X, \tilde{\alpha_X}$. Since $(\alpha_X)^* = (\tilde{\alpha}_X)^*$ for every $X \in C$, $\alpha = \tilde{\alpha}$. This shows bijection between α and β.

□

2023S #2 Let p, q be the distinct prime numbers and consider the number field $K = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. Describe all the subfields of K and the inclusion between them.

Solution: We have $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$ are linearly disjoint, means $\mathbb{Q}(\sqrt{p}) \cap \mathbb{Q}(\sqrt{q}) = \mathbb{Q}$, if not, then there is $a, b \in \mathbb{Q}$ with $a\sqrt{p} + b = \sqrt{q}$. Taking square for the both side we made $\sqrt{p}$ is rational. Also $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is a splitting field this is Galois. By the disjointness, we have the Galois group $\mathbb{Z}/2 \times \mathbb{Z}/2$ there are exactly 3 nontrivial proper subgroup. That has to be correspond into $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{q}), \mathbb{Q}(\sqrt{pq})$ that they are disjoint with each other, and $\mathbb{Q}$ are trivial subfield. Claim: $\mathbb{Q}(\sqrt{p} + \sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Clearly we have

$\mathbb{Q}(\sqrt{p},\sqrt{q}) \subset \mathbb{Q}(\sqrt{p},\sqrt{q})$. On the other hand $\mathbb{Q}(\sqrt{p}+\sqrt{q}) \supset \mathbb{Q}(\sqrt{pq})$. But there should no intermediate field except for $\mathbb{Q}(\sqrt{p},\sqrt{q})$. So $Q(\sqrt{p},\sqrt{q}) = K$(Alternatively we can divide $\frac{p^2-q^2}{\sqrt{p}+\sqrt{q}} = \sqrt{p}-\sqrt{q}$)

2023S #3 Given an example of an infinite field extension $K \subset L$ such that only finitely many field automorphism fixing K.

Solution: Consider the following examples

(a) Claim: The only surjective ring homomorphism from $\mathbb{R} \to \mathbb{R}$ is the identity map. Lemma: Any ring homomorphism $f : \mathbb{R} \to \mathbb{R}$ is uniquely determined by $f(1)$ and this is identity. Proof: First of all $f(1) = 1$ because this is a ring homomorphism. For $n \in \mathbb{Z}$ $f(n) = nf(1)$. Also for the rational number $\frac{r}{s}$, we have $f(\frac{r}{s})f(s) = rf(1)$ and $f(\frac{r}{s})sf(1) = rf(1)^2$. Then by additivity, so f is identity over $\mathbb{Q}$. We will prove f is indeed a continuous function, so that all continuous function is determined by the dense set. Indeed, if $x \geqslant 0$ then $x = y^2$ for some real $y.$, hence $f(x) = f(y)^2 \geqslant 0$ which implies f preserve a order. And hence $|y-x| \leqslant \frac{1}{n}$ implies $|f(y)-f(x)| \leqslant \frac{1}{n}|f(1)|$, that implies f is continuous.

$[\mathbb{R} : \mathbb{Q}]$ is not a finite, the reason is $\mathbb{Q}$ is countable but $\mathbb{R}$ is uncountable. And automorphism fixing $\mathbb{Q}$ is identity.

(b) Consider $\mathbb{F}_p \subset \mathbb{F}_p(x)$. This case $\mathbb{F}_p(x)$ is a transendental extension. So the degree of extension is ∞

Claim: The $\mathrm{Gal}(\mathbb{F}_p(t)/\mathbb{F}_p)$ is finite group. In general, the Galois group $Gal(k(t)/k)$ is a $PGL(2,k)$. This solution refered to the Cox "Galois Theory" proposition 7.5.5 and Theorem 7.5.7 Proposition 7.5.5 Assume $\alpha \in k(t)$ is a rational function not is k and write $\alpha = \frac{a(t)}{b(t)}$ where $a(t), b(t) \in F[t]$ are relatively prime. Then

1.α is transcendental

2.$a(x) - \alpha b(x) \in k(\alpha)[x]$ is irreducible over $k(\alpha)[x]$

3.$k(\alpha) \subset k(t)$ is a finite extension of degree $[k(t), k(\alpha)] = max(deg(a), deg(b))$

If α is algebraic over k then there is an algebraic relationship

$$\alpha^n + a_1\alpha^{n-1} + \ldots a_n = 0$$

with $n \geqslant 1$ and $a_1 \ldots a_n \in k$. Substituting $\alpha = \frac{a(t)}{b(t)}$ then by multiplying $b(t)^n$ then

$$a(t)^n = b(t)(p(t))$$

for some polynomial p. Since $k(x)$ is UFD it contradict they are relatively prime. Without loss of generalities, we can assume $b(t)$ is constant. Then there is a algebraic equation of $a(t)$ that is contradicting for the fact that t is a transcendental over t.

We will prove $a(x) - \alpha b(x)$ is irreducible over $k(x,\alpha)$. $a(x) - \alpha b(x)$ is irreducible over $k[x,\alpha]$ suppose not, then we can write it as a

product $p(x,\alpha)q(x,\alpha)$. The degree of α for $a(x)-\alpha b(x)$ is one, either $p(x,\alpha)$ $q(x,\alpha)$ is a polynomial of x. Suppose $p(x,\alpha) \in k[x]$ that means $p(x)$ divide both $a(x)$ and $b(x)$ contradicting $a(x)$ and $b(x)$ are relatively prime. This shows $a(x)-\alpha b(x)$ is irreducible over $k[\alpha,x]$. Clearly $a(x)-\alpha b(x) \in k(\alpha)[x]$ if this decomposed into the $p(x,\alpha,\frac{1}{\alpha})$ and $q(x,\alpha,\frac{1}{\alpha})$ then by multiplying sufficiently large α, then $\alpha^k a(x)-\alpha^{k+1}b(x)$ is factored into the $k[\alpha,x]$. But again, sine $k[\alpha,x]$ is UFD, and $a(x)-\alpha b(x)$ is irreducible on $k[x,\alpha]$,$a(x)-\alpha(t)b(x)$ is irreducible in $k(\alpha)[x]$.

Since α is rational function of t we have $k(\alpha) \subset k(\alpha,t) = k(t)$. t is vanishes in $a(x)-\alpha b(x)$. Then compare the coefficient of $a(x)$ and $b(x)$, since $\alpha \notin k$ these coefficient doesn't vanish, so the degree of this polynomial in terms of x is $max(deg(a), deg(b))$.

We will claim that given $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a invertible matrix then $g \cdot t = \frac{at+b}{ct+d}$ gives automorphism. To be presise there is a morphism from $GL(k,2) \to Gal(k(t),k))$. This action of g fixes element of F.

We can see $\frac{at+b}{ct+d}$ gives a transcendental function. With degree, 1 as this is a root of $(ct+d)x-at-b$. This means $k(\frac{at+b}{ct+d}) = k(t)$.

There are inverse automorphism $\frac{dt-b}{-ct+a}$.So showed this embedded into the matrix to the automorphism group of $k(t)/k$

This is surjective, because by the above argument we showed, the degree 1 automorphism must be a smaller than degree one in both denominators and numerators, so a form of $\frac{at+b}{ct+d}$. $\frac{dt-b}{-ct+a}$ is the inverse, and this to be exist, we have to have $ad-bc \neq 0$.

We can compute kernel is multiple of identity by solving the equation $t = \frac{at+b}{ct+d}$. This equation implies $ct^2-(a-d)t+b=0$ so $c=b=0$ and $a=d$.

□

2023S #4 Let $M_n(K)$ be the ring of $n \times n$ matrix with coefficients in a field K, describe all possible ring homomorphism $M_n(K) \to K$

Solution: When $n=1$, the homomorphism of the field is $End(K)$.

When $n>1$, notice that M_{ij} the matrices with a 1 in the (i,j) entry and other entries are 0. As being a ring, $M_n(K)$ are generated by M_{ij} as a $K-$module, so ring homomorphisms are determined by how M_{ij} mapped under f. Moreover, if $i \neq j$, then $M_{ij}^2 = 0$, so $f(M_{ij}^2) = f(M_{ij})^2 = 0 \to f(M_{ij}) = 0$. Moreover, if $f(M_{ii}) \neq 0$, then for $i \neq j$, $M_{ii}M_{jj} = 0$, so this ensures $M_{jj} = 0$ at most one diagonal entry can map to something nontrivial (and it must map to 1, as the identity maps to 1).

However, for $n>1$, consider the matrix M, such that 1 all entires are 1. $f(M) = f(M_{ii}) + f(M-M_{ii}) = 1$, but then $1 = f(M)^2 = f(M^2) = f(n \cdot M) = n \cdot f(M) = n$. So, there are no ring homomorphisms for $n>1$.

□

Alternate Solution: Alternatively, since $M_n(k)$ is a simple ring, so every ring homomorphism to the other ring k are injective (otherwise kernel would be a nontrivial two sided ideal.) So the image under homomorphism is always noncommutative. However k is commutative, so we cannnot embeded $M_n(K)$. Contradiction.

□

Extra problem Show there is no homomorphism from $\phi : M_n(K) \to M_m(K)$ for $n > m$.

According to the argument above, ϕ is injective homomorphism.
1. Restrict to the morphism to the $GL_n(k)$ then this will be a morphism of the algebraic group whose image is contained in $GL_m(k)$ as invertible elements map to invertible. We know the (krull)dimension of $(n+1)^2 - 2n - 1 = n^2 - n$. But the left hand side has dimension less than $n^2 - n$ so there is no such a injection.
2. $M_n(k)$ are minimally generated by the elementary matrix E_{ij} for $0 \leqslant i, j \leqslant n$. And $M_m(k)$ is generated less number of generator, thus generator maps to generator, this shouldn't be injective.

2023S #5 Let A be a local commutative noetherian ring and M a finitely generated A-module such that every exact sequence $0 \to M'' \to M' \to M \to 0$ remains exact after tensoring with the residue field k of A. Show that M is free.

Solution: Since M is already finitely generated, there exists k such that $A^k \to M$ is a surjection. In particular, without loss of generalities pick k is the smallest integer r satisfying the above property. By the statement of the problem we have the following exact sequence.

$$0 \to M'' \to A^r \to M \to 0$$

Note M'' is a kernel of the map $A^r \to M$, which is a submodule of the finitely generated submodule over the Noetherian ring, thus this is a finitely generated A-module. Tensoring by the residue field $A/J(A) \cong k$ gives

$$0 \to M'' \otimes k \to A^r \otimes k \to M \otimes k \to 0$$

Since $M \otimes k$ is a module over vector space, there exist n such that $M \otimes k \cong k^n$ and $k^k \cong k^n \otimes M'' \otimes k$. We will claim that $n = k$. If not we will show that the module will be generated by fewer elements.

Consider the following form of Nakayama's lemma for vector spaces. If M is finitely generated module over A, images of elements $\overline{m_1} \dots \overline{m_n}$ of $M/J(A)M$ generate as $A/J(A)$ module, then M is spanned by $m_1 \dots m_n$

Proof. Using the other version of Nakayama's lemma, $M = JM + N \to M = N$ for $N \subset M$. Then this claim is same as $N = \sum Rm_i$. □

Apply the above Nakayama's lemma, $n = k$, so the $M'' \otimes k = 0$. Again using the Nakayama's lemma for M'', implies $M'' = 0$. This implies $A^r \cong M$ so that M is free. □

2023S #6 Let A be commutative ring, and let $s \in A$. Let $S = \{1, s, s^2, \dots\}$. Show the following are equivalent.

(a) The canonical morphism $A \to S^{-1}A$ is surjective

(b) There is $N > 0$ such that $s^n A = s^N A$ for all $n \geqslant N$.

(c) For n large enough, the ideal $s^n A$ is generated by an element e with $e^2 = e$

Solution

(c) $\implies$ (b): There is some N for which $\forall n \geqslant N$,then $s^N A \supset S^n A$. By hypothesis there is an idempotent $eA = S^N A$. Since $e^2 = e, S^N A = eA = e^2 A = eS^N A = S^N eA = S^{2N} A$. If we take k large enough so that $n \leqslant 2^k N$ then we have $S^{2^k N} A \subset S^n \subset S^N A$ so that we have $S^N A = S^n$.

(b) $\implies$ (a): $s^N \in s^N A = s^{N+1} A$. So, $s^N = s^{N+1} a$ for some $a \in A$. In other words,

$$s^N (1 - sa) = 0$$

Thus, $\frac{a}{1} \equiv \frac{1}{s}$ in $S^{-1}A$. So, the canonical morphism $A \to S^{-1}A$ is surjective on $S^{-1}A$.

(a) $\implies$ (c): If the canonical morphism is surjective, then there is some $a \in A$ such that $\frac{a}{1} \equiv \frac{1}{s}$. So, there exists some s^N such that $s^N = s^{N+1} a$. Set $e = s^N a^N$. Then,

$$(s^N) a^N = (s^{N+N} a^N) a^N = (s^N a^N)^2$$

Moreover, $s^N a^N$ generates all of $s^N A$ (which is equal to $s^n A$ for all $n \geqslant N$ by a simple inclusion argument), as $s^N = s^N (s^N a^N) \in s^N A$.

2023S #7 Let k be a field and let $A = k[x, y]/(x^2, xy, y^2)$.

(a) Determine the invertible elements of A

(b) Determine the ideals of A

(c) Determine the principal ideals of A

Solution: (a) The invertible elements are $\{\alpha_1 x + \alpha_2 y + \alpha_3 : \alpha_3 \neq 0\}$.

(b) The full list of ideals are all of the principal ideals, 0, A, and $\langle x, y \rangle$.

(c) The principal ideals are those of the form $\langle x \rangle$, $\langle y \rangle$, and $\langle x + \frac{a}{b} y \rangle$ for any $a, b \neq 0$.

□

2023S #9 Let G be a non-abelian finite group of order pq where p and q are prime numbers with $q > p$. Determine the degrees of the irreducible characters of G, and determine the number of irreducible characters of a given degree.

Solution: The dimension of the irreducible representation divide the order of the group. The order of the group is pq for two primes p and q where $q > p$. We couldn't have the degree q and pq representation because $q^2 > pq$ as well as $(pq)^2 > pq$. Thus it is enough to count the number of the representation of degreee p and 1. Note that the number of the 1 dimensional irreducible representation is same as the $|G/[G,G]|$. We will count the cardinality of $[G,G]$. We shouldn't have $[G,G] = \{e\}$ because of the non-abelian hypothesis. So $|G/[G,G]| = p, q, 1$. We cannot have 1, because let n be the number of the conjugation classes then the dimension, group order formula of G gives $1 + p^2 n = pq$.But since right hand side is 0 mod$p$ but left side is 1. That cannnot be happen.
If $|[G,G]| = p$, then there is a normal subgroup $[G,G]$ of order q, also notice by the Sylow's theorem, there are unique normal sylow q group. By the internal direct product theorem, it would be a internal direct product between $q-$sylow subgroup P_p and $[G,G]$. Both group is commutative, so group would be a abelian.
Thus $|[G,G]| = q$ and there are p different 1-dimensional irreducible representation. There are $\frac{q-1}{p}$ degree p irreducible characters. This also indirectly shows that such a non-abelian pq group exist only if $q|p-1$.
Note that you can also use the fact strcture theorem of the non-abelian pq group. □

2023S #10 Let A be an artinian ring and let M be an A-module. Let $B = \mathrm{End}_A(M)$. Let $f \in B$ such that $f(M) \subset J(A) \cdot M$, where $J(A)$ is the Jacobson radical. Show that $f \in J(B)$.

Solution: There are four steps.

(a) Show $J(A)$ is nilpotent.

(b) $I = \{f \mid f(M) \subset J(A) \cdot M\}$ is an ideal.

(c) We want to show that $1 - hf$ is invertible for all $h \in End_A(M)$, but $hf \in I$ because I is an ideal, so it suffices to show $1 - f$ is invertible for all $f \in I$.

(d) f is nilpotent. Then

$$(1 + f + f^2 + \ldots + f^N)(1 - f) = 1 - f^{N+1} = 1$$

so $1 - f$ is invertible.

Here once see step (a) and (b), rest is just following (c) and (d) so just see a nontrivial claims of (a) and (b). *Lemma.* Jacobson radical $J(A)$ of Artinian ring A is nilpotent ideal.

Proof. $J(A)$ is an ideal of Artinian ring, so the chain $J^i(A) \subset J^{i+1}(A)$ would stablize. Let K be an ideal that stablize, $I = J^i(A) = J^{i+1}(A) = \dots$. If $I \neq 0$ then nothing to prove,

$$\mathcal{F} = \{I \subset R | K \text{an ideal and } IK \neq 0\}$$

$\mathcal{F}$ is not empty because $I \in \mathcal{F}$, and by Artinian condition there is an minimal ideal, put it K. We will show that K is finitely generated. $IK \neq 0$ now choose element $x \in K$ such that $Ix \neq 0$, such element x exist, otherwise $IK = \sum Ix = 0$, so $Ix = 0$ and indeed by the hypothesis of being minimal of $(x) = K$. This shows not just finitely generated, but K is principally generated. Since K is finitely generated, $IK = K$ we can use Nakayama's lemma(Note $I \subset J(A)$.) So $K = 0$. This means that there is no notrivial element in the family so $I = 0$. □

Returning to the problem, consider the set

$$I = \{g \in B \mid g(M) \subset J(A) \cdot M\}$$

By construction, this is a left ideal. Moreover, for any $g \in I$, we know g is nilpotent. This is because for any $n \geqslant 1$

$$f^n(M) \subset f(J(A)^{n-1}M) \subset J(A)^n M$$

□

5 Fall 2022

2022F #1 Find all the subfield of $F = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$

Solution. Consider the normal closure N of F, denote their Galois group $G := Gal(N/\mathbb{Q})$.

Claim: $G = (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

Proof. $x^3 - 2$ and $x^3 - 3$. Since F does not contain 3rd root of unity ω, F is not a splitiing field for $x^3 - 2$ or $x^3 - 3$. Notice F is totally real field, so $F \cap \mathbb{Q}(\omega) = \mathbb{Q}$. These polynomial split on $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \omega)$. Since $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \omega), F] = 2$ there is no intermediate field between them, we can see $N = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \omega)$. Consider the Galois group $Gal(N/F) \cong \mathbb{Z}/2\mathbb{Z}$. It is generated by an action $\rho \in G$ $\rho : \omega \to \omega^{-1}$. Since $\sqrt[3]{2}$ and $\sqrt[3]{3}$ are linearly disjoint, $[N : \mathbb{Q}] = 18$. Let $\sigma, \tau \in G$ be elements permuting roots of $x^3 - 3$ and $x^3 - 2$ respectively $\sigma : \sqrt[3]{2} \to \sqrt[3]{2}\omega$ and $\tau : \sqrt[3]{3} \to \sqrt[3]{3}$. Notice, $F = \mathbb{Q}(\omega, \sqrt[3]{2})\mathbb{Q}(\omega, \sqrt[3]{3})$, and $\mathbb{Q}(\omega, \sqrt[3]{3}) \cap \mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\omega)$. So the Galois group of $Gal(N/\mathbb{Q}(\omega)) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. By considering the actions of ω, we can compute relation $\rho\sigma\rho^{-1} = \sigma^{-1}$ and $\rho\tau\rho^{-1} = \tau^{-1}$. □

By the Galois correspondence, any intermediate field E such that $\mathbb{Q} \subsetneq E \subsetneq F \subset N$ correspond to the subgroup H such that $\{e\} \subset \{\rho\} \subsetneq H \subsetneq G$. As ρ is order 2 and G is order 18, the only possible order for H is 6. Since $\langle\rho\rangle \subset H$, H is semi-direct product between $\langle\rho\rangle$ and order 3 elements of G.There are 6 order 3 elements in G,$\{\sigma, \tau, \sigma\tau, \sigma^2\tau^2, \sigma^2\tau, \sigma\tau^2\}$. There are 4 different groups generated by these elements namely $\langle\sigma, \rho\rangle, \langle\tau, \rho\rangle, \langle\sigma\tau, \rho\rangle = \langle\sigma^2\tau^2, \rho\rangle, \langle\sigma^2\tau, \rho\rangle = \langle\tau\sigma^2, \rho\rangle$.
Counting $\langle\rho\rangle$ and G together, we see there are 6 subfields. □

2022F #2 Let $P(X) = x^6 + 3$

(a) Determine the splitting field over $\mathbb{Q}$

(b) Determine the isomorphism type of the Galois group of $P(X)$ over $\mathbb{Q}$.

Solution: (a) Let $\zeta = e^{\frac{2\pi}{6}}$ then the splitting field is $\mathbb{Q}(\zeta, \sqrt[6]{-3})$ for $1 \leqslant i \leqslant 6$. Since $\zeta = \frac{1}{2} + \frac{i\sqrt{3}}{2} \in \mathbb{Q}(\sqrt[6]{-3})$ thus indeed $\mathbb{Q}(\zeta, \sqrt[6]{-3}) = \mathbb{Q}(\sqrt[6]{-3})$. This implies extension is generated by $\sqrt[6]{-3}$. $\mathbb{Q}(\sqrt[6]{-3})$ is 6 dimensional over $\mathbb{Q}$ vector space, we have $[\mathbb{Q}(\sqrt[6]{-3}) : \mathbb{Q}] = 6$.

(b) The group of order 6 is either $\mathbb{Z}/6\mathbb{Z}$ or S_3. The Galois correspond says normal subgroup correspond normal subfield. Here $\mathbb{Q}(\sqrt[3]{3})$ is a subfield but not Galois over $\mathbb{Q}$ so this is not abelian. Thus Galois group is S_3.

□

2022F #4 List all conjugacy classes of $GL(2, F_p)$.

