1. (January 2015 Problem 3) Let V be a subspace of $\mathbb{C}^n$ spanned by the basis vectors $e_1, \ldots, e_m$, and let E be the set of matrices A in $M_n(\mathbb{C})$ such that $AV \subseteq V$.

(a) Show that E is an algebra.

$M_n(\mathbb{C})$ is a $\mathbb{C}$-algebra, so we will show that E is a $\mathbb{C}$-algebra.
Let $A, B \in E$.
Then $(A-B)V \subseteq AV + BV \subseteq V+V = V$, so $A-B \in E$. ← E is closed under addition and negation

Also $(AB)V = A(BV) \subseteq AV \subseteq V$, so $AB \in E$. ← E is closed under multiplication

If $\lambda \in \mathbb{C}$, then $(\lambda A)V = \lambda(AV) \subseteq \lambda V = V$ ← E is closed under scalar multiplication

Therefore E is a $\mathbb{C}$-algebra.

(b) Compute all the two sided ideals of E.

First, observe that elements of E must have the form $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ where A is $m \times m$, B is $m \times (n-m)$, C is $(n-m) \times (n-m)$.

Let I be a 2-sided ideal, and let $M \in I$, $M \neq 0$. Then there is a nonzero coordinate of M, say $m = M_{ij}$.

Let E_{rs} denote the matrix with 1 in the (r,s) coordinate and zeros elsewhere.

Then $E_{ii} M E_{jj} = m E_{ij} \in I$ ← The matrix with m in the (i,j) coordinate and zeros elsewhere
Thus $E_{ij} = \frac{1}{m} \cdot m E_{ij} \in I$.

Now suppose (i,j) is in block A. Then if (r,s) is in block A, then $E_{ri} E_{ij} E_{js} = E_{rs} \in I$.
Thus we have shown that if $M \in I$ has a nonzero entry in block A, then I contains all matrices of the form $\begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}$ for any $n \times n$ matrix A.
A similar argument works for block B and for block C. ← Same argument

Now again, assume (i,j) is in block A. If (r,s) is in block B, then we get $E_{rs} \in I$,
Thus we have shown that if $M \in I$ has a nonzero entry in block A, then I also contains matrices with any content in blocks A or B, i.e. of the form $\begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix}$.
The same argument works for matrices of the form $\begin{bmatrix} 0 & B \\ 0 & C \end{bmatrix}$.

Thus the two-sided ideals are $\left\{ 0, E, \begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & B \\ 0 & C \end{bmatrix}, \begin{bmatrix} 0 & B \\ 0 & 0 \end{bmatrix} \right\}$

Note: The reason we can't use the same reasoning for $A \to C$, $B \to A$, etc. is because the argument $E_{ri} E_{ij} E_{js} = E_{rs} \in I$ requires E_{ri} and E_{js} to be in E, which will not be the case, since (r,i) or (j,s) will occur in the bottom left zero-block.

2. (August 1997 Problem 5) Let R be a ring with 1, and let V be a left R-module. Suppose X and Y are R-submodules of V such that $V = X \oplus Y$. If θ is any R-homomorphism from X to Y, define $W_\theta \subseteq V$ to be the set of elements $x - \theta(x) \in V$ for all x.

(a) Show that W_θ is an R-submodule of V and that $V = W_\theta \oplus Y$.

Since θ is an R-homomorphism, we have

$$(x-\theta(x)) - (y-\theta(y)) = (x-y) - \theta(x-y) \in W_\theta$$

$$r(x-\theta(x)) = rx - \theta(rx) \in W_\theta$$

So W_θ is an R-module. It is contained in V since it is contained in $X-Y$.

Define $\varphi: X \oplus Y \to W_\theta \oplus Y$ by $\varphi(x,y) = (x-\theta(x), \theta(x)+y)$.
$\varphi(x,y) = 0 \Rightarrow x-\theta(x) = 0 \Rightarrow x = \theta(x)$. Since $X \cap Y = \{0\}$, we have $x = \theta(x) = 0$.
$\theta(x) + y = 0 \Rightarrow y = 0$.

So φ is injective.

Now let $(w,y) \in W_\theta \oplus Y$. Then $w = x - \theta(x)$ for some $x \in X$, and $\varphi(x, y-\theta(x)) = (w,y)$.
So φ is surjective and therefore an isomorphism.

(b) Conversely, suppose U is an R-submodule of V such that $V = U \oplus Y$. Prove that $U = W_\theta$ for some R-homomorphism $\theta : X \to Y$.

