Math 762 **Spring 2016**
Homework 4 **Drew Armstrong**

Problem 1. Cokernel of a Direct Sum. Here's something that confused me in class, so I'll have you prove it. (Just like you have to wear a coat when your mother is cold.) Let R be a ring and suppose we have a homomorphism $\varphi : M_1 \oplus M_2 \to N_1 \oplus N_2$ of R-modules. Since $\oplus$ is both the product **and** the coproduct in R-Mod, there exist canonical injections and projections as in the following diagram:

$$\begin{tikzcd}
M_1 \arrow[dr, "\iota_1"] \arrow[rrr, "\varphi_{11}"] & & & N_1 \\
& M_1 \oplus M_2 \arrow[r, "\varphi"] & N_1 \oplus N_2 \arrow[ur, "\pi_1"] \arrow[dr, "\pi_2"] & \\
M_2 \arrow[ur, "\iota_2"] \arrow[rrr, "\varphi_{22}"] & & & N_2
\end{tikzcd}$$

Define the "component homomorphisms" $\varphi_{ij} := \pi_i \circ \varphi \circ \iota_j : M_j \to N_i$ for $i, j \in \{1, 2\}$ and assume that φ_{12} and φ_{21} are both the zero map. In this case prove that we have an isomorphism

$$\frac{N_1 \oplus N_2}{\operatorname{im}\varphi} \approx \frac{N_1}{\operatorname{im}\varphi_{11}} \oplus \frac{N_2}{\operatorname{im}\varphi_{22}}.$$

Proof. First note that the map φ is uniquely determined by its components $\varphi_{11}, \varphi_{12}, \varphi_{21}, \varphi_{22}$. Indeed, by the universal property of the **coproduct** $M_1 \oplus M_2$ we see that φ is uniquely determined by the maps $\varphi_{*1} := \varphi \circ \iota_1$ and $\varphi_{*2} := \varphi \circ \iota_2$. Then from the universal property of the **product** $N_1 \oplus N_2$ we see that the map φ_{*1} is uniquely determined by the maps $\varphi_{11} = \pi_1 \circ \varphi_{*1}$ and $\varphi_{21} = \pi_2 \circ \varphi_{*1}$. Similarly, φ_{*2} is uniquely determined by φ_{12} and φ_{22}. In summary, for a general element $m = m_1 + m_2 \in M_1 \oplus M_2$ we have

$$\begin{aligned}
\varphi(m) &= \varphi(m_1 + m_2) \\
&= \varphi_{*1}(m_1) + \varphi_{*2}(m_2) \\
&= (\varphi_{11}(m_1) + \varphi_{21}(m_1)) + (\varphi_{12}(m_2) + \varphi_{22}(m_2)) \\
&= (\varphi_{11}(m_1) + \varphi_{12}(m_2)) + (\varphi_{21}(m_1) + \varphi_{22}(m_2)).
\end{aligned}$$

But we can make this clearer using matrix notation:

$$\varphi(m) = \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} \varphi_{11}(m_1) + \varphi_{12}(m_2) \\ \varphi_{21}(m_1) + \varphi_{22}(m_2) \end{pmatrix}.$$

Then since we have assumed that φ_{12} and φ_{21} are the zero maps this simplifies to

$$\varphi(m) = \begin{pmatrix} \varphi_{11} & 0 \\ 0 & \varphi_{22} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} \varphi_{11}(m_1) \\ \varphi_{22}(m_2) \end{pmatrix},$$

and it follows that $\operatorname{im}\varphi = \operatorname{im}\varphi_{11} \oplus \operatorname{im}\varphi_{22}$.

Next consider the quotient maps $p_1 : N_1 \twoheadrightarrow N_1/\operatorname{im}\varphi_{11}$ and $p_2 : N_2 \twoheadrightarrow N_2/\operatorname{im}\varphi_{22}$. Composing these with π_1 and π_2 gives us two maps

$$\begin{aligned}
p_1 \circ \pi_1 &: N_1 \oplus N_2 \to N_1/\operatorname{im}\varphi_{11}, \\
p_2 \circ \pi_2 &: N_1 \oplus N_2 \to N_2/\operatorname{im}\varphi_{22},
\end{aligned}$$

and then from the universal property of the coproduct there exists a unique homomorphism Φ such that the following diagram commutes:

$$\begin{tikzcd}
 & N_1 \arrow[r, "p_1"] & N_1/\operatorname{im}\varphi_{11} \\
N_1 \oplus N_2 \arrow[ur, bend left, "\pi_1"] \arrow[dr, bend right, "\pi_2"'] \arrow[r, dashed, "\Phi"] & \frac{N_1}{\operatorname{im}\varphi_{11}} \oplus \frac{N_2}{\operatorname{im}\varphi_{22}} \arrow[ur] \arrow[dr] & \\
 & N_2 \arrow[r, "p_2"'] & N_2/\operatorname{im}\varphi_{22}
\end{tikzcd}$$