Solution: The matrix on the vector space has rational canonical form

$$\begin{pmatrix} C(f_1) & 0 \\ 0 & C(f_2) \end{pmatrix}$$

with $f_1|f_2$ or $C(f_1)$. In the former case, f_1 and f_2 has both degree 1 so that rational canonical form is a diagonal matrix so there are $p-1$ different conjugacy classes. In the latter case, $f_1 = x^2 + ax + b$ and

$$C(f_1) = \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}$$

This matrix is invertible iff $b \neq 0$ so that there are $p(p-1)$ different conjugacy classes. To sum up, there are $p(p-1)+p-1 = p^2-1$ conjugacy classes. □

2022F #5 Let G be the group presented by

$$G = \langle a, b | a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1} \rangle$$

You may use that G has order 8. Compute the character table of G.

Solution: Since G has order 8 and is not abelian, as $a^{-1} \neq a$ (a is of order 4), we know G is either D_4 or the quaternion group. (If you are familiar with the quaternions, you could see immediately that this is the quaternion group presentation). We note that this assumption (along with $a \neq b$) gives us the 8 elements directly

$$G = \{ab, ba, a, a^{-1}, b, b^{-1}, a^2 = b^2, e\}$$

(or alternatively) We have a unique presentations of the elements of group by $a^i b^j$ so that we can easily figure out that $\langle a^2 \rangle$ is normal subgroup. We can compute the commutator group by quotienting out by $a^2\rangle$ so that we have a presentation of $G/\langle a^2 \rangle \cong \langle a, b | a^2 = b^2 = 1, bab = a \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

From the group presentation we have the following conjugacy classes (which gives us the number of irreducible representations)

$$bab^{-1} = a^{-1} \tag{1}$$

$$aba^{-1} = b^{-1} \tag{2}$$

$$bbab^{-1} = ba^{-1} \tag{3}$$

We note that $a^2 = b^2$ is its own conjugacy class, as this commutes with both a and b so is in the center of the group. Since e is also its own

conjugacy class, we have 5 conjugacy classes 2 containing one element each and 3 containing 2 elements.

To compute the character table, we will start by noting that there must be an identity character. We note that the sum of the dimensions of the characters squared must equal the size of the group, and we note that we must have a character for each conjugacy class. This means $8 = 1+1+1+1+2^2$ is the only way to allocate dimensions. For 1-dimensional characters, we can make a guess. Let's compute the character that takes a to -1 and b to 1. We know that this is irreducible if it is well defined, as it has dimension 1. This gives us $a^3 \mapsto -1$, $b^3 \mapsto 1$ and $ab, ba \mapsto -1$, and $a^2, b^2, e \mapsto 1$, and thus is well defined. Similarly, we look at the character that takes $b \mapsto -1$ and $a \mapsto 1$. Finally, we take the characters $b \mapsto -1$ and $a \mapsto -1$. All three of these are well-defined 1-dimensional characters (one can compute that these are in fact linearly independent). So we have

	$\{e\}$	$\{a^2\}$	$\{a, a^{-1}\}$	$\{b, b^{-1}\}$	$\{ab, ba\}$
E	1	1	1	1	1
R_1	1	1	-1	1	-1
R_2	1	1	1	-1	-1
R_3	1	1	-1	-1	1
R_4	2	x_1	x_2	x_3	x_4

To calculate the last row, we use the following orthogonality relation

$$0 = \langle \chi_\alpha, \chi_\beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}$$

We can compute inner products:

$$\langle E, R_4 \rangle = \frac{1}{8}(2 + x_1 + 2x_2 + 2x_3 + 2x_4) = 0$$

$$\langle R_1, R_4 \rangle = \frac{1}{8}(2 + x_1 - 2x_2 + 2x_3 - 2x_4) = 0$$

$$\langle R_2, R_4 \rangle = \frac{1}{8}(2 + x_1 + 2x_2 - 2x_3 - 2x_4) = 0$$

$$\langle R_3, R_4 \rangle = \frac{1}{8}(2 + x_1 - 2x_2 - 2x_3 + 2x_4) = 0$$

Adding all 4 of these equations, we get:

$$1 + \frac{1}{2}x_1 = 0 \implies x_1 = -2$$

Which tells us $x_1 = -2$. Now, we use the normality condition: $\frac{1}{|G|}\langle \chi_\alpha, \chi_\alpha \rangle = 1$

$$\langle R_4, R_4 \rangle = \frac{1}{8}(4 + 4 + 2|x_2|^2 + 2|x_3|^2 + 2|x_4|^2) = 1$$

This means:

$$1 + \frac{1}{4}(|x_2|^2 + |x_3|^2 + |x_4|^2) = 1$$

Noting that the magnitudes need to be greater than or equal to 0, and thus all three of them must be 0. The final character table is:

	$\{e\}$	$\{a^2\}$	$\{a, a^{-1}\}$	$\{b, b^{-1}\}$	$\{ab, ba\}$
E	1	1	1	1	1
R_1	1	1	-1	1	-1
R_2	1	1	1	-1	-1
R_3	1	1	-1	-1	1
R_4	2	-2	0	0	0

□

2022F #6 Let G be a finite group, let V be a finite-dimensional complex vector space and let $\pi : G \to GL(V)$ an irreducible representation. Let H be an abelian subgroup of G. Show that $dim(V) \leqslant [G : H]$.

Proof. Let $\rho : G \to GL(V)$ be a irreducible representation. Then it defines the restriction to the ρ_H. Let W be a irreducible representation of H, which is one dimensional. Let V' be the subvector space of V such that generated by the images of $\oplus_{g\in G} gW$. Note that this V' is invariant undet the action of G, so this is also a subrepresentation of V. However V is irreducible, and $V' \neq 0$ so $V = V'$. Given two different vector spaces to be coincide $g'W = gW$, this is equivalent $g^{-1}g'W = W$ that means $g'^{-1}g \in H$. In other words, there is some $h \in H$ such that $g = g'h$. It means the image under G is determined by the representative class of G/H. Since the number of different images are atmost $[G : H]$ because it is so the dimension of V is at most $[G : H]$.
Alternatively let χ_H be a restriction of V to the subgroup H.

Claim. $\langle \chi_H, \chi_H \rangle \geqslant \chi_V(1)$

Proof. The character restrict to H can be written as the direct sum of irreducible representation λ_i of H, $\chi_H = \sum m_i \lambda_i$. Since χ_H is a just restriction of H, we have $\chi_V(1) = \chi_H(1)$. In particular the representation of the abelian group is $\lambda_i : G \to \mathbb{C}^\times$. And order is finite, all $\chi_i(g_j)$are root of unity. $\chi_H(1) = \chi_V(1) = \sum m_i$ where m_i are integers. Taking the inner product, $\langle \chi_H, \chi_H \rangle = \sum m_i m_j \langle \lambda_i, \lambda_j \rangle = (\sum m_i^2) \geqslant \sum m_i$. □

Since χ_V is irreducible character, we have $\sum_{g\in G} |\chi_V(g)|^2 = |G|$ by the orthogonalities. So the restriction to the H gives $\sum_{h\in H} |\chi_V(h)|^2 \leqslant |G|$ Since $\langle \chi_H, \chi_H \rangle = \frac{|\chi_V|^2}{|H|}$ we have $\chi_V(1) \leqslant \langle \chi_H, \chi_H \rangle \leqslant \frac{|G|}{|H|}$. □

2022F #7 Let S be a multiplicatively closed subset of a commutative ring R. Show that for a prime ideal $\mathfrak{p}$ in R disjoint from S, the ideal $\mathfrak{p}R[S^{-1}]$ in the localization $R[S^{-1}]$ is prime. Show that this gives a one-to-one correspondence between prime ideals in R that are disjoint from S and prime ideals in $R[S^{-1}]$.

Solution. Let $\pi : R \to R[S^{-1}]$ be the localization, defined by $a \to \frac{a}{1}$.

Lemma 1. For any ideal $J \subset R[S^{-1}]$, $\langle \pi(\pi^{-1}(J)) \rangle = J$.

Proof. It is clear $\langle \pi(\pi^{-1}(J)) \rangle \subset J$. For the reverse inclusion, let $\frac{a}{s} \in J$. Then $s\frac{a}{s} \in J$, with $a \in R$, thus $a \in \pi^{-1}J$. This means $\frac{a}{1} \in \pi(\pi^{-1}(J))$. So that $(\frac{1}{s})(\frac{a}{1}) = \frac{a}{s} \in \langle \pi(\pi^{-1}J) \rangle$

□

Lemma 2. For any ideal $I \subset R$, $\pi^{-1}(\langle \pi(I) \rangle) = \{a \in R : \exists s \in S : sa \in I\}$. Also $\langle \pi(I) \rangle = R[S^{-1}] \leftrightarrow I \cap S \neq \varnothing$

Proof. Let $I' = \{i \in R : \exists s \in S : si \in I\}$. Suppose $i \in I'$, there exist $s \in S$: $si = a \in I$. Then $\frac{i}{1} = \frac{a}{s} \in \pi I$. So $i \in \pi^{-1}(\pi I)$. Conversely, let $i \in \pi^{-1}(\pi I)$, so that $\frac{i}{1} = \frac{a}{s}$ for some $a \in I$ and $s \in S$. Then $\exists t \in S : t(si - a) = 0$ so $tsi = ta \in I$ and we can find $ts \in S$, so that $its \in I$, which means $i \in I'$. Now $\pi I = R[S^{-1}] \leftrightarrow \frac{1}{1} \in \pi I \leftrightarrow 1 \in \pi^{-1}(\pi I)$ In particular if I is any prime ideal disjoint with S the $\mathfrak{p}' = \mathfrak{p}$ □

Returning to the original problem, pick an ideal $\mathfrak{q} \subset R[S^{-1}]$ then prove $\pi^{-1}\mathfrak{q}$ is a prime ideal that is not intersecting with S. First of all this does not intersect with S, otherwise contradicts with lemma 1. This is prime ideal because preimage of prime ideal is prime.Suppose $\mathfrak{p} \subset R$ is a prime, such that $\mathfrak{p} \cap S = \varnothing$. Let $\mathfrak{q} = \pi\mathfrak{p}$. Suppose $\frac{a}{s}\frac{a'}{s'} \in q$ then $\frac{aa'}{ss'} = \frac{p}{u}$ for some $p \in \mathfrak{p}$ and $u \in S$. Then there is some $t \in S : t(uaa' - ss'p) = 0$ Since $\mathfrak{p} \cap S = \varnothing$ and $\mathfrak{p}$ is prime, we get $aa' \in \mathfrak{p}$ so either $a \in \mathfrak{p}$ or $a' \in \mathfrak{p}$. This shows bijective correspondences. □

2022F #8 Let A be a commutative ring. Show that the following are equivalent.

(a) Every prime ideal of A is equal to an intersection of maximal ideals of A.

(b) For every ideal I, the intersection of all prime ideals of A/I is equal to the intersection of all maximal ideals of A/I.

Solution Sketch: (a) $\implies$ (b): the intersection of prime ideals of A/I corresponds exactly to the intersection of all prime ideals of A that contain I. Since every prime ideal of A (containing I) is equal to an intersection of maximal ideals of A (containing I), this is exactly equal to the intersection

of all maximal ideals of A that contain I (as maximal ideals are prime), which then corresponds to the intersection of all maximal ideals of A/I.

(b) $\implies$ (a): Let $I = P \subset A$ be a prime ideal. Then, A/I is a domain, so (0) is a prime ideal of A/I. Thus the intersection of all prime ideals of A/I is (0), and must be equal to the intersection of all maximal ideals of A/I. This corresponds to saying the intersection of all maximal ideals containing P is equal to P. □

2022F #9 Let $\phi : Ab \to Gp$ be the inclusion/forgetful functor. Show that ϕ has a left adjoint α. Does α have a left adjoint? Does ϕ have a right adjoint?

Solution Sketch $\alpha : Gp \to Ab$ the abelianization functor is left adjoint to ϕ. ϕ has no right adjoint because it does not commute with colimits. As a counterexample, consider the coproduct $\mathbb{Z} \times \mathbb{Z}$ in the category of abelian groups. Then, $\phi(\mathbb{Z} \times \mathbb{Z}) = \mathbb{Z} \times \mathbb{Z}$ remains abelian. However, taking the coproduct last gives us $\phi(\mathbb{Z}) * \phi(\mathbb{Z}) = \mathbb{Z} * \mathbb{Z}$ which is not abelian.

Moreover, α does not have a left adjoint because it does not commute with limits. Consider the inclusion $f : A_3 \to S_3$. Then, α does not preserve this inclusion. $\alpha(f) : A_3 \to \mathbb{Z}/2\mathbb{Z}$ is the trivial homomorphism. So in particular, α does not preserve the fiber product of the diagram $A_3 \to S_3$ consisting of two f arrows. If we take the fiber product first, we get A_3. If we take the fiber product last, we get $A_3 \times A_3$.

Note: any functor that preserves limits must preserve monomorphisms because of this. Similarly, any functor that preserves colimits must preserve epimorphisms.

2022F #10 Compute the Jacobson radical $J(R)$ for the following rings R.

(a) Let $R = End_R(V)$, for a real vector space V of countably infinite dimension. Compute $J(R)$.

(b) For any finite extension field F of $\mathbb{Q}$, let R be the integral closure of $\mathbb{Z}$ in F. Compute $J(R)$.

Solution. (a) (a)We claim $J(R) = 0$. Pick $x \in J(R)$, prove there exist $a \in End_R(V)$ such that $1 - ax$ is not invertible. Let the basis of vector space be $\{e_1 \dots\}$ and x maps $\{x(e_1) \dots\}$ to other basis. Define a linear operator y such that $y(x(e_1)) = e_1$ and $y(x(e_i)) = x(e_i)$. In particular, $(1 - y(x))e_1 = 0$ so this is not injective, so it shouldn't have a left inverse. Note: even though the linear operator is not injective, it could still have a right inverse. So Jacobson radical is 0 because it is asking only the left inverse.

(b) (b) Note that R is Dedekind domain, in particular all prime ideals are maximal ideal.
Lemma: R has infinitely many prime ideals.
Proof: There are infinitely many nonzero primes of $\mathbb{Z}$. Let p, q are

distinct primes of $\mathbb{Z}$, then $pR + qR = R$. This means pR and qR are relatively primes, as being ideal of Dedekind ring, we have the unique decomposition to product of prime ideals that means pR and qR is contained in all distinct prime ideals.
If $J(R) \neq 0$ then as a prime ideal decomposition of $J(R)$ we can decomposed into a product of finitely many prime ideals. That means $J(R)$ is contained in only finitely many maximal ideals. But we just show that R has infinitely many prime ideals. Contradiction.

□

6 Spring 2022

2022S #1 Let F be a field of characteristic not 2 and let the symmetric group Sn act on the polynomial ring $F[X_1, \ldots, X_n]$ by permuting the variables, for $n \geqslant 2$. Let $A = (F[X_1, \ldots, X_n])^{A_n}$ and $B = (F[X_1, \ldots, X_n])^{S_n}$ be the fixed subrings, where $A_n < S_n$ is the alternating group.

(a) Show that A is an integral extension of B.

(b) Show that $A = B[\delta]$ for some $\delta \in A$ such that $\Delta := \delta^2$ belongs to B.

(c) For $n = 2$,describe Δ as a polynomial in $e_1 = X_1 + X_2$ and $e_2 = X_1X_2$.

Solution: (a) We can show in general $F[X_1 \ldots X_n]$ is integral over $F[X_1 \ldots X_n]^G$ because for given polynomial $p \in F[X_1 \ldots X_n]$ then $\prod_{g\in G}(y - g\cdot p)$ has $G-$invariant coefficient. Note that $F[X_1 \ldots X_n]^{S_n} \subset F[X_1 \ldots X_n]^{A_n} \subset F[X_1 \ldots X_n]$.

(b) *Claim.* $\delta = \prod_{i<j}(x_i - x_j)$
Let $f \in A$. Then define $g = (1, 2)f$. Note that we get same g for the any permutation (i, j) because $(1, 2)f = (1, 2)(1, 2)(i, j)f = (i, j)f$. We can decompose function as $f = \frac{1}{2}(f+g)+\frac{1}{2}(f-g)$. We will prove that $f + g$ is symmetric and $f - g$ is divisible by δ. If we act π which is product of even permutations, then $\pi(f + g) = f + \pi(1, 2)f$. Since the cycle length is preserved under the conjugacy, we can find some 2 cycle by $\pi(1, 2)\pi^{-1} = (i, j)$ so we have $\pi(1, 2)f = (i, j)\pi f = g$. For the similar argument, we see invariance of the odd cycle. On the other hand, we can check $f-g$ change sign under the action of the odd cycle, and preserve sign under the even sign. Any polynomial whose action by the transposition change the sign is divided by the δ. Because $h(\ldots x_i \ldots x_j \ldots) = -h(\ldots x_j \ldots x_i \ldots)$ implies $h(\ldots x_i \ldots x_i \ldots) = 0$ and since polynomial is UFD that is divided all factors $(x_i - x_j)$ with $i < j$.

Alternatively Lemma:We can use the fact that invariant ring and the localization are commute, namely if we are given the $R = F[x_1 \ldots x_n]$ domain(here we actually not need to be domain though) then $Frac(R^G) = Frac(R)^G$ according to Atiyah Macdonald Exercise 12, Chapter 5.
Take $\frac{a}{s} \in Frac(A)^G$. Then $\frac{a\prod_{\sigma\in G/1}\sigma(s)}{\prod_{\sigma\in G}\sigma(s)} = \frac{a'}{s'}$. With this new expression, denominator is $G-$invariant. Let the action of $\sigma \in G$ then $\frac{a'}{s'} = \frac{\sigma(a')}{\sigma(s')}$. Since this is integral domain we have $a' = \sigma(a')$ so $\frac{a}{s} = \frac{a'}{s'} \in S^G A^G$ where $S = R/\{0\}$.

According to lemma we have $Frac(R^{A_n}) = Frac(R)^{A_n}$ and $Frac(R^{S_n}) = Frac(R)^{S_n}$. By Galois correspondence $[Frac(R)^{A_n} : Frac(R)^{S_n}] = [S_n : A_n]$. Degree 2 extensions, the elements to add is discrimnant δ. Since $\delta \in R$ we showed the statement. □

2022S #2 (Omit the text of the problem)

Solution: I guess it wouldn't asked it again, idea is we can take left derived functor $\to Tor(Z,M) \to Tor(Z,N) \to$. Since M is free so flat, $Tor(Z,M) = 0$. By hypothesis $coker(Tor(Z,M) \to Tor(Z,N)) = 0$ that means $Tor(Z,N) = 0$ □

2022S #3 Let G be a finite p-group and let $H < G$ be a proper subgroup. We write as usual $H^g = g^{-1}Hg$ for every $g \in G$.

(a) Show that the normalizer $N_G(H)$ of H in G is strictly larger than H.

(b) Show that if H is not normal in G then there exists another proper subgroup $H < K < G$ and $g \in G$ such that $K^g = K$ but $H^g \neq H$.

Solution: (a) Let H act on the right cosets G/H by right translation. Since H is proper subgroup, the number of such cosets is divisible by p. At least one of these is fixed by H, namely the coset H. By the fixed point theorem the number of the different orbits fixed by H is divisible by p. Hence there is some $g \in G/H$ such that $Hgh = Hg$ for all $h \in H$. This implie $ghg^{-1} \in H$ for all $h \in H$ so $gHg^{-1} \subset H$. Since they have same cardinalities we have $gHg^{-1} = H$. Hence $g \in N_G(H)/H$ and $N_G(H) > H$.
Alternative solution:(At least this solution feels me more natural) Prove by induction, when $G = \mathbb{Z}/p\mathbb{Z}$, there is only one proper subgroup $\{e\}$ and in this case, normalizer is entire group, so statement is true. Assume the case for p^{n-1} and prove for p^n. There exist a group $H < G$ such that $N_G(H) = H$. Note that p group has a nontrivial center Z, and for any element of center $z \in Z$, $H^z = H$ so $Z \subset N_G(H)$ so $Z \subset H$. Thus $H/Z \subset G/Z$. By the induction hypothesis, the normalizer of H/Z in G/Z properly contained in the normalizer. This means there is $\overline{x} \notin H/Z$ such that $\overline{x}H/Z\overline{x}^{-1} = H/Z$.
Let $h \in H$ we have $\overline{x}hZ\overline{x}^{-1} = h'Z$ for some $h' \in H$. Therefore $xhx^{-1}Z = h'Z$ so $xhx^{-1}z = h'z'$ implies $xhx^{-1} = h'z'z^{-1}$ since $z', z' \in H$ we have $xhx^{-1} \in H$

(b) Take the normalizer, then $G \supset N_G(H) \supset H$ and since H is not normal $G \neq N_G(H)$. Pick $K = N_G(H)$, Then $N_G(N_G(H))$ is strickly contain $N_G(H)$ by (a). So pick $g \in N_G(N_G(H))/N_G(H)$ so statement holds.

□

2022S #4 Let R be commutative, $M \in R - Mod$.

(a) Show $Hom_R(-,M) : (R-Mod)^{op} \to R - Mod$ admit a left adjoint.

(b) Show that for every $R-$module X,the module $\mathrm{Hom}_R(X,M)$ is a direct summand of $\mathrm{Hom}_R(\mathrm{Hom}_R\ (\mathrm{Hom}_R(X,M),M),M)$.

We note

For $Hom_R(-,M) : R-mod \to (R-mod)^{op}$ So it is self adjoint functor.

(a) Consider the unit η and counit ϵ for the functor $Hom(-,M)$ so that

$$\eta_X : Hom_R(X,M) \to Hom_{R^{op}}(M, Hom_R(X,M))) \cong Hom_R(Hom_R(X,M),M)$$

$$\epsilon_X : Hom_R(Hom_R(X),M),M) \to Hom_R(X,M)$$

such that $\epsilon \circ \eta = Id$.Thus there is an exact sequence

$$0 \longrightarrow Hom_R(X,M) \underset{\epsilon}{\overset{\eta}{\rightleftarrows}} Hom_R(Hom_R(Hom_R(X,M),M),M) \longrightarrow Coker\eta \longrightarrow 0$$

since this split, $Hom_R(X,M)$ is a direct summand.

