Homework for
Algebra I

Nicholas Camacho
Department of Mathematics
University of Iowa
Fall 2017

Beware: Some solutions may be incorrect!

Exercise 1. In this problem, we define a homomorphism from a finite group G to an abelian subgroup $A \leq G$, and give an application to finding normal subgroups.

Let G be a finite group, $A \leq G$ an abelian subgroup, and $x_1, \ldots, x_n$ any set of left coset representatives:

$$G = x_1 A \cup \cdots \cup x_n A.$$

We obtain a homomorphism $G \to S_n$ by the action of G on the coset space G/A: for each $g \in G$, the corresponding permutation π is defined by

$$g x_i A = x_{\pi(i)} A.$$

So for each $g \in G$, there exist unique elements $a_1, \ldots, a_n$ such that $g x_i = x_{\pi(i)} a_i$. Define a map $\phi \colon G \to A$ by $\phi(g) = a_1 \cdots a_n$.

(a) Prove that ϕ is a group homomorphism.

Proof. First note that ϕ is well defined since for each $g \in G$, we have unique elements $a_1, \ldots, a_n$ in the above definition. Let $g, h \in G$ and write

$$g x_i = x_{\pi_g(i)} a_i \text{ and } h x_i = x_{\pi_h(i)} b_i \quad \text{for all } 1 \leq i \leq n.$$

Then for each i,

$$g h x_i = g x_{\pi_h(i)} b_i = x_{\pi_g(\pi_h(i))} a_{\pi_h(i)} b_i.$$

So,

$$\phi(gh) = \prod_{i=1}^{n} a_{\pi_h(i)} b_i = \prod_{i=1}^{n} a_i \prod_{i=1}^{n} b_i = \phi(g)\phi(h).$$

□

(b) Prove that ϕ is independent of the choice of coset representatives $x_1, \ldots, x_n$.

Proof. Choose another set of coset representatives $\{y_1, \ldots, y_n\}$ so that $x_i A = y_i A$ for all $1 \leq i \leq n$. Let $g \in G$, and write $g y_i = y_{\tilde{\pi}(i)} b_i$ for all $1 \leq i \leq n$. Then define a map $\tilde{\phi} : G \to A$ by $\tilde{\phi}(g) = b_1 \cdots b_n$. We show that $\phi(g) = \tilde{\phi}(g)$. Notice that for all $1 \leq i \leq n$,

$$y_{\tilde{\pi}(i)} A = g y_i A = g x_i A = x_{\pi(i)} A,$$

and so in fact $\pi(i) = \tilde{\pi}(i)$ for all $1 \leq i \leq n$. Also we have

$$y_{\pi(i)} b_i y_i^{-1} = g = x_{\pi(i)} a_i x_i^{-1},$$

which gives

$$b_i = y_{\pi(i)}^{-1} x_{\pi(i)} a_i x_i^{-1} y_i.$$

Notice that $y_{\pi(i)}^{-1} x_{\pi(i)}, x_i^{-1} y_i \in A$ for all $1 \leq i \leq n$, and since A is abelian, we get

$$\tilde{\phi}(g) = \prod_{i=1}^{n} b_i = \prod_{i=1}^{n} y_{\pi(i)}^{-1} x_{\pi(i)} a_i x_i^{-1} y_i = \prod_{i=1}^{n} a_i = \phi(g).$$

□

Exercise 2. In this problem, we investigate Sylow subgroups of small symmetric groups.

(a) Let $H \leq S_4$ be a Sylow 2-subgroup of the symmetric group. Give an explicit isomorphism between H and a commonly known group. *Note: theory will only take you so far in this problem– you will probably have to get out some scratch paper and experiment with computations. Once you have a good guess at the answer, write down an explicit isomorphism.*

Solution: Since Sylow 2-subgroups are conjugate to one another, it suffices to find the isomorphism type of a particular Sylow 2-subgroup of S_4. Consider the Sylow 2-subgroup

$$H = \langle(1234), (24)\rangle = \{(), (1234), (24), (13)(24), (1432), (12)(34), (13), (14)(23)\}.$$

Since $|(1234)| = 4$ and $|(24)| = 2$ and

$$(1234)(24) = (12)(34) = (24)(1234),$$

then it seems that $H \cong D_8$, the dihedral group of order 8. If we write

$$D_8 = \left\langle r, s \mid 1 = r^4 = s^2, rs = sr^{-1} \right\rangle = \{1, r, s, rs, r^2, r^3, sr^2, sr^3\},$$

then define a map $H \to D_8$ by $(1234) \mapsto r$ and $(24) \mapsto s$.

(b) Determine the number of Sylow 2-subgroups of S_4.

Solution:

We have $|S_4| = 4! = 24 = 2^3 \cdot 3$. By Sylow's Theorems, if $n_p(S_4)$ denotes the number of Sylow p-subgroups of S_4, we get that $n_2(S_4) \in \{1, 3\}$. Since we have the Sylow 2-subgroup

$$K = \langle(1342), (14)\rangle = \{(), (1342), (14), (14)(23), (1243), (12)(34), (23), (13)(24)\},$$

which is not equal to H from part (a) since $(23) \in K - H$, then $n_2 > 1$, and so $n_2 = 3$. For completeness, the last Sylow 2-subgroup of S_4 is

$$L = \langle(1423), (12)\rangle = \{(), (1423), (12), (12)(34), (1324), (13)(24), (34), (14)(23)\},$$

which is distinct from H and K since $(12) \in L - (H \cup K)$.

(c) Find the isomorphism type and number of Sylow 2-subgroups of S_5.
Hint: the isomorphism type follows easily from your previous work. It is then useful in computing the number.

Solution:

Since $S_4 \leq S_5$ (viewing S_4 inside S_5 as all the elements of S_5 which fix 5), then the isomorphism type of Sylow 2-subgroups of S_5 is D_8, since S_4 contains at least some of the Sylow 2-subgroups of S_5. By Sylow's theorems, we get that $n_2(S_5) \in \{1, 3, 5, 15\}$ and $n_2(S_5) \geq 3$, thus $n_2(S_5) \in \{3, 5, 15\}$. But we have the Sylow 2-subgroups

$$H' = \langle(1235), (25)\rangle = \{(), (1235), (25), (13)(25), (1532), (12)(35), (13), (15)(23)\},$$
$$K' = \langle(1352), (15)\rangle = \{(), (1352), (15), (15)(23), (1253), (12)(35), (23), (13)(25)\},$$
$$L' = \langle(1523), (12)\rangle = \{(), (1523), (12), (12)(35), (1325), (13)(25), (35), (15)(23)\},$$

which are distinct from H, K, and L from (a) and (b), and so $n_2(S_5) = 15$.

Thinking about this in a different way: We chose to view S_4 inside of S_5 as all those permutations which fix the number 5. However, we could have just as easily identified S_4 inside of S_5 as all those elements that fixed, say, $j \in \{1, \ldots, 5\}$. If, for example $j = 2$, then we would relabel all the elements in S_4 by the rule $1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 5$, to get another "copy" of S_4 inside of S_5. So, we get 5 distinct "copies" of S_4 inside S_5, and hence 5 distinct "copies" of the subgroups $H, K, L \leq S_4$ inside S_5, giving a total of 15 Sylow 2-subgroups.

Exercise 3. In this problem, we investigate composition series of abelian groups.

(a) Let G be an abelian group, not assumed to be finite. Prove that if G is simple, then G is actually finite, and furthermore $|G|$ is prime.

Proof. We prove the contrapositive statement. If G is infinite and cyclic, then $G \cong \mathbb{Z}$, which is not simple. If G is infinite and not cyclic, pick $x \in G - \{1\}$. Since G is abelian, $\langle x \rangle \trianglelefteq G$, and since G is not cyclic, $\langle x \rangle$ must be a proper normal subgroup, i.e., G is not simple.

Now, write $|G| = p_1 \cdots p_n$ for primes $\{p_i\}_{i=1}^n$. If there exists distinct $i, j \in \{1, \ldots, n\}$ so that $p_i \neq p_j$, then $\langle p_i \rangle$ is a proper normal subgroup of G, because then $\langle p_i \rangle \triangleleft G$ and $|\langle p_i \rangle| < |G|$. Hence $|G| = p^\alpha$ for a prime p and $\alpha \in \mathbb{Z}^+$. By Cauchy, we find $x \in G$ with $o(x) = p$. If $\alpha > 1$, then $\langle x \rangle$ is a proper normal subgroup of G, and so we must have $|G| = p$, as desired. □

(b) Let G be an infinite abelian group. Prove that G does not have any composition series.