In terms of matrix notation we have

$$\Phi(n) = \Phi \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{pmatrix} n_1 + \operatorname{im}\varphi_{11} \\ n_2 + \operatorname{im}\varphi_{22} \end{pmatrix},$$

and it follows that Φ is a surjective homomorphism with $\ker \Phi = \operatorname{im}\varphi_{11} \oplus \operatorname{im}\varphi_{22}$. Finally, the 1st Isomorphism Theorem tells us that

$$\frac{N_1}{\operatorname{im}\varphi_{11}} \oplus \frac{N_2}{\operatorname{im}\varphi_{22}} = \operatorname{im}\Phi \cong \frac{N_1 \oplus N_2}{\ker \Phi} = \frac{N_1 \oplus N_2}{\operatorname{im}\varphi_{11} \oplus \operatorname{im}\varphi_{22}} = \frac{N_1 \oplus N_2}{\operatorname{im}\varphi}.$$

□

[Remark: I'm still unhappy about this. Clearly the matrix notation is the correct way to think about the problem, but one must first **justify** the matrix notation from the universal properties. Apparently, this is a game that can be played in any additive category; unfortunately, I couldn't find a convincing exposition anywhere. After all these years matrices still seem like magic.]

Problem 2. Chinese Remainder Theorem for PIDs. Let R be a PID and consider any element $a \in R$ with unique prime factorization $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d}$.

(a) Prove that there exist elements $r_1, \ldots, r_d \in R$ such that the following identity holds in the field of fractions:
$$\frac{1}{a} = \frac{r_1}{p_1^{\alpha_1}} + \cdots + \frac{r_d}{p_d^{\alpha_d}}.$$
[Hint: Use induction on d.]

(b) Use part (a) to construct an isomorphism of R-modules
$$\frac{R}{(a)} \approx \frac{R}{(p_1^{\alpha_1})} \oplus \cdots \oplus \frac{R}{(p_d^{\alpha_d})}.$$

Proof. (a): Let R be a PID and consider two coprime elements $p, q \in R$ (that is, assume that p and q have no common non-unit divisor). Now consider the ideal

$$(p, q) := \{ax + by : x, y \in R\}.$$

Since R is a PID we must have $(p,q) = (r)$ for some $r \in R$. If $(r) \neq (1)$ then since $(p) \subseteq (p,q) = (r)$ and $(q) \subseteq (p,q) = (r)$ we see that r is a common non-unit divisor of p and q, which is a contradiction. We conclude that $(p,q) = (r) = (1)$ and hence there exist $x, y \in R$ such that $1 = px + qy$.

Now consider any element $a \in R$ with prime factorization $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d}$. First note that $p_1^{\alpha_1}$ and $a/p_1^{\alpha_1} = p_2^{\alpha_2} \cdots p_d^{\alpha_d}$ are coprime so by the above remarks there exist $r_1, r_1' \in R$ such that

$$1 = r_1(p_2^{\alpha_2} \cdots p_d^{\alpha_d}) + r_1' p_1^{\alpha_1}.$$

We can divide both sides by a to get

$$\frac{1}{a} = \frac{r_1}{p_1^{\alpha_1}} + \frac{r_1'}{p_2^{\alpha_2} \cdots p_d^{\alpha_d}}$$

and then by induction on d there exist elements $r_2', \ldots, r_d' \in R$ such that

$$\frac{1}{p_2^{\alpha_2} \cdots p_d^{\alpha_d}} = \frac{r_2'}{p_2^{\alpha_2}} + \cdots + \frac{r_d'}{p_d^{\alpha_d}}.$$

Finally, combining the two previous equations gives

$$\frac{1}{a} = \frac{r_1}{p_1^{\alpha_1}} + \cdots + \frac{r_d}{p_d^{\alpha_d}} \tag{1}$$

where $r_i := r_1' r_i' \in R$ for $i \in \{2, \ldots, d\}$.

(b): Let $a \in R$ be as above. We have an obvious homomorphism of R-modules

$$\Phi : R \to \frac{R}{(p_1^{\alpha_1})} \oplus \cdots \oplus \frac{R}{(p_d^{\alpha_d})}$$

defined by $\Phi(s) := (s + (p_1^{\alpha_1}), s + (p_2^{\alpha_2}), \ldots, s + (p_d^{\alpha_d}))$ and the kernel of this homomorphism is obviously the intersection of ideals:

$$\ker \Phi = (p_1^{\alpha_1}) \cap (p_2^{\alpha_2}) \cap \cdots \cap (p_d^{\alpha_d}).$$

If we can show that $\ker \Phi = (a)$ and that Φ is surjective then we will be done by the 1st Isomorphism Theorem.