2022S #5 Let R be a commutative ring and let G be a finite group. Prove that R with trivial G action is a projective RG-module if and only if the order of G is invertible in R.

Solution: There is a surjective RG-module homomorphism $\phi : RG \to R$ where $\phi(\sum a_i g_i) \to \sum a_i$, so R is projective if and only if ϕ has a injective right inverse.
If R is projective $R[G]$ module then $\theta : R \to RG$ is a injective right inverse, so that $\phi\theta = id_R$. Since we have the trivial action for R to be an homomorphism, $\theta(g \cdot 1) = \theta(1)$ for all $g \in G$. As G act R trivially, so $\theta(1)$ contain all terms of g_i because that is the only way to make action g invariant, so $\theta(1) = b\sum g_i$ for some $b \in R$. Note this is a injective as a $R-$module, and to make $\phi\theta(1) = 1$ $b = \frac{1}{|G|}$ which can only occur when $|G|$ is invertible in R.
Assume $|G|$ is invertible in R then above θ is well defined, and we can repeate above argument so that see θ has left inverse and splite, this means R is projective $R[G]$ module $\square$

2022S #7 Let K/F be a finite separable field extension, and let L/F be any field extension. Show that $K \otimes_F L$ is a product of fields.

Solution: Since K is a finite separable extension, we can find an element $\alpha \in K$ such that $F(\alpha) \cong F[x]/m_\alpha$. Since m_α is separable, we can use Chinese remainder theorem to we can factorize into a product of irreducible polynomials.

$$F[x]/m_\alpha \otimes L \cong \prod_{\alpha'} L[x]/m_{\alpha'}$$

Since $L[x]$ is PID, all prime ideals are maximal ideals. So $L[x]/m_{\alpha'}$ is a field. $\square$

2022S #9 Let A be a (unital) algebra of dimension n over a field F. Prove that there is a (unital) F -algebra homomorphism from $A \otimes_F A^{op}$ to the F -algebra of $n \times n$ matrices, where A^{op} is the opposite algebra.

Solution. We have the morphism $(a,b) \in A \otimes_F A^{op} \to M_n(F) \cong End_F(A) \ni \phi_{a,b}(x)$ by $\phi_{a,b}(x) = (axb)$. This morphism is is $F-$algebra homomorphism because $(a \otimes b) \cdot (c \otimes d) = (ac \otimes db)$. $\phi_{c,d} \circ \phi_{a,b}(x) = acxdb = \phi_{ac,db}(x)$. The image of this homomorphism is not trivial, because if $\phi_{a,b}(x) = axb = x$ for all x then for example $\phi_{a,b}(1) = ab = 1$ so a is a left inverse of b. $\phi_{a,b}(a) = a = 1$, so $a = 1$ similarly for b.

The explicit way of seeing map is we can take an basis as a $F-$vector spaces e_i, then multiplication of $a = \sum a_{ij}e_i$ and $b = \sum b_{ij}e_i$ can be written as $ae_ib = \sum A_{ij}e_j$. We can collect a data for A_{ij} so that we can form a matrix.

When ring is simple so the morphism is isomorphism for the dimension reason. (Note, this can be solved with Jacobson density theorem as well without assuming tensor product of simple module is simple.)

□

2022S #10 Let F be a field characteristic not 2 and let $K = F(\sqrt{a}, \sqrt{b})$ be a biquadratic field extension (of degree 4) of F, for $a, b \in F^\times$ not squares. Suppose that $b = r^2 - as^2$ for some $r, s \in F$ (i.e., b is a norm for the quadratic extension $F(\sqrt{a})/F$). Prove that there is a field extension L of K that is Galois over F with Galois group the dihedral group of order 8.

Solution: Consider the extension $F[\sqrt{r - \sqrt{a}s}]$, first we will see that $F[\sqrt{a}] \neq F[\sqrt{r - \sqrt{a}s}]$. That can be seen by the field norm as follows. Suppose not, then we have $\sqrt{r - \sqrt{a}s} = c_1 + c_2\sqrt{a}$ taking norm

$$N_{F(\sqrt{a}/F)}\sqrt{r - \sqrt{a}s} = \sqrt{b}$$

But by the definition of norm that implies $\sqrt{b} \in F$.That is contradiction. Few words for why norm being $\sqrt{b}$, Take square for $\sqrt{r - s\sqrt{a}}$ so that this will be $r - s\sqrt{a}$, taking norm on this, we get b, so the norm should be the square root of b

We can also use this method to prove $F(\sqrt{r - s\sqrt{a}s}) \neq F(\sqrt{r - \sqrt{a}s}, \sqrt{r + \sqrt{a}s})$. Suppose otherwise, then we have $\sqrt{r - \sqrt{a}s} = c_1 + c_2\sqrt{r + s\sqrt{s}}$ for $c_1, c_2 \in F(\sqrt{a})$. Taking field trace over $F(\sqrt{a}, \sqrt{r - s\sqrt{a}})/F(\sqrt{a})$ then we figure out $c_1 = 0$ Few words for why c_1 should be 0, assumption is $F(\sqrt{r - s\sqrt{a}s}) = F(\sqrt{r - \sqrt{a}s}, \sqrt{r + \sqrt{a}s})$ but hypothesis is both side field of degree 2, this means since $F(\sqrt{r - s\sqrt{a}})$ is also degree 2 extensions. So the trace of $\sqrt{r - \sqrt{a}s}$ over $F(\sqrt{r - s\sqrt{a}})/F(\sqrt{a})$ is 0. Similarly, trace of $\sqrt{r + s\sqrt{a}}$ over $F(\sqrt{r + s\sqrt{a}})$ is 0.

because they are basis of vector space. On the other hand, we can multiple $\sqrt{r + s\sqrt{a}}$ again, then we have $\sqrt{b} \in F(\sqrt{a})$ again. That is a contradiction. We figured out this as the Galois extension of order 8 with non-Galois intermediate field(Which is $F(\sqrt{r - s\sqrt{a}})$ as being minimal polynomial $T^4 - 2rT^2 + b$, as third terms of polynomial vanishes because+- conjugation killing each other second

terms are form of all sums of products of two roots combinations are products of each $\pm$ conjugations and real conjugations. in case products of $\pm$ conjugations, their sums are $-2r = -(r + s\sqrt(a)) - (r - s\sqrt{a})$ In case of real conjugations their sums are $0 = \sqrt{b} - \sqrt{b}$. For the case of $1st$ coefficient, it has to have $\sqrt{b}$ and just suming all the rest in different way so multiplication of 1st coefficient so this is the polynomial.
Furthermore, we didn't show the top field is not Galois, this is obviously the splitting field, so enough to show this is a separable extensions. Notice, that characteristic is not 2 so the derivative is not vanishing. The root is $\pm\sqrt{r}$ and 0 and we can check $r^2 - 2r^2 + r^2 - as^2 \neq 0$ so separable extensions. That implies the Galois group is order 8 with a nonnormal subgroup. Relying on the classification of the group of order 8 that is a dihedral group. $\square$

7 Fall 2021

Fall 2021 Question 2 Let K be a field, and consider the ring $R = K[x]/(x^2)$. Show that every free submodule N of an $R-$module M is a direct summand of M.

Solution Sketch $k[x]/(x^2)$ is injective module on its own. Any products of injective module is injective, thus exact sequence splits.

Solution
Lemma 1: If R is PID, and I is nonzero proper ideal, then R/I is injective left R/I module.
Proof: By Baer's criterion, it suffice to extend a map $f : J/I \to R/I$ to the $R/I \to R/I$ such that J is an ideal containing I. Since R is PID $I = Ra$, and $I \subset J = Rb$ thus we find $c \in R$ such that $bc = a$. The $R/I-$module R/I is generated by $x = 1 + I$ and J/I is generated by bx.
Now let the homomorphism f be $f(bx) = sx$ for some $s \in R$. Since $bcx = ax = 0$ we have $0 = cf(bx) = csx$. This implies $cs \in Ra$. Therefore $cs = ra = rbc$ for some $r \in R$. since R is domain cancelling c gives $s = rb$ so that $f(bx) = sx = rbx$. Define $g : R/I \to R/I$ to be multiplication by r. Now g extend f for $g(bx) = rbx = f(bx)$. Thus R/I is self injective.

Lemma. Any direct sum of injective module over Noetherian ring is injective.
Proof: Show for family of injective module I_i and finitely generated module M, we have $Hom(M, \oplus I_i) \cong \oplus Hom(M, I_i)$. First notice in general there is an injective $\oplus Hom(M, I_i) \to Hom(M, \oplus I_i)$ by coordinate wise embedding. M is finitely generated, the image of a homomorphism from M to $\oplus_i N_i$ is contained in the direct sum of finitely many I_i. Since Hom commutes with forming finite direct sums, ϕ is surjective as well. For Noetherian ring, ideal is finitely generated. $Hom_R(R, I_i) \to HomR(a, I_i)$ is surjective. Since a is finitely generated, the above isomorphism implies that $Hom(R, \oplus_i) \to Hom(a, \oplus I_i)$ is surjective as well. Baer's criterion now implies that $\oplus E_i$ is injective.
Here, the argument of finitely generatedness then preserve colimit is indeed rephrased as compact object preserve colimit as a $hom(M, -)$. The compact object is the object M such that $Hom(M, -)$ preserve direct sum.

Proof of the claim: N is free submodule of M. Since R is PID, N is injective by above two claims. We have the exact sequence $0 \to N \to M \to coker \to 0$. Since N is injective the sequence split so N is direct summand of M.

So injective module preserved by the product over any rings
Lemma. Any direct product of injective module is injective.
Proof: If I_i is injective, then given a morphism from a module $A \to I_i$ and injection $A \to B$. We have the unique lift of the morphism to $B \to I_i$. Thus if A has morphism to the all I_i, it raise morphism to the $A \to \prod I_i$.

Then any injection $A \to B$ lift into $B \to \prod I_i$. So any product of injective modules are injective.

Alternate Solution
Consider the family of R-submodules of $L \leqslant M$ with $L \cap N = 0$. When ordered by inclusion, these submodules. If we take the union of these modules there are upper bound so this satisfy the conditions of Zorn's Lemma. There exists a maximal such submodule $L_0 \leqslant M$ such that $L_0 \cap N = 0$. Suppose for the sake of contradiction that $M \neq N \oplus L_0$. Then we can pick $m \in M$ with $m \notin N \oplus L_0$. If $Rm \cap (N \oplus L_0) = \varnothing$ then $(Rm + L_0) \cap N = \varnothing$ that contradict to the maximality of L_0. Thus $(Rm + L_0) \cap N \neq \varnothing$. In particular there is $l_1 \in L_0, n \in N$ such that $(k_2 x + k_1)m + l_1 = n$.Here $k_1 = 0$ because otherwise $x(k_1 m + l_1 - n) = 0$ means $m \in N \oplus L_0$. We have $xm + l_1 = n$. $Ann(n) = x$ because if $xn \neq 0$ then $xl_1 = xn \neq 0$ contradict to $L_0 \cap N = \varnothing$. Thus we can find $n \in N$ such that $xn \neq 0$ and $l \in L_0$ such that $xm = xn + l$ so that $x(m-n) \in L_0$.
Claim: $(R(m-n) + L_0) \cap N = \varnothing$
Again since $n \notin N \oplus L_0$, there is no $k_1 \in k$ $k_1(m-n) + l = n'$ for some $n' \in N$. So if intersect it must be a form of $k_2 x(m-n) + l = n'$. But since $k_2 x(m-n) \in L_0$ and L_0 doesn't intersect with N we have an empty intersection with $(R(m-n) + L_0)$ and N. Due to the maximality of N we have $R(m-n) \subset L_0$ but it contradict to the fact $m \notin L_0 \oplus N$.

Fall 2021 Question 3 Show that there are no simple groups of order $24p$, where p is a prime number greater than 11.

Solution First of all, for $p > 23$ there would be a unique sylow p group, so it would be impossible. All prime $p > 11$ and $p \neq 23$ the matter is same.So matter is when $p = 23$. In this case, we can have $n_{23} = 1, 24$ and prove $n_{23} = 24$ is impossible. Assume $n_{23} = 24$. In this case, $[G : N_G(P_{23})] = 24$ for a Sylow 23 subgroup P_{23} of G. So $P_{23} = N_G(P_{23})$ by the order counting. There are $23 \cdot 24 - 22 \cdot 24 = 24$ elements whose order is not 24. Let X be the set of elements whose order is not 23. Consider the orbit stabilizer on this set by the conjugate action by the P_{23}. This action is well defined because action by the conjugation preserve the order.Then $|X| \equiv |X^{P_{23}}| (mod 23)$. That is $|X^{P_{23}}|$ is either 1 or 24.

In case of 1, $X^{P_{23}} = \{e\}$. Means that only fixed element by the conjugation is 1, and by the orbit stablizer the orbit of $X - e$ is single orbit. But it will contradic to the Cauchy's theorem where it claim there is an element of order 2 or 3 and order is invariant under the conjugation map. That means action by the conjugation fixes everything. But then for element $x \in X$, $px = xp$ for all $p \in P_{23}$ this means $x \in C_G(P_{23})$ the centeralizer of P_{23}. That contradict for the fact we can take some $x \notin P_{23}$ such that $x \in N_G(P_{23})$.
Alternatively We can simplify this steps by computing the number of Sylow 23 group which is 24, then consider the sylow 3 group, that can have $n_3 = 4, 46$ and here $n_3 = 4$ is impossible because if so G permute Sylow 4 subgroup by the conjugation action, and that yeilds nontrivial

homomorphism $\phi : G \to S_4$ and that has a kernel as $4! = 48$ and $|G| = 24 * 23$. If $n_3 = 46$ the order of the group is much bigger.

Fall 2021 Question 5 Consider a sequence of sets S_i for $i \geqslant 0$ and maps $\phi_i : S_i \to S_{i-1}$ for $i \geqslant 1$. Suppose that there exists a positive integer N such that the orders of the images of the maps ϕ_i are bounded above by N. Show that $\varprojlim S_i$ is finite.

Solution

Let's define $T_i = \cap_{m=0}^{\infty} Im(\phi_i \circ \dots \phi_{i+m})$. By the given hypothesis, we have $|T_{i-1}| \leqslant |T_i| \leqslant N$, and $\phi_i(T_i) = T_{i-1}$. Let's denote $S = \varprojlim S_i$ and $T = \varprojlim T_i$ We will now show $S = T$. Let's $\pi_i : S \to S_i$ and $\pi_i' : T \to T_i$ be a projection for the each component. Since $T_i \subset S_i$, and the image of π_i will factor through T_i so there is a set of morphisms q_i, $q_i : S \to T_i$ such that $\pi_i = p_i \circ q_i$ that lift to the surjective morphism $S \to T$ on to the image. Conversely we have $\pi_i' : T \to T_i$ we have $p_i : T_i \to S_i$ is injective. There is a morphism $p : S \to T$ by the universal property of the limit
Claim: p is injective.
Limit is the right adjoint of the diagonal functor, so it is enough to prove that any right adjoint functor preserve monomorphism. $f : X \to Y$ is a monomorphism if for every Z the hom-functor $Hom(Z, -)$ takes it to an injective function between hom-sets $f^* : Hom(Z, X) \to Hom(Z, Y)$. Since $\varprojlim$ is a right adjoint functor, $Hom(\Delta Z, -) \cong Hom(Z, \varprojlim -)$. $f : Hom(\Delta Z, X) \to Hom(\Delta Z, Y)$ is injective. So $\varprojlim(f) : Hom(Z, \varprojlim X) \to Hom(Z, \varprojlim Y)$ is also a injective. Thus limit preserve a monomorphism(injective).
For the surjectivity, in the category of the set, limit can be written as the

$$S = \{(s_i)_{i \in \mathbf{N}} | \phi_i(s_i) = s_{i-1}\}$$

so all elements of S is inside of the T, thus this is also surjection. For proving the finiteness, we can observe that almost all of T_i are isomorphism (means that cardinalities of T_i are the same). That is because the cardinalities of T_i are bounded by N. So we can identify isomorphic pair of T_i's. Under this identification,we can rename T_i'. T_i' are finite distinct sets, think $\{T_i'\}_i$ as the finite sequences with cardinalities at most N. T is subset of $\prod T_i$ so this is a finite set.

Alternatively Let T_i be given and for large n

Fall 2021 Question 7 Define commutative $\mathbb{Q}$-algebras $A = \mathbb{Q}, B = \mathbb{Q}[x]$, and $C = \mathbb{Q}[x]/(x(x-1))$. Let $A \to C$ and $B \to C$ be the unique $\mathbb{Q}$-algebra homomorphisms such that x in B maps to x in C. Describe the pullback (also called "fiber product") $R = A \times_C B$ in the category of commutative $\mathbb{Q}$-algebras, as the quotient by an explicit ideal of the polynomial ring over $\mathbb{Q}$ on some set of generators. Is R noetherian?

Solution $R = \{(a, b) \in \mathbb{Q} \times \mathbb{Q}[x] | (a, b), a \equiv bmodx(x-1)\} \leftrightarrow \{f \in \mathbb{Q}[x] | f(0) = f(1) = a\}$. Find out the generators by surjection

$$\mathbb{Q}[x_{i,j}]/\{(x_{i,j}x_{k,l} - x_{i+k,j+l}), (x_{i,j} - x_{i+1,j-1} - x_{i,j-1})\} \to R$$

by mapping $x_{i,j} \to x^i(x-i)^j$. We can easily see this is a surjective morphism and and well defined morphism because $\{(x_{i,j}x_{k,l} - x_{i+k,j+l}), (x_{i,j} - x_{i+1,j-1} - x_{i,j-1})\}$ maps to 0 in R by chasing relations. We want to show that there is no kernels hence isomorphism. Observe any term of degree higher than 1, can reduce the degree by the first relation, so without loss of generalities, we can put $\sum\sum q_{ij}x_{ij}$. Furthermore, using the second relations, we can reduces indecies of j. So we can assume $j = 1$. Mapping $\sum q_j x_{j1}$ into R make relation $(x-1)(\sum q_j x^j) = 0 \to q_j = 0$ thus there is no kernel.
We haven't figured out why this is a Noetherian.

Fall 2021 Question 8 Let A be a commutative ring and T an $A-$module. Define a functor from $A-$ modules to $A-$modules by $F(M) = M \otimes_A T$. What is the right adjoint functor of F? Show that if F has a left adjoint, then T must be a flat A-module, and also a finitely generated A-module.

Solution: By the Hom-tensor adjunction Hom is the right adjoint of the tensor product $Hom(M \otimes T, N) \cong Hom(M, Hom(T, N))$ If F has a left adjoint then it is also left exact. As tensor products are already right exact, this implies $- \otimes_A T$ is an exact functor, thus T has to be a flat module. As being right adjoint It must preserve a limit. Consider the natural map

$$T \otimes_A \prod_{i\in I} A \to \prod T \otimes_A A \cong \prod_{i\in I} T$$

For any index set I. Setting $I = T$, the right hand side has a natural elements $\prod_{t\in T} t$ which lists every elements T and by hypothesis this map is an isomorphism so there must be elements $\sum_{j=1}^n t_j \otimes (\prod_{i\in T} a_{ij})$ mapping to it. This element expresses every elements $t \in T$ as a linear combination of a finite collection of elements t_j, because

$$\sum_{j=1}^n t_j \otimes (\prod_{i\in T} a_{ij}) \mapsto \prod_{i\in T}\sum_{j=1}^n a_{ij}t_j = \prod_{t\in T} t.$$

It follows that T is finitely generated.

Appendix: Proof of the functor admit left adjoint is left exact Prove F preserve zero object and equalizer. For proving preserve zero object Z let G be their left adjoint $\eta : Hom(G(A), Z) \cong Hom(A, F(Z))$ is a bijective, thus there is only a unique morphism from $Hom(A, F(Z))$. Preserve equalizer for the morphsim ϕ_1, ϕ_2. Let f be a equalizer and there is a morphism τ such that $G\phi_1 \circ \tau = G\phi_2 \circ \tau$. By the naturality of η^{-1}, $\phi_1 \circ \eta^{-1}\tau = \phi_2 \circ \eta^{-1}\tau$, so there is τ_0 such that $f \circ \tau_0 = \eta^{-1}\tau$ and we have $Gf \circ \eta\tau_0 = \tau$.

Fall 2021 Qustion 9 The outer automorphism group of a group H is the quotient of the group of automorphisms of H by the subgroup of inner automorphisms. It is known that the outer automorphism group of every finite simple group is solvable. Using that, show that if G is a finite group

with a normal subgroup N such that both N and G/N are nonabelian simple groups, then G is isomorphic to the product group $N \times (G/N)$.
Solution Note that left splite of the exact sequence implies group will be decomposed into the product of the group, but right splite of the group may implies group will splite as a semidirect product.

https://web.math.ucsb.edu/ atrisal/Group

We have the exact sequence $1 \to N \to G \to G/N \to 1$. We will claim this is left split. Since N is a subgroup, there is a injection $i : N \to G$.We have the morphism $f : G \to Aut(N)$ by the conjugation action. The inner automorphism $\phi : N \to Inn(N)$ is injective as N is simple so there is nonontrivial kernel so image is either identity or itself, and it is not identity because N is nonabelian. Thus we can define the map $G/N \to Aut(N)/Inn(N) = Out(N)$. By the hypothesis $Out(N)$ is solvable and G/N is simple. Note that the kernel of the map would be a normal subgroup, and image must be $\{e\}$ or G/N. Note the image of this map is trivial because if the kernel was $\{e\}$, then G/N would be isomorphic to a subgroup of a solvable group, and so G/N solvable. But nonabelian solvable group has to have a nontrivial normal subgroup such that quotient by that is abelian. But since G/N is simple such an normal subgroup doesn't exist. Which means $f(G) = Inn(N)$ by the conjugation. Fix isomorphism $k : f(G) \cong N$ we have an isomorphism $(k \circ f) \circ f = Id$. Left split of the group gives direct product, so we showed what we want.