Proof. By contradiction. Write $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ where G_i/G_{i-1} is simple for all $1 \leq i \leq n$. Then for all $1 \leq i \leq n$, G_i/G_{i-1} is simple abelian, and so by part (a), we find $\{p_i\}_{i=1}^n$ so that $|G_i/G_{i-1}| = p_i$. Since cosets partition a group, we get

$$|G| = p_n|G_{n-1}| = p_n p_{n-1}|G_{n-2}| = \cdots = p_n \cdots p_1|G_0| = p_n \cdots p_1 < \infty,$$

a contradiction. □

Optional challenge problem, not for credit. Suppose that $|G| = pn$, where p is the smallest prime dividing $|G|$, and $p \nmid n$. Prove that G has a normal subgroup N of order n (in particular, G is not simple). *Hint: there is an obvious choice of abelian subgroup of order p, which you should use as A in the transfer homomorphism from Problem 1. Then it would be enough to show the transfer homomorphism is surjective, and use $N = \ker \phi$. To do this, you can show that $\phi(a) = a^n$ for each $a \in A$. This requires some cleverness involving a study of the permutation π from the definition of the transfer.*

Exercise 1. Let F be a field and fix $n \in \mathbb{Z}_{>0}$. Let $B \leq GL_n(F)$ be the subgroup of invertible upper-triangular matrices.

(a) Prove that $B \cong U \rtimes D$ where U is the subgroup of upper-triangular matrices with 1s down the diagonal, and D is the subgroup of invertible diagonal matrices.

Proof. First notice that no element of B has a diagonal entry 0, for otherwise such a matrix b would have 0 as an eigenvalue, giving that $\det(b) = 0$, contradicting that b is invertible. Next, notice that if $g = (g_{ij}), h = (h_{ij}) \in B$, then the (i,i)-entry of gh is

$$(gh)_{ii} = \sum_{k=1}^{n} g_{ik}h_{ki} = g_{ii}h_{ii}, \tag{$\mathfrak{D}$}$$

where the last equality follows from the fact that $g_{ik} = 0$ when $k < i$ and $h_{ki} = 0$ when $k > i$. Notice also that ($\mathfrak{D}$) gives that the (i,i)-entry of g^{-1} is g_{ii}^{-1}.

We use the theorem for recognizing semi-direct products. Let I denote the identity element in $GL_n(F)$. That $U \cap D = I, I \in U$, and $I \in D$ is clear. Also ($\mathfrak{D}$) immediately gives that $D \leq B$ since for $g, h \in D$, gh^{-1} is diagonal. Similarly, if $g, h \in U$ then gh^{-1} has 1s on its diagonal, and so $U \leq B$.

To show that $U \trianglelefteq B$, let $b \in B$ and $g \in U$. It follows from ($\mathfrak{D}$) that the diagonal entries of bg are precisely the diagonal entries of b, and moreover that bgb^{-1} has diagonal entries 1.

Finally, we show that $B = UD$, from which it follows from the recognition theorem for semi-direct products that $B = UD \cong U \rtimes D$.

Since $U \trianglelefteq B$, then $UD \leq B$. Let $b = (b_{ij}) \in B$. Define matrices $g = (g_{ij}) \in U, h = (h_{ij}) \in D$ in the following way: Let h have the same diagonal as b. Let g have 1s on its diagonal and for $i < j$, define $g_{ij} = b_{ij}b_{jj}^{-1}$ (here, we know that $b_{jj} \neq 0$ by the first remark of the proof). Then by the computation in ($\mathfrak{D}$), we have that the diagonal of gh is precisely the diagonal of b. Also, the (i,j)-entry of gh for $1 \leq i < j < n$, (i.e., an entry of the upper triangle) is

$$(gh)_{ij} = \sum_{k=1}^{n} g_{ik}h_{kj} = g_{ij}h_{jj} = b_{ij}b_{jj}^{-1}b_{jj} = b_{ij},$$

where the second equality follows from the fact that $h_{kj} = 0$ if $k \neq j$. Hence $gh = b$ and so $UD = B$. ☕

(b) Fix $n = 2$. Clearly we can identify $D \cong F^{\times} \times F^{\times}$ (you don't need to write it out). Show that $U \cong F$, the additive group of the field.

Proof. Consider the map $f : U \to F$, $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mapsto a$. That f is a bijection is clear. Also

$$f\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right) = f\left(\begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}\right) = a + b = f\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\right) + f\left(\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right),$$

and so f is a group homomorphism, giving $U \cong F$. ☕

(c) Still with $n = 2$, describe the homomorphism $\varphi\colon D \to Aut(U)$ explicitly in terms of these identifications.

Solution:

For any $d \in D, u \in U$, we make the identifications $d \mathrel{\widehat{=}} (1, d)$ and $u \mathrel{\widehat{=}} (u, 1)$. Under these identifications, the map φ must satisfy $\varphi(d)(u) = dud^{-1}$. So if $a \in F$ and $b, c \in F^\times$, then

$$\underbrace{\begin{bmatrix} b & 0 \\ 0 & c \end{bmatrix}}_{=:d} \underbrace{\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}}_{=:u} \begin{bmatrix} b & 0 \\ 0 & c \end{bmatrix}^{-1} = \begin{bmatrix} 1 & bac^{-1} \\ 0 & 1 \end{bmatrix}.$$

So under the identifications $D \cong F^\times \times F^\times$ and $U \cong F$, we get that the map φ must be given by $(b, c) \mapsto (a \mapsto bac^{-1})$.

Exercise 2. Let F be a finite field with q elements.

(a) Compute the order of $GL_2(F)$.

Solution:

For any element $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(F)$, we can make any choice from F for a and d. We need $ad \neq bc$. So if $a = 0$ or $d = 0$, then we can pick any nonzero elements for b and c, giving $|F^\times| = q - 1$ choices for each b and c. If both $a \neq 0$ and $d \neq 0$, then $ad \neq bc$ becomes $0 \neq d^{-1}a^{-1}bc$, giving that neither b nor c can be zero; again we get $q - 1$ choices for each b and c. Hence the order of $GL_n(F)$ is $q^2(q-1)^2$.

(b) Find the center of $GL_2(F)$ and use this information to compute the order of $PGL_2(F) = GL_2(F)/Z(GL_2(F))$.

Solution:

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(GL_2(F))$ and $\begin{bmatrix} e & f \\ g & h \end{bmatrix} \in GL_2(F)$. Then

$$\begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} = \begin{bmatrix} ea + fc & eb + fd \\ ga + hc & gb + hd \end{bmatrix}, \tag{🦇}$$

This must hold for all $e, f, g, h \in F$, (provided of course $eh - fg \neq 0$), so let's pick these wisely in order to determine what values we can have for a, b, c, d. First let $h = e = 0$ and let $f = g = 1$. Then (🦇) becomes

$$\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix},$$

and so $a = d$ and $b = c$. So, if we use this fact along with letting $e = f = h = 1$ and $g = 0$, then (🦇) becomes

$$\begin{bmatrix} a & a + b \\ b & b + a \end{bmatrix} = \begin{bmatrix} a + b & b + a \\ b & a \end{bmatrix}.$$

This gives $b = 0$. So $Z(GL_2(F))$ is contained in the set of matrices which are multiples of the identity matrix. Conversely, for $e, f, g, h \in F$ so that $eh - fg \neq 0$, and $a \in F$, we have

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae & af \\ ag & ah \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

Hence
$$Z(GL_2(F)) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in F, a^2 \neq 0 \right\} = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in F^\times \right\}.$$
So $|Z(GL_2(F))| = q-1$, which gives $|PGL_2(F)| = |GL_2(F)|/|Z(GL_2(G)| = q^2(q-1)$.

(c) Find the orders of $SL_2(F)$ and $PSL_2(F)$.
(*Hint: use your previous work and the most important homomorphism for matrix groups.*)

Solution:

Consider the determinant homomorphism $\det : GL_2(F) \to F^\times$. If $a \in F^\times$, then the diagonal matrix with diagonal entries a and 1_F has determinant a. Hence det is a surjective group homomorphism from $GL_2(F)$ to $F^\times$ with $\text{Ker}(\det) = SL_2(F)$, and so $GL_2(F)/SL_2(F) \cong F^\times$. Therefore we have
$$|SL_2(F)| = \frac{|GL_2(F)|}{|F^\times|} = q^2(q-1).$$
When we found the center of $GL_2(F)$, we only relied on the fact that matrices in $GL_2(F)$ have nonzero determinant. Hence the same argument applies if we restrict our attention to $SL_2(F)$. So
$$Z(SL_2(F)) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in F^\times, a^2 = 1 \right\} = \left\{ \begin{bmatrix} 1_F & 0 \\ 0 & 1_F \end{bmatrix}, \begin{bmatrix} -1_F & 0 \\ 0 & -1_F \end{bmatrix} \right\}.$$
Therefore, $|PSL_2(F)| = |SL_2(F)|/|Z(SL_2(F))| = q^2(q-1)/2$.