Let $x \in X$. Since $x \in V = U \oplus Y$, x can be uniquely written $x = u+y$ for $u \in U$, $y \in Y$.
Thus there is a well-defined map $\theta: X \to Y$ which sends x to its projection to Y in $U \oplus Y$.
This is clearly an R-homomorphism.

Now let $u = x+y$. Then $x = u-y$, so $\theta(x) = -y$, and we get $u = x - \theta(x)$.

3. (August 2014 Problem 1) For $n \geq 1$ consider the ring $R = M_n(\mathbb{Z}/4\mathbb{Z})$ of $n \times n$ matrices with entries in the ring $\mathbb{Z}/4\mathbb{Z}$. It is naturally a $\mathbb{Z}/4\mathbb{Z}$-algebra.

(a) Prove that $R \otimes_{\mathbb{Z}/4\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is isomorphic to $M_n(\mathbb{Z}/2\mathbb{Z})$. (Make sure to provide a careful description of the isomorphism you construct.) Use general properties of tensor products to argue that the natural map

$$M_n(\mathbb{Z}/4\mathbb{Z}) = R \to R \otimes_{\mathbb{Z}/4\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = M_n(\mathbb{Z}/2\mathbb{Z})$$

is surjective.

Define $\varphi: R \times \mathbb{Z}/2\mathbb{Z} \to M_n(\mathbb{Z}/2\mathbb{Z})$ by $(A, x) \longmapsto \overline{xA}$ (where $\overline{xA} = xA \bmod 2$)
Now φ is $\mathbb{Z}/4\mathbb{Z}$ bilinear, since for $x, y \in \mathbb{Z}/2\mathbb{Z}$, $A, B \in R$, and $a, b \in \mathbb{Z}/4\mathbb{Z}$, we have

$$\varphi(aA+bB, x) = \overline{x(aA+bB)} = \overline{axA} + \overline{bxB} = a\varphi(A,x) + b\varphi(B,x)$$
$$\varphi(A, ax+by) = \overline{(ax+by)A} = \overline{axA} + \overline{byA} = a\varphi(A,x) + b\varphi(A,y)$$

Thus by the Universal Property of Tensor Products, φ induces a map $\tilde{\varphi}: R \otimes \mathbb{Z}/2\mathbb{Z} \to M_n(\mathbb{Z}/2\mathbb{Z})$.
$\tilde{\varphi}$ is surjective, since $\varphi(E_{ij} \otimes 1) = \overline{E_{ij}}$, and so we can map to any matrix $\overline{M} \in M_n(\mathbb{Z}/2\mathbb{Z})$ by summing the appropriate E_{ij} with $\sum E_{ij} = M \in R$

To show that $\tilde{\varphi}$ is injective, we construct an inverse $\psi: M_n(\mathbb{Z}/2\mathbb{Z}) \to R \otimes \mathbb{Z}/2\mathbb{Z}$
For $A = (a_{ij}) \in \mathbb{Z}/2\mathbb{Z}$, define $\psi(A) = \sum_{ij} E_{ij} \otimes a_{ij}$
ψ is clearly $\mathbb{Z}/4\mathbb{Z}$-linear. It remains to show that $\psi \circ \varphi = \mathrm{id}$.
Since both maps are linear, it is enough to show $\psi \circ \varphi(x) = x$ for pure tensors x.
Let $a_{ij} = A_{ij}$. We have

$$\psi \circ \varphi(A \otimes b) = \psi(\overline{bA}) = \sum_{i,j} E_{ij} \otimes \overline{a_{ij} b} = \sum_{i,j} a_{ij} E_{ij} \otimes b = A \otimes b$$

Thus we have shown that $R \otimes_{\mathbb{Z}/4\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong M_n(\mathbb{Z}/2\mathbb{Z})$
Now we want to show that $R \to R \otimes_{\mathbb{Z}/4\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is surjective.
Consider the exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

The tensor product is right exact.

This gives an exact sequence

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}/4\mathbb{Z}} M_n(\mathbb{Z}/4\mathbb{Z}) \to \underbrace{\mathbb{Z}/4\mathbb{Z} \otimes_{\mathbb{Z}/4\mathbb{Z}} M_n(\mathbb{Z}/4\mathbb{Z})}_{M_n(\mathbb{Z}/4\mathbb{Z})} \twoheadrightarrow \underbrace{\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}/4\mathbb{Z}} M_n(\mathbb{Z}/4\mathbb{Z})}_{M_n(\mathbb{Z}/2\mathbb{Z})} \to 0$$

(b) Describe the kernel K of the above surjective map

$$M_n(\mathbb{Z}/4\mathbb{Z}) \to M_n(\mathbb{Z}/2\mathbb{Z})$$

The map is reduction mod 2, so the kernel is the set of matrices with every entry divisible by 2, so $M_n(2\mathbb{Z}/4\mathbb{Z}) \cong M_n(\mathbb{Z}/2\mathbb{Z})$

(c) Find all two-sided ideals of the ring R. (Hint: Use the computations above.)