8 Spring 2021

Spring 2021 Problem 1 Prove that the direct sum $\coprod \mathbb{Z}/p\mathbb{Z}$ over all prime integers p is not a direct summand of the product $\prod \mathbb{Z}/p\mathbb{Z}$.

Solution Suppose it is the direct summand. Notice $\prod \mathbb{Z}/p\mathbb{Z}$ is an abelian group. This means that all subgroup is normal. We can write $\prod \mathbb{Z}/p\mathbb{Z} = \coprod \mathbb{Z}/p\mathbb{Z} \oplus K$. Taking the quotient by the $\coprod \mathbb{Z}/p\mathbb{Z}$, we would figure out the module $K \cong \prod \mathbb{Z}/p\mathbb{Z}/\coprod \mathbb{Z}/p\mathbb{Z}$. We will prove K is not a subgroup. Suppose this is a subgroup, then notice, every elements of K is divisible. Pick $(b_i) \in \prod \mathbb{Z}/p\mathbb{Z}$. For every n, we can pick $(a_i) \in \coprod \mathbb{Z}/p\mathbb{Z}$ as the element such that 0 everywhere for the prime nondivide p and 0 for prime dividing n, we put $(-b_p)$. So as the representative of K we can take $(b_i - a_i)$. This is divisible by n. However, any elements of $\prod \mathbb{Z}/p\mathbb{Z}$ is divisible by p because fix (b_i), if for all p there is elements (c_i) such that $(b_i) = p(c_i)$ then each entry of p part is 0. So it is impossible.

Spring 2021 Problem3 Prove that every group generated by two involutions (elements of order 2) is solvable.
solution Let group G is generated by x and y order 2.Consider $\langle xy \rangle$. Note that $(xy)^{-1} = yx$. Therefore, $x(xy)x^{-1} = yx, yxyy^{-1} = yx$ that implies this is a normal subgroup. Let put that as N Since $[x, y] = xyxy \in \langle xy \rangle$ so quotient is abelian. Also is generated by xN and yN. On the other hand, if $x \in N$ then there exists $n \in \mathbb{Z}$ such that $x = (xy)^n$, and since x has order 2 we may assume $n > 0$. Pick n, so $(yx)^{n-1}y = 1$. And $(yx)^{n-1}$, so $y(xy)^{n-2}x = y$. Therefore,$(xy)^{n-2} = x$. Contradicting the minimality, so n must be $1, 2$. If $n = 1$, then $y = (yx)^0 = 1$, which contradicts the assumption that y has order 2.. Therefore, $n = 2$. But then $yx = y$, so $x = 1$, again a contradiction. Thus $x \notin N$. Symmetrically, $y \notin N$. Thus, G/N is abelian, nontrivial, generated by two elements of order 2. But since $xN = yN$ is cyclic of order 2. So show what we want.
Spring 2021 Problem 5 Let G be a finite group and let $g \in G$. Suppose for every irreducible complex character χ of G we have $|\chi(g)| = |\chi(1)|$. Prove that g is in the center of G.(Here I naturally interpret field has characteristic 0)

Solution Let $\rho_i(g)$ be a irreducible representation of G. Let $g \in G$ be $|\chi_{\rho_i}(g)| = |\chi_{\rho_i}(1)|$ for all irreducible representation ρ_i. $\rho(g)$ has a finite order $\rho^n = I$ for some $n \in \mathbb{Z}$. In particular this implies that minimal polynomial is separable polynomial. So the matrix is diagonalizable. Also eigenvalues are root of unity because it is finite order. For the irreducible representation $\chi(1)$ is a dimension of the vector space. Let ξ_i be a distinct eigenvalues, then $|\sum \xi_i| \leqslant \sum |\xi_i| = dimV$ by triangle inequalities. Equality hold only if they are colinear. That is all ξ_i are same. In that case $\rho_i(g)$ is diagonal matrix.
For that reason $\rho_i(gh) = \rho_i(hg)$ for any element h in G. Let the regular representation be ρ_R. ρ_R can be decomposed into a direct sum of irreducible representations $\rho_R = \sum a_i\rho_i$. $\rho_R(g)$ still commute with

all elements $h \in G$. Regular representation is faithful so in particular $\rho(gh) = \rho(hg)$ implies $gh = hg$. Thus $g \in Z(G)$.

Solution 2: Pick element $g \in G$ such that $|\chi_i(g)| = |\chi_i(1)|$ for all irreducible character χ. Using the column orthogonality, we have $|C_G(g)| = \sum_{\chi_i} |\chi_i(g)| = \sum |\chi_i(1)| = |G|$ means g commute all the element of G so it is in the center.

Spring 2021 Problem 7 Let p be a prime number, k a field of characteristic p and G be a (finite) p-group. Let M be a finitely generated kG-module that admits a k-basis B such that $G \cdot B \subset B \cup -B$ (i.e. $\forall g \in G, \forall b \in B$, we have $g \cdot b = \pm b'$ for $b' \in B$). Show that M admits a $k-$basis B' invariant under G (i.e. $G \cdot B' \subset B'$ without sign).

Solution: When $p = 2$ then the statement is trivially true(because $1 = -1$) so assume p is a odd prime. Consider a cycle of the group action by g to the basis. Then for any orbit of the action doesn't map b to $-b$. Because otherwise, the group will be even order, which contradicts the hypothesis of being p group. Thus B will be separated into the nonintersecting union of the orbits $B \cup -B = \cup_{b \in B} Gb \cup \cup_{b \in B} -Gb$. In that case, $\cup Gb$ generate the entire vector space.

Spring 2021 Problem 9 Let R be a commutative ring and A, B be two (not necessarily commutative) R-algebras. Consider the functor $\mathrm{Hom}_{R-Alg}(A \otimes_R B, -) : R - Alg \to Sets$, from R-algebras to sets. Construct two homomorphisms $f : A \to A \otimes_R B$ and $g : B \to A \otimes_R B$ and show that they induce an injection

$$\eta_C : \mathrm{Hom}_{R-Alg}(A \otimes_R B, C) \to \mathrm{Hom}_{R-Alg}(A, C) \times \mathrm{Hom}_{R-Alg}(B, C)$$

natural in $C \in R - Alg$. Identify the image of η_C explicitly.

Solution: Define $f(a) = a \otimes 1$ and $g(b) = 1 \otimes b$. This induces a map $h \mapsto (h \circ f, h \circ g)$. Suppose $(h \circ f, h \circ g) = (0, 0)$. Then, $h(a \otimes 1) = h(1 \otimes b) = 0$. Then, $h(a \otimes b) = h((a \otimes 1)(1 \otimes b)) = h(a \otimes 1)h(1 \otimes b) = 0$. As every tensor is a sum of multiples of simple tensors, this implies $h = 0$, thus η_C is injective.

Suppose $f_1 : A \to C$ and $f_2 : B \to C$ are given. In order to define $h : A \otimes_R B \to C$ such that $\eta_C(h) = (f_1, f_2)$, we require $h(a \otimes 1) = f_1(a)$ and $h(1 \otimes b) = f_2(b)$. However, note that as $(a \otimes 1)(1 \otimes b) = a \otimes b = (1 \otimes b)(a \otimes 1)$, in order for h to be well-defined, we also need $f_1(a)f_2(b) = f_2(b)f_1(a)$. So this is a necessary condition.

We then see this is sufficient as if we can define h on all simple tensors $a \otimes b$, then we can define h for any tensor in $A \otimes_R B$. Thus,

$$\text{im } \eta_C = \{(f_1, f_2) \in \mathrm{Hom}_{R-Alg}(A, C) \times \mathrm{Hom}_{R-Alg}(B, C) \mid f_1(a)f_2(b) = f_2(b)f_1(a) \text{ for all } , a \in A, b \in B\}.$$

Spring 2021 Problem 10 Let A be a ring. Let $m, n \geqslant 1$ and P be a right A-module such that $P^n \cong A^m$. Show that $S \to P \otimes_A S$ defines a

bijection between the set of isomorphism classes of simple A-modules and that of simple $End_A(P)$-modules.

Solutions

Let S be a simple right A modules, then prove $P \otimes S$ is simple left $End_A(P)$ module. Prove the categorical equivalence between left $End_A(P)$ module and right R-module. To do that functor $P \otimes_A -$ has quasi-inverse, $Hom(P, A) \otimes -$. We will denote $Q = Hom_R(P, A)$. Which means given any module left R module M, we need to show $Q \otimes_{End(A)} \otimes P \otimes_A M \cong M$. To do that we can show $Q \otimes P \cong A$.

Let define $tr(P) = \sum g_i P$ with $g \in Hom_R(P, A)$. We will claim $tr(P) = A$. This is true because $P^n \cong A^{m-1} \oplus A$ and this give a spliting exact sequence is a surjective morphisms $\sum g_i : P^n \to A$.

Define the pair of $f \in End_A(P), p \in P, \alpha f \otimes p = f(p)$ this morphism define a surjection. To show injecitivity, any element of $Q \otimes P$ can be written as $\sum q_i \otimes p_i$. Suppose this maps to 0, then $0 = \alpha(\sum q_i' \otimes p_i') = \sum q_i'(p_i')$. Since we showed the surjection, we have $\sum q_i(p_i) = 1$, then $\sum q_j' \otimes p_j' = \sum \sum (q_i(p_i)) q_j' \otimes p_j' = \sum q_i() \cdot p_i \circ q_j \otimes p_j$. Using left $End_R(P)$ strcture, we have $\sum q_i \otimes p_i \cdot q_j() p_j = \sum q_i \otimes p_i(0) = 0$. This shows one direction of Morita equivalence(Actually you need to show the other direction, but it is not appropriate problem in qual...

9 Fall 2020

Fall 2020 Problem 6 Let $K_1 \subset K_2 \subset K_3$ be fields with K_3/K_2 and K_2/K_1 both Galois. Let L be a minimal Galois extension of K_1 containing K_3. Show that if the Galois groups $\mathrm{Gal}(K_3/K_2)$ and $\mathrm{Gal}(K_2/K_1)$ are both p-groups, then so is the Galois group $\mathrm{Gal}(L/K_1)$.

Solution
Define $N_3 = \mathrm{Gal}(L/K_3)$, $N_2 = \mathrm{Gal}(L/K_2)$, and $N_1 = \mathrm{Gal}(L/K_1)$. By the Galois correspondence, we have a chain or normal subgroups $N_3 \lhd N_2 \lhd N_1$. (Although we don't know whether $N_3 \lhd N_1$. In fact, if N_3 is normal then it must be trivial by the following claim.)

Claim: If $H \subset N_3$ is a subgroup of N_3 which is normal in N_1, then $H = \{e\}$.

Suppose $H \subset N_3$ is normal in N_1. Then there is a fixed field $K_3 \subset L^H \subset L$, and because $H \lhd N_1$ is normal we know H is a normal extension of K_1. And since L is separable, the subfield L^H is also separable. Therefore, L^H is a Galois extension of K_1 containing K_3, so by construction $L^H = L$ and $H = \{e\}$.

Claim: There is an injective homomorphisms $\varphi : N_1 \hookrightarrow S_{N_1/N_3}$. In particular, for any $g \in N_1$, the order of g is the least common multiple of all cycles in the cycle decomposition of $\varphi(g)$.

This comes because N_1 acts on N_1/N_3. (Note that N_1/N_3 is not a group, but just a set of cosets.) This group action defines a homomorphisms $N_1 \hookrightarrow S_{N_1/N_3}$, and the kernel is contained in N_3, because kernel mean $g \in Ker \leftrightarrow hN_3 = ghN_3$ for all $h \in G$ i.e $h^{-1}gh \in N_3$, in particular $h = e$ gives $g \in N_3$. Since kernel is normal subgroup, and $h^{-1}gh$ is contained in N_3 for all h, we see $ker \subset N_3$. It is trivial by the previous claim. The second claim follows because an injective homomorphism preserves order.

Now for a given $g \in N_1$, we argue that the length of every cycle in the cycle decomposition of $\varphi(g)$ is a power of p. Since the cycle decomposition of $\varphi(g)$ partitions N_1/N_3, choose a coset hN_3 for some $h \in N_1$. g acts on hN_3 by mapping to

$$hN_3 \xrightarrow{g} ghN_3 \xrightarrow{g} g^2hN_3 \xrightarrow{g} \ldots \xrightarrow{g} g^khN_3 = hN_3$$

and eventually this cycle must end, so there is some k such that $g^khN_3 = hN_3$. This is the length of the cycle containing hN_3 in the cycle decomposition of $\varphi(g)$, and we show that k is a power of p.

Claim: k is the minimal positive integer such that $g^k \in hN_3h^{-1}$.

This just comes from rearranging $g^khN_3 = hN_3$ to $h^{-1}g^khN_3 = N_3$, so $h^{-1}g^kh \in N_3$, and $g^k \in hN_3h^{-1}$.

Also, note that because N_2 is a normal subgroup of N_1, we have hN_3h^{-1} a normal subgroup of N_2, and $N_2/N_3 \cong N_2/hN_3h^{-1}$ by conjugating by h. We will write $N_3' = hN_3h^{-1}$.

Now let n be the order of gN_2 in N_1/N_2, and let m be the order of g^nN_3' in N_2/N_3'. Because $N_1/N_2 = \mathrm{Gal}(K_2/K_1)$ and $N_2/N_3' \cong N_2/N_3 = \mathrm{Gal}(K_3/K_2)$ are p-groups, both n and m are powers of p.

Claim: $k = nm$.

First, we see that $g^{nm} \in N_3'$, because $(g^nN_3')^m = g^{nm}N_3' = N_3'$ in N_2/N_3' by the definition of m.

Now suppose the $g^d \in N_3'$. Because $N_3' \subset N_2$, this means $g^dN_2 = N_2$, and so n divides d by the definition of n. So we can write $d = n\frac{d}{n}$.

But this means that $g^dN_3' = (g^nN_3')^{\frac{d}{n}} = N_3'$, so m divides $\frac{d}{n}$ by the definition of m. So we see $nm \mid d$.

This exactly proves that k is the smallest positive integer such that $g^k \in N_3'$, and so we conclude that the length of the cycle that contains hN_3 in the cycle decomposition of $\varphi(g)$ is a power of p. Because this is true for all g and all $h \in N_1$, we see that N_1 is a p-group, as desired. $\square$

Alternatively(May be this is better and theoretically motivated)
Up to the point showing there is no normal subgroup H that is not contained in N_3 are same. We will show that using that fact, G is solvable group.
Consider the commutator sequeuence $N_1^1 := [N_1, N_1], N_1^i := [N_1^{i-1}, N_1^{i-1}]$, first of all N_1/N_2 is a solvable group as being $p$group are solvable. Thus for sufficiently large i we have $N_1^i/N_2 = \{e\}$ means $N_1^i \leqslant N_2$. Moreover N_2/N_3 is solvable by same argument, so there is j such that $N_1^{i+j} \leqslant N_2^j \leqslant N_3$. But since there is no normal subgroup of N_3 is normal, but N_1^{i+j} is a characteristic subgroup, so N_1^{i+j} is normal subgroup of $N_1 \to N_1^{i+j} = \{e\}$. In particular N_1 is solvable group.
Then by Spring 2019 Problem 1, the minimal normal subgroup of finite solvable group is a product of $\mathbb{Z}/q\mathbb{Z}$ and there exist a normal subgroup of

N_1 such that contains N_3, for example N_2 is an example of normal subgroup. Let N be a minimal normal subgroup contains N_3. $|N_2/N_3| = p^n$ for some n as this is a p group. $[N_2 : N_3] = [N_2 : N][N : N_3]$ where $[N : N_3]$ can only have a product of some prime q as $q^k = [N : e] = [N : N_3][N_3 : e]$ and $N \neq N_3$ this means $p = q$.

Fall 2020 Problem 7 Let R be a Dedekind domain with quotient field K and I a nonzero ideal in R. Show both of the following.

(a) R/I is a principal ideal ring

(b) If J is a fractional ideal of R, then there exist x such that $I + xJ = R$.

Solution a) We claim that if R is a Dedekind domain and $\mathfrak{p} \subset R$ is a prime ideal, then the ideals of $R/\mathfrak{p}^n$ take the form $\overline{\mathfrak{p}^k}, 0 \leqslant k \leqslant n$ and are in fact principal. Indeed, by the ideal correspondence theorem, any ideal of $R/\mathfrak{p}^n$ corresponds to an ideal J of R that contains $\mathfrak{p}^n$. But since R is Dedekind, the prime factorization for J must divide the prime factorization for $\mathfrak{p}^n$, i.e. $J = \mathfrak{p}^k$ for $0 \leqslant k \leqslant n$.
First we show $A/\mathfrak{p}^n$ is Principal ideal ring. Note since $A/\mathfrak{p}^n$ has unique maximal ideal $\overline{p}$, so this is a local ring. Pick $a \in \mathfrak{p} \backslash \mathfrak{p}^2$, this is possible if not $\mathfrak{p} = p^2$. The ideal of Dedekind ring is finitely generated, so by Nakayama's lemma $\mathfrak{p} = 0$, contradiction. So we can take a. Then $\overline{a}$ is proper ideal of $A/\mathfrak{p}^n$ that is nonzero. Also it is not contained in $\overline{\mathfrak{p}^2}$. This shows $A/\mathfrak{p}^n$ is principal ideal ring generated by $(a)^k$ for $1 \geqslant k \geqslant n-1$.
Moreover, by the Chinese Remainder Theorem, if $I = {\mathfrak{p}_1}^{n_1} ... {\mathfrak{p}_t}^{n_k} \subset R$, then

$$R/I \cong R/{\mathfrak{p}_1}^{n_1} ... \times R/\mathfrak{p}_t{}_k^n.$$

Thus, any ideal of R/I takes the form $\overline{(a_1)^{n_1}} ... \times \overline{(a_k)^{n_k}}$, where $a_i \in \mathfrak{p}_i \backslash \mathfrak{p}_i^2$. This shows that every ideal of R/I is generated by a single element, i.e. R/I is a principal ideal ring.

b)Without loss of generalities, we can treat J as an ideal of R by multiplying $x' = dx$. Let $a \in J$ so we can find ideal $\mathfrak{c}$ such that $\mathfrak{c}J = aR$.(This is allowed for example Merkuriev's note define a Dedekind ring as such we can find $\mathfrak{c}$.) Moreover $R/\mathfrak{c}I$ is a principal ideal ring so $\mathfrak{c}/\mathfrak{c}I = (\overline{b})$. Thus $\mathfrak{c} = \mathfrak{c}I + bR$. Multiplying J for bothside we have

$$J\mathfrak{c} = \mathfrak{c}JI + bJR$$

$$aR = aI + bJ$$

divide by a we get

$$R = I + \frac{b}{a}J$$

Comment: This is similar to the technique to prove that (fractional)ideal of Dedekind domain is generated by at most two element. Proof is following, given an ideal I and element $a \in I$, the ring O/a is principal ideal ring, so the ideal I/a is generated by at most one element.

Fall 2020 Problem9 Let G be a finite group, F a field, and V a finite dimensional F-vector space with $G \to GL(V)$ a faithful irreducible representation. Show that the center $Z(G)$ of G is cyclic.

Solution When F is algebraically closed, then due to the Schur's lemma, $Z(G)$ map to a scaler multiplication, and the group is finite so image of $Z(G)$ will be a root of unity of $F^\times$. For every integer m there are at most m distinct elements of order m because they are roots of $x^m - 1$ and because $F[x]$ is UFD.

We will prove the subgroup generated by root of unity of the $F^\times$ is cyclic. Note $F^\times$ is abelian, so we can apply the structure theorem of finitely generated abelian group so that it can be written as the $\prod \mathbb{Z}/p_i^{k_i}$ for primes and the subgroup generated by $m-$th roots of unity be $\mu_m = \prod \mathbb{Z}/p_i^{k_i}$. It is enough to prove these primes are distinct so that group will be cyclic. Let $q_1 \dots q_n$ be distinct primes appear on p_i's and l_i be a largest exponents among same primes, then any elements $g \in \mu_m$, $g^{\prod q_i^{l_i}} = 1$ and this is the smallest number that makes possible, so $\prod q_i^{l_i} = m$. However, the $|\mu| \geqslant m$ and since there are at most $m-$th root of unities to be exist, so all primes are the same. In particular, if ρ is faithful, $Z(G)$ is embedded as a cyclic subgroup.

If the non-closed case, still by the Schur's lemma, we can embed $Z(G)$ to the a division algebra $End_F(F[G])$ contains F.
We will prove following claim, finite abelian subgroup of multplicative group of the division algebra is cyclic. Let D be a division ring with the center Z. Let A be a finite abelian subgroup of $D^\times$ and put $k = \sum_{g \in A} Zg$. Center of division ring is field, so k is Z algebra as well as A is a commutative domain and $A \subset k$. k is a finite dimensional vector space over Z and thus every element of H is algebraic over Z. Let $0 \neq c \in k$ and suppose that $q(x) = x^m + \ldots + a_1 x + a_0 \in Z[x]$ is the minimal polynomial of c over Z. Then $a_0 \neq 0$ and so $c(c^{m-1} + \ldots + a_1)(-a_0^{-1}) = 1$. This means every element c has multiplicative inverse, therefore F is a field. As we show the case of field, every finite abelian subgroup of multiplicative group of field is cyclic. In particular $A \subset F^\times$.

Fall 2020: Problem 10 Let C, D be categories, where C admits coequalizers. Let $F : C \to D$ be a functor that preserves coequalizers. F also satisfies if h an arrow such that $F(h)$ is an isomorphism, then h is an isomorphism. Show F is faithful.

