1. Galois Connections. Let \((P, \leq)\) and \((Q, \leq)\) be partially ordered sets. We say that a pair of functions \(* : P 
rightarrow Q : *\) is a Galois connection if for all \(p \in P\) and \(q \in Q\) we have
\[
p \leq q^* \iff q \leq p^*.
\]
Since this relation is symmetric in \(P\) and \(Q\), you need only prove half of parts (a)-(d) below.

(a) Prove that for all \(p \in P\) and \(q \in Q\) we have
\[
p \leq p^{**} \quad \text{and} \quad q \leq q^{**}.
\]
\textit{Proof.} For all \(p \in P\) we have \(p^{**} \leq p^{*}\) from the reflexivity of partial order. Then putting \(q = p^{*}\) in the definition of Galois connection gives \((p^{*}) \leq (p)^{*} \implies (p) \leq (p^{*})^{*} = p^{**}\). \(\square\)

(b) Prove that for all \(p_1, p_2 \in P\) and \(q_1, q_2 \in Q\) we have
\[
p_1 \leq p_2 \implies p_2^{*} \leq p_1^{*} \quad \text{and} \quad q_1 \leq q_2 \implies q_2^{*} \leq q_1^{*}.
\]
\textit{Proof.} Consider \(p_1, p_2 \in P\) such that \(p_1 \leq p_2\). By part (a) and the transitivity of partial order we have \(p_1 \leq p_2 \leq p_2^{*}\) and then from the definition of Galois connection we have \((p_1) \leq (p_2)^{*} \implies (p_2) \leq (p_1)^{*}\). \(\square\)

(c) Prove that for all \(p \in P\) and \(q \in Q\) we have
\[
p^{***} = p^{*} \quad \text{and} \quad q^{***} = q^{*}.
\]
\textit{Proof.} Consider any \(p \in P\). On the one hand, part (a) tells us that \((p^{*}) \leq (p)^{*}\). On the other hand, part (a) says that \(p \leq p^{*}\) and then part (b) gives \((p) \leq (p^{*})^{*} \implies (p^{*})^{*} \leq (p)^{*}\). Finally, the antisymmetry of partial order gives \(p^{***} = p^{*}\). \(\square\)

(d) We say that an element \(p \in P\) (resp. \(q \in Q\)) is \texttt{**-closed} if \(p^{**} = p\) (resp. \(q^{**} = q\)). Prove that the Galois connection \(* : P \nrightarrow Q : *\) restricts to an order-reversing bijection between **-closed elements.

\textit{Proof.} Let \(P^{*} \subseteq P\) and \(Q^{*} \subseteq Q\) denote the images of the functions \(* : Q \rightarrow P\) and \(* : P \rightarrow Q\), respectively. I claim that \(P^{*} \subseteq P\) is precisely the subset of **-closed elements. Indeed, if \(p^{**} = p\) then \(p = (p^{*})^{*}\) is the image of \(p^{*}\). Conversely, if \(p = q^{*}\) for some \(q \in Q\) then by part (c) we have \(p^{**} = (q^{*})^{**} = (q^{*}) = p\). Similarly, we can show that \(Q^{*} \subseteq Q\) is the subset of **-closed elements in \(Q\). It follows immediately that the functions \(* : Q^{*} \nrightarrow P^{*} : *\) are inverse to each other, hence they are bijections. [The fact that they reverse order follows from (b).] \(\square\)

(e) Finally, suppose that \(P\) and \(Q\) have bottom and top elements \(0_P, 1_P \in P\) and \(0_Q, 1_Q \in Q\). In this case draw a picture of the bijection from part (d).
2. Image and Preimage. Let $R$ be a ring and let $\varphi : M \to N$ be a homomorphism of (left) $R$-modules with kernel $\ker \varphi \subseteq M$ and image $\im \varphi \subseteq N$. For any (left) $R$-modules $Q \subseteq P$ let $\mathcal{L}(P, Q)$ be the lattice of submodules of $P$ that contain $Q$, and let $\mathcal{L}(P) := \mathcal{L}(P, 0)$.

(a) For every submodule $A \subseteq M$ prove that the image $\varphi(A) := \{ n \in N : \exists a \in A, \varphi(a) = n \}$ is a submodule of $N$.