First we will show that $\ker \Phi = (a)$. Indeed, for each i we know that $p_i^{\alpha_i}$ divides a and hence we have $(a) \subseteq (p_i^{\alpha_i})$. Then from the universal property of intersection it follows that $(a) \subseteq \ker \Phi$. Conversely, since R is a PID we have $\ker \Phi = (r)$ for some $r \in R$. Since $\ker \Phi \subseteq (p_i^{\alpha_i})$ this implies that $p_i^{\alpha_i}$ divides r for each i. Now consider the following general argument: If elements $p, q \in R$ both divide an element $r \in R$ then there exist elements $k, \ell \in R$ such that $r = pk$ and $r = q\ell$. If in addition p, q are coprime then from part (a) there exist elements $x, y \in R$ such that $1 = px + qy$. Now multiply both sides of this equation by r to get

$$\begin{aligned} r &= rpx + rqy \\ &= (q\ell)px + (pk)qy \\ &= (pq)\ell x + (pq)ky \\ &= pq(\ell x + ky). \end{aligned}$$

In summary, if p, q both divide r and if p, q are coprime then their product pq divides r. Going back to our problem, we know that each $p_i^{\alpha_i}$ divides r and that the elements $p_i^{\alpha_i}, p_j^{\alpha_j}$ are coprime for $i \neq j$. By induction this implies that their product a divides r, and hence $\ker \Phi = (r) \subseteq (a)$.

Next we will show that Φ is surjective. (This is the actual hard part, which goes back to Sun Tzu in the 3rd century A.D.) To do this we first multiply boths sides of equation (1) by a to obtain

$$1 = r_1 a_1' + r_2 a_2' + \cdots + r_d a_d', \tag{2}$$

where $a_i' := a/p_i^{\alpha_i} = \prod_{i \neq j} p_j^{\alpha_j} \in R$ for each i. Now consider an arbitrary element

$$(s_1 + (p_1^{\alpha_1}), s_2 + (p_2^{\alpha_2}), \ldots, s_d + (p_d^{\alpha_d}))$$

of the codomain of Φ. I claim that this element equals $\Phi(s)$ for the special element

$$s := s_1 r_1 a_1' + s_2 r_2 a_2' + \cdots + s_d r_d a_d' \in R.$$

Indeed, since a_i' is divisible by $p_j^{\alpha_j}$ for all $i \neq j$ we see that $s + (p_i^{\alpha_i}) = s_i r_i a_i' + (p_i^{\alpha_i})$. But then from (2) we have

$$r_i a_i' = 1 - \sum_{i \neq j} r_j a_j'$$

and it follows that

$$s + (p_i^{\alpha_i}) = s_i r_i a_i' + (p_i^{\alpha_i}) = s_i - s_i \sum_{i \neq j} r_j a_j' + (p_i^{\alpha_i}) = s_i + (p_i^{\alpha_i}),$$

as desired. Pretty clever, right? □

[Remark: We will use the same clever trick on Problem 4.]

Problem 3. Idempotents = Internal Direct Sums. Let R be any ring and let M be a (left) R-module. Let $E = \mathrm{End}_R(M)$ be the (noncommutative) ring of endomorphisms. We say that an endomorphism $e \in E$ is idempotent if $e^2 = e \circ e = e$.

(a) Given $e \in E$, prove that e is idempotent if and only if $\mathrm{id} - e$ is idempotent. We call this an orthogonal pair of idempotents because $e \circ (\mathrm{id} - e) = (\mathrm{id} - e) \circ e = 0$.

(b) If $e \in E$ is idempotent, prove that M decomposes as a direct sum of R-submodules

$$M = \mathrm{im}\, e \oplus \mathrm{im}\, (\mathrm{id} - e).$$

(c) Conversely, if $M = M_1 \oplus M_2$ is a direct sum of (left) R-submodules prove that there exist idempotents $e_1, e_2 \in E$ such that $\mathrm{im}\, e_1 = M_1$, $\mathrm{im}\, e_2 = M_2$, $e_1 + e_2 = \mathrm{id}$ and $e_1 \circ e_2 = e_2 \circ e_1 = 0$. [Hint: Think of $\oplus$ as the product in R-Mod.]