(d) **Optional.** If F is a finite field with q elements, compute the orders of $GL_n(F)$ and $PGL_n(F)$. You can get explicit formulas. What about $SL_n(F)$ and $PSL_n(F)$?

Exercise 1. Let $B \leq GL_n(F)$ be the subgroup of invertible upper-triangular matrices (F is an arbitrary field).
Taking $n = 3$, prove that B is a solvable group, but not nilpotent. For more of a challenge, prove the same for arbitrary n.

Proof. If $F = \mathbb{F}_2$, then $B = U$ and so B is in fact nilpotent by Exercise 3 below. Suppose $F \neq \mathbb{F}_2$. We saw in the last homework that for $a = (a_{ij}), b = (b_{ij}) \in B$, the (i,i)-entry of the matrix ab is $a_{ii}b_{ii}$. Since $(a_{ij})(a_{ij})^{-1} = I$, then the (i,i)-entry of a^{-1} is a_{ii}^{-1}. So if we consider the commutator of a and b, we get that the (i,i)-entry of $aba^{-1}b^{-1}$ is $a_{ii}b_{ii}a_{ii}^{-1}b_{ii}^{-1} = 1$. Hence $B^{(1)} = [B,B] \leq U$, where U is the subgroup of B consisting of all matrices with 1s on their diagonal. Then, the computation

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & af - cd \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

shows that $U^{(1)} = [U,U] \leq A$, where

$$A = \left\{ \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : a \in F \right\}.$$

So $B^{(2)} \leq U^{(1)} \leq A$. Then, the computation

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

shows that $A^{(1)} = [A,A] = I$. So $B^{(3)} \leq U^{(2)} \leq A^{(1)} = I$, and so the derived series of B terminates. Hence B is solvable.

It is not hard to see that the $Z_0(B) = Z(B)$ is the set of scalar matrices, S. Now suppose $aS \in Z(B/S)$ and $bS \in B/S$. Then

$$abS = baS \iff aba^{-1}b^{-1} \in S \cap U = I \iff ab = ba \iff a \in Z(B) = S \iff aS = S.$$

So, $Z_1 = \pi^{-1}(Z(B/S)) = S$, and then $Z_2 = \pi^{-1}(Z(B/S)) = S$, and so on. So we get ascending central series

$$Z_0 = Z_1 = Z_2 = Z_3 = Z_4 = \cdots$$

which never reaches B. Hence B is not nilpotent. (*Really* not nilpotent). $\square$

Exercise 2. These miscellaneous exercises concern p-groups and nilpotent groups.

(a) Let p be a prime and V an n-dimensional vector space over the finite field $\mathbb{F}_p$. Suppose $\varphi \in GL(V)$ has order a power of p. Show that φ has a nonzero fixed point in V (i.e., there exists $0 \neq v \in V$ such that $\varphi(v) = v$).

Proof. Suppose φ has order p^α for some $\alpha \in \mathbb{Z}_{>0}$. Then the minimal polynomial for φ divides $x^{p^\alpha} - 1 = (x-1)^{p^\alpha}$. But then 1 is an eigenvalue for φ, and so φ fixes a nonzero vector.

Alternatively, notice that V has p^n elements. If we let the group $\langle\varphi\rangle$ act on V (by evaluation, $\varphi^j.v = \varphi^j(v)$) we partition the set V into orbits, say, $\mathcal{O}_{w_1}, \dots, \mathcal{O}_{w_k}$, and so $p^n = |V| = \sum_{i=1}^k |\mathcal{O}_{w_i}|$. So p divides the order of each orbit. In particular, we can write

$$p^n = |V| = m\mathcal{N}_1 + \ell_1\mathcal{N}_p + \ell_2\mathcal{N}_{p^2} + \cdots + \ell_\alpha\mathcal{N}_{p^\alpha},$$

for some integers $m, \ell_1, \dots, \ell_{p^\alpha}$, where $\mathcal{N}_1$ is the number of orbits of size 1 and $\mathcal{N}_{p^j}$ is the number of orbits of size p^j. Now, $\mathcal{N}_1 \geq 1$, since the orbit of 0_V has size 1. But $p|\mathcal{N}_1$ and so there are at least p orbits of size 1, giving that φ fixes a nonzero element of V − in particular, it fixes at least $p-1$ nonzero vectors. □

(b) Use (a) to prove that there exists a chain of subspaces

$$V_0 = 0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = V, \qquad \dim_F V_i = i,$$

with $\varphi(V_i) = V_i$ for all i. (Such a chain is called a *complete flag* in V; the set of all complete flags in V is an algebraic variety over any field F, generalizing projective space $\mathbb{P}(V)$ (and a compact manifold if $F = \mathbb{R}$ or $F = \mathbb{C}$).

Proof. By induction. For $n = 1$, let $V_1 = \operatorname{span}\{w_1\}$ where w_1 is a vector fixed by φ. So $V_0 \subset V_1$ is a chain of subspaces with $\dim_F V_i = i$ and $\varphi(V_i) = V_i$, $i = 1, 2$.

Suppose the claim is true for $1 \leq k < n$. We need to find a subspace $V_{k+1} \supset V_k$ for which $\varphi(V_{k+1}) = V_{k+1}$. First consider the space V/V_k. Since $\varphi(V_k) = V_k$, then φ induces a well-defined transformation

$$\tilde{\varphi} : V/V_k \to V/V_k, \quad a + V_k \mapsto \varphi(a) + V_k.$$

Since also $\varphi^{-1}(V_k) = V_k$, then $\tilde{\varphi}$ has a well-defined inverse, $b + V_k \mapsto \varphi^{-1}(b) + V_k$. So $\tilde{\varphi} \in GL(V/V_k)$, and so we can apply part (a) to find $w_{k+1} + V_k \in V/V_k$ fixed by $\tilde{\varphi}$, where $w_{k+1} + V_k \neq 0_V + V_k$. Then $\tilde{W} := \operatorname{span}\{w_{k+1} + V_k\}$ is a subspace of V/V_k, and so by the correspondence theorem, there is a subspace $V_{k+1} \supset V_k$ for which $V_{k+1}/V_k = \tilde{W}$ and $\dim_F V_{k+1} = k+1$.

Now, the coset representative w_{k+1} is an element of $V_{k+1} \sim V_k$ and also spans $V_{k+1} \sim V_k$. So if $\{v_1, \dots, v_k\}$ is a basis for V_k, then $\{v_1, \dots, v_k, w_{k+1}\}$ is a basis for V_{k+1}. Now, $\varphi(v_i) \in V_k$ for all $1 \leq i \leq n$, and

$$\varphi(w_{k+1}) + V_k = \tilde{\varphi}(w_{k+1} + V_k) = w_{k+1} + V_k \in V_{k+1}/V_k,$$

which means $\varphi(w_{k+1}) \in V_{k+1}$. Hence $\varphi(V_{k+1}) = V_{k+1}$, completing the induction. □

Exercise 3. Let $U \leq SL_n(F)$ be subgroup of upper-triangular matrices with 1s on the diagonal (F is an arbitrary field). Taking $n = 3$, prove that U is a nilpotent group. How does U relate to Problems 1 and 2(b)? For more of a challenge, prove the same for arbitrary n.

Proof. We saw in Exercise 1 that $U^{(1)} \leq A$. Then the computation

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

shows that $[U, U^{(1)}] \leq [U, A] = I$. Hence we have the descending central series

$$U \triangleright U^{(1)} \triangleright [U, [U^{(1)}]] = I,$$

and so U is nilpotent. $\square$

Problem 1. *Skills developed: working with properties of maps rather than choosing elements. This can simplify certain kinds of proofs by not introducing extra symbols too keep track of. It is particularly useful when you have several interacting maps.*
Let $f\colon A \to B$ be a morphism in an arbitrary category $\mathcal{C}$ (so the proofs should not make reference to "elements"). Prove each of the following:

(a) If f is a retraction, then f is an epimorphism.

Proof. There exists $g : B \to A$ such that $fg = 1_B$. So if $g_1 f = g_2 f$, then $g_1 f g = g_2 f g \implies g_1 1_B = g_2 1_B \implies g_1 = g_2$. □

(b) If f is a section, then f is a monomorphism.

Proof. There exists $g : B \to A$ such that $gf = 1_A$. So if $fg_1 = fg_2$, then $gfg_1 = gfg_2 \implies 1_A g_1 = 1_A g_2 \implies g_1 = g_2$. □

(c) The morphism f is an isomorphism if and only if f is a monomorphism and a retraction. (This is if and only if f is an epimorphism and a section; the proof is similar so don't turn it in.)

Proof. ($\Rightarrow$) There exists $g : B \to A$ such that $fg = 1_B$ and $gf = 1_A$. The former is the definition of a f begin a retraction. If $fg_1 = fg_2$, then $gfg_1 = gfg_2 \implies 1_A g_1 = 1_A g_2 \implies g_1 = g_2$, and so f is a monomorphism.