Solution Suppose F is not faithful. Then there exists $f \neq g : X \to Y$ such that $F(f) = F(g) : F(X) \to F(Y)$.

Recall that the coequalizer of two arrows is the object resulting from taking Y and identifying $\{f(x) \sim g(x), \forall x \in X\}$. Let $\pi : Y \to coeq(f, g)$ be the projection onto the coequalizer. Since $f \neq g$, $coeq(f, g)$ must be strictly smaller than Y. So, π is not an isomorphism.

Since F preserves coequalizers, $F(\pi) : F(Y) \to coeq(F(f), F(g))$. And,

since $F(f) = F(g)$, the coequalizer is exactly $F(Y)$. Thus $F(\pi)$ is an isomorphism. This is a contradiction, as π is not an isomorphism.

So, F is faithful.

10 Spring 2020

Spring 2020: Problem 2 Let G be a finite group of order $n > 1$ and consider its group algebra $\mathbb{Z}[G]$ embedded in $\mathbb{Q}[G]$. Let $A = \mathbb{Z}[G]/\mathfrak{a}$ for the ideal a generated by $g - 1$ for all $g \in G$.
(a) Prove that the algebra $\mathbb{Q}[G]$ is the product of $\mathbb{Q}$ and $\mathbb{Q} \cdot \mathfrak{a}$, where $\mathbb{Q} \cdot \mathfrak{a}$ is the $\mathbb{Q}-$span of a in $\mathbb{Q}[G]$.
(b) Let B be the projected image of $\mathbb{Z}[G]$ in $\mathbb{Q}\cdot\mathfrak{a}$. Prove that $A\otimes_{\mathbb{Z}[G]}B \cong G$ as groups if and only if G is a cyclic group.

Solution

(a)We need to cook up isomorphism as a ring, so for the (central) idempotent $e_1 = \frac{1}{|G|}\sum_{g\in G} g$ and $e_2 := 1 - e_1$ define a projection to the subring $\mathfrak{Q}[G]$ to $\mathbb{Q}$ and $\mathbb{Q} \cdot \mathfrak{a}$. We can easily check e_1 is idempotent. We have $gx = x$ so the image of $e_1\mathbb{Q}[G] \cong \mathbb{Q}x. \cong \mathbb{Q}$.
On the other hand, $g(1 - e) = g - e$. Since $g - e$ and as $aug(g - e) = 0$, $g - e \in \mathbb{Q}\mathfrak{a}$. On the other hand $(g - 1)e_2 = g - 1$, so e_2 is central idempotent. We have a decomposition as a ring of $\mathbb{Q}[G] \cong \mathbb{Q} \times \mathbb{Q}\mathfrak{a}$.
(b) There is an natural isomorphism of the ring defined by $\mathbb{Z}[G]/\supset \otimes_{\mathbb{Z}[G]} B \cong B/\mathfrak{a}$ by by sending $[a]\otimes b \to [ab]$. Furthermore, we have $\mathbb{Z}[G] \to B \to B/\mathfrak{a}$ where the first surjection is the multiplication map by e_2. Let π be the composition of these surjective ring homomorphisms, $\pi : \mathbb{Z}[G] \to B/\mathfrak{a}$, defined on elements by $\pi(l) = [e\cdot l]$. Since $\mathbb{Z}[G]$ is generated as a $\mathbb{Z}$ module by g for $g \in G$, let us consider the image of g for $g \in \mathbb{Z}[G]$. We have:

$$\pi(g) = [g - e] = [1 - e]$$

Therefore, $\pi(g) = \pi(h)$ for all $g, h \in G$, and since π is surjective, $B/\mathfrak{a}_{\mathbb{Z}}$ is cyclic as an abelian group and is thus isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some n. Furthermore, $\pi(|G|) = [\sum 1 - g_i] = 0$, so n divides $|G|$. We have that n is exactly equal to $|G|$, since $[e], [2e], \ldots, [|G|e]$ are all distinct modulo $\mathfrak{a}_{\mathbb{Z}}$ as the difference are element of group ring with rational coefficient. Therefore, $A \otimes_{\mathbb{Z}[G]} B \cong \mathbb{Z}/|G|\mathbb{Z}$ as a group and is thus congruent to G if and only if G is cyclic.

Spring 2020: Problem 4 Compute the dimension of the tensor products of two algebras $\mathbb{Q}[\sqrt{2}]\otimes\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}]\otimes_{\mathbb{Z}}\mathbb{R}$ over $\mathbb{R}$. Is $\mathbb{R}\otimes_{\mathbb{Z}}\mathbb{R}$ finite dimensional over $\mathbb{R}$?

solution

Spring 2020: Problem 7 Let G be a $p-$group and N be a non-trivial normal subgroup.
(a) Show that N contains a non-trivial element of the center $Z(G)$ of G.
(b) Give an example where $Z(N) \nsubseteq Z(G)$.
solution (a) Consider the G conjugate action of N. Then the fixed point of N^G is the intersection of $Z(G)$ and N, as they commute with the all the element of G. $e \in N^G$ and see if there is nontrivial element. By the

orbit stabilizer for the action of p group, $|N| \equiv |N^G|(modp)$ but since $|N| \equiv 0(modp)$ so $|N^G| \geqslant p > 1$.

(b) For given p, we can construct examples, when p^2 it is abelian so p^3 is the minimum examples of such a group exist. Consider $(C_p \times C_p) \ltimes C_p$ or $(C_{p^2}) \ltimes C_p$ both works. Where $\ltimes$ are nontrivial semi direct product. Nontrivial semidirect product exist, because $Aut(C_p \times C_p) = (p^2-1)(p^2-p)$ and $Aut(C_{p^2}) = p^2-p$ so both are multiplication of p and the nontrivial multiplication exist. This product is noncommutative and in particular as being nontrivial homomorphism $C_p \ni r \to \phi \in Aut(C_p \times C_p)$ there is an $a \in C_p \times C_p$ (or similarly on C_{p^2} cases) $\phi(a) = b \neq a$. So multiplication of $(a, r^k)(0, r) = (b, r^{k+1})$ but $(0, r)(a, r^k) = (a, r^{k+1})$. So $(0, r) \notin Z(G)$. But $(0, r) \in Z(N)$ as being C_p cyclic.

Spring 2020: Problem 8 Let R be a ring.
(a) Show that an $R-$module X is indecomposable if $End_R(X)$ is local. (Recall that a ring is local if the sum of non-invertible elements remains non-invertible).
(b) Suppose that every finitely generated R-module M is isomorphic to $X_1 \oplus \cdots \oplus X_m$ with all $End_R(X_i)$ local. Show that such a decomposition is unique: If $X_1 \oplus \cdots \oplus X_m \cong Y_1 \oplus \cdots \oplus Y_n$ then $m = n$ and there is a bijection $\sigma \in S_n$ and isomorphisms $X_i \cong Y_{\sigma(i)}$.
(c) Give an example of an isomorphism $X_1 \oplus X_2 \cong Y_1 \oplus Y_2$ with $End(X_i)$ and $End(Y_i)$ local that is not the direct sum of any isomorphisms $X_i \cong Y_i$, even up to renumbering the Y_i.

Solution
(a) Prove if R-module X is decomposable then $End_R(X)$ is not local. Suppose $X = X_1 \oplus X_2$ for proper submodule X_i. Then consider the projection $\pi_i : X \to X_i$, so they are not invertible. However, $\pi_1 + \pi_2$ is invertible, as being identity. This means $End_R(X)$ is not local.
(b) Consider mapping from $Hom(\oplus X_i, \oplus Y_j) = \oplus_{ij} Hom(X_i, Y_j)$. So the isomorphism from $\oplus X_i \cong \oplus Y_j$ can be written in the form of matrices. $A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1,n} \\ \alpha_{21} & \dots & \alpha_{2,n} \\ \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{nm} \end{pmatrix}$ and $B = \begin{pmatrix} \beta_{11} & \dots & \beta_{1,m} \\ \beta_{21} & \dots & \beta_{2,m} \\ \dots & \dots & \dots \\ \beta_{n1} & \dots & \beta_{mn} \end{pmatrix}$ Since each i $BA = I$ so for each i we have $1 = \sum \beta_{ji}\alpha ij$. This is an invertible endomorphism from X_i to X_i, By the (a) and assumption one of the element has to be invertible, Let denote that $\beta_{ji}\alpha_{ij}$ is invertible then it means there is an exact sequence $0 \to ker\beta_{ji} \to Y_j \to X_i \to 0$ which is splite. By hypothesis we can assume to take Y_i is indecomposable so α_{ij} induces isomorphism of $X_i \cong Y_j$. Let permute the modules and without loss of generalities put X_1 maps Y_1.
Prove by induction, since α_{ij} has inverse,we can define a automorphism

$A' = \begin{pmatrix} 1 & 0 & \dots & 0 \\ -\alpha_{21} \circ \alpha_{11}^{-1} & 1 & \dots & 0 \\ \dots & \dots & \dots & 0 \\ -\alpha_{n1} \circ \alpha_{11}^{-1} & 0 & \dots & 1 \end{pmatrix}$ So we have $A'A$ has as a first row, mapping identitcally on X_1 to Y_1. We have module decomposition of $X_2 \oplus \cdots \oplus X_n \cong Y_2 \oplus \cdots \oplus Y_m$. This gives by induction, isomorphism of the modules.
(c) Think about the decomposition of the vector space as $X = e_1 \oplus e_2$ and same decomposition as Y. Then the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ gives isomorphism between X but it doesn't give componentwise isomorphism.

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

Solution Sketch:

We define the following natural transformation

$$\begin{aligned} \alpha_{M,N} : S^{-1}Hom_r(M,N) &\to Hom_{S^{-1}R}(S^{-1}M, S^{-1}N) \\ \frac{f}{s'} &\mapsto \left(\frac{m}{s} \mapsto \frac{f(m)}{s's} \right) \end{aligned}$$

If M is finitely presented, then there exists $m, n \in \mathbb{N}$ such that

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

is an exact sequence. The contravariant Hom functor is a right adjoint and thus preserves left exact sequences. Also, localization is exact, so we get the following exact sequence

$$0 \to S^{-1}Hom(M,N) \to S^{-1}Hom(R^n, N) \to S^{-1}Hom(R^m, N)$$

Since α is a natural transformation, it preserves exact sequences, and applying it we get

$$0 \to Hom(S^{-1}M, S^{-1}N) \to Hom(S^{-1}R^n, S^{-1}N) \to Hom(S^{-1}R^m, S^{-1}N)$$

By the five lemma, it suffices to show α is an isomorphism for the last two terms. Thus we have been reduced to the case of $M = R^m$.

α is injective, as $\frac{f(r)}{ss} 0 \iff f(r) = 0$ for all $r \in R^m$. Then, $f = 0$ and in particular $\frac{f}{s} = 0$.

For surjectivity, let $g : S^{-1}R^m \to S^{-1}N$ and let $e_1, \dots, e_m$ be the standard basis for R^m. Then $g(e_i) = \frac{n_i}{s_i}$ for each $i \in [m]$. Let $s = s_1 \cdots s_m$ and

define

$$\begin{aligned} f : R^n &\to N \\ e_i &\mapsto n_i s_1 \cdots \hat{s_i} \cdots s_m \end{aligned}$$

Then, $\frac{f}{s}$ maps via α to g. So, this is an isomorphism.

Fall 2019 Problem 4 Find all isomorphism classes of simple (i.e., irreducible) left modules over the ring $M_n(\mathbb{Z})$ of n-by-n matrices with $\mathbb{Z}-$entries with $n \geqslant 1$.

Solution Appeal to the Morita equivalence:According to the Morita equivalence, there is a bijection between simple $\mathbb{Z}$-module and simple $M_n\mathbb{Z}$ module by the tensor product $\mathbb{Z}^n \otimes -$. Simple module over $\mathbb{Z}$ is of the form $\mathbb{Z}/p\mathbb{Z}$, as any simple module can be represented by $\mathbb{Z}x$ as there is no submodule, equivalently $\mathbb{Z}x \cong \mathbb{Z}/Annx$, and by existence of the maximal ideal $\mathfrak{m}$ contain ideal $Annx$ so if $Annx$ is not maximal, there is a submodule in $\mathbb{Z}/Annx$ by $\mathfrak{m}/Annx$. Thus all simple submodule is $\mathbb{Z}^n \otimes \mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^n$.

Fall 2019: Problem 5 Let $R \neq 0$ be a commutative ring. Let $t_B : R - Mod \to R - Mod$ be the functor that sends $t_B(M) = M \otimes B$.

(a) Show that t_B commutes with colimits

(b) Construct an R-module B for every R such that t_B doesn't commute with limits in $R - Mod$.

Solution

(a) $Hom(B, \_\_)$ is right adjoint to t_B, with a natural isomorphism $Hom(M \otimes B, N) \cong Hom(M, Hom(B, N))$.

So, t_B is a left adjoint, and thus commutes with colimits.

(b) (This solution secretely assume R is not a field, indeed when R is a field this is most difficult because any R module will be a flat so tensor is preserved)Since $R \neq 0$, let $a \in R$ be a nonzero element. Then, $B = R/aR$. Consider the map

$$\begin{aligned} f : R &\to R \\ r &\mapsto ar \end{aligned}$$

Consider the fiber product of two instances of $f : R \to R$. Since $a \neq 0$, $f \neq 0$, so the fiber product is not direct product $\neq R \times R$. On the other hand, if we apply t_B we get

$$\begin{aligned} t_B(f) : R \otimes R/aR &\to R \otimes R/aR \\ b \otimes c &\mapsto a(b \otimes c) = b \otimes ac \equiv 0 \end{aligned}$$

Since $t_B(f)$ is the trivial map, the fiber product after applying t_B becomes

$$t_B(R) \times_f t_B(R) = \{(a_1, a_2) | a_i \in R \otimes B, f(a_1) = f(a_2)\} = R \otimes R/aR \times R \otimes R/aR = (R \times R) \otimes R/aR$$

So, t_B does not commute with the fiber product.

(seems like assuming $R = Z$) Alternative examples: Direct product and direct sum is same concept in the finite cases, so if we want to construct the examples of noncommuting with direct product and tensor product, we have to do with infinite.
Show infinite direct products $(\prod \mathbb{Z}/p^n\mathbb{Z}) \otimes \mathbb{Q} \ncong \prod(\mathbb{Z}/p^n\mathbb{Z} \otimes \mathbb{Q})$. Because right hand side is 0. Left hand side, there is a nontorsion element, for example, $(1, 1, \dots)$. Suppose this is torsion there is n such that $n(1, 1, 1, \dots) = 0$. But since n is finite, it doesn't kill all entries. Thus this is not a torsion. (otherway of saying, this is element of order infinite). This means as a equivalent classes $(1, 1 \dots) \otimes 1 \neq 0$ so as a module this doesn't commute with infinite direct product.

(genuine alternative example): Pick B as non-finitely generated A module, then if it commute with direct product then it preserve $\prod A^I \otimes B \cong B^I$ for any indices I. In particular we have an isomorphism $\phi : A^{|B|} \otimes B \cong B^B$ Considering the identity map $id : B \to B$ as an element of the product B^B by putting same index as an same element. Pick an $Id \in Hom(B, B) = B^B$ then there is an element $\sum f_i \otimes m_i \in A^{|B|} \otimes B = Hom(A, B) \otimes B$. Thus $Id = \phi(\sum m_i \otimes f_i) = \sum f_i m_i$ for some finite collection of elements $m_i \in B$ and $f_i : B \to A$. Evaluating both sides of this equation at an element $m \in M$ we find $m = \sum m_i f_i(m)$. This implies B is finitely generated by m_i as A-module, contradict with the fact B is not finitely generated as A module.

Fall 2019 Problem 6 Classify all finite subgroups of $GL(2, \mathbb{R})$ up to conjugacy.
Solution Let G be a finite subgroup of $GL(2, \mathbb{R})$,take $g \in G$ so that $g^n = I$. Take the determinant, so $\det g^n = 1 \leftrightarrow (\det g)^n = 1$. Since g is a matrix of real component, $detg = \pm 1$. So we have two cases, either $G \subset SO(2)$ or $G \subset O(2)$. The case of $SO(2)$, consider the finite subgroup of $G \subset SO(2)$. This is cyclic group C_n. The simplest way is claim any finite subgroup of mulitplicative group of the field is cyclic. More directly, G is generated by some finite elements $\{e^{2\pi i\theta_j}\}$ In particular θ are rational number as being finite order. Indeed we can reduce generators, for example let $\theta_j = \frac{p_j}{q_j}, i\theta_k = \frac{p_k}{q_k}$ be two different generators where p_j, q_k and p_k, q_k are relatively prime, then by Bezout theorem we can find some m, n such that $\frac{m(p_k q_j) + n(p_j q_k)}{q_j q_k} = \frac{gcd(p_k q_j, p_j q_k)}{q_j q_k}$. Obviously $\frac{gcd(p_k q_j, p_j q_k)}{q_j q_k}$ generate both of elements, θ_j, θ_k cyclically. So all finite subgroup of $S0(2)$ is C_n.
Since $SO(2)$ is a kernel of the determinant map from $O(2)$, so there is an isomorphism $O(2) \cong SO(2) \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ so that same as semi direct product of dihedral group.

Fall 2019 Problem 8 Let M be a finitely generated module over an integral domain R. Show that there is a nonzero element $u \in R$ such that

the localization $M[1/u]$ is a free module over $R[1/u]$.
Solutions Let $K = Frac(R)$ so that $M \otimes K$ is a finite dimensional vector space. Thus we can choose the bases for the vector space $M \otimes K$ as $m_1 \otimes 1 \dots m_n \otimes 1$. Due to the finitely generatedness we have the map $\phi : R^n \to M$ by $\phi(e_i) = m_i$.

$$0 \to ker\phi \to R^n \to M \to coker\phi \to 0$$

Since the fractionalization is exact, $\otimes K$ is an exact functor, so

$$0 \to ker\phi \otimes K \to K^n \to M \otimes K \to coker\phi \otimes K \to 0$$

is still exact. Since by the choice of m_i, middle is an isomorphism. This implies $Ker\phi \otimes K$ and $coker\phi \otimes K$ is 0 so that $Ker\phi$ and $coker\phi$ are torsion modules. Here since $Ker\phi$ is a submodule of the free module, so torsion free and $ker\phi = 0$. On the other hand, $coker\phi$ is also finitely generated module because they are quotient of finitely generated module. Let the generators be $\{\overline{n_1} \dots \overline{n_k}\}$ and since they are torsion, there exist $f_i \in R/\{0\}$ such that $f_i n_i = 0$. Let $u = \prod f_i$ then localization at f will garunteed to vanish $coker\phi$, as each f are units so $n_i = \frac{f}{f} u = 0$ then these image is always vanishing. Thus $M[1/u]$ is free $R[1/u]$ module.

Fall 2019 Problem 9 Let A be a unique factorization domain which is a $\mathbb{Q}$-algebra. Let K be the fraction field of A. Let L be a quadratic extension field of K. Show that the integral closure of A in L is a finitely generated free A-module.

Solution: Let B be a integral closure of A in L. Since A is Q-algebra, K is characteristic 0. Then by the quadratic formula(alternatively, since $-1 \in K$ we can use Hilbert theorem 90) we can find a square free element $b \in K$ such that $L = K(\sqrt{b})$. Furthermore since A is UFD, b can be uniquely represented as a fraction $\frac{p}{q}$, we can multilply appropriate elements so that we can claim $b \in A$. We claim $B \cong A \oplus A\sqrt{b}$.
Consider the A-module map $A \oplus A\sqrt{b} \to B$ sending $(x, y\sqrt{b})$ to $x + y\sqrt{b}$. This map really lands in B, since if $x, y \in A$ then the trace $-2x$ and norm $x^2 - by^2$ which both lie in A, so that the minimal polynomial of this has coefficients in A that is

$$t^2 - 2xt + x^2 - by^2 = 0$$

The map is clearly injective if not $(x + y\sqrt{b}) = x_1 + y_1\sqrt{b}$ for $x_1 \neq x$ and $y_1 \neq y$. But $\sqrt{b}$ and 1 is linearly independent so this map is injective.
To show an isomorphism of module, we will show the morphism is surjective. Let $x + y\sqrt{b} \in B$ for $x, y \in K$. Then we will show $\alpha = x + y\sqrt{b}$ is a solution of a monic polynomial of coefficient A then in fact $x, y \in A$. We will prove the minimal polynomial over field K will be same things as irreducible polynomial over A. Let m_α be a minimal monic polynomial

over K and k_α be a monic polynomial of minimal degree which has a root as α. We have $m_\alpha | k_\alpha$ We can multiply appropriate number d so that we can make $dm_\alpha \in A[x]$ and their contents 1. dm_α is irreducible as $K[x]$ so irreducible as $A[x]$.By the Gauss lemma state A is a UFD K is a fraction field,. Then a non-constant polynomial m_α is irreducible if and only if it is irreducible in $A[x]$ and contents 1. Thus $k_\alpha | dm_\alpha$. So they have same degree. By the choice of m we chose m_α is monic so indeed $k_\alpha = m_\alpha$.
If the minimal polynomial polynomial of α has degree 1 then since A is integrally closed in K then $x + y\sqrt{b} \in A$. If the The minimal polynomial of $x + y\sqrt{b}$ is $f(t) = t^2 - 2xt + (x^2 - by^2)$. Since $x + y\sqrt{b}$ is integral over A there is a irreducible polynomial m such that $x + \sqrt{b}y$ is a root of m. its trace and norm lie in A. The trace is $-2x$, which of course lands in A whenever $x = \frac{a}{2}$ for some $a \in A$.A is a $\mathbb{Q}$-algebra, so if $a \in A$ then $\frac{a}{2} \in A$ also, and we conclude $x \in A$. To show $y \in A$, we look at the norm $x^2 - by^2$, which must lie in A as well. Since we already know $x \in A$, we get that $by^2 \in A$. Then $y^2 = \frac{c}{b}$ for $c \in A$. But b is squarefree, so by looking at irreducible factorizations we see that b has to divide a, so since $y \in K$ but there is no denominator $y \in A$ that $A \oplus A\sqrt{b} \to B$ is surjective, hence an isomorphism.