Proof. Consider any elements $n_1, n_2 \in \varphi(A)$ and $r \in R$. Since $n_1, n_2 \in \varphi(A)$ there exist $a_1, a_2 \in A$ such that $n_1 = \varphi(a_1)$ and $n_2 = \varphi(a_2)$. Then since $\varphi$ is a homomorphism of $R$-modules we have

$$\varphi(a_1 + ra_2) = \varphi(a_1) + r\varphi(a_2) = n_1 + rn_2.$$ 

Finally, since $A \subseteq M$ is a submodule we have $a_1 + ra_2 \in A$, and it follows that $n_1 + rn_2 \in \varphi(A)$ as desired. \hfill \Box

(b) For every submodule $B \subseteq N$ prove that the preimage $\varphi^{-1}(B) := \{ m \in M : \exists b \in B, \varphi(m) = b \}$ is a submodule of $M$.

Proof. Consider any elements $m_1, m_2 \in \varphi^{-1}(B)$ and $r \in R$. Since $m_1, m_2 \in \varphi^{-1}(B)$ there exist $b_1, b_2 \in B$ such that $\varphi(m_1) = b_1$ and $\varphi(m_2) = b_2$. Then since $\varphi$ is a homomorphism of $R$-modules we have

$$\varphi(m_1 + rm_2) = \varphi(m_1) + r\varphi(m_2) = b_1 + rb_2.$$ 

Finally, since $B \subseteq N$ is a submodule we have $b_1 + rb_2 \in B$, and it follows that $m_1 + rm_2 \in \varphi^{-1}(B)$ as desired. \hfill \Box

(c) For all submodules $A \subseteq M$ and $B \subseteq N$ prove that we have

$$\varphi(A) \subseteq B \iff A \subseteq \varphi^{-1}(B).$$

Proof. By definition we have

$$\varphi(A) \subseteq B \iff \forall a \in A, \varphi(a) \in B \iff \forall a \in A, \exists b \in B, \varphi(a) = b \iff \forall a \in A, a \in \varphi^{-1}(B) \iff A \subseteq \varphi^{-1}(B).$$ 

\hfill \Box
(d) For all submodules \( A \subseteq M \) and \( B \subseteq N \) you may assume without proof that
\[
\varphi^{-1}(\varphi(A)) = A \lor \ker \varphi \quad \text{and} \quad \varphi(\varphi^{-1}(B)) = B \land \im \varphi.
\]
Quote from Problem 1 to obtain a poset isomorphism \( \mathcal{L}(M, \ker \varphi) \cong \mathcal{L}(\im \varphi) \).

Proof. From part (c) we see that \( \varphi : \mathcal{L}(M)^{\text{op}} \cong \mathcal{L}(N) : \varphi^{-1} \) is a Galois connection in the sense of Problem 1, thus from Problem 1(d) we obtain an order-reversing bijection between the subposets of “closed submodules” in \( \mathcal{L}(M)^{\text{op}} \) and \( \mathcal{L}(N) \). Equivalently, we obtain an order-preserving bijection (i.e. a poset isomorphism) between closed submodules in \( \mathcal{L}(M) \) and \( \mathcal{L}(N) \).

It remains only to determine the closed submodules. By assumption \( A \subseteq M \) is \( \varphi^{-1}\varphi \)-closed if and only if \( A = A \lor \ker \varphi \), and from the universal property of \( \lor \) this is equivalent to saying that \( \ker \varphi \subseteq A \). Similarly, a submodule \( B \subseteq N \) is \( \varphi\varphi^{-1} \)-closed if and only if \( B = B \land \im \varphi \), which is equivalent to \( B \subseteq \im \varphi \). \( \square \)

(e) Prove that we have an isomorphism of (left) \( R \)-modules \( M/\ker \varphi \cong \im \varphi \). [Hint: Show that the surjective homomorphism \( (m + \ker \varphi) \mapsto \varphi(m) \) is well-defined and injective.]

Proof. For all elements \( m_1, m_2 \in M \) we have
\[
(m_1 + \ker \varphi) = (m_2 + \ker \varphi) \iff (m_1 - m_2) \in \ker \varphi
\]
\[
\iff \varphi(m_1 - m_2) = 0
\]
\[
\iff \varphi(m_1) = \varphi(m_2).
\]
The \( \Rightarrow \) direction proves that the map is well-defined and the \( \Leftarrow \) direction proves that it is injective. [This result is often called the 1st Isomorphism Theorem.] \( \square \)

(f) Conclude that we have an isomorphism of posets \( \mathcal{L}(M, \ker \varphi) \cong \mathcal{L}(M/\ker \varphi) \).