Let $I \subseteq R$ be a 2-sided ideal. If $M \in I$ and $M \neq 0$, then M has a nonzero entry m.
Say m is in the (i,j)-coordinate.
Now $E_{ii}, E_{jj} \in R$, so $E_{ii} M E_{jj} = m E_{ij} \in I$.
Also, for any coordinates (r,s), $E_{ri}, E_{js} \in R$, so $E_{ri}(mE_{ij})E_{js} = mE_{rs} \in I$.
Thus $I = M_n(J)$ for an ideal $J \subseteq R$.
So $I = \{0, R, M_n(\mathbb{Z}/2\mathbb{Z})\}$

The two-sided ideals of $M_n(R)$ are just $\{M_n(J) : J \text{ a two-sided ideal of } R\}$

4. (January 2000 Problem 2) Let R be a (not necessarily commutative) ring with 1 and suppose that R can be written as the sum $R = \sum_{i=1}^{m} I_i$, where the I_i are finitely many (two-sided) ideals of R satisfying $I_i \cap I_j = 0$ whenever $i \neq j$.

(a) Prove that, for every simple R-module M, there exists a unique subscript k such that $MI_k \neq 0$.

If $MI_i = 0$ for every $i = 1, \ldots, m$, then $MR = \sum_{i=1}^{m} MI_i = 0$, and so $M = 0$.

Thus every simple module M has $MI_k \neq 0$ for some subscript k.

Now since $MI_k \subseteq M$ is a submodule, and M is simple, we must have $M = MI_k$.

Now for $i \neq k$, we have

$$MI_i = (MI_k)I_i = M(I_k I_i) \subseteq M(I_k \cap I_i) = 0.$$

(b) Show that if $i \neq j$, then every left R-module homomorphism $\theta : I_i \to I_j$ is the zero map.

Let $\theta : I_i \to I_j$. Then $\theta(I_i)I_i \subseteq \theta(I_i) \cap I_i = 0$.

Since θ is a left R-module homomorphism, and $I_i \subseteq R$, we get

$$\theta(I_i) = \theta(I_i I_i) = \theta(I_i)I_i = 0.$$

1. (January 2014 Problem 1) If R is a commutative ring and I is an ideal, we denote by $\sqrt{I}$ the *radical* of I, which is by definition the set of $r \in R$ such that $r^n \in I$ for some natural number n.

   (a) Prove that $\sqrt{I}$ is an ideal of R.

Let $a,b \in \sqrt{I}$, $r \in R$. We want to show $a-b \in I$, and $ra \in I$.

Since $a,b \in I$, there are n,m with $a^n \in I$, $b^m \in I$.
We have $(a-b)^{m+n} = \sum_{i=1}^{n+m} c_i a^{m+n-i} b^i$

Since $\max(m+n-i, i) \geq m,n$ for each i, each term in the sum is in $\sqrt{I}$, and so $a-b \in \sqrt{I}$.

Also, $(ra)^n = r^n a^n \in I$, so $ra \in \sqrt{I}$. Thus $\sqrt{I}$ is an ideal.

   (b) Give an example of an ideal in $\mathbb{Q}[x,y]$ such that I is non-principal but $\sqrt{I}$ is principal.

$I = (x^2, xy)$ is not principal. For if $I = (f)$, then $f \mid x^2$ and $f \mid xy$, so $f = 1$ or $f = x$. Any $g \in I$ can be written as $g = p_1 x^2 + p_2 xy$ and so every $g \in I$ has degree ≥ 2, which eliminates the possibility of $f = 1, x$.

Now $\sqrt{I} = (x)$. Since $x^2 \in I$, $x \in \sqrt{I}$, and thus $(x) \subseteq \sqrt{I}$.
Also, if $r \in \sqrt{I}$, then $r^n = p_1 x^2 + p_2 xy$ for some $n \Rightarrow x \mid r^n \Rightarrow x \mid r$.

$\mathbb{Q}[x,y]$ is a UFD
x is irreducible.