□

Fall 2019 Problem 10 Compute the Galois groups of the Galois closures of the following field extensions:
a. $\mathbb{C}(x)/\mathbb{C}(x^4 + 1)$,
b. $\mathbb{C}(x)/\mathbb{C}(x^4 + x^2 + 1)$, where $\mathbb{C}(y)$ denotes the field of rational functions over $\mathbb{C}$ in a variable y.

Solution: a. Compute the minimal polynomial respect to the x. That is $t^4 + 1 - (x^4 + 1) = t^4 - x^4$. That is clearly irreducible over $\mathbb{C}(x^4 + 1)$. $\mathbb{C}(x)$ has all roots of $t^4 - x^4$, i.e $\pm x, \pm ix$. This means $\mathbb{C}(x)$ is a split field of $t^4 - x^4$ thus normal. $\mathbb{C}(x^4 + 1)$ is characteristic 0, so perfect and any extension separable. Sum both we have a Galois extension.The Galois group is generate to permute among roots that is $\sigma : x \to ix$ and σ^i transitively maps between roots of $\mathbb{C}$. σ generate Galois group so $Gal(\mathbb{C}(x)/\mathbb{C}(x^4 + 1)) = \mathbb{Z}/4\mathbb{Z}$
b. Compute the minmal polynomial, that is $t^4 + t^2 + 1 - (x^4 + x^2 + 1) = t^4 - x^4 + t^2 - x^2 = (t-x)(t+x)(t-i\sqrt{x^2+1})(t+i\sqrt{x^2+1})$. $\sqrt{x^2+1} \notin \mathbb{C}(x)$ because if so

$$\sqrt{x^2 + 1} = ax + b$$

$$x^2 + 1 = a^2x^2 + 2abx + b^2$$

$a = \pm 1, b = \pm 1$ both case $2ab \neq 0$.(or we can see that $x^2+1 = (x-i)(x+i)$ and since UFD, we can see this is square free) Thus the normal closure over $\mathbb{C}(x)$ is $\mathbb{C}(x, \sqrt{x^2+1})$. $\mathbb{C}(x, \sqrt{x^2+1})/\mathbb{C}(x)$ is a degree 2 extension with the minimal polynomial $t^2 - x^2 + 1$. Then $\mathbb{C}(x, \sqrt{x^2+1})/\mathbb{C}(x^4 + x^2 + 1)$ is

a degree 8 extension. So here there are few ways to see what is the Galois group of this extension.
1st way: Since $\mathbb{C}(x)/\mathbb{C}(x^4+x^2+1)$ is not Galois so the corresponding Galois group is nonabelian. The nonabelian group of order 8 is either D_4 or quaternion group. But in particular since there is non Galois intermidiate extension, there is a nonnormal subgroup and all subgroup of quaternion group is normal. By the classification of the group of order 8 with a nonnormal subgroup is D_8
OK I am not sure this is actually working. (2nd way: There is a Galois action on $\mathbb{C}(x,\sqrt{x^2+1})/\mathbb{C}(x)$ such that

$$\sigma : \sqrt{x^2+1} \to -\sqrt{x^2+1}$$

$$\sigma : x \to x$$

Extend this action to $\mathbb{C}(\sqrt{x^2+1},x)/\mathbb{C}(x^4+x^2+1)$. Since Galois group permute roots of minimal polynomial, we can map of order 4

$$\tau : x \to i\sqrt{x^2+1}$$

under this map $\tau : -x \to -i\sqrt{x^2+1}$ and

$$\tau(i\sqrt{x^2+1})^2 = -\tau(x^2+1) = -(\tau(x)^2) - 1 = x^2$$

so $\tau(i\sqrt{x^2+1}) = \pm x$. If $\tau(i\sqrt{x^2+1}) = x$. Then there is also a automorphism $\rho(x) = -x$ and $\kappa(x) = -i\sqrt{x^2+1}$
, $\tau(i\sqrt{x^2+1}) = -x$.
$\sigma \neq \tau^2$, and check if $\sigma\tau\sigma = \tau^3$

$$\sigma\tau\sigma(x) = -x = \tau^3(x)$$

$$\sigma\tau\sigma(\sqrt{x^2+1}) = \sigma\tau(-\sqrt{x^2+1}) = \sigma(x) = x$$

and

$$\tau^3(\sqrt{x+1}) = \tau^2(-x) = \tau(-i\sqrt{x^2+1}) = x$$

This is a relation of dihedral group, so D_4) □

Spring 2019 Problem 1 Let G be a finite solvable group and $1 \neq N \subset G$ be a minimal normal subgroup. Prove that there exists a prime p such that N is either cyclic of order p or a direct product of cyclic groups of order p

Solution First see N is an abelian group: The commutator group $[N, N]$ is a characteristic subgroup of N, let $\phi \in Aut(N)$ then $aba^{-1}b^{-1} \in N, \phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} \in [N, N]$. The characteristic subgroup of a normal subgroup is normal, as there is an embedding into $\psi : G \to Aut(N)$ by the conjugation, and by the conjugation, characteristic subgroup are preserved. So $[N, N]$ is normal in G. Since N is the minimal normal subgroup $[N, N]$ is either N or $\{e\}$. If $\{e\}$ then N is abelian and showed what we want. If $[N, N] = N$, then as subgroup of solvable group is solvable, there is a proper normal subgroup N_1 in N such that N/N_1 is normal, but by the universality of the abelian quotient $N = [N, N] \leqslant N_1$ shows $N/N_1 = \{e\}$, contradiction for the properness of N_1.
Let p be the prime order dividing N, then by Cauchy's theorem, there is an element $x \in N$ such that $x^p = e$. Let N' be a subgroup of N such that $\{x \in N | x^p = e\}$. Note N' is a subgroup because N is abelian group. Then N' is a characteristic subgroup, because for $\phi \in Aut(N), x \in N'$, $\phi(x)$ has order 1 or p. This means N' is a nontrivial normal subgroup of G that contained in N. By the minimality of N, $N = N'$. By the structure theorem of the abelian finite abelian group this is cyclic of order p or direct product of cyclic groups of order p.

Spring 2019 Problem 2 An additive group (abelian group written additively) Q is called divisible if any equation $nx = y$ with $0 \neq n \in \mathbb{Z}, y \in Q$ has a solution $x \in Q$. Let Q be a divisible group and A is a subgroup of an abelian group B. Give a complete proof of the following: every group homomorphism $f : A \to Q$ can be extended to a group homomorphism $B \to Q$.

Solution We use Zorn's Lemma. Consider the partially ordered set P of all pairs (C, g) where C is a subgroup of B containing A and $g : C \to G$ is an extension of f. Let $(C, g) \leqslant (D, h)$ if $C \leqslant D$ and $g = h|C$. The set P is nonempty since it contains (A, f). Also any tower (C_α, g_α) in P has an upper bound $(\cup C_\alpha, \cup g_\alpha) \in P$. By Zorn's Lemma, P has a maximal element, say (C, g). We claim that $C = B$ and g is the desired extension of f to B. Suppose $C < B$. Then there exists an $x \in B$ so that $x \notin C$. Either $x + C$ has finite order in B/C or it has infinite order.
In the second case, $<C, x> = C \oplus \langle x \rangle$ so $g : C \to G$ can be extended to $g \oplus 0 : C \oplus \langle x \rangle \to G$ contradicting the maximality of (C, g).
In the first case, let n be the order of $x + C$ in B/C, i.e., $n > 0$ is smallest positive integer so that $nx \in C$. Since G is divisible there is a $z \in G$ so that $nz = g(nx)$. We can linearly extend $g : C \to G$ by homomorphism $g + h : C + \langle x \rangle \to G$ where $h : \langle x \rangle \to G$ is given by $h(x) = z$(This + sign means not addition but nondisjoint sum as a set). This contradicts the maximality of (C, g). They can extend to a morphism.

Spring 2019 Problem 7 Let F be a field and let R be the ring of 3×3 matrices over F with $(3,1)$ and $(3,2)$ entry equal to 0. Thus $\begin{pmatrix} F & F & F \\ F & F & F \\ 0 & 0 & F \end{pmatrix}$

(a) Determine the Jacobson radical J of R.
(b) Is J a minimal left (respectively, right) ideal?

Solution (a) First way(?): The element of R preserve $span\{e_1, e_2\}$. If the first 2×2 block matrix of $x \in J(R)$ 2×2 block of matrix is not zero matrix, then either $Ae_1, Ae_2 \neq 0$. Without loss of generalities, $Ae_1 \neq 0$ then we can find the matrix $B \in R$ such that $BAe_1 = e_1$. So $1 - BA$ is not invertible matrix as there is a kernel.
Also $(3,3)$ component a_{33} has to be 0 as well, because if not we can find the matrix with whose $(3,3)$ component is $\frac{1}{a_{33}}$ so mapping e_3 to e_3. So has to be $\begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix}$
(b) J is the minimal left ideal but not minimal right ideal. Pick $x = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ Claim: $J = Rx$. Pick any element in $\begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} \in J$.
Then $\begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{13} & 0 & 0 \\ 0 & a_{23} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$
So J is generated by $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ on the other hand, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{13}^{-1} & 0 & 0 \\ 0 & a_{23}^{-1} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix}$
so J is minimal ideal.

thus minimal. On the other hand this is not minimal right ideal, as $\begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ is a proper right ideal contained in J i.e
$\begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} = \begin{pmatrix} 0 & 0 & a_{13}a_{33} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Spring 2019 Problem 8 Prove that every finite group of order n is isomorphic to a subgroup of $GL_{n-1}(\mathbb{C})$.
Solution Let G be a group of order n, then this group can be embedded into S_n. Then S_n can be embedded into $GL_n(\mathbb{C})$ by the regular representation. Regular representation can be decomposed into the $n-1$ dimensional tautological representations and trivial representation. Then restrict representations to the tautological subspace, we define a representations of S_n to $GL_{n-1}(\mathbb{C})$. Show this representation is a faithful representation i.e define an embedding. Suppose there is an element mapped into identity in $res : x \in GL_n(\mathbb{C}) \to GL_{n-1}(\mathbb{C}), I = res(x) \in GL_{n-1}(\mathbb{C})$.

Then the restriction of x to the one dimensional complement is also mapped to identity, as one dimensional complement is a trivial representation. As $x \in GL_n(\mathbb{C})$ it is a identity matrix. Thus all the map from $G \to S_n \to GL_n(\mathbb{C}) \to GL_{n-1}(\mathbb{C})$ are embedding so by composing it G is embedded into the $GL_{n-1}(\mathbb{C})$

Spring 2019 Problem 9 a) Find a domain R and two nonzero elements $a, b \in R$ such that R is equal to the intersection of the localizations $R[1/a]$ and $R[1/b]$ (in the quotient field of R) and $aR + bR \neq R$.
b) Let C be the category of commutative rings. Prove that the functor $C \to Sets$ taking a commutative ring R to the set of all pairs $(a, b) \in R^2$ such that $aR + bR = R$ is not representable
Solutions (a) Lemma: We pick $R = \mathbb{Z}[x, y], a = x, b = y$ then $\mathbb{Z}[x, y, y^{-1}] \cap \mathbb{Z}[x, x^{-1}, y] = \mathbb{Z}[x, y]$. But $x\mathbb{Z}[x, y] + y\mathbb{Z}[x, y] \neq \mathbb{Z}[x, y]$. The second statement is obvious: we can take $1 \in \mathbb{Z}[x, y]$ but not in $x\mathbb{Z}[x, y] + y\mathbb{Z}[x, y]$.For the first statement, we have $k[x, y] \subset k[x, y, x^{-1}] \cap k[x, y, y^{-1}]$. Conversely, pick anything $p \in k[x, y, x^{-1}] \cap k[x, y, y^{-1}]$, then we can wrote $p = \frac{f}{x^n} = \frac{g}{y^m}$. That means $fy^m = gx^n$ so y divides g, so $\frac{g}{y^m} = p \in k[x, y]$.
(b) Observe, the statement (a), then consider the fiber product

$$\begin{array}{ccc} k[x,y] & \longrightarrow & k[x,y,y^{-1}] \\ \downarrow & & \downarrow \\ k[x,y,x^{-1}] & \longrightarrow & k(x,y) \end{array}$$

Now prove by the contradiction, suppose F is representable. Then representable functor preserves limit and moreover F preserve inclusions so in particular the following diagram is also a fiber product,

$$\begin{array}{ccc} F(k[x,y]) & \longrightarrow & F(k[x,y,y^{-1}]) \\ \downarrow & & \downarrow \\ F(k[x,y,x^{-1}]) & \longrightarrow & F(k(x,y)) \end{array}$$

By assumption, as the fiber product over sets of inclusion map is intersection, we have $F(k[x, y]) = F(k[x, y, x^{-1}]) \cap F(k[x, y, y^{-1}])$. We see from (a) $(x, y) \notin F(k[x, y])$ But we have $(x, y) \in F(x, y, y^{-1}) \cap F(k[x, y, y^{-1}])$ because $xk[x, y, y^{-1}] + yk[x, y, y^{-1}] = k[x, y, y^{-1}]$ and $xk[x, y, x^{-1}] + yk[x, y, x^{-1}] = k[x, y, y^{-1}]$

Spring 2019 Problem 10 Let C be an abelian category. Prove that TFAE:
(1) Every object of C is projective.
(2) Every object of C is injective.

solution Suppose all objects are projective, let there be a monomorphism $\phi : M \to N$ and morphism $i : M \to I$.Construct morphism $\varphi : N \to I$ such that $i = \varphi \circ \phi$. Since all objects are projective, exact sequence splits, so $N = M \oplus coker\phi$ so define $\varphi = \phi|_M$ and 0 for $coker\phi$. Then any morphism lift so I is injective.

Fall 2018 Problem5 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.

Solution: One direction $R - S \supset \cup_{\mathfrak{p} \cap S = \varnothing} \mathfrak{p}$ is true. On the other hand, Let $x \notin S$. We want x to be in the union of prime ideals. We want to find a $\mathfrak{p}$ prime ideal not meeting S such that $x \in \mathfrak{p}$. Now, consider

$$A = \{I | x \in I \text{and} I \cap S = \varnothing\}$$

with the partial order $\subseteq$.
Claim: $(x) \in A$. Proof. We need to check $(x) \cap S = \varnothing$. If 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 $A \neq \varnothing$. We can apply Zorn's lemma to A to find a maximal element. Let $\{I_\alpha\}_{\alpha \in \Lambda}$ be a chain of ideals in A. Thus, by Zorn's lemma, A has a maximal element $\mathfrak{m} \in A$. This $\mathfrak{m}$ is a prime ideal. Let $a, b \notin \mathfrak{m}$ show $ab \notin \mathfrak{m}$. Then, $\mathfrak{m} \subsetneq \mathfrak{m} + (a), \mathfrak{m} + (b)$, so $(\mathfrak{m} + (a)), (\mathfrak{m} + (b)) \cap S \neq \varnothing$. Choose $s \in (\mathfrak{m} + (a)) \cap S$ and $t \in (\mathfrak{m} + (b)) \cap S$. Then, $st \in (\mathfrak{m} + (a))(\mathfrak{m} + (b)) \subset \mathfrak{m} + (ab)$. If $ab \in \mathfrak{m}$, then $st \in \mathfrak{m} + (ab) = \mathfrak{a}$ and $st \in S$. It contradict to the $S \cap \mathfrak{m} = \varnothing$
(b) $\implies$ If R is a UFD and P is a prime containing a nonzero $r = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, then at least one p_i belongs to P. $\impliedby$ Show that if every prime ideal contains principal prime ideal, then UFD. Let $S = R^\times \cup \{p_1 p_2 \dots p_k | p_i \text{ are primes elements }\}$. S is a set of all elements of R that can be uniquely factorlizeable

This is also the satured multiplicative subset generated by primes and units. We want to show that $R - S = (0)$. 0 is prime which doesn't intersect with S, we have $R - S \supset \{0\}$. Suppose $R - S$ contains an $r \neq 0$. Then, by part a), there exists a prime ideal $\mathfrak{p} \subset R - S$ such that $r \in \mathfrak{p}$.But then, $\mathfrak{p}$ contains a principal prime $(p) \subseteq \mathfrak{p}$. The principal prime ideal is generated by a prime element, so $p \in S$, contradicting the fact that $\varnothing \neq (p) \cap S \subseteq \mathfrak{p} \cap S = \varnothing$. Therefore, every non-zero non-unit a R has a factorization into a finite product of prime and, thus, irreducible elements. Since an irreducible element will be a product of prime elements, it must be a product of one prime element. Irreducible elements of R are prime so R is a UFD, as quoting the following theorem. **Theorem** R is a UFD if and only if every irreducible element is prime.

(The idea of last part is the existence of the element r guaranteed the existence of the prime ideal that disjoint with $R - S$. But by hypothesis such a prime ideal associate with the prime element $p \in S$.) $\square$

Fall 2018: Problem 7 Let $F : C \to D$ be a functor with right adjoint $G : D \to C$. Show that F is fully faithful iff the unit $\eta : Id_C \to GF$ is an isomorphism

Solution Suppose $\eta_Y : Y \to GF(Y)$ is an isomorphism for $Y \in C$. Then, as functors preserve isomorphisms,

$$R^X(\eta_Y) : Hom(X, Y) \to Hom(X, GF(Y))$$

gives an isomorphism by precomposition of η_Y. By adjunctness, we have

$$Hom(X, Y) \cong Hom(X, GF(Y)) \cong Hom(F(X), F(Y))$$

for all X, Y. Moreover, if ϕ is the adjunction isomorphism, we know by naturality of the unit that $\phi \circ F(f) = \eta \circ f$. So, the above isomorphism is exactly by the functor F. Thus, F is fully faithful.

Conversely, if F is fully faithful, then we have

$$Hom(X, Y) \cong Hom(F(X), F(Y)) \cong Hom(X, GF(Y))$$

for all $X \in C$. By (contravariant) Yoneda's Lemma, this implies that the map $\eta_Y : Y \to GF(Y)$ inducing this isomorphism is an isomorphism.

Fall 2018 Question 10 Consider the real algebra $A = \mathbb{R}[x, y] = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ where x and y are the classes of X and Y respectively. Let $M = A(1 + x) + Ay$ be the ideal generated by $1 + x$ and y. (This is the M obius band.)
(1) Show that there is an A-linear isomorphism $A^2 \cong M \oplus M$ mapping the canonical basis to $(1 + x, y)$ and $(-y, 1 + x)$.
(2) Show that there is an A-linear isomorphism $A \cong M \otimes_A M$ mapping 1 to $((1 + x) \otimes (1 + x)) + (y \otimes y)$.

(a) Consider the linear transformation $Q = \begin{pmatrix} 1+x & -y \\ y & 1+x \end{pmatrix}$ $Q : A^2 \to M \oplus M$. That map canonical basis of e_1, e_2 to M by $(1, 0) \to (1+x, y) \subset M$ and $(0, 1) \to (-y, 1 + x) \subset M$.
Injectivity: Since $x^2 + y^2 - 1$ is a prime ideal, so A is integral domain. So the quotient field exist, let denote it as F. Let $(a, b) \in KerQ \otimes F$ for $a, b \in F$. Which satisfies

$$a(1 + x) - by = 0$$

$$ay + b(1 + x) = 0$$

Thus $a = \frac{by}{1+x}$ substitute the equation $\frac{by^2}{1+x} + b(1 + x) = 0$ multiple $(1 + x)$ for both side then $by^2 + b(1 + x)^2 = 0$ making equation easier we have $2b(x + 1) = 0$ so $b = 0$ so as $a = 0$ since there is no solution on F, so there is no solution on A as well. Thus injective.
For surjective, we have $Q(1 - x, 0) = (y^2, y(1 - x)), Q(0, y) = (-y^2, y(1 +$

$x)$). so $Q(1-x,0)+Q(0,y)=(0,2y).(0,y)\in Im(Q)$, similarly $Q(0,1-x)+Q(-y,0)=(2y,0)\in Im(Q), Q(1+x,0)+Q(0,-y)=(2+2x,0)\in Im(Q), Q(0,1+x)+Q(y,0)\in(0,2x+2)\in Im(Q)$

Alternatively, we can show by the inverses: It is obvious that Q maps A^2 to $M\oplus M$, conversely construct the inverse matrix $Q^{-1}=\frac{1}{2(1+x)}\begin{pmatrix}1+x & y\\ -y & 1+x\end{pmatrix}$show that $Q^{-1}(M\oplus M)\subset A^2$ the general elements of $M\oplus M$ can be written as $\begin{pmatrix}p_1(x,y)(1+x)+q_1(x,y)y\\ p_2(x,y)(1+x)+q_2(x,y)y\end{pmatrix}$ for $p_i,q_i\in\mathbb{R}[x,y]$. When it acts Q we have $\frac{1}{2(1+x)}\begin{pmatrix}1+x & y\\ -y & 1+x\end{pmatrix}\begin{pmatrix}p_1(x,y)(1+x)+q_1(x,y)y\\ p_2(x,y)(1+x)+q_2(x,y)y\end{pmatrix}$
$=\frac{1}{2(1+x)}\begin{pmatrix}p_1(1+x)^2+q_1(1+x)y+p_2(1+x)y+q_2y^2\\ -p_1(1+x)y-q_1y^2+p_2(1+x)^2+q_2(1+x)y\end{pmatrix}$ since $y^2=1-x^2$ so y^2 is divisible by $(1+x)$ so the image is on A^2. Since Q and Q^{-1} is well defined inverse map each other, they are isomorphism.