Proof. The \( R \)-module isomorphism \( \im \varphi \cong M/\ker \varphi \) from part (e) induces a poset isomorphism \( \mathcal{L}(\im \varphi) \cong \mathcal{L}(M/\ker \varphi) \). Then combining this with part (d) gives
\[
\mathcal{L}(M, \ker \varphi) \cong \mathcal{L}(\im \varphi) \cong \mathcal{L}(M/\ker \varphi).
\]
[This result is often called the Correspondence Theorem. See the picture from 1(e).] \( \square \)

3. Direct Product of Rings. Let \( \text{CRng} \) be the category of commutative rings and consider \( R, S \in \text{CRng} \). We define the direct product ring \( R \times S \) as the Cartesian product set with componentwise addition and multiplication. Note that it has a unit: \( (1_R, 1_S) \in R \times S \).

(a) Prove that \( R \times S \) is the categorical product in \( \text{CRng} \). [Hint: You can assume that the Cartesian product is the categorical product in \( \text{Set} \).]

Proof. The definition of categorical product is given by the following diagram:

\[
\begin{array}{ccc}
T & \xrightarrow{\varphi_R \times \varphi_S} & R \times S \\
\downarrow \varphi_S & & \downarrow \pi_R \\
S & & \\
\end{array}
\]

By assumption we know that there exist set functions \( \pi_R : R \times S \to R \) and \( \pi_S : R \times S \to S \) such that for all set functions \( \varphi_R : T \to R \) and \( \varphi_S : T \to S \) there exists a unique set
function $\varphi_R \times \varphi_S : T \to R \times S$ making the above diagram commute. Explicitly, these functions are given by

$$\pi_R(r, s) = r, \quad \pi_S(r, s) = s, \quad \text{and} \quad (\varphi_R \times \varphi_S)(t) = (\varphi_R(t), \varphi_S(t)).$$

To lift this diagram to the category $\mathsf{CRng}$, first note that $\pi_r$ and $\pi_S$ are clearly ring homomorphisms. If $T \in \mathsf{CRng}$ and if $\varphi_R$ and $\varphi_S$ are ring homomorphisms then it is also clear that the function $\varphi_S \times \varphi_R$ defined by $(\varphi_R \times \varphi_S)(t) = (\varphi_R(t), \varphi_S(t))$ is a ring homomorphism. Finally, the uniqueness of the ring homomorphism $\varphi_R \times \varphi_S$ follows from the uniqueness of the underlying set function.

(b) If $R \cong S \times T$ for some $R, S, T \in \mathsf{CRng}$ where neither of $S$ or $T$ is the zero ring, prove that $R$ contains a nontrivial idempotent, i.e., an element $e \in R$ such that $e^2 = e$ and $e \notin \{0_R, 1_R\}$.

Proof. Since $S$ and $T$ are both nonzero rings we have $0_S \neq 1_S$ and $0_T \neq 1_T$. Now I claim that $e := (1_S, 0_T) \in R \times S$ is a nontrivial idempotent. Indeed, since $0_S \neq 1_S$ and $0_T \neq 1_T$ we see that $e \neq (0_S, 0_T) = 0_R$ and $e \neq (1_S, 1_T) = 1_R$, hence $e$ is nontrivial. And $e$ is idempotent because

$$e^2 = (1_S, 0_T)(1_S, 0_T) = (1_S 1_S, 0_T 0_T) = (1_S, 0_T) = e.$$

[Note that $f = (0_S, 1_T) = 1_R - e$ is another perfectly good choice.] $\square$

(c) Given any ring $R \in \mathsf{CRng}$ and an element $e \in R$, prove that

$e$ is a nontrivial idempotent $\iff 1_R - e$ is a nontrivial idempotent.

Proof. First note that $e \notin \{0_R, 1_R\}$ if and only if $(1_R - e) \notin \{0_R, 1_R\}$. Now assume that $e^2 = e$. From this it follows that

$$(1_R - e)^2 = (1_R)^2 - e - e + e^2 = 1_R - e - f + f = (1_R - e).$$

Finally, if $f := (1_R - e)$ satisfies $f^2 = f$ then the same computation shows that $e = (1_R - f)$ satisfies $e^2 = e.$ $\square$

(d) If $e \in R$ is idempotent, prove that $eR := \{er : r \in R\}$ is a commutative ring with unit element $e \in eR$. But note that $eR \subseteq R$ is (probably) not a subring.