Proof. (a): Consider $e \in E = \mathrm{End}_R(M)$. If $e^2 = e$ then we have

$$\begin{aligned}
(\mathrm{id} - e)^2 &= (\mathrm{id} - e) \circ (\mathrm{id} - e) \\
&= \mathrm{id} \circ \mathrm{id} - e \circ \mathrm{id} - \mathrm{id} \circ e + e \circ e \\
&= \mathrm{id} - e - \cancel{e} + \cancel{e} \\
&= (\mathrm{id} - e).
\end{aligned}$$

Conversely, suppose that $(\mathrm{id} - e)^2 = (\mathrm{id} - e)$. Then by the same argument it follows that $e = (\mathrm{id} - (\mathrm{id} - e))$ is idempotent. Finally, if $e^2 = e$ we note that

$$e \circ (\mathrm{id} - e) = e \circ \mathrm{id} - e \circ e = e - e = 0$$

and

$$(\mathrm{id} - e) \circ e = \mathrm{id} \circ e - e \circ e = e - e = 0.$$

(b): Now suppose that $e \in E$ is idempotent. In this case I claim that M decomposes as a direct sum $M = \mathrm{im}\, e \oplus \mathrm{im}\, (\mathrm{id} - e)$. To see this, first note that for all $m \in M$ we have

$$\begin{aligned}
m = \mathrm{id}(m) &= (e + (\mathrm{id} - e))(m) \\
&= e(m) + (\mathrm{id} - e)(m) \\
&\in \mathrm{im}\, e + \mathrm{im}\, (\mathrm{id} - e),
\end{aligned}$$

hence $M = \mathrm{im}\, e + \mathrm{im}\, (\mathrm{id} - e)$. Next consider any element $m \in \mathrm{im}\, e \cap \mathrm{im}\, (\mathrm{id} - e)$, i.e., such that there exist $n_1, n_2 \in M$ with $m = e(n_1) = (\mathrm{id} - e)(n_2)$. Applying e to both sides gives

$$\begin{aligned}
(e \circ e)(n_1) &= (e \circ (\mathrm{id} - e))(n_2) \\
e(n_1) &= 0(n_2) \\
e(n_1) &= 0,
\end{aligned}$$

and hence $m = e(n_1) = 0$. We conclude that $\mathrm{im}\, e \cap \mathrm{im}\, (\mathrm{id} - e) = 0$, as desired.

(c): Finally, suppose that we have submodules $M_1, M_2 \subseteq M$ such that $M = M_1 \oplus M_2$. We will think of this as a categorical product with canonical projections $\pi_1 : M_1 \oplus M_2 \to M_1$ and $\pi_2 : M_1 \oplus M_2 \to M_2$. By the universal property, there exists a unique endomorphism $e_1 : M_1 \oplus M_2 \to M_1 \oplus M_2$ such that the following diagram commutes:

$$\begin{tikzcd}
 & & M_1 \\
M_1 \oplus M_2 \arrow[r, dashed, "e_1"] \arrow[urr, bend left, "\pi_1"] \arrow[drr, bend right, "0"'] & M_1 \oplus M_2 \arrow[ur, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
 & & M_2
\end{tikzcd}$$

Similarly, there exists a unique endomorphism $e_2 : M_1 \oplus M_2 \to M_1 \oplus M_2$ such that

$$\begin{tikzcd}
 & & M_1 \\
M_1 \oplus M_2 \arrow[r, dashed, "e_2"] \arrow[urr, bend left, "0"] \arrow[drr, bend right, "\pi_2"'] & M_1 \oplus M_2 \arrow[ur, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
 & & M_2
\end{tikzcd}$$

I claim that e_1, e_2 is the desired pair of orthogonal idempotents. The proof of this is immediate after we observe how e_1, e_2 behave in terms of the matrix notation from Problem 1. That is, observe that for all elements $m = (m_1, m_2) \in M_1 \oplus M_2$ we have

$$e_1(m) = \begin{pmatrix} \mathrm{id} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} m_1 \\ 0 \end{pmatrix} \quad \text{and} \quad e_2(m) = \begin{pmatrix} 0 & 0 \\ 0 & \mathrm{id} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} 0 \\ m_2 \end{pmatrix}.$$

$\square$

[Remark: This is a very important and basic observation that somehow never gets treated in algebra textbooks. I don't know why. You can find it in books on algebraic geometry or representation theory, but they will assume there that you already know it. Actually, there is a lot of "advanced linear algebra" that falls into this gap, including the following two problems.]