(b) Construct the inverse image as the composition of

$$M\otimes M\xrightarrow{\mu}F\xrightarrow{\times\frac{1}{2(1+x)}}F$$

where μ is a multiplication maps $a\otimes b\to ab$. Denote g as the compositions of μ and multiplication map $\frac{1}{2(x+1)}$.
The generators of $M\otimes M$ are $(1+x)\otimes y,(1+x)\otimes(1+x),(y)\otimes(1+x),y\otimes y$. The reason is, M is a projective A module, so the tensor by M preserve inclsuion. First we need to check g is in the image of A. $g((1+x)\otimes y)=\frac{1}{2(1+x)}(y(1+x))=\frac{1}{2}(y)\in A$, same for $y\otimes(1+x)$. $g((1+x)\otimes(1+x))=\frac{1}{2(1+x)}((1+x)(1+x))=\frac{1}{2}(1+x)\in A, g(y\otimes y)=\frac{1}{2(1+x)}y^2=\frac{1}{2}(1-x)$. Let f be the given map,
Show $gf(1)=1$: $g((1+x)\otimes(1+x)+y\otimes y)=\frac{1}{2}(1+x)+\frac{1}{2}(1-x)=1$
Show $fg=Id$ there are 2 cases: $f(\frac{y}{2})=\frac{y}{2}((1+x)\otimes(1+x)+y\otimes y)=\frac{1}{2}((1+x)\otimes y(1+x)+y^2\otimes y)=\frac{1}{2}((1+2x+x^2)\otimes y+(1-x^2)\otimes y)=(1+x)\otimes y$
$f(\frac{1\pm x}{2})=\frac{1}{2}(((1+x)\otimes(1+x))+(y\otimes y))\pm\frac{x}{2}(((1+x)\otimes(1+x))+(y\otimes y))=\frac{1}{2}(((1+2x+x^2)\otimes(1\pm x)+(y^2)\otimes(1\pm x))=\frac{1}{2}(1+2x+x^2+(1-x^2))\otimes(1\pm x)=(1+x)(1\pm x)$ when $+$ it is $(1+x)\otimes(1+x)$ when $-$ it is $(1+x)\otimes(1-x)=(1-x^2)\otimes 1=y^2\otimes 1=y\otimes y$.

Spring 2018: Problem 3 Let $\mathbb{Z}^n, (n > 1)$ be column vectors with integer coefficients. Prove that for every non-zero left ideal I of $M_n(\mathbb{Z}), I\mathbb{Z}^n$ (the subgroup generated by products αv with $\alpha \in I$ and $v \in \mathbb{Z}^n$) has finite index in $\mathbb{Z}^n$.

Solution Let $A \in I$ since A is a nonzero matrix, there is a vector $Av \neq 0$. Then there is a matrix $B_i \in M_n(\mathbb{Q})$ such that $B_i(Av) = e_i$. Since B_i are $n \times n$ matrices, so there is an integer b_i such that $b_i B_i \in M_n(\mathbb{Z})$ and $b_i B_i Av = b_i e_i$. Since I is ideal, $b_i B_i A \in I$, so we saw each $b_i e_i \in I\mathbb{Z}^n$. We have $span\langle b_1 e_i \dots b_n e_n \rangle \subset I\mathbb{Z}^n$. We have finite index $[\mathbb{Z}^n : \langle b_1 e_1 \dots b_n e_n \rangle] = b_1 \dots b_n$ as well as we have a projection(surjection) from $\mathbb{Z}^n/\langle b_1 e_1 \dots b_n e_n \rangle$ to $\mathbb{Z}^n/I\mathbb{Z}^n$ by 3rd isomorphism theorem $(\mathbb{Z}^n/\langle b_1 e_1 \dots b_n e_n \rangle)/(I\mathbb{Z}^n/\langle b_1 e_1 \dots b_n e_n \rangle) \cong \mathbb{Z}^n/I\mathbb{Z}^n$. Thus the index $[\mathbb{Z}^n : I\mathbb{Z}^n]$ is bounded above by $b_1 \dots b_n$

Alert You may also think naively try to pick an element $f \in I$ where $f\mathbb{Z}^n$ is full dimensional sublattics, and compare the index(which is a covolume) by compare the determinant. However, in this case index is $\det f$. However for example ideal generated by $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ may not have a element with nonzero determinant.

Spring 2018: Problem 4 Let p be a prime number, and let D be a central simple division algebra of dimension p^2 over a field k. Pick $\alpha \in D$ not in the center and write K for the subfield of D generated by α. Prove that $D \otimes_k K \cong M_p(K)$.

Solution: Note there is a two fact: $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$ and tensor of simple algebra and central simple algebra is simple(in the note).Since K is a field extension of k, $D \otimes_k K$ is a central simple algebra over K. Moreover, $\dim_K D \otimes_k K = \dim_k D = p^2$. So, it must be of the form

$$D \otimes_k K \cong M_s(D')$$

for some finite dimensional division ring D' over K. Let the dimension of D' over K be n. Then, $\dim_{D'} M_s(D') = s^2$ so $\dim_K M_s(D') = s^2 n = p^2$. Thus, n must be a square i.e $n = m^2$ and $sm = p$. As p is prime, either $s = 1$ or $m = 1$.

If $m = 1$, then $n = 1$ so $D' \cong K$ and we have $D \otimes_k K \cong M_p(K)$, which is what we want.

Otherwise, $s = 1$, and $D \otimes_k K \cong D'$ is a division ring. Note since K is free k module, the tensor product $\otimes_k K$ is exact functor. Thus this preserve inclusion, $K \otimes_k K \subset D \otimes_k K$

We show that this is a contradiction by showing the existence of nonzero zero divisors in $K \otimes_k K \subset D \otimes_k K$.

$$K \otimes_k K \cong \frac{k[x]}{(m_\alpha)} \otimes_k K \cong \frac{K[x]}{(m_\alpha)} \quad \cong \frac{K[x]}{(f_1 \cdots f_\ell)} \cong \frac{K[x]}{(f_1)} \times \cdots \times \frac{K[x]}{(f_\ell)}$$

The second line comes from the fact that m_α is no longer irreducible over K, as $\alpha \in K$. Then, since K is a field, $K[x]$ is a PID and any two irreducibles are coprime. So, by Chinese Remainder Theorem, we can decompose into a product of quotients in the last line. In particular, $\ell \geqslant 2$, so $e_1 e_2 = 0$ are nonzero zero divisors. So, $D \otimes_k K$ cannot be a division ring and $s \neq 1$.

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

Solution: Since B is commutative, I is actually a nilpotent ideal. Let $n \in \mathbb{N}$ be the smallest such that $I^n = 0$. Then consider the filtration

$$\begin{aligned} I &\supset I^2 \supset \cdots \supset I^n \\ I &\cong \frac{I}{I^2} \oplus I^2 \\ &\cong \frac{I}{I^2} \oplus \cdots \oplus \frac{I^{n-1}}{I^n} \end{aligned}$$

So, it suffices to show that $\frac{I^k}{I^{k+1}}$ is finitely generated over A. Then I is finitely generated over A, and $B \cong B/I \oplus I$ is finitely generated over A.

Notice that since B is Noetherian, every ideal is finitely generated. So, I is finitely generated over B. Let $\{x_1, \ldots, x_s\}$ generate I over B. Then, I/I^2 is finitely generated by the same generators over B/I. Similarly, these generators yield finite generators for $\frac{I^k}{I^{k+1}}$ over B/I. So, $\frac{I^k}{I^{k+1}}$ is finitely generated over B/I, which is finitely generated over A. So, $\frac{I^k}{I^{k+1}}$ is finitely generated over A and we are done.

Fall 2017: Question 2 Let G be a finite group of order a power of a prime number p. Let $\Phi(G)$ be the subgroup of G generated by elements of the form g^p for $g \in G$ and $ghg^{-1}h^{-1}$ for $g, h \in G$. Show that $\Phi(G)$ is the intersection of the maximal proper subgroups of G.

Solution Let H_i are all maximal proper subgroup of G.
Show $\Phi(G) \subset \cap_i H_i$. First, show all maximal subgroup H_i are normal. When $|G| = p$ then statement is trivial, so assume $|G| = p^m$ all maximal proper subgroup are normal then prove it for $|G| = p^{m+1}$. Note all the index p subgroup is normal for index p subgroup H_i, $[G : N_G(H_i)][N_G(H_i) : H_i] = p$. Well known fact: subgroup of smallest prime index is normal.

Also apply the well known fact: A normal subgroup of p-group H intersect nontrivially to the center $Z(G)$. This can be seen by the conjugation action to G to H, so

$$|H| = |H^G| + [G : stab(x)]$$

and $H^G = H \cap Z(G)$. By the fixed point theorem for p-group $H^G \neq \{e\}$.

Thus there is an intersection with $Z(G)$. Apply Cauchy's theorem, pick order $p$elements $x \in Z(G) \cap H_i$, $H/x \subset G/\langle x \rangle$ is a maximal subgroup of $G\langle x \rangle$ then by the induction hypothesis $|H/\langle x \rangle| = p^{m-1}$ so $|H| = p^m$. Quotient $G/H_i \cong \mathbb{Z}/p\mathbb{Z}$ means any H_i contains commutator $[G, G]$ as $\mathbb{Z}/p\mathbb{Z}$ being abelian. Any p-th power of G contained in H_i. $\Phi(G) \subset \cap_i H_i$.

On the other hand, prove $\cap_i H_i \subset \Phi(G)$. Suppose $x \notin \Phi(G)$. Note $\Phi(G)$ is a characteristic subgroup as all bijection of the group preserve the form g^p and $ghg^{-1}h^{-1}$. Then $G/\Phi(G) \cong \prod \mathbb{Z}/p\mathbb{Z}$, as $\Phi(G)$ contains all p-th powers. Then as a right hand side isomorphism $x\Phi(G)$ is represented by $(x_1, x_2 \dots x_n)$ and at least one of the coordinate $x_j \neq 0$. Let $C_j = \prod_{i=1, i\neq j}^n \mathbb{Z}/p\mathbb{Z}$ are maximal proper subgroup of $G/\Phi(G)$. So $x\Phi(G)$ is not contained in C_j. Let $\pi : G \to G/\Phi(G)$ be a projection, due to the the subgroup correspondence preimage of the proper maximal subgroup is maximal, so $x \notin \pi^{-1}(C_j)$ this shows $x \notin \Phi(G)$.

Fall 2017 Question 3 Let k be a field and A a finite dimensional $k-$algebra. Denote by $J(A)$ the Jacobson radical of A. Let $t : A \to k$ be a morphism of $k-$vector space such that $t(ab) = t(ba)$ for all $a, b \in A$. Assume $ker(t)$ contains no nonzero left ideal. Let M be the set of elements a in A such that $t(xa) = 0$ for all $x \in J(A)$. Show that M is the largest semi-simple left A-submodule of A.

SolutionSince $ker(t)$ contains no-nozero left ideal of A, it is either $ker(t) = A$ or 0. In case of $ker(t) = A$ then A doesn't have a nontrivial left ideal so A is a simple ring. So A itself is the largest semisimple submodule of A.

A is simple so $J(A) = 0$.

In case $ker(t) = 0$ in this case t is injective morphism of vector space, so this is isomorphism.(As a vector space $A \cong k^n$ so injection has to be $k \to k$). So $M = A$ because $J(A)$.Thus $J(A) = 0$ and A is Artinian

because finite dimensional $k-$algebra. A is semisimple so M is largest semisimple left A module.

(Otherway of showing $J(A)$)Then $M = A$ because otherwise there is an $b \in A$ such that $t(xb) = k_1$ for some $k_1 \in k, k_1 \neq 0$. We have $t(1 - x\frac{b}{k_1}) = 0$ implies $1 - x\frac{b}{k_1}$ is noninvertible.

Fall 2017: Question 5 Let A be a ring and M an $A-$module that is a finite direct sum of simple $A-$module. Let $f \in End_{\mathbb{Z}}(M)$. Assume $f \circ g = g \circ f$ for all $g \in End_A(M)$
(a) Show that the map $f_n : M^n \to M^n$ defined by $f_n(m_1 \dots m_n) = (f(m_1) \dots f(m_n))$ commutes with all elemets of $End_A(M^n)$.
(b) Deduce that given any family $(m_1 \dots m_n) \in M^n$ there exists $a \in A$ such that $f_n(m_1 \dots m_n) = a(m_1 \dots m_n)$.

Solution (a)Since $g \in End_A(M^n) = Hom(\oplus_i M, \oplus_j M) = \oplus_j Hom(M^n, M)$ so any morphism from j-th entry $g_j \in Hom(M^n, M) \cong Hom(M, M)^n$ so $g(m_1 \dots m_n) = \sum_i g_{ij}(m_i)$ for each $g_{ij} \in Hom(M, M) = End_A(M)$ so can be identify as the $n \times n$ matrix with the A coefficient. In particular fix each entry i we have n different ways to map to the M of codomain. Thus once I apply the matrix we get

$$\begin{aligned}
g(f_n(m_1, \dots, m_n)) &= (g_1(\sum_{i=1}^n f(m_i)), \dots, g_n(\sum_{i=1}^n f(m_i))) \\
&= \left(\sum_{i=1} g_{i1}(f(m_i)), \dots, \sum_{i=1}^n g_{in}(f(m_i)) \right) \\
&= \left(\sum_{i=1} f(g_{i1}(m_i)), \dots, \sum_{i=1}^n f(g_{in}(m_i)) \right) \\
&= f_n \left(\sum_{i=1} g_{i1}(m_i), \dots, \sum_{i=1}^n g_{in}(m_i) \right) \\
&= f_n(g(m_1, \dots, m_n)).
\end{aligned}$$

Therefore, f commutes with all elements of $\mathrm{End}_A(M^n)$. so it commute.
(b) Let denote $m = (m_1 \dots m_n)$. M^n is semi-simple, and Am is a submodule. Since any semisimple module is projective, we can find a complement B to make a direct sum $Am \oplus B \cong M$. Let π_m be a projection, to the $M^n \to M^n$ where $(a, b) \mapsto (a, 0)$. Note that π_m is identity on Am. Then $f_n(m) = f_n(\pi_m m) = \pi f_n(m) \in Am$.

Fall 2017 Question 8 Let F be a field and $f, g \in F[x]$ be a nonconstant relatively prime elements with $d = max\{f, g\}$. Prove the degree of extension $[F(x) : F(\frac{f}{g})] = d$.

solution It is clear that minimal polynomial has degree $\leqslant d$ as $p(x) = \frac{f}{g}g(T) - f(T)$ Lemma: Suppose we have $\sum P(x)_i f^i g^{d-i} = 0$ and $deg(P(x)) < d$ then $P_i(x) = 0$.

Proof: Without loss of generalities, $deg(g) = d$. Then $\sum^{i=1\ N} P_i f^{d-i} g^i$ can be divisible by g. So P_N cannot be divisible by g by degree. Hence by induction, we have the statement.

Given a minimal polynomial of x over $F(\frac{f}{g}) = \sum \frac{P_i(\frac{f}{g})}{Q_i(\frac{f}{g})} x_i$. Kill off denominators so we can write with $\sum \tilde{P_i}(\frac{f}{g}) x^i$. Moreover we can kill off the denominator g so that we will have $\sum\sum (a_{ijk} x^k) f^i g^{d-i}$. Note the degree of x is at most $d-1$ so it satisfies hypothesis of lemma so all coefficient $a_{ijk} = 0$ and so polynomial itself is also 0 minimal polynomial has to have degree d.

Spring 2017: Question 2 Let G be a group with representations $G := \{x, y | x^4 = y^5 = e, xyx^{-1} = y^2\}$ with order 2. Compute the character table.

solution Compute the number of 1-dimensional representation by seeing commutator group. $\langle y \rangle$ is an normal subgroup. The quotient of G by $\langle y \rangle$ is group of order 4 thus abelian. Since group of order 5 is cyclic, so $\langle y^5 \rangle$ has to be the commutator subgroup.

One conjugacy class is $\langle y, y^2, y^3, y^4 \rangle$.Also notice by the conjugation by x, the number of x factor will not change, i.e $y^{-1}xy = y^2 x$. Moreover $y^{-1}y^2xy = yxy = y^3x, y^{-1}y^3xy = y^2xy = y^4x$ etcetc we figure out all conjugacy classes so that using orthogonalities, we will see the character table.

Spring 2017: Question 3 Find the number of subgroups on index 3 in the free group $F_2 = \langle u, v \rangle$ on two generators

Solution I just copypast a personal dialogue with Harahm Park Thanks for sharing the solutions!

i think maybe one way to make the argument more precise is to say that conjugacy classes of index 3 subgroups of a group G are in bijective correspondence with transitive actions of G on a 3 point set, up to isomorphism as G-sets

if H ≤ G is index 3 then as 3 is prime, either N_G(H) = H or N_G(H) = G, accordingly either H has 3 conjugates or 1 conjugate in G

if H is normal, then the corresponding G-set is isomorphic to the *group* G/H with the natural left G-action. Conversely if H ≤ G is so that the coresponding G-set X admits a group structure so that g –> g*e_X is a group homomorphism, then H is normal

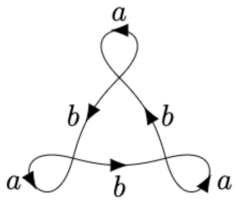
in total there are 7 isomorphism classes of transitive actions of F_2 on a 3 element set, and of these 4 correspond to normal subgroups of F_2, coming from the 4 surjective homomorphisms F_2 –> C_3 up to automorphism of C_3

this gives 3*(7 - 4) + 4 = 13 subgroups of F_2 of index 3 (edited)

if I think of the free group on 2 letters as being generated by a & b, then you can split into cases based on the cycle type of the permutations that a and b are sent to

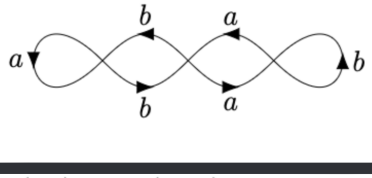
if a is sent to the identity, then in order to have a transitive action b has to be sent to a 3-cycle. up to permutting the indices, this gives one isomorphism class:

$a \mapsto e,\ b \mapsto (1\,2\,3)$

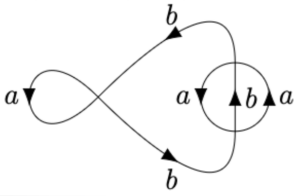


if a is sent to a transposition, then b has to be sent to either a different transposition, or a 3-cycle. again up to permuting indices, there is one isomorphism class for each of these choices, which gives 2 additional isomorphism classes

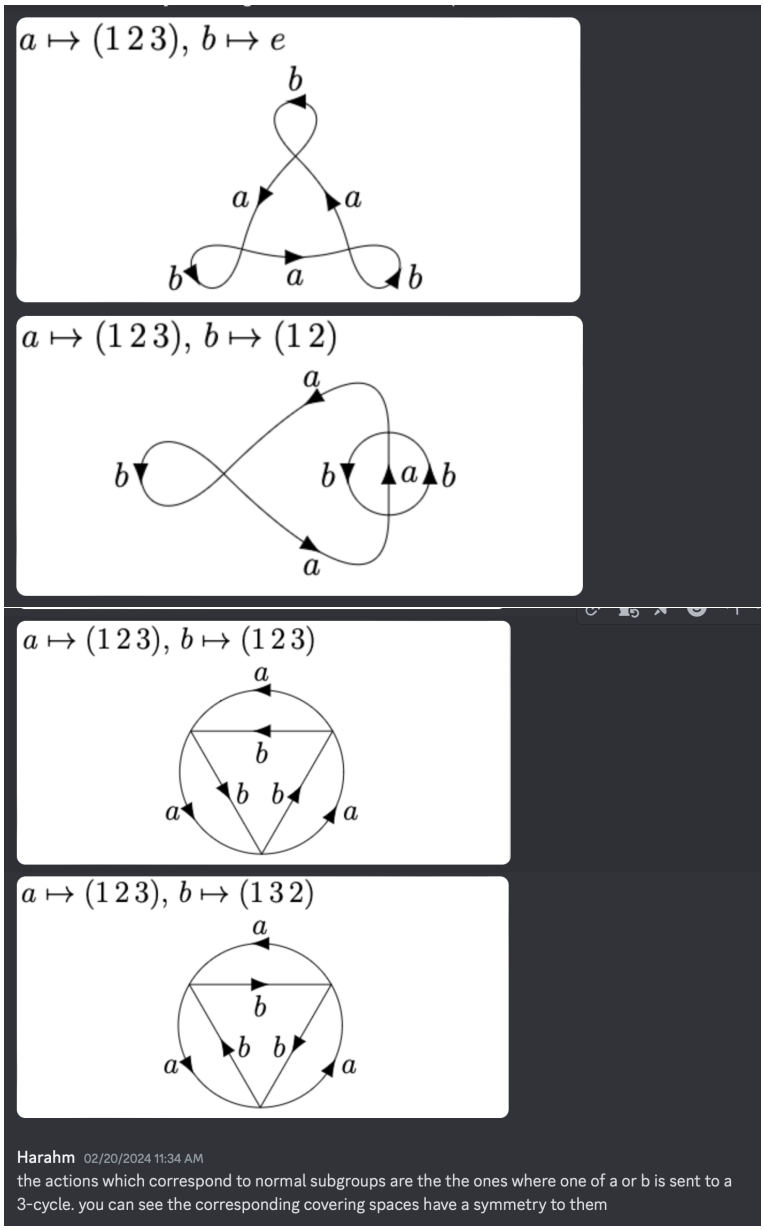
$a \mapsto (1\,2),\ b \mapsto (2\,3)$



$a \mapsto (1\,2),\ b \mapsto (1\,2\,3)$



if a is sent to a 3-cycle, then either b can be sent to the identity, a transposition, the same 3-cycle, or the inverse 3-cycle. this gives 4 additional isomorphism classes



Spring 2017: Question 8 Let M be an abelian group. Prove

$$F : Rings^{op} \to Sets$$
$$R \mapsto \{\text{left } R - Mod \text{ structures on } M\}$$

is a functor. Is F representable?