Proof. We would usually write $eR$ as the principal ideal $(e) \subseteq R$. To see that this is indeed an ideal note that for all $er_1, er_2 \in eR$ and $r_3 \in R$ we have

$$er_1 - r_3(ern2) = e(r_1 - r_3r_2) \in eR.$$ 

In particular we see that $(eR, +, 0_R)$ is an abelian group and that multiplication is a commutative and associative operation $eR \times eR \to eR$ that distributes over $+$. It remains only to show that $e \in eR$ is a unit element. To see this, observe that for all $er \in eR$ we have $e(er) = e^2t = er$.

Finally, observe that $eR \subseteq R$ is a subring if and only if $e \in \{0_R, 1_R\}.$ $\square$

(e) Finally, suppose that $R \in \mathsf{CRng}$ contains a nontrivial idempotent $e \in R$. In this case prove that $R$ is isomorphic to a direct product of nonzero rings. This is the converse of part (b). [Hint: Use parts (c) and (d).]

(a) Use the fact that $K[x]$ is a Euclidean domain to prove that $K[x]$ is a PID. [Hint: Consider a nonzero ideal $0 \subseteq I \subseteq K[x]$ and let $m(x) \in I$ be a monic polynomial of minimal degree.]

Proof. Suppose that $I \subseteq K[x]$ is a nonzero ideal and let $m(x) \in I$ be a monic polynomial of minimal degree. Note that $(m(x)) \subseteq I$. Now consider any polynomial $f(x) \in I$. Since $m(x)$ is monic we can use long division to obtain polynomials $q(x), r(x) \in K[x]$ such that $f(x) = q(x)m(x) + r(x)$ and such that $r(x) = 0$ or $\deg(r) < \deg(m)$. Since $I$ is an ideal we have $r(x) = q(x)m(x) - f(x) \in I$. Then if $r(x) \neq 0$ we find that $\deg(r) < \deg(m)$, which contradicts the minimality of $\deg(m)$. It follows that $r(x) = 0$ and hence $f(x) = q(x)m(x) \in (m(x))$. Since this is true for all $f(x)$ we have $I \subseteq (m(x))$, and hence $I = (m(x))$. \hfill $\square$

(b) Given a monic polynomial $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in K[x]$, prove that (the images of) $1, x, x^2, \ldots, x^{n-1}$ are a basis for the $K$-vector space $K[x]/(m(x))$.

Proof. A general $K$-linear combination of the elements $1, x, \ldots, x^{n-1} \in K[x]/(m(x))$ is just a coset $r(x) + (m(x))$ where $r(x) \in K[x]$ satisfies $r(x) = 0$ or $\deg(r) \leq n - 1$. To prove “spanning”, consider any element $f(x) + (m(x)) \in K[x]/(m(x))$. Dividing the polynomial $f(x)$ by the monic polynomial $m(x)$ gives $f(x) = q(x)m(x) + r(x)$ where $r(x) = 0$ or $\deg(r) \leq n - 1$. The result now follows from the fact that $f(x) + (m(x)) = r(x) + (m(x))$. To prove “independence”, assume for contradiction that there exists a nonzero polynomial $r(x) \in K[x]$ such that $\deg(r) \leq n - 1$ and $r(x) + (m(x)) = 0 + (m(x))$. The fact that $r(x) \in (m(x))$ means that we have $r(x) = f(x)m(x)$ for some nonzero $f(x) \in K[x]$ and the fact that $K$ is a domain implies that $n = \deg(m) \leq \deg(m) + \deg(f) = \deg(r) \leq n - 1$, which is the desired contradiction. \hfill $\square$
(c) “Multiplication by $x$” defines a $K$-linear endomorphism $K[x]/(m(x)) \to K[x]/(m(x))$. Find the matrix of this endomorphism in terms of the basis from part (b). We will call this matrix $C_m \in \text{Mat}_n(K)$.

**Proof.** To find the matrix we just need to know what “multiplication by $x$” does to the basis elements. Note that we have

$$x \cdot 1 = x,$$
$$x \cdot x = x^2,$$
\[ \vdots \]
$$x \cdot x^{n-2} = x^{n-1},$$
$$x \cdot x^{n-1} = x^n = -a_0 1 - a_1 x - \cdots - a_{n-1} x^{n-1},$$

where each polynomial is interpreted as the coset in $K[x]/(m(x))$ that it generates. The corresponding matrix is

$$C_m = \begin{pmatrix}
1 & -a_0 \\
& 1 & -a_1 \\
& & \ddots & \ddots \\
& & & 1 & -a_{n-1}
\end{pmatrix},$$

where we interpret the blank entries as zeroes. [This is called the companion matrix of the monic polynomial $m(x)$.] \qed

(d) You may assume without proof that $m(x)$ is both the minimal polynomial and the characteristic polynomial of the matrix $C_m$. In this case, prove that $m(x)$ is both the minimal and the characteristic polynomial of the transpose matrix $(C_m)^T$.