($\Leftarrow$) Since f is a retraction, there exists $g : B \to A$ such that $fg = 1_B$. Since f is a monomorphism, $fgf = 1_B f = f = f 1_A$ implies $gf = 1_A$. Hence f is an isomorphism. □

Problem 2. *Skills developed: practice applying definition of "functor" in a more familiar setting. Creating examples to understand abstract properties.*
Let **Groups** be the category of groups, and **Rings** be the category of rings with 1 (morphisms are ring homomorphisms sending 1 to 1).

(a) Given a group G, let $Ab(G)$ be the largest quotient of G which is abelian. Show that Ab is a functor from **Groups** to itself.

Proof. The largest abelian quotient of a group is that obtained by quotienting by its commutator subgroup. Let $f : G \to H$ be a group homomorphism and let H' denote the commutator subgroup of H. The composition $\pi_H \circ f : G \to H/H'$ is a map from G to an abelian group; so $\pi_H \circ f$ must factor through G/G'. In particular, the map $\psi : G/G' \to H/H'$ given by $xG' \mapsto (f \circ \pi_H)(x)$ is the unique, well-defined homomorphism and makes the diagram commute:

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_G"'] & H \arrow[r, "\pi_H"] & H/H' \\ G/G' \arrow[urr, "\psi"'] & & \end{tikzcd}$$

So we define $Ab(f) = \psi$. Let $g : H \to K$ be a group homomorphism, and consider the diagram

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dd, "\pi_G"] & H \arrow[r, "g"] \arrow[d, "\pi_H"] & K \arrow[r, "\pi_K"] & K/K' \\ & H/H' \arrow[urr, "Ab(g)"] & & \\ G/G' \arrow[ur, "Ab(f)"] \arrow[uurrr, bend right, "Ab(gf)"] & & & \end{tikzcd}$$

We have $Ab(gf) \circ \pi_G = \pi_K \circ g \circ f$. On the other hand,

$$Ab(g) \circ Ab(f) \circ \pi_G = Ab(g) \circ \pi_H \circ f = \pi_K \circ g \circ f,$$

and so $Ab(gf) = Ab(g) \circ Ab(f)$. Now, if $1_G : G \to G$ is the identity homomorphism on G, then $Ab(1_G) \circ \pi_G = \pi_G \circ 1_G = \pi_G$, which means $Ab(1_G) = 1_{G/G'}$. Hence Ab is a covariant functor. $\square$

(b) Show that the map from **Rings** to **Groups**, defined on objects by sending a ring R to its group of units $R^\times$, extends to a functor between these categories. Show by example that it is neither faithful nor full.

Solution:

Let $F : \mathbf{Rings} \to \mathbf{Groups}$ be the map $R \mapsto R^\times$. For $f : R \to S$, a ring homomorphism, define $F(f) : R^\times \to S^\times$ by $F(f)(r) \mapsto f(r)$. Since f is a group homomorphism, it must send units to units, so $F(f)$ is well-defined. If we have two ring homomorphisms $f : R \to S, g : S \to A$, then

$$F(gf)(r) = g(f(r)) = g(F(f)(r)) = F(g)(F(f)(r)) = (F(g) \circ F(f))(r).$$

Also, $F(1_R)(r) = 1_R(r) = r$ implies $F(1_R) = 1_{R^\times} = 1_{F(R)}$, and so F is a covariant functor.

Consider the group homomorphism $f : \mathbb{Z}^\times \to \mathbb{Z}^\times$ given by $1 \mapsto -1$. This map is in $\mathrm{Hom}_{\mathbf{Groups}}(\mathbb{Z}^\times, \mathbb{Z}^\times)$. However, since $\mathrm{Hom}_{\mathbf{Rings}}(\mathbb{Z}, \mathbb{Z}) = \{1_\mathbb{Z}\}$, and $F(1_\mathbb{Z}) = 1_{\mathbb{Z}^\times} \neq f$, then F is not full.

Now let x be transcendental over an integral domain R, and consider the evaluation ring homomorphism $eval_a : R[x] \to R$, $f(x) \mapsto f(a)$, for $a \in R$. Now, $(R[x])^\times = R^\times$, and so for $r \in R^\times$, $eval_a(r) = r$. Therefore if we pick distinct $a, b \in R$, we get that $F(eval_a) = F(eval_b)$, yet $eval_a \neq eval_b$, showing that F is not faithful.

Problem 3. *Skills developed: more practice with functors and getting used to passing back and forth between equivalent definitions (abstract vs. concrete).*
Recall that a group G determines a category with one object $\mathbf{G}$. Let K be a field, and $\mathbf{Vec}_K$ the category of K-vector spaces. A *representation* of a group G on a K-vector space V is a group homomorphism $\rho\colon G \to GL(V)$. Given a representation ρ, define a functor $F_\rho\colon \mathbf{G} \to \mathbf{Vec}_K$. Conversely, given a functor $F\colon \mathbf{G} \to \mathbf{Vec}_K$, define a representation of G on a vector space.
Think about why these two processes are "inverse" to one another, so the concept of a representation is equivalent to this particular kind of functor. In general, a functor from any category $\mathcal{C}$ to $\mathbf{Vec}_K$ can be interpreted (or defined) as a representation of $\mathcal{C}$.

Solution:

First, suppose we have representation $\rho : G \to GL(V)$ for a vector space V over K. Define a map $F_\rho : \boldsymbol{G} \to \mathbf{Vec}_K$ by $F_\rho(G) = V$, and for any morphism $g \in \mathrm{Hom}_\mathbf{G}(G, G)$,

$$F_\rho(g) = \rho(g) \in \mathrm{Hom}_{\mathbf{Vec}_K}(V, V).$$

If 1_G is the identity in $\mathrm{Hom}_\mathbf{G}(G, G)$, then $F_\rho(1_G) = \rho(1_G) = 1_{GL(V)} = 1_V$ since ρ is a group homomorpism. If $g, h \in \mathrm{Hom}_\mathbf{G}(G, G)$, then $F_\rho(gh) = \rho(gh) = \rho(g)\rho(h) = F_\rho(g)F_\rho(h)$, and so F_ρ is a covariant functor.

Now, suppose we have a (covariant) functor $F : \mathbf{G} \to \mathbf{Vec}_K$. Let V be the vector space $F(G)$. Then define a representation of G on V, $\rho : G \to GL(V)$ by $\rho(g)(v) = F(g)(v)$ for all $g \in G = \mathrm{Hom}_\mathbf{G}(G, G)$ and for all $v \in V$. Then for $g, h \in G$

$$\rho(gh) = F(gh) = F(g)F(h) = \rho(g)\rho(h),$$

and so ρ is a group homomorphism. Now, we check that $\rho(g)$ is actually an element of $GL(V)$:

$$\rho(g)\rho(g^{-1}) = F(g)F(g^{-1}) = F(gg^{-1}) = F(1_G) = 1_{F(G)} = 1_V,$$

and similarly, $\rho(g)^{-1}\rho(g) = 1_V$.

Problem 1. *Skills developed: Interpreting and testing an abstract definition in familiar settings.*
In each category below, decide whether there exists a free object on an arbitrary set X. If so, prove it by constructing the free object and demonstrating the definition holds. If not, choose a specific set X and prove that no free object on X can exist.
Each category below is a familiar concrete category. Just treat the objects as having underlying sets as you usually would, without writing U for the "underlying set" functor.

(a) The category **Sets** of all sets.

(b) The category **Fields** of fields.

(c) The category **Finite-Groups** of *finite* groups.

(d) The category **Top** of topological spaces and continuous functions.

Solution: Fix an object X in **Sets**.

(a) If X is any set, the object X in **Sets** together with the identity map $1_X : X \to X$ is free on X: For any map $f : X \to B$, there is a unique map $g : X \to B$ such that $g \circ 1_x = f$; namely, $g = f$.

(b) Let X be any set. Let $i : X \to F$ and $f : X \to K$ be set maps, where F and K are fields with $\text{char}(K) \neq \text{char}(F)$. But $\text{Hom}(F, K) = \varnothing$. So no free object on X exists.

(c) Let $X = \{\mathfrak{D}\}$ be the one element set. Let G and H be finite groups of relatively prime order. Let $i : X \to G$ and $g : X \to H$ be set maps where $i(\mathfrak{D}) = 1_G$ and $g(\mathfrak{D}) \neq 1_H$. The only element in $\text{Hom}(G, H)$ is the trivial map $f : G \mapsto \{1_H\}$. But this map does not satisfy $f \circ i = g$ since $f(i(\mathfrak{D})) = 1_H$ but $g(\mathfrak{D}) \neq 1_H$. So no free object on X exists.