Solution Need to define what F takes morphisms to, and check $F(f \circ g) =$

$F(g) \circ F(f)$ and $F(Id) = Id$.

If $f : R' \to R$, then

$$F(f) : F(R) \to F(R')$$
$$\gamma \mapsto r' \cdot_{F(f)(\gamma)} m = f(r) \cdot_\gamma m$$

gives an R'- Mod structure.

If we also have $g : R'' \to R'$,

$$F(g) \circ F(f) : F(R) \to F(R'')$$
$$\gamma \mapsto r'' \cdot_{F(g)\circ F(f)(\gamma)} m = g(r'') \cdot_{F(f)(\gamma)} m = f \circ g(r'') \cdot_\gamma m$$

so $F(g) \circ F(f) = F(f \circ g)$.

Finally, $F(Id_R) : F(R) \to F(R)$ simply takes an R-module structure γ to one that acts by applying I_R, giving γ. So, $F(Id_R) = Id_{F(R)}$, and this is a contravariant functor.

F is corepresented by $End(M)$. Let $\alpha : F \to R_{End(M)}$.

$$\alpha_R : F(R) \to Hom(R, End(M))$$
$$\gamma \mapsto (r \mapsto f_r)$$

where $f_r : M \to M$ is left multiplication by r.

Spring 2017 Question 9: Let R be a ring. Prove that if the left free R-modules R^n and R^m are isomorphic for some positive integers n and m, then R^n and R^m are isomorphic as right R-modules.

Solution: Let $\phi : R^n \to R^m$ be a left R-module isomorphism.

Claim: $\mathrm{Hom}(-, R) : \mathrm{Left} - R\mathrm{Mod} \to \mathrm{Right} - R\mathrm{Mod}$ is a functor.

Proof of claim: Let M be a left R-module, we first show that $\mathrm{Hom}(M, R)$ is a right R-module. As the category of left R-modules is an abelian category, $\mathrm{Hom}(M, R)$ is an abelian group. We then see, with the group action $(\psi \cdot r)(m) = \psi(rm)$, $\mathrm{Hom}(M, R)$ is a right R-module as

$$((\psi_1+\psi_2)\cdot r)(m) = (\psi_1+\psi_2)(rm) = \psi_1(rm)+\psi_2(rm) = (\psi_1\cdot r)(m)+(\psi_2\cdot r)(m)$$

and

$$(\psi\cdot(r_1+r_2))(m) = \psi((r_1+r_2)m) = \psi(r_1m+r_2m) = \psi(r_1m)+\psi(r_2m) = (\psi\cdot r_1)(m)+(\psi\cdot r_2)(m)$$

and

$$(\psi\cdot(r_1r_2))(m) = \psi((r_1r_2)m) = \psi(r_1(r_2m)) = (\psi\cdot r_1)(r_2m) = ((\psi\cdot r_1)\cdot r_2)(m)$$

and

$$(\psi \cdot 1_R)(m) = \psi(1_Rm) = \psi(m).$$

We now show that, for any $f : M \to N$, where M, N are left R-modules, the map $\mathrm{Hom}(f, R) : \mathrm{Hom}(N, R) \to \mathrm{Hom}(M, R)$ where $g \mapsto g \circ f$ is a right R-module homomorphism. However, we see that

$$((g_1+g_2)\circ f)(m) = (g_1+g_2)(f(m)) = g_1(f(m))+g_2(f(m)) = (g_1\circ f)(m)+(g_2\circ f)(m)$$

and

$$((g \circ f) \cdot r)(m) = (g(f(rm)) = g(r \cdot f(m)) = (g \cdot r)(f(m)).$$

Thus, $\mathrm{Hom}(f, R)$ is a right R-module homomorphism.

As Hom is additive, we note that $\mathrm{Hom}(\oplus_i M_i, R) = \oplus_i \mathrm{Hom}(M_i, R)$. We then see that $\mathrm{Hom}(R, R) \cong R$ via the map $\psi \mapsto \psi(1)$ and its inverse $a \mapsto \ell_a$ given by $\ell_a(r) = ar$ and by additivity of Hom, we have $\mathrm{Hom}(R^n, R) = R^n$ and $\mathrm{Hom}(R^m, R) = R^m$. As functors send isomorphisms to isomorphisms, we have that $\mathrm{Hom}(\phi, R) : R^m \to R^n$ is an isomorphism of R^n and R^m as right R-modules.

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.

Solution: Consider $\mathrm{Gal}(K/F) \subset S_p$ where p is prime. Note that, letting α be a root of f, $p = [F(\alpha) : F]$, and $F(\alpha) \subset K$. So by the tower lemma, $p \mid [K : F] = |\mathrm{Gal}(K/F)|$. Thus, by Cauchy's theorem, there exists an element σ of order p in $\mathrm{Gal}(K/F)$. However as p is prime, the only elements of order p are exactly p-cycles. Thus, σ permutes the roots of f cyclically.

Fall 2016: Problem 6 Let F be a field of characteristic $p > 0$. Prove that for every $a \in F$, the polynomial $x^p - a$ is either irreducible or split into a product of linear factors.

Solution: There are two cases. Let α be a root of $x^p - a$ in some field extension L of F. Then, $f(x) = x^p - \alpha^p = (x - \alpha)^p \in F[X]$. Suppose that f is not irreducible. Then, $f = gh$ for some non-unital $g, h \in F[X]$. However as $F[X] \subset L[X]$, we also have $f = gh$ as a factorization in $L[X]$. Thus, as $f(x) = (x-\alpha)^p$, we have $g = (x-\alpha)^r = x^r - r\alpha x^{r-1} + \cdots \in F[X]$. In particular, $r\alpha \in F$ but as g and h are non-unital, $1 \leqslant r \leqslant p-1$, thus $r^{-1}r\alpha = \alpha \in F$, which implies $x - \alpha \in F[X]$, and as $f = (x-\alpha)^p$, f splits into a product of linear factors over $F[X]$.

Fall 2016: Problem 7 Let $f \in \mathbb{Q}[X]$ and $\xi \in \mathbb{C}$ a root of unity. Show that $f(\xi) \neq 2^{1/4}$.

Solution: Suppose $f(\xi) = 2^{1/4}$. This implies that $2^{1/4} \in \mathbb{Q}(\xi)$, and thus $\mathbb{Q}(2^{1/4}) \subset \mathbb{Q}(\xi)$. As ξ is a root of unity, $\mathbb{Q}(\xi)$ is a cyclotomic (and thus cyclic) extension. Thus, $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ is cyclic, and thus abelian. As $\mathbb{Q}(2^{1/4})$ is a subfield of $\mathbb{Q}(\xi)$, by assumption, $\mathrm{Gal}(\mathbb{Q}(2^{1/4})/\mathbb{Q})$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$. As $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ is abelian, $\mathrm{Gal}(\mathbb{Q}(2^{1/4})/\mathbb{Q})$ must be a normal subgroup, implying $\mathbb{Q}(2^{1/4})/\mathbb{Q}$ is a normal extension.

However, note that the minimal polynomial of $2^{1/4}$ over $\mathbb{Q}$ is $x^4 - 2$ (by Eisenstein), which has complex roots, but $\mathbb{Q}(2^{1/4}) \subset \mathbb{R}$. Thus, $\mathbb{Q}(2^{1/4})$ is not a normal extension, which is a contradiction.

Fall 2016: Problem 9 F a field, $a \in F$. Define the functor

$$G : Comm\ F\text{-}Alg \to Sets$$
$$R \mapsto \left(\frac{R[x]}{(x^2 - a)}\right)^\times$$

Show G is representable.

Solution G is represented by

$$A := \frac{F[x_1, x_2, y_1, y_2]}{(x_1y_1 + ax_2y_2 - 1, x_2y_1 + x_1y_2)}$$

Let $\alpha : G \to R^A$ be the natural isomorphism.

$$\begin{aligned} \alpha_R : G(R) &\mapsto Hom(A, R) \\ b_1 + b_2 x &\mapsto f : A \to R \end{aligned}$$

where if $c_1 + c_2 x$ is the inverse to $b_1 + b_2 x$,

$$\begin{aligned} f : A &\to R \\ x_1 &\mapsto b_1 \\ x_2 &\mapsto b_2 \\ y_1 &\mapsto c_1 \\ y_2 &\mapsto c_2 \end{aligned}$$

The motivation behind this comes from representing $R[x]/(x^2 - a) \cong R \times R$. Notice that

$$\frac{R[x]}{(x^2 - a)} = \{b_1 + b_2 x : b_1, b_2 \in R\} \cong R \times R$$

Then, (b_1, b_2) and (c_1, c_2) correspond to a unit pair in $R[x]/(x^2 - a)$ iff

$$(b_1 + b_2 x)(c_1 + c_2 x) = b_1 c_1 + a b_2 c_2 + x(b_2 c_1 + b_1 c_2) = 1$$

This induces exactly two relations on the pairs: $b_1 c_1 + a b_2 c_2 = 1$, $b_2 c_1 + b_1 c_2 = 0$.

Thus, an element of $G(R)$ corresponds exactly to some homomorphism from A to R which maps x_1, x_2 to the unit (b_1, b_2) and y_1, y_2 to the inverse (c_1, c_2).

Notice that F can map to any F-algebra. In adding these variables and inducing restrictions on where they can map to, we are limiting our homomorphisms precisely up to a choice of unit.

Spring 2016 Show that if G is a finite group acting transitively on a set X with at least two elements, then there exists $g \in G$ which fixes no points of X

Solution Suppose any elements $g \in G$ fixes some elements of X then given $g \in G$ we can find $x \in X$ such that $g \in Stab(x)$. Since identity fixes x so that means $\sum_{x \in X} |stab(x)| > |G|$. However by the orbit stabilizer $|stab(x)| = \frac{|G|}{orb(x)} = \frac{|G|}{|X|}$. We have $\sum_{x \in A} \frac{|G|}{|A|} = |G|$ that is contradiction to our hypothesis.

Spring 2015 problem 3 Let R be the unital ring, prove that R is division ring iff all R module is free

Solution
I will provide two solutions of if all R module is free then R is a division ring. R be a unital ring such that all R module is projective, R is a semi-simple ring. By the Artin Wedderburn theorem, R is a direct product of the matrices $R \cong \prod M_i(D_i)$ for some division algebra D_i. Regard $M_i(D)$ itself as a R module. If R is decomposed into the product of more than 2 matrix ring. Note free module is torsion free, so there is no element $r \in R$ such that such that $rM_i(D) = 0$. But here we can chose $r = (r_1 \dots r_{i-1}, 0, r_{i+1} \dots r_n)$ is an anihilator. So we have $R \cong M_n(D)$ for just one division ring D_i. We will also show $n = 1$ so that we can claim actually it is a division ring. Claim when $n \neq 1$, D^n is a $M_n(D)$ module which is not free, if D^n is a free then $D^n \cong M_n(D)^m$ for some $m \in \mathbb{Z}$. Compare the dimension of both side over D. We have n dimension over D for the left hand side, but as a D module right hand side is $(n^2)^m$ dimension, they have wrong dimensions.
The second solution: Let I be a maximal left ideal of R and put $M = R/I$. Then M is a simple left R-module: it has no nonzero proper submodules. By assumption M is free: there is a basis $\{x_i\}$. M has to be isomorphic to Rx_1 if not, $M \cong \oplus Rx_i$ then because M is simple, if $i \geqslant 2$ then module wouldn't be simple. Moreover, since x_1 is a basis element, we have $Rx_1 \cong R$ as R-modules. This means R is a simple also left R-module. This means it has no nonzero proper left ideals and is thus a division ring.

Spring 2015: Problem 7 Determine the ring endomorphisms of $\mathbb{F}_2[t, t^{-1}]$, where t is an indeterminate.

Solution:

The ring endomorphisms must send $1 \mapsto 1$ and $0 \mapsto 0$. The only restriction is that t must map to a unit of the ring, as t^{-1} must map to its inverse. So, it suffices to find all the units of the ring.

If two Laurent polynomials are inverses, then their leading terms will multiply to give the leading term of the product. Since this is equal to 1, the sum of their degrees is equal to 0. Similarly, their last terms will multiply to give the last term of the product, which must also be 1. Thus, the sum of their smallest exponents is also 0. So, $p(t)$ can actually only have one term t^n. So, the set of units of R is just $\{t^n : n \in \mathbb{Z}\}$. This determines all ring homomorphisms.

Spring 2015: Problem 9 Let G be a finite group of order p^n. Show that $\mathbb{F}_p[G]$ has a unique maximal 2-sided ideal.

Solution Sketch: First we find a maximal 2-sided ideal. An ideal is maximal iff R/I is a field. Since $\mathbb{F}_p$ is a field, we can take the augmentation map

$$\epsilon : \mathbb{F}_p[G] \to \mathbb{F}_p$$
$$\sum_g a_g \cdot g \mapsto \sum_g a_g$$

which is clearly surjective. Then $I_G := \ker(\epsilon)$ is a 2-sided maximal ideal. For the uniquness, since I is two sided maximal ideal, for a Jacobson radical $J(R)$ we have $I \supset J(R)$. We will prove I is nilpotent ideal so that I is contained in $J(R)$.
We can prove the fact by an induction. If $|G| = p^n$ then augemented ideal will be vanish by the p^n power. When $n = 1$ then G is cyclic, in particular commutative. I is generated by $(e - g)$ for all $g \in G$. As $\sum a_g g \in I \to \sum a_g(g - e)$ as $\sum a_g = 0$. And since

$$(e - g)^p = e - g^p = 0$$

so $I^p = 0$, and I is nilpotent. Assume the statement is true for $n - 1$ and prove the statement for n. For a p-group G, there are non-trivial center C exist. C is also a p-group. Thus by the Cauchy theorem there is an element $x \in C$ of order p. Let Z be a group generated by x. We will define a map $F_p[G] \to F_p[G/Z]$ induced by the morphism $G \to G/Z$.
lemma: There is a canonical morphism $\pi : F_p[G] \to F_p[G/Z]$ and the kernel is $I_Z F_p[G] = F_p[G]I_Z$ where I_Z is unique maximal two sided ideal for $F_p[Z]$.
Proof: Surjectivity and the equality are obvious because Z is normal subgroup. We will prove $ker\pi = I_{G/Z}$, let $Z = \{z_i\}$ and $\{k_j\} = G/Z$. Any elements of G can be uniquely representable with $z_i k_j = g_{ij}$. Let $\xi \in Ker\pi$, then $\xi = \sum r_{i,j} g_{i,j}$ for $r_i \in \mathbb{F}_p$. Then $\phi(\xi) = \sum_j (\sum_i r_{i,j}) z_j = 0$ so $\sum_i r_{i,j} = 0$ therefore $\xi = \sum_j (\sum_i r_{ij} z_i) k_j \in I_Z F_p[G]$. Other inclusion is obvious.

Since Z is the center of G, any ideal $I \subset F_p[Z]$ will be commute with the ideal in $F_p[Z]$. Now I_Z is generated by $(g - e)$, so $\pi(I_G) \to I_{G/Z}$ is surjective. By the induction hypothesis $\pi(I_G)^{p^{n-1}} = 0$ this means $I_G^{p^{n-1}} \subset ker\pi$. Again by the hypothesis and the they are center $Ker(\pi)^p = I_Z^p F_p[G]^p = 0$ so I is nilpotent ideal. Thus $I_G^{p^n} = 0$

Spring 2014 Problem 5 Let G be a finite group acting transitively on a finite set X. Let $x \in X$ and P be a Sylow subgroup of the stabilizer of x in G. Show that $N_G(P)$ acts transitively on X^P.

Solution Let $S := stab(x)$. Then pick $y \in X^P$, $stab(y) = gSg^{-1}$. Since P acts y trivially, $P \leqslant Stab(y) = gSg^{-1}$. Means $g^{-1}Pg \leqslant S$, g preserve P in S. Take by Sylow's theorem we can take $g' \in S$ such that $g'Pg'^{-1} = g^{-1}Pg$, so that $g'^{-1}g^{-1}$ normalize P. Since normalizer is a group $(g'^{-1}g^{-1})^{-1} \in N_G(P)$ and $gg'x = y$.

Fall 2014: Problem 1 Let G be a finite group. Let $\mathbb{Z}[G]$ be the group algebra with augmentation ideal A. Show that $A/A^2 \cong G/[G,G]$ as abelian groups.

Solution Sketch: Define the following group homomorphism

$$\begin{aligned} f : \frac{G}{[G,G]} &\to \frac{A}{A^2}[g] && \mapsto [e-g] \\ \prod_g g^{a_g} &\leftarrow\!\shortmid \sum_g -a_g \cdot g \end{aligned}$$

Just check that each are well defined, and is a group homomorphism. And, that they are inverses of course.

Fall 2014: Problem 2 Let $\mathbb{F}_p$ denote the field of p elements. Consider the covariant functor F from the category of commutative $\mathbb{F}_p$-algebras with a multiplicative identity to abelian groups sending a ring R to $F(R) = \{\zeta \in R : \zeta^p = 1\}$.

(a) Give an example of a finite local ring R such that $F(R)$ has p^2 elements

(b) Let $Aut(F)$ be the set of natural transformations of F to itself inducing a group automorphism of $F(A)$ for all commutative rings A with identity. Prove F is representable and compute the order of $Aut(F)$ using Yoneda's Lemma

Solution Sketch

(a) For $p \geqslant 3$, take $R = \frac{\mathbb{F}_p[x]}{(x^3)}$. For $p = 2$, take $R = \frac{\mathbb{F}_p[x]}{(x^4)}$

(b)
$$F(R) \cong Hom\left(\frac{\mathbb{F}_p[x]}{(x^p-1)}, R\right)$$

Let $A = \frac{\mathbb{F}_p[x]}{(x^p-1)}$. By Yoneda's Lemma, $Nat(F,F) = Nat(R^A, R^A) \cong Hom(A,A)$. Moreover, $A \mapsto R^A$ is a fully faithful functor, so it preserves and reflects isomorphisms.

Since $Aut(F)$ is the set of natural isomorphisms $\alpha : F \to F$, the order of $Aut(F)$ is exactly the number of automorphisms of A (by Yoneda's isomorphism).

Notice that

$$\frac{\mathbb{F}_p[x]}{(x^p-1)} \cong \frac{\mathbb{F}_p[x]}{((x-1)^p)} \cong \frac{\mathbb{F}_p[x]}{(x^p)}$$

So, it suffices to find the number of automorphisms of $A' = \frac{\mathbb{F}_p[x]}{(x^p)}$. Let $f : A' \to A'$, and let

$$y = f(x) = a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$$

f is an automorphism iff there exists an inverse f^{-1} that will send $f^{-1}(y) = b_{p-1}y^{p-1} + \cdots + b_1 y + b_0 = x$. Notice that x is of order p, and automorphisms preserve order, so y must be of order p as well. So, we must have $a_0 = 0$. Moreover, if we look at the linear term of $f^{-1}(y)$, we get the coefficient $b_1 a_1 = 1$, so $a_1 \neq 0$. Now we show these conditions are sufficient. Each polynomial term gives us a condition, where the quadratic term gives $b_1 a_2 + b_2 a_1^2 = 0$. The expression for the x^i coefficient uniquely determines the value of b_i. By induction, this system can be solved for each b_i if $a_1 \neq 0$ and $a_0 = 0$.

So, there are exactly $(p-1)p^{p-2}$ automorphisms in $Aut(F)$.

Fall 2014: Problem 8 Let A be a ring. Assume there is an infinite chain of left ideals $I_0 \subset I_1 \subset \cdots \subset A$ such that $I_i \neq I_{i+1}$ for all $i \geqslant 0$. Show that A has a left ideal that is not finitely generated as a left A-module.

Solution Sketch:

Let $I = \bigcup_{i=0}^{\infty} I_i$. This is a left ideal of A, and it is nontrivial, otherwise $1 \in I$, which means $1 \in I_n$ for some n, which would stop the ascending chain.

Moreover, it cannot be finitely generated, otherwise it suffice to let I be only a finite union of the I_n ideals in the chain, again contradicting the infinite ascending chain.

Spring 2013 Problem 7 Let $F = \mathbb{F}_2$ be the field with 2 elements. Show that there is a ring homomorphism $F[GL2(F)] \to M_2(F)$ that sends the element g in the group ring to the matrix $g \in M_2(F)$. Show that this homomorphism is surjective. Let K be the kernel; since it is a left ideal, it is a (left) $GL_2(F)-$module. Is this module indecomposable? (Reminder: a module is indecomposable if it is not the direct sum of two proper submodules.) Describe the simple modules in its composition series.

solution Surjection can be proved by observing there are 6 elements for $F[GL_2(F)]$ such that $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $e_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $e_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ $e_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$e_5 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ $e_6 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ as a vector space, and mapping to a 4dimensional vector space spanned by the elementary matrices. For example, $e_1 - e_2$, $e1 - e_3, e_4 - e_5, e_4 - e_6$ are basis. The Kernel is $v_1 := e_1 + e_5 + e_6, v_2 := e_2 + e_3 + e_4$ easily check linearly independent, and by rank nullity kernel has to be $2-$dimension.

$GL_2(F)$ permute among the vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ so there is an isomorphism between $GL_2(F)$ and S_3. So without loss of generalities, we regard it as a S_3 representation on F^2 $v_1 + v_2$ is invariant under the all the representation, and we can show that there is no invariant space outside of the kernel. For arbitrary elements in kernel can be written as $av_1 + bv_2$. If we permute v_1 and v_2 then would be $b_{v1} + a_{v2}$ adding each other then would be in the kernel. So there is only one S_3 module inside of the K. Quotient of K by $v_1 + v_2$ we have some 1dimensional S_3 module represented by v_1(or v_2). 1dimensional representation of S_3 are trivial or sign, but since this is F_2 these are coincide.