**Proof.** Consider any matrix $A \in \text{Mat}_n(K)$ and recall that the minimal polynomial is the unique monic polynomial $f(x) \in K[x]$ of minimum degree satisfying $f(A) = 0 \in \text{Mat}_n(K)$. First note that $f(A)^T = f(A^T)$ for all polynomials $f(x) \in K[x]$ and hence we have $f(A) = 0 \iff f(A^T) = 0$. It follows that $A$ and $A^T$ have the same minimal polynomial. Then recall that the characteristic polynomial of $A$ is defined as $\det(xI_n - A) \in K[x]$. Since

$$\det(xI_n - A) = \det((xI_n - A)^T) = \det(xI_n - A^T),$$

we conclude that $A$ and $A^T$ have the same characteristic polynomial. In particular, both of these statements are true when $A = C_m$. \qed

(e) Define a (finitely-generated and torsion) $K[x]$-module structure on $M = K^n$ by letting $x$ act as the matrix $(C_m)^T$. Since $K[x]$ is a PID we know (from the FTFGMPID) that there exist unique, monic, nonconstant polynomials $f_1(x), f_2(x), \ldots, f_d(x)$ such that $M \cong \bigoplus_{i=1}^d K[x]/(f_i(x))$ as $K[x]$-modules. Use part (d) to compute these polynomials. [Hint: You can quote results from class.]

**Proof.** From class we know that $f_d(x)$ is the minimal polynomial of $(C_m)^T$ and that $\prod_{i=1}^d f_i(x)$ is the characteristic polynomial of $(C_m)^T$. And from part (d) we know that $m(x)$ is the minimal and the characteristic polynomial of $(C_m)^T$. Since the polynomials $f_i(x)$ are nonconstant this implies that $d = 1$ and $f_d(x) = m(x)$. \qed
(f) Finally, prove that there exists an invertible matrix $P \in \text{GL}_n(K)$ such that

$$PC_m P^{-1} = (C_m)^T.$$ 

**Proof.** Recall that a $K[x]$-module is the same as a pair $(V, \varphi)$ where $V$ is a $K$-vector space and $x$ acts on $V$ by the $K$-linear endomorphism $\varphi \in \text{End}_K(V)$. Furthermore, recall that a morphism of $K[x]$-modules $(V_1, \varphi_1) \to (V_2, \varphi_2)$ is the same as a $K$-linear function $\Phi : V_1 \to V_2$ satisfying $\Phi \circ \varphi_1 = \varphi_2 \circ \Phi$. Thus an isomorphism of $K[x]$-modules is the same as an isomorphism of $K$-vector spaces $\Phi : V_1 \to V_2$ satisfying $\Phi \circ \varphi_1 \circ \Phi^{-1} = \varphi_2$. After choosing bases for $V_1$ and $V_2$ this becomes a matrix equation:

$$P[\varphi_1]P^{-1} = [\varphi_2].$$

Finally, consider the $K[x]$-modules corresponding to pairs $(K^n, C_m)$ and $(K^n, (C_m)^T)$. From part (e) we know that each of these is isomorphic to $K[x]/(m(x))$ as a $K[x]$-module, hence they are isomorphic to each other. It follows from the above observations that there exists an invertible matrix $P \in \text{GL}_n(K)$ such that

$$PC_m P^{-1} = (C_m)^T.$$ 

[Remark: This strange result would be quite difficult to prove directly. Indeed, I have no idea how to find such a matrix $P$ for a specific companion matrix $C_m$. (The situation is easier for a Jordan block $J_\lambda \in \text{Mat}_n(K)$: if $P$ is the anti-identity matrix (with 1s on the anti-diagonal) then we have $PJ_\lambda P^{-1} = (J_\lambda)^T$.) Now let $K$ be any field and consider any matrix $A \in \text{Mat}_n(K)$. From part (f) and the existence of Rational Canonical Form we conclude that there exists a matrix $P \in \text{GL}_n(K)$ such that

$$PAP^{-1} = A^T.$$ 

Strange but true!]