Problem 4. Generalized Eigenspaces of a Matrix. Let K be a field and consider a matrix $A \in \mathrm{Mat}_n(K)$. Let $\varphi_A : K[x] \to \mathrm{Mat}_n(K)$ be the canonical homomorphism from the free algebra $K[x]$ $(= K\langle x \rangle)$. Since $K[x]$ is a PID we know that the kernel has the form $\ker \varphi_A = (m_A(x))$ for some unique monic polynomial $m_A(x)$ called the minimal polynomial of A. Let $m_A(x) = f_1(x)^{m_1} \cdots f_d(x)^{m_d}$ be the unique factorization into irreducible polynomials (note that $m_A(x)$ is not necessarily irreducible because $\mathrm{Mat}_n(K)$ is not an integral domain). Then by Problem 2 there exist polynomials $g_i(x) \in K[x]$ such that

$$\frac{1}{m_A(x)} = \sum_i \frac{g_i(x)}{f_i(x)^{m_i}}. \tag{3}$$

For each i we define the polynomial $p_i(x) := m_A(x) g_i(x) / f_i(x)^{m_i} = g_i(x) \prod_{i \neq j} f_j(x)^{m_j}$ and the matrix $P_i := p_i(A) = \varphi_A(p_i(x)) \in \mathrm{Mat}_n(K)$.

(a) Prove that we have $\sum_i P_i = I$.

(b) Prove that for $i \neq j$ we have $P_iP_j = 0$.
(c) Prove that for all i we have $P_i^2 = P_i$. [Hint: Use (a) and (b).]
(d) Conclude from Problem 3 that we have a direct sum decomposition of K-subspaces

$$K^n = \bigoplus_{i=1}^{d} \operatorname{im} P_i.$$

Proof. (a): Multiplying both sides of equation (3) by $m_A(x)$ gives

$$1 = p_1(x) + \cdots + p_d(x)$$

and then applying φ_A to both sides gives

$$\begin{aligned} I = \varphi_A(1) &= \varphi_A(p_1(x) + \cdots + p_d(x)) \\ &= \varphi_A(p_1(x)) + \cdots \varphi_A(p_d(x)) \\ &= P_1 + \cdots + P_d. \end{aligned}$$

(b): Note that for all $i \neq j$ we have $m_A(x)|p_i(x)p_j(x)$. That is, there exists a polynomial $h(x) \in K[x]$ such that $p_i(x)p_j(x) = m_A(x)h(x)$. Then applying φ_A to both sides gives

$$P_iP_j = p_i(A)p_j(A) = m_A(A)h(A) = 0h(A) = 0.$$

(c): Now for all i we have

$$\begin{aligned} P_i = P_iI = P_i \sum_j P_j \\ = P_i^2 + \sum_{i \neq j} P_iP_j = P_i^2 + \sum_{i \neq j} 0 = P_i^2. \end{aligned}$$

(d): To prove the direct sum, first note that $P_2 + \cdots + P_d$ is idempotent since

$$(P_2 + \cdots + P_d)^2 = (P_2^2 + \cdots P_d^2) + \sum_{\substack{i,j \in \{2,\ldots,d\} \\ i \neq j}} \cancel{P_iP_j} = (P_2^2 + \cdots + P_d^2) + 0 = (P_2 + \cdots + P_d).$$

Thus $P_1, (P_2 + \cdots + P_d)$ is an orthogonal pair of idempotents and from Problem 3 we obtain

$$K^n = \operatorname{im} P_1 \oplus \operatorname{im}(P_2 + \cdots + P_d).$$

Now we will use induction. Define the subspace $V := \operatorname{im}(P_2 + \cdots + P_d) \subseteq K^n$. With respect to the direct sum $K^n = \operatorname{im} P_1 \oplus V$ we can write each projection P_i as a block matrix. Furthermore, by the properties in parts (b) and (c) we must have

$$P_1 = \left(\begin{array}{c|c} P_1' & 0 \\ \hline 0 & 0 \end{array}\right) \quad \text{and} \quad P_i = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & P_i' \end{array}\right) \text{ for } i \in \{2, \ldots, d\}$$

where the smaller matrices $P_1', P_2', \ldots, P_d'$ are also idempotent and the matrices $P_2', \ldots, P_d'$ are pairwise orthogonal. Then from part (a) we have

$$I = \sum_i P_i = \left(\begin{array}{c|c} P_1' & 0 \\ \hline 0 & P_2' + \cdots + P_d' \end{array}\right)$$

so that $P_2' + \cdots + P_d' = I'$ where I' is the identity matrix on the subspace V. Finally, by induction on d we have

$$V = \bigoplus_{i=2}^{d} \operatorname{im} P_i'$$

and the fact that $\operatorname{im} P_i' = \operatorname{im} P_i$ for all $i \in \{2, \ldots, d\}$ completes the proof. $\square$

[Remark: All that mumbling about eigenspaces in the linear algebra textbooks and this is what's really going on. There aren't even any eigenvalues yet; those appear in Problem 5.]