(d) Let X be any set, and $D(X)$ be the object in **Top** which has the underlying set X and is given the discrete topology. Then $D(X)$ together with the identity set map, $i : X \to D(X)$, is free on X: Given any set map $f : X \to T$ for an object T in **Top**, there exists a unique map $g : X \to T$ such that $g \circ i = f$; namely, $f = g$ since i is the identity set map. Although f is a set map, it can be considered as a continuous function $f : D(X) \to T$, since any map out of $D(X)$ is continuous.

Problem 2. *Skills developed: Construction of a categorical equivalence.*
Let K be a field, and K-Mod the category of K-modules (i.e., vector spaces). Let $R = \mathrm{Mat}_{2\times 2}(K)$ be the ring of 2×2 matrices over K, and R-Mod the category of left R-modules. We will show that K-Mod and R-Mod are equivalent categories, despite that fact that K and R are clearly not isomorphic rings.

(a) Define a map on objects $F\colon K\text{-Mod} \to R\text{-Mod}$ by sending a vector space V to the R-module $V \oplus V$, where R acts on $(v_1, v_2) \in V \oplus V$ by the standard matrix multiplication formula.
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} av_1 + bv_2 \\ cv_1 + dv_2 \end{bmatrix}$$
Show how to make F a functor in the most natural way.

Solution: For a linear map $\alpha : V \to W$ of K-modules, define $F(\alpha) : V \oplus V \to W \oplus W$ by $(v_1, v_2) \mapsto (\alpha(v_1), \alpha(v_2))$. If we have another linear map $\beta : W \to L$, then
$$F(\beta \circ \alpha)(v_1, v_2) = (\beta \circ \alpha(v_1), \beta \circ \alpha(v_2)) = F(\beta)(\alpha(v_1), \alpha(v_2)) = F(\beta)F(\alpha)(v_1, v_2).$$
In addition, $F(1_V)(v_1, v_2) = (v_1, v_2) = 1_{V\oplus V}(v_1, v_2) = 1_{F(V)}$ where 1_V is the identity linear map in V. Hence F is a covariant functor.

(b) Let e be primitive idempotent in R, for concreteness let's take $e = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$. Check (but don't turn in) that the ring eRe is isomorphic to the field K, where $a \in K$ is identified with the matrix $\left[\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right]$. Also check that eM is a left eRe-module, and thus can be considered as a K-vector space. Therefore, we can define a map on objects $G\colon R$-mod $\to K$-mod by sending an R-module M to eM. Show how to make G a functor in the most natural way.

Solution: For a morphism $f : M \to N$ in R-mod, define $G(f) : eM \to eN$ by $em \mapsto ef(m)$. If $g : N \to L$ is another R-mod hom, then
$$G(g \circ f)(em) = e(g \circ f)(m) = eg(f(m)) = G(g)(ef(m)) = G(g)G(f)(em).$$
Moreover, if $1_M : M \to M$ is the identity on M, then $G(1_M)(em) = em = 1_{eM}(em) = 1_{G(M)}(eM)$. So G is a covariant functor.

(c) It is easy to see that GF is exactly the identity functor on K-mod. (Check this but don't turn it in.) On the other hand, FG is not exactly the identity functor, but $FG(M) \simeq M$ for all $M \in R$-mod. Show that the functor FG is isomorphic to the identity functor on R-mod. This shows that R-mod and K-mod are equivalent categories.

Solution: For an R-module M, we have $FG(M) = F(eM) = eM \oplus eM$. We want a natural isomorphism $\eta : 1_{R\text{-Mod}} \implies FG$, i.e., a natural transformation η so that for any morphism $\alpha : M \to N$ in R-mod, the diagram commutes:
$$\begin{array}{ccc} M & \xrightarrow{\quad\alpha\quad} & N \\ {\scriptstyle\eta_M}\downarrow & & \downarrow{\scriptstyle\eta_N} \\ eM \oplus eM & \xrightarrow{FG(\alpha)} & eN \oplus eN \end{array}$$

Define the components of η by $\eta_M : m \mapsto (em, e'm)$ where $e' = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. Let $r = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in R$ and $m \in M$. Then

$$\eta_M(rm) = (erm, e'rm) = (\left[\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right] m, \left[\begin{smallmatrix} c & d \\ 0 & 0 \end{smallmatrix}\right] m)\,.$$

On the other hand,

$$\begin{aligned} r\eta_M(m) = r(em, e'm) = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \left[\begin{smallmatrix} em \\ e'm \end{smallmatrix}\right] &= \left[\begin{smallmatrix} aem+be'm \\ cem+de'm \end{smallmatrix}\right] \\ &= \begin{bmatrix} a\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] m + b\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] m \\ c\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] m + d\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] m \end{bmatrix} \\ &= \begin{bmatrix} \left[\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right] m \\ \left[\begin{smallmatrix} c & d \\ 0 & 0 \end{smallmatrix}\right] m \end{bmatrix}. \end{aligned}$$

So $\eta_M(rm) = r\eta_M$. It's easy to see that η_M is additive. So the components of M are indeed R-module homomorphisms.

This generalizes to $n \times n$ matrices over arbitrary rings with essentially the same proof. In general, two rings S_1, S_2 such that the categories S_1-mod and S_2-mod are equivalent are said to be "Morita equivalent" rings.

Optional challenge problem, not for credit. *Skills developed: Introduction to adjoint functors.*
Let $\mathcal{C}$ be a (concrete) category, and $Forget\colon \mathcal{C} \to \mathbf{Sets}$ the forgetful functor. If the free object on a set X exists in $\mathcal{C}$ (call it $Free(X)$), the relation between free objects and forgetful functors can be summarized by the fact that for any $A \in Ob(\mathbb{C})$, there is a bijection of sets:

$$\mathrm{Hom}_{\mathbb{C}}(Free(X), A) \cong \mathrm{Hom}_{\mathbf{Sets}}(X, Forget(A))$$

which is functorial in both X and A.

This generalizes to the concept of *adjoint functors*: Let $F\colon \mathbb{C} \to \mathbb{D}$ and and $G\colon \mathbb{D} \to \mathbb{C}$ be functors such that, for all $A \in \mathbb{C}$ and $B \in \mathbb{D}$, there is a bijection of sets

$$\mathrm{Hom}_{\mathbb{D}}(F(A), B) \cong \mathrm{Hom}_{\mathbb{C}}(A, G(B))$$

which itself is functorial in both A and B. Then F is said to be a *left adjoint* to G, which is *right adjoint* to F, and (F, G) is a pair of adjoint functors.

Let **Dom** be the category of integral domains with injective morphisms, and $G\colon \mathbf{Fields} \to \mathbf{Dom}$ be the inclusion functor. Construct a left adjoint functor F to G. (There is an essentially unique way to do this– you may have even seen it in a previous algebra course without the language of adjoint functors.) *Hint: figure out what $F(\mathbb{Z})$ is, then use this idea to get $F(R)$ for a general domain R.*

Problem 1. Fix a homomorphism of groups $f\colon A \to B$. Let $\mathcal{C}$ be the category whose objects are pairs (X, φ) such that $\varphi\colon X \to A$ is a group homomorphism satisfying $f\varphi = 0$. A morphism $(X, \varphi) \to (Y, \psi)$ in $\mathcal{C}$ is given by a group homomorphism $g\colon X \to Y$ satisfying $\varphi = \psi g$. Prove that $\mathcal{C}$ has a terminal object by explicitly describing it.

Proof. Consider the object $(\ker f, \iota)$ where $\iota : \ker f \hookrightarrow A$ is inclusion. If (X, φ) is any other object, then by assumption $f\varphi = 0$, i.e. $\operatorname{im}\varphi \subseteq \ker f$. So $g = \varphi$ is a morphism $g : (X, \varphi) \to (\ker f, \iota)$ such that $\varphi = \iota g$ since $\iota g(x) = \iota\varphi(x) = \varphi(x)$. This definition is g is obviously unique since if $\varphi = \iota\tilde{g}$, then $g = \varphi = \iota\tilde{g} = \tilde{g}$.

$$\begin{tikzcd}
A \arrow[r, "f"] & B \\
X \arrow[u, "\forall\varphi"] \arrow[r, dashed, "\exists! g"'] & \ker f \arrow[ul, "\iota"']
\end{tikzcd}$$

Problem 2. Let R be ring, and $M \in R\text{-}\mathrm{Mod}$. Define

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

(a) Prove that if R is an integral domain (a commutative ring with no zero divisors), then $\mathrm{Tor}(M)$ is a submodule of M, called the *torsion submodule*.