Problem 5. Jordan-Chevalley Decomposition. Now let K be an **algebraically closed** field and consider a matrix $A \in \mathrm{Mat}_n(K)$. In this problem we will prove that there exist unique matrices $S, N \in \mathrm{Mat}_n(K)$ such that:

- S is diagonalizable and N is nilpotent,
- $A = S + N$,
- $SN = NS$.

(a) Since K is algebraically closed we can factor the minimal polynomial as $m_A(x) = \prod_i (x-\lambda_i)^{m_i}$ for some $\lambda_i \in K$ and $m_i \in \mathbb{N}$. Let P_i be the projections from Problem 4 corresponding to the factors $f_i(x)^{m_i} = (x-\lambda_i)^{m_i}$. Prove that $(A-\lambda_i I)^{m_i} P_i = 0$.

(b) Existence: Prove that the matrix $S := \sum_i \lambda_i P_i$ is diagonalizable and that the matrix $N := A - S$ is nilpotent. Then since $S = \sum_i \lambda_i p_i(A)$ for some polynomials $p_i(x)$ it automatically follows that $SN = NS$. [Hint: Use Problem 4 to show that S has a basis of eigenvectors. To show that N is nilpotent, note that for all polynomials $h(x) \in K[x]$ we have $h(N) = \sum_i h(A - \lambda_i I)P_i$. Then use part (a).]

(c) Uniqueness: I need to come up with a good hint for this.

Proof. (a): Let K be algebraically closed and suppose that

$$m_A(x) = \prod_{i=1}^{d} (x-\lambda_i)^{m_i}$$

for some $\lambda_i \in K$ and $m_i \in \mathbb{N}$, where $i \neq j$ implies $\lambda_i \neq \lambda_j$. As in Problem 4 there exist polynomials $g_i(x) \in K[x]$ such that

$$\frac{1}{m_A(x)} = \frac{g_1(x)}{(x-\lambda_1)^{m_1}} + \cdots + \frac{g_d(x)}{(x-\lambda_d)^{m_d}}.$$

Then we define the polynomials $p_i(x) := g_i(x)\prod_{i\neq j}(x-\lambda_j)^{m_j} \in K[x]$ and evaluate at A to obtain the projection matrices

$$P_i := p_i(A) = g_i(A)\prod_{i\neq j}(A-\lambda_j I)^{m_j} \in \mathrm{Mat}_n(K).$$

Finally, multiplying both sides (on the left or the right; it doesn't matter) by $(A-\lambda_i I)^{m_i}$ gives

$$(A-\lambda_i I)^{m_i} P_i = g_i(A)\prod_{j}(A-\lambda_j I)^{m_j} = g_i(A) m_A(A) = g_i(A)0 = 0.$$

(b): **Existence:** Define the matrices $S := \sum_i \lambda_i P_i$ and $N := A - S$. To show that S is diagonalizable, first note that every (nonzero) vector in the subspace $\operatorname{im} P_j \subseteq K^n$ is a λ_j-eigenvector of S. Indeed, for any $P_j u \in \operatorname{im} P_j$ note that Problem 4 parts (b) and (c) imply

$$S(P_j u) = \left(\sum_i \lambda_i P_i\right)(P_j u) = \left(\sum_i \lambda_i P_i P_j\right) u = (\lambda_j P_j) = \lambda_j (P_j u).$$

Then from Problem 4(d) we have a direct sum decomposition

$$K^n = \bigoplus_{i=1}^{n} \operatorname{im} P_i. \tag{4}$$

By concatenating bases for these subspaces we obtain a basis for K^n consisting of eigenvectors for S, hence S is diagonalizable. [And in this case equation (4) is an actual (i.e., not only a "generalized") eigenspace decomposition for the matrix S.]

To show that N is nilpotent, first note that

$$N = A - S = AI - S = \sum_i AP_i - \sum_i \lambda_i P_i = \sum_i (A - \lambda_i I)P_i.$$

Note that A commutes with each of the projection matrices P_i. Indeed, **all** matrices in this problem commute because they are all polynomials evaluated at A. Thus by Problem 4 parts (b) and (c) we see that for any polynomial $h(x) \in K[x]$ we have $h(N) = \sum_i h(A - \lambda_i I)P_i$. In particular, for any $m \in \mathbb{N}$ we have

$$N^m = \sum_i (A - \lambda_i I)^m P_i.$$

Finally, if we take $m := \max\{m_1, \ldots, m_d\}$ then it follows from part (a) that $N^m = \sum_i 0 = 0$ and we conclude that N is nilpotent.

(c): **Uniqueness:** I finally came up with a good hint but it was too late. Nevertheless, some of the students (Nuno Cardoso, Qian Chen, Eric Ling, David Udumyan) still came up with nice answers. All of the answers were along the following lines. The hint that I *would* have given is contained in a Lemma after the proof.

Suppose that we have another decomposition $A = S' + N'$ where $S' \in \text{Mat}_n(K)$ is diagonalizable, $N' \in \text{Mat}_n(K)$ is nilpotent, and $S'N' = N'S'$. Since $S + N = A = S' + N'$ we have $S - S' = N' - N$. If we can show that $S - S'$ is diagonalizable and that $N' - N$ is nilpotent then we will be done. Indeed, if the matrix $B := S - S' = N' - N \in \text{Mat}_n(K)$ is both diagonalizable and nilpotent then there exists an invertible matrix $P \in \text{GL}_n(K)$ such that $PBP^{-1} = 0$ (since zero is the only possible eigenvalue of a nilpotent matrix), and we conclude that $B = P^{-1}0P = 0$.

To show that $N' - N$ is nilpotent we first note that $NN' = N'N$. Indeed, since N is a polynomial in A it suffices to show that N' commutes with A, and this is true because

$$N'A = N'(S' + N') = N'S' + N'N' = S'N' + N'N' = (S' + N')N' = AN'.$$

Then we can apply the binomial theorem to get

$$(N' - N)^m = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (N')^{m-k} N^k. \tag{5}$$

Since N' and N are nilpotent there exist $m_1, m_2 \in \mathbb{N}$ such that $(N')^{m_1} = 0$ and $N^{m_2} = 0$. Finally, let $m \geq m_1 + m_2$. Then for all k we have for all $k \in \mathbb{N}$ that $(m - k) \geq m_1$ or $k \geq m_2$ (since otherwise $m = (m - k) + k < m_1 + m_2$), and hence $(N')^{m-k} N^k = 0$. It follows from equation (5) that $(N' - N)^m = \sum_{k=0}^m 0 = 0$, hence $N' - N$ is nilpotent.

Then to see that $S - S'$ is diagonalizable, first note that S' commutes with A:

$$S'A = S'(S' + N') = S'S' + S'N' = S'S' + N'S' = (S' + N')S' = AS'.$$

Now consider the eigenspace decomposition (4) for the matrix S. Since each projection matrix P_i is a polynomial in A we have $S'P_i = P_i S'$ and hence for all vectors $u \in K^n$ we have

$$S'(P_i u) = (S'P_i)u = (P_i S')u = P_i(S'u).$$

In other words, S' preserves each subspace $\operatorname{im} P_i \subseteq K^n$. If we write $r_i := \dim(\operatorname{im} P_i)$ then by concatenating bases in (4) we obtain an invertible matrix $Q \in \text{GL}_n(K)$ and (possibly non-invertible) matrices $S_i' \in \mathrm{Mat}_{r_i}(K)$ such that

$$QSQ^{-1} = \begin{pmatrix} \boxed{\lambda_1 I_{r_1}} & & & 0 \\ & \boxed{\lambda_2 I_{r_2}} & & \\ & & \boxed{\ddots} & \\ 0 & & & \boxed{\lambda_d I_{r_d}} \end{pmatrix} \quad \text{and} \quad QS'Q^{-1} = \begin{pmatrix} \boxed{S_1'} & & & 0 \\ & \boxed{S_2'} & & \\ & & \boxed{\ddots} & \\ 0 & & & \boxed{S_d'} \end{pmatrix}.$$

Since we assumed that S' is diagonalizable, the Lemma below implies (by induction) that each submatrix $S_i \in \mathrm{Mat}_{r_i}(K)$ is diagonalizable. That is, there exist invertible matrices $U_i \in \mathrm{GL}_{r_i}(K)$ such that each $U_i S_i' U_i^{-1} \in \mathrm{Mat}_{r_i}(K)$ is a **diagonal matrix**. Now by defining

$$U := \begin{pmatrix} \boxed{U_1} & & & 0 \\ & \boxed{U_2} & & \\ & & \boxed{\ddots} & \\ 0 & & & \boxed{U_d} \end{pmatrix} \in \mathrm{GL}_n(K)$$

we conclude that the matrix

$$(UQ^{-1})(S - S')(UQ^{-1})^{-1} = \begin{pmatrix} \boxed{\lambda_1 I - U_1 S_1' U_1^{-1}} & & & 0 \\ & \boxed{\lambda_2 I - U_2 S_2' U_2^{-1}} & & \\ & & \boxed{\ddots} & \\ 0 & & & \boxed{\lambda_d I - U_d S_d' U_d^{-1}} \end{pmatrix}$$

is diagonal, hence $S - S'$ is diagonalizable. $\square$

[The hard part of the uniqueness proof is contained in the following unavoidable lemma. In retrospect, this could have been the heart of a nice problem on "Simultaneous Diagonalization".]