Proof. First $\mathrm{Tor}(M) \neq \varnothing$ since $r \cdot 0_M = 0_M$ for any $r \in R - \{0_R\}$. Let $m, n \in \mathrm{Tor}(M)$ with $r, s \in R$ nonzero such that $r \cdot m = 0_M$ and $s \cdot n = 0_M$. Since R is an integral domain, $rs \neq 0_R$ and so if $t \in R$,

$$rs \cdot (m + tn) = rs \cdot m + rs \cdot tn = s \cdot 0_M + rt \cdot 0_M = 0_M.$$

So $m + tn \in \mathrm{Tor}(M)$ and hence $\mathrm{Tor}(M)$ is a submodule of M.

(b) Prove that $\mathrm{Tor}\colon R\text{-}\mathrm{Mod} \to R\text{-}\mathrm{Mod}$ is a functor when R is an integral domain.

Proof. Since R is an integral domain and M is an R-module, then $\mathrm{Tor}(M)$ is a submodule of M by (a). If $f : M \to N$ is an $R\text{-}\mathrm{Mod}$ morphism, define $\mathrm{Tor}(f) : \mathrm{Tor}(M) \to \mathrm{Tor}(N)$ by $m \mapsto f(m)$. Since f is a morphism in $R\text{-}\mathrm{Mod}$, we have $f(\mathrm{Tor}(M)) = \mathrm{Tor}(N)$; indeed, if $m \in \mathrm{Tor}(M)$ with $r \in R$ nonzero such that $r \cdot m = 0_M$, then $r \cdot f(m) = f(r \cdot m) = f(0_M) = 0_N$. With this definition, Tor is clearly a covariant functor.

(c) Let R be the ring of 2×2 matrices over a field. Show that $\mathrm{Tor}(R)$ is not a submodule of R.
Hint: you don't even have to specify the field because you will only need the elements 0 and 1.

Proof. Let $r = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ and $s = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Then

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

So $r, s \in \mathrm{Tor}(R)$. However, $\mathrm{Tor}(R)$ is not even an additive group since $r+s \notin \mathrm{Tor}(M)$. If so, then there exists a nonzero $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in R$ such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

contradicting that $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \neq 0_R$. ☕

Problem 3. Fix a ring homomorphism $\phi : R \to S$, and let M be a left S-module. Recall from class that M can also be considered a left R-module by *restriction of scalars*: $r \cdot m = \phi(r)m$ for $r \in R,\ m \in M$. The notations ${}_SM$ and ${}_RM$ can be used to clarify whether M is being considered as an S- or R-module at any given point, but it is always the same set (this is OK since ϕ is fixed, otherwise ϕ needs to be in the notation if several ring homomorphisms $R \to S$ are relevant). Prove that ϕ induces a functor $\phi^* \colon S\text{-}\mathrm{Mod} \to R\text{-}\mathrm{Mod}$.
Hint: ϕ^* doesn't do anything to the elements of a module, it just sends ${}_SM$ to ${}_RM$, and it doesn't do anything to morphisms, they are the same maps of sets. The only thing to check is that if $f \colon M \to N$ is an S-module homomorphism, then $\phi^*(f)$ is actually an R-module homomorphism.

Proof. Define $\phi^*({}_SM) = {}_RM$, and for a morphism $f : {}_SM \to {}_SN$ of S-modules, define $\phi^*(f) : {}_RM \to {}_RN$ by $m \mapsto f(m)$. If $m, m' \in {}_RM$ and $r \in R$, then

$$\begin{aligned} \phi^*(f)(m + r \cdot m') = f(m + r \cdot m') = f(m + \phi(r)m') &= f(m) + f(\phi(r)m) \\ &= f(m) + \phi(r)f(m) \\ &= f(m) + r \cdot f(m), \end{aligned}$$

and so $\phi^*(f)$ is indeed and R-module morphism. It's clear the ϕ^* is a covariant functor:

$$\begin{aligned} &\phi^*(g \circ f)(m) = (g \circ f)(m) = g(f(m)) = \phi^*(g)(f(m)) = \phi^*(g)\phi^*(f)(m) \\ &\phi^*(1_{{}_SM})(m) = 1_M(m) = m = 1_{{}_RM}(m) = 1_{\phi^*({}_SM)}(m). \end{aligned}$$

☕

Problem 1. Prove that the following are equivalent for a ring R: (i) every left R-module is projective, (ii) every left R-module is injective.

Proof. We show that each of these statements is equivalent to the statement: *(iii)* Every short exact sequence in R-mod splits.

(i) $\iff$ (iii) If $0 \to A \hookrightarrow B \twoheadrightarrow C \to 0$ is an s.e.s., then (i) implies that $B \twoheadrightarrow C$ has a retraction, i.e., the s.e.s. splits. Conversely, if C is any R-module and $\pi : B \twoheadrightarrow C$ is any surjective map, then we get an s.e.s. $0 \to \ker \pi \hookrightarrow B \twoheadrightarrow C \to 0$, which splits by assumption. So there exists a retraction of π, showing that C is projective.

(ii) $\iff$ (iii) If $0 \to A \hookrightarrow B \twoheadrightarrow C \to 0$ is an s.e.s., then (ii) implies that $A \hookrightarrow B$ has a section, i.e., the s.e.s. splits. Conversely, if A is any R-module and $i : A \hookrightarrow B$ is any injective map, then we get an s.e.s. $0 \to A \hookrightarrow B \twoheadrightarrow B/\operatorname{im}(i) \to 0$, which splits by assumption. So there exists a section of i, showing that A is injective. ☕

Problem 2. This exercise introduces the concept of *pushout* to prove an equivalent condition for a module to be injective that was stated but not proved in class. Given homomorphisms of R-modules $g_1 \colon M \to N_1$ and $g_2 \colon M \to N_2$, the *pushout* of g_1, g_2 is the R-module

$$N_1 \oplus_M N_2 := N_1 \oplus N_2 / \{(g_1(m), -g_2(m)) \ \mid \ m \in M\}.$$

The pushout fits into a commutative diagram

$$\begin{tikzcd} M \arrow[r, "g_1"] \arrow[d, "g_2"] & N_1 \arrow[d, "f_1"] \\ N_2 \arrow[r, "f_2"] & N_1 \oplus_M N_2 \end{tikzcd}$$

where each f_i is inclusion of the summand followed by the quotient.

(a) Prove that if g_1 is injective, then f_2 is injective.

Proof. Let $L := \{(g_1(m), -g_2(m)) \ \mid \ m \in M\}$ and suppose $f_2(n) = (0_{N_1}, 0_{N_2}) + L$. From the definition of the map f_2, we find $m \in M$ so that$(g_1(m), -g_2(m)) = (0_{N_1}, n)$. Since g_1 is injective $m = 0_M$, which gives $n = -g_2(m) = 0_{N_2}$.

(b) Let Q be an R-module such that every injective map $h \colon Q \to M$ splits. Prove that Q is injective. *Hint: use an appropriate pushout and part (a).*

Proof. Given a diagram

$$\begin{tikzcd} L \arrow[r, hook, "g_1"] \arrow[d, "g_2"] & M \\ Q & \end{tikzcd}$$

we can consider the pushout of g_1, g_2:

$$\begin{tikzcd} L \arrow[r, hook, "g_1"] \arrow[d, "g_2"] & M \arrow[d, "f_1"] \\ Q \arrow[r, "f_2"] & M \oplus_L Q \end{tikzcd}$$

By hypothesis, we have a retraction of g_1, say $\pi : M \to L$. Define $f := g_2 \circ \pi$. Then $f \circ g_1 = g_2 \circ \pi \circ g_1 = g_2 \circ 1_L = g_2$, i.e., f lifts g_2 along g_1, showing that Q is injective.

$$\begin{tikzcd} L \arrow[r, hook, "g_1"] \arrow[d, "g_2"] & M \arrow[d, "f_1"] \arrow[dl, dashed, "f"'] \\ Q \arrow[r, "f_2"] & M \oplus_L Q \end{tikzcd}$$

Remark: There is a "dual" notion of pullback that can be used to prove directly the analogous characterization of projective modules, without going through the characterization that a projective module is a direct summand of a free module.

Problem 3. We proved in class that every $\mathbb{Z}$-module embeds in an injective $\mathbb{Z}$-module. In this exercise, we show that this is true for any ring S. The first optional problem below, on coextension of scalars, may be helpful. You may quote any of those results without proving them.

(a) If Q is an injective $\mathbb{Z}$-module, prove that $\operatorname{Hom}_{\mathbb{Z}}(S,Q)$ (coextension of scalars from $\mathbb{Z}$ to S) is an injective S-module.

Proof. Suppose we have a diagram
$$\begin{tikzcd} L \arrow[r, hook, "\psi"] \arrow[d, "h"'] & M \\ \operatorname{Hom}_{\mathbb{Z}}(S,Q) & \end{tikzcd}$$

Using the map p from the first optional problem below, we can extend this diagram and, using the injectivity of Q, we find a $\mathbb{Z}$-module homomorphism g such that $p \circ h = g \circ \psi$.

$$\begin{tikzcd} L \arrow[r, hook, "\psi"] \arrow[d, "h"'] & M \arrow[ddl, "g"] \\ \operatorname{Hom}_{\mathbb{Z}}(S,Q) \arrow[d, "p"'] & \\ Q & \end{tikzcd}$$

In the first optional problem below, we prove that there exists a unique map f from M to $\operatorname{Hom}_{\mathbb{Z}}(S,Q)$ such that $p \circ f = g$, defined by $f : m \mapsto (f_m : s \mapsto g(s.m))$. So, $p \circ h = p \circ f \circ \psi$. Now let $\ell \in L$, $s \in S$ and put $h(\ell) = h_\ell$. Then

$$f_{\psi(\ell)}(s) = sf_{\psi(\ell)}(1_S) = sp(f_{\psi(\ell)}) = sp(h_\ell) = sh_\ell(1_s) = h_\ell(s),$$

showing that f lifts h along ψ, and so $\operatorname{Hom}_{\mathbb{Z}}(S,Q)$ is injective.

$$\begin{tikzcd} L \arrow[r, hook, "\psi"] \arrow[d, "h"'] & M \arrow[dl, dashed, "f"'] \arrow[ddl, "g"] \\ \operatorname{Hom}_{\mathbb{Z}}(S,Q) \arrow[d, "p"'] & \\ Q & \end{tikzcd}$$

(b) Let M be an arbitrary S-module, and Q be an injective $\mathbb{Z}$-module containing M. Find an injective map $i \colon M \to \operatorname{Hom}_{\mathbb{Z}}(S,Q)$.

Solution:

Define a map $f : M \to \operatorname{Hom}_{\mathbb{Z}}(S,M)$ by $m \mapsto (f_m : s \mapsto s.m)$. If $s_1, s_2 \in S$ and $n \in \mathbb{Z}$, then $f_m(s_1 + ns_2) = s_1.m + ns_2.m = f_m(s_1) + nf_m(s_2)$, so f_m is a $\mathbb{Z}$-module homomorphism. If $f_m(s) = f_{m'}(s)$ for all $s \in S$, then $s.m = s.m'$ implies $m = m'$, so f is injective. Now, since $M \subseteq Q$ then $\operatorname{Hom}_{\mathbb{Z}}(S,M) \subseteq \operatorname{Hom}_{\mathbb{Z}}(S,Q)$, and so we can define

$$i : M \overset{f}{\hookrightarrow} \operatorname{Hom}_{\mathbb{Z}}(S,M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(S,Q).$$

Optional problem, not for credit.

(a) Let $\varphi\colon R \to S$ be a ring homomorphism. Show how $\varphi_* M := \mathrm{Hom}_{R\text{-mod}}(S, M)$ is a functor from the category of left R-modules to the category of left S-modules. Start by giving the specific left S-module action on $\varphi_* M$. *Note: we did not prove this completely in class, only discussed the idea. Part of the problem is to show that $\varphi_* M$ is actually a left S-module.*

Solution:

For $\alpha \in \mathrm{Hom}_R(S, N)$ and $s \in S$, define $s.\alpha := (s\alpha : t \mapsto \alpha(ts))$. Let $s_1, s_2 \in S$, $r \in R$. Notice that $(r.s_2)s = (\varphi(r)s_2)s = \varphi(r)(s_2 s) = r.s_2 s$. So

$$s\alpha(s_1 + r.s_2) = \alpha(s_1 s + (r.s_2)s) = \alpha(s_1 s + r.(s_2 s)) = s\alpha(s_1) + r.s\alpha(s_2),$$

and so $s\alpha \in Hom_R(S, N)$. Moreover

$$\begin{aligned} & s_1.(s_2.\alpha) = s_1(s_2\alpha : t \mapsto \alpha(ts_2)) = (s_1 s_2 \alpha : t \mapsto s_2\alpha(ts_1) = \alpha(ts_1 s_2)) = s_1 s_2.\alpha, \\ \text{and} \qquad & 1_S.\alpha = (1_S\alpha : t \mapsto \alpha(t1_S) = \alpha(t)) = \alpha, \end{aligned}$$

shows that this rule gives an S-module structure on $\mathrm{Hom}_R(S, N)$.

For f in R-Mod, define $\varphi_* f = f_*$. If $M \xrightarrow{f} N \xrightarrow{g} L$ is in R-Mod, and α is in $\mathrm{Hom}_R(S, M)$, then

$$\begin{aligned} & (\varphi_*(g \circ f))(\alpha) = (g \circ f)_*(\alpha) = g \circ f \circ \alpha = (g_* \circ f_*)(\alpha) = (\varphi_*(g) \circ \varphi_*(f))(\alpha), \\ \text{and} \qquad & \varphi_*(1_M)(\alpha) = (1_M)_*(\alpha) = 1_M \circ \alpha = \alpha = 1_{\mathrm{Hom}_R(S,M)}(\alpha) = 1_{\varphi_* M}(\alpha). \end{aligned}$$

Hence $\varphi_* : R\text{-Mod} \to S\text{-Mod}$ is a covariant functor.

(b) For any ${}_R N$, there is a canonical homomorphism of left R-modules

$$p\colon \varphi_* N = \mathrm{Hom}_R(S, N) \to N \qquad h \mapsto h(1).$$

Check, but don't write up, that this is actually a homomorphism of left R-modules. Then prove that for any left S-module M, and given homomorphism of left R-modules $g\colon M \to N$, there is a unique homomorphism of left S-modules $f\colon M \to \varphi_* N$ such that $g = p \circ f$.

Proof. Define $f : M \to \mathrm{Hom}_R(S, N)$ by the rule $m \mapsto (f_m : s \mapsto g(s.m))$.

$$\begin{tikzcd} & M \arrow[dl, dashed, "f"'] \arrow[ddl, "g"] \\ \mathrm{Hom}_R(S,Q) \arrow[d, "p"'] & \\ Q & \end{tikzcd}$$

If $m_1, m_2 \in M$, and $s, t \in S$ then

$$(f_{m_1} + s.f_{m_2})(t) = f_{m_1}(t) + s.f_{m_2}(t) = f_{m_1}(t) + f_{m_2}(ts) = g(t.m_1) + g(ts.m_2),$$

and on the other hand

$$(f(m_1 + s.m_2))(t) = f_{m_1+s.m_2}(t) = g(t.m_1 + t.(s.m_2)) = g(t.m_1) + g(ts.m_2),$$

which shows that f is an S-module homomorphism. Moreover,

$$p(f(m)) = f_m(1_S) = g(1_S.m) = g(m).$$

(c) Let $\varphi\colon \mathbb{C}[x] \to \mathbb{C}$ be the quotient ring homomorphism with kernel generated by x. Give a general description of $\varphi_* M$ for any $\mathbb{C}[x]$-module M. *It may help to compute some examples such as* $\varphi_*\left(\frac{\mathbb{C}[x]}{(x^n)}\right)$, $\varphi_*\left(\frac{\mathbb{C}[x]}{((x-1)^n)}\right)$, $\varphi_*\mathbb{C}[x]$.

Optional challenge problem, not for credit. Find the universal property that the pushout satisfies. Create a category for which the pushout is a coproduct.

Problem 1. In this problem we generalize some familiar facts about dimensions of vector spaces to length of modules.

(a) Prove that "length is additive on short exact sequences": let $0 \to A \to B \to C \to 0$ be a short exact sequence of left R-modules, and suppose that B is of finite length. Prove that $\ell(B) = \ell(A) + \ell(C)$.

Proof. Let

$$0 = A_0 \subset A_1 \subset \cdots \subset A_{\ell(A)} = A \subseteq B$$

be a composition series for A inside B. Extend this to get a composition series in B:

$$0 = A_0 \subset A_1 \subset \cdots \subset A_{\ell(A)} = A \subset B_1 \subset B_2 \cdots \subset B_n = B.$$

So $\ell(B) = \ell(A) + n$, and $A \subset B_1 \subset B_2 \cdots \subset B_n = B$ consists of *all* the submodules of B containing A. Then by the correspondence isomorphism theorem, we have a chain in $\overline{B} = B/A$

$$\overline{0} = \overline{A} \subset \overline{B_1} \subset \overline{B}_2 \subset \cdots \subset \overline{B_n} = \overline{B}.$$

By the cancellation isomorphism theorem,

$$\overline{B}_1/\overline{A} \cong B_1/A \quad \text{and} \quad \overline{B}_{i+1}/\overline{B}_i \cong B_{i+1}/B_i \quad \text{for all } 2 \leq i \leq n-1.$$

so the chain in $\overline{B}$ has all simple factors, giving a composition series for $\overline{B}$. So

$$\overline{B} = n = \ell(B) - \ell(A).$$

Since $B/A \cong C$, then $\ell(C) = \ell(B) - \ell(A)$.