Lemma. Let K be any field and consider any block diagonal matrix

$$A = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right) \in \mathrm{Mat}_n(K).$$

If A is diagonalizable then each of the matrices A_1 and A_2 is diagonalizable.

Proof. By assumption we have a matrix $P \in \mathrm{GL}_n(K)$ and scalars $\lambda_j \in K$ such that

$$AP = P \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}. \tag{6}$$

If $p_j \in \mathrm{Mat}_{n\times 1}(K)$ is the j-th column of P then the equation (6) just says that $Ap_j = \lambda_j p_j$ for all j. Then the fact that P is invertible tells us that A has a basis of eigenvectors. Now assume that we have

$$A = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right)$$

for some matrices $A_1 \in \mathrm{Mat}_{n_1}(K)$ and $A_2 \in \mathrm{Mat}_{n_2}(K)$ with $n = n_1 + n_2$. We wish to show that each of A_1 and A_2 has a basis of eigenvectors. To do this, we partition the matrix P as

$$P = \left(\begin{array}{c} P_1 \\ \hline P_2 \end{array}\right) \tag{7}$$

with $P_1 \in \mathrm{Mat}_{n_1 \times n}(K)$ and $P_2 \in \mathrm{Mat}_{n_2 \times n}(K)$. If we rewrite the diagonal matrix as $D := \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ then equation (6) becomes

$$\begin{aligned} AP &= PD \\ \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right) \left(\begin{array}{c} P_1 \\ \hline P_2 \end{array}\right) &= \left(\begin{array}{c} P_1 \\ \hline P_2 \end{array}\right) D \\ \left(\begin{array}{c} A_1 P_1 \\ \hline A_2 P_2 \end{array}\right) &= \left(\begin{array}{c} P_1 D \\ \hline P_2 D \end{array}\right). \end{aligned}$$

The equation $A_1 P_1 = P_1 D$ says that the columns of P_1 are eigenvectors of A_1 and similarly $A_2 P_2 = P_2 D$ says that the columns of P_2 are eigenvectors of A_2. We only need to show that there are enough linearly independent columns. That is, we want to show that P_1 has column rank n_1 and P_2 has column rank n_2. But recall that the column rank of a matrix equals its row rank (this the Fundamental Miracle of Linear Algebra; I won't prove it here). Let $\mathrm{rk}(P)$, $\mathrm{rk}(P_1)$, and $\mathrm{rk}(P_2)$ denote the row ranks of P, P_1, and P_2, respectively. By definition we have $\mathrm{rk}(P_1) \leq n_1$ and $\mathrm{rk}(P_2) \leq n_2$, and and since P is invertible we know that $\mathrm{rk}(P) = n$. Furthermore, equation (7) tells us that $\mathrm{rk}(P) \leq \mathrm{rk}(P_1) + \mathrm{rk}(P_2)$. Then since

$$n_1 + n_2 = n = \mathrm{rk}(P) \leq \mathrm{rk}(P_1) + \mathrm{rk}(P_2) \tag{8}$$

we must have either $n_1 \leq \mathrm{rk}(P_1)$ or $n_2 \leq \mathrm{rk}(P_2)$; without loss say $n_1 \leq \mathrm{rk}(P_1)$. Together with $\mathrm{rk}(P_1) \leq n_1$ this implies $\mathrm{rk}(P_1) = n_1$ and subtracting this equation from both sides of (8) gives $n_2 \leq \mathrm{rk}(P_2)$, which implies that $\mathrm{rk}(P_2) = n_2$. We conclude that each of A_1 and A_2 has a basis of eigenvectors, hence each is diagonalizable. □

[Remark: What is the Jordan-Chevalley Decomposition of a Jordan block? From this you will see that the Jordan Canonical Form easily implies the existence of Jordan-Chevalley Decomposition. However, the proof given here is **much** more direct than the one using Smith Normal Form. I learned this beautiful proof (of existence; the proof of uniqueness isn't so beautiful) from Goodman and Wallach's book on "Representations and Invariants of the Classical Groups". I think it deserves to be better known, which is why I'm putting it here (you're welcome, internet). I would love to know more about the history of this proof but the paper trail seems to end with Humphreys' book on Lie Algebras, and he doesn't remember where he learned the proof. More work needs to be done on investigating the history of linear algebra; too bad there isn't a funding agency willing to pay for it.]

[Ending Remark: Once again, I think that a lot of fundamental concepts of representation theory are sadly under-represented in standard algebra textbooks. This all falls into the gap of "things that we don't teach but we expect people to know anyway". Maybe some day I'll write my own algebra textbook; by which I mean: maybe some day I'll organize all of this crap on my webpage into a single pdf file with a table of contents and nice crap like that. The acknowledgements section will be the hardest part to write, and may end up filling most of the book.]