(b) Use (a) to prove the "sum-intersection formula" for modules of finite length: if $K, N \subseteq M$ are submodules and have finite length, then

$$\ell(K + N) + \ell(K \cap N) = \ell(K) + \ell(N).$$

The point of the exercise is use (a) to prove this– don't try to do it by explicitly considering chains in all these spaces.

Proof. We have the exact sequences

$$0 \longrightarrow N \longrightarrow K + N \longrightarrow \frac{K+N}{N} \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow K \cap N \longrightarrow K \longrightarrow \frac{K}{K \cap N} \longrightarrow 0,$$

so by part (a),

$$\ell(K + N) = \ell(N) + \ell\left(\frac{K+N}{N}\right) \quad \text{and} \quad \ell\left(\frac{K}{K \cap N}\right) = \ell(K) - \ell(K \cap N).$$

By the lattice isomorphism theorem, we get $\ell\left(\frac{K+N}{N}\right) = \ell\left(\frac{K}{K \cap N}\right)$, and so

$$\ell(K + N) + \ell(K \cap N) = \ell(N) + \ell(K).$$

Problem 2. This problem generalizes the fact that a linear operator on a finite dimensional vector space is injective if and only if it is surjective if and only if it is an isomorphism. Prove (a) carefully. For (b), just briefly indicate the main ideas of a proof (a few sentences).

(a) Let M be a Noetherian left R-module, and $f\colon M \to M$ a surjective homomorphism. Show that f must be an isomorphism.

Proof. We have a chain

$$\ker f \subseteq \ker f^2 \subseteq \ker f^3 \subseteq \cdots \subseteq M,$$

and since M is Noetherian, there exists an n so that $\ker f^n = \ker f^k$ for all $k \geq n$. We claim that $\ker f^n = \{0_M\}$, which will give $\ker f = 0$.

Notice that $\ker f^n = ker f^n \cap M = \ker f^n \cap \operatorname{im} f^n$ since f is surjective. Suppose $m \in \ker f^n$. Then there exists $m' \in M$ so that $f^n(m') = m$. Then

$$0 = f^n(m) = f^n(f^n(m') = f^{2n}(m') \implies m' \in \ker f^{2n} = \ker f^n,$$

so $0 = f^n(m') = m$. ☕

(b) Let N be an Artinian left R-module, and $g\colon N \to N$ an injective homomorphism. Show that g must be an isomorphism.

Proof. Consider the descending chain $M \supseteq \operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \operatorname{im} f^3 \supseteq \ldots$, which stabilizes since N is Artinian; say $\operatorname{im} f^n = \operatorname{im} f^{n+1}$. If $x \in N$, then $f^n(x) \in \operatorname{im} f^{n+1}$, so there exists $x' \in N$ so that $f^n(f(x')) = f^n(x)$. Since f^n is injective, $f(x') = x$. ☕

Problem 3. Let R be a commutative ring, not necessarily Noetherian, and M a Noetherian R-module. Let $I = \operatorname{ann}_R(M)$. Prove that R/I is a Noetherian ring.
Question for thought, not graded: if "Noetherian" is replaced by "Artinian" in this problem, would the statement be true?

Proof.

After spending way too much time on this problem, I looked online. I was close, but just couldn't finish the argument. I'm pretty disappointed.

Since M is Noetherian, it is finitely generated and so we can write $M = \sum_{i=1}^n Rm_i$ for $m_i \in M$. Define an R-module homomorphism

$$\varphi : R \to M \oplus \cdots \oplus M, \quad r \mapsto (rm_1, \ldots, rm_n).$$

Then $\ker \varphi = \{r \in R : rm_i = 0\ \forall i\} = I$, so we get a well-defined and injective map $R/I \to M \oplus \cdots \oplus M$. So R/I is isomorphic to a submodule of the Noetherian module $M \oplus \cdots \oplus M$, and hence R/I is Noetherian. ☕

Problem 4. Let $R = M_2(K[[t]])$ be the ring of 2×2 matrices with entries in $K[[t]]$, the ring of formal power series over a field K (defined in class and on the last homework). Let $\mathfrak{m} = (t)$ be the unique maximal ideal of $K[[t]]$, consisting of power series with 0 constant term. Let $S \subseteq R$ be the subring of matrices of the form

$$\begin{bmatrix} K[[t]] & K[[t]] \\ \mathfrak{m} & K[[t]] \end{bmatrix}.$$

These are matrices that are "upper-triangular modulo t". Prove that the Jacobson radical of S is

$$J(S) = \begin{bmatrix} \mathfrak{m} & K[[t]] \\ \mathfrak{m} & \mathfrak{m} \end{bmatrix}.$$

Hint: you can show $J(S)$ is contained in the right hand side by finding two simple S-modules (both 1-dimensional over K) and showing that the intersection of their annihilators is the right hand side. These may take some work to find, they are not exactly the same as modules appearing in other examples in class. Then you can show the right hand side is contained in the left imitating techniques demonstrated in class for upper triangular matrices.

Proof. Let $\left[\begin{smallmatrix} \mathfrak{m} & K[[t]] \\ \mathfrak{m} & \mathfrak{m} \end{smallmatrix}\right] = U$. Let $x \in U$ and $r, s \in S$ with $r_i, x_i, s_i \in K[[t]]$ for all $1 \leq i \leq 4$. Then

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \underbrace{\begin{bmatrix} r_1 & r_2 \\ tr_3 & r_4 \end{bmatrix}}_{=r} \underbrace{\begin{bmatrix} tx_1 & x_2 \\ tx_3 & tx_4 \end{bmatrix}}_{=x} \underbrace{\begin{bmatrix} s_1 & s_2 \\ ts_3 & s_4 \end{bmatrix}}_{=s}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} r_1tx_1 + r_2tx_3 & r_1x_2 + r_2tx_4 \\ tr_3tx_1 + r_4tx_3 & tr_3x_2 + r_4tx_4 \end{bmatrix} \begin{bmatrix} s_1 & s_2 \\ ts_3 & s_4 \end{bmatrix}$$

$$= \begin{bmatrix} 1 + (r_1tx_1 + r_2tx_3)s_1 + (r_1x_2 + r_2tx_4)ts_3 & (r_1tx_1 + r_2tx_3)s_2 + (r_1x_2 + r_2tx_4)s_4 \\ (tr_3tx_1 + r_4tx_3)s_1 + (tr_3x_2 + r_4tx_4)ts_3 & 1 + (tr_3tx_1 + r_4tx_3)s_2 + (tr_3x_2 + r_4tx_4)s_4 \end{bmatrix}$$

Since the product of the anti-diagonal elements of $1 + rxs$ is in $\mathfrak{m}$ and the product of the diagonal elements has constant term 1, then $\det(1 + rxs)$ has constant term 1, hence $\det(1 + rxs) \notin \mathfrak{m}$. Since $\mathfrak{m}$ contains precisely the non-units of $K[[t]]$, then $\det(1 + rxs)$ is invertible, and hence $1 + rxs$ is invertible, so $U \subseteq J(S)$.

Conversely, by restriction of scalars via the map $\varphi : S \to \overline{S}, t \mapsto 0$, the left $\overline{S}$-module

$$M_1 := \begin{bmatrix} K \\ 0 \end{bmatrix} = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} : x \in K \right\}$$

becomes a left S-module. Viewing K inside $\overline{S}$ as scalar multiples of the identity, M_1 is 1-dimensional over K, and hence simple. So M_1 is simple as an S-module. The annihilator of M_1 in $\overline{S}$ is

$$\operatorname{ann}_{\overline{S}}(M_1) = \begin{bmatrix} \mathfrak{m} & K[[t]] \\ \mathfrak{m} & K[[t]] \end{bmatrix}.$$

Viewing K^2 as 2-vectors with entries in K, we have that K^2 is a left $\overline{S}$-module. We have a chain of submodules $0 \subset M_1 \subset K^2$, and since $M_2 = K^2/M_1$ has dimension 1 over K, it's a simple K module, and so M_2 is a simple $\overline{S}$-module, and therefore a simple S module. Now

$$M_2 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} K \\ 0 \end{bmatrix} \right\} = \left\{ \begin{bmatrix} 0 \\ y \end{bmatrix} + \begin{bmatrix} K \\ 0 \end{bmatrix} \right\}.$$

And we have $\operatorname{ann}_{\overline{S}}(M_2) = \left[\begin{smallmatrix} K[[t]] & K[[t]] \\ \mathfrak{m} & \mathfrak{m} \end{smallmatrix}\right]$. So we get $J(S) \subset \operatorname{ann}_{\overline{S}}(M_1) \cap \operatorname{ann}_{\overline{S}}(M_2) = U$. ☕