   (c) This notation of radical doesn't work so well for noncommutative rings, even for two sided ideals. For instance, we might define $\sqrt{0}$ in the ring $M_2(\mathbb{R})$ of 2×2 matrices to be the set of all elements r such that $r^n = 0$ for some natural number n. Show that, with this definition, $\sqrt{0}$ is *not* an ideal.

E_{12} and E_{21} are nilpotent, but $E_{12} E_{21} = E_{11}$ is not ($E_{11}^2 = E_{11}$).
We could also show that $E_{12} + E_{21}$ has nonzero determinant, and thus is not nilpotent.

2. (August 2013 Problem 4) Recall that a left module P for a ring R is said to be *projective* if, for every surjection of left R-modules $f : N \to P$, there is a map $g : P \to N$ such that g followed by f is the identity on P.

(a) Prove that a free R-module is projective.

Let $F = R^{\kappa}$ be a free R-module, and let $f : M \twoheadrightarrow F$ be a surjection of R-modules.
We want to find $g : F \to M$ such that $f \circ g = id$.
Fix a basis $\{b_\alpha\}$ for F.
For each b_α, there is $a_\alpha \in M$ with $f(a_\alpha) = b_\alpha$.
Define $g(b_\alpha) = a_\alpha$. Then since F is a free R-module, g extends to a homomorphism on F.
Clearly $f \circ g = id$, so F is projective.

(b) Prove that a left R-module M is projective if and only if there is another left module N such that $M \oplus N$ is a free R-module.

($\Rightarrow$) First assume M is projective.

Every module is surjected onto by a free module (a presentation)

Choose a presentation $F \xrightarrow{f} \!\!\!\rightarrow M$ where F is free.
Since M is projective, there is $g : M \to F$ such that $f \circ g = id_M$.

$$0 \to \ker(f) \to F \underset{g}{\overset{f}{\rightleftarrows}} M \to 0$$

By the splitting lemma, $F = \ker(f) \oplus M$.

Splitting Lemma:
Given a short exact sequence

$$0 \to A \xrightarrow{q} B \xrightarrow{r} C \to 0$$

The following are equivalent:
1. **Left Split**: There exists a map $t : B \to A$ such that $t \circ q = id_A$
2. **Right Split**: There exists a map $u : C \to B$ such that $r \circ u = id_C$
3. **Direct Sum**: $B = A \oplus C$, with $q : A \to B$ the natural injection, and $r : B \to C$ the natural projection.

$$0 \to A \underset{t}{\overset{q}{\rightleftarrows}} A \oplus C \underset{u}{\overset{r}{\rightleftarrows}} C \to 0$$

proof of Splitting lemma

Alternatively (without citing splitting lemma), let $K = \ker(f)$. We want to show $K \cap M = 0$, and $F = K + M$.

Since $f \circ g = id_M$, $g : M \to F$ is injective, so we are actually thinking about M as $g(M) \leq F$

If $a \in K \cap M$, then $a = g(b)$ for some $b \in F$, and $f(a) = 0$. We have
$0 = f(a) = f(g(b)) = b \Rightarrow a = g(b) = g(0) = 0$. So $K \cap M = 0$.

Now let $a \in F$. We want to show $a \in K + M$. Write $a = (a - g(f(a))) + g(f(a))$.
Now $f(a - g(f(a))) = f(a) - f \circ g(f(a)) = f(a) - f(a) = 0$, so $(a - g(f(a))) \in K$.
Clearly $g(f(a)) \in M$ ← Remember that M denotes $g(M) \leq F$.

($\Leftarrow$) Suppose $F = M \oplus N$ is free, and let $f : L \twoheadrightarrow M$ be a surjection of R-modules.
Define $f' : L \oplus N \to M \oplus N$ by $f'(l, n) = (f(l), n)$, i.e. $f' = f \oplus id_N$. Then f' is a surjection.
By part (a), since $M \oplus N$ is free, there is $g' : M \oplus N \to L \oplus N$ such that $f' \circ g' = id_{M \oplus N}$.
Define $g : M \to L$ by $g = g'|_M$, i.e. $g(m) = l$, where $g'(m, 0) = (l, 0)$.
Then $f \circ g = id_M$, since

we are just considering these equivalent

$$f(g(m)) \equiv f'(g'(m, 0)) = (m, 0) \equiv m.$$

(c) In linear algebra, a "projection" is a matrix A such that $A^2 = A$. More generally, if R is a commutative ring, we might say that an R-projection is an R-module homomorphism $A : R^n \to R^n$ such that $A^2 = A$. For R a commutative ring, prove that a finitely generated R-module M is projective if and only if it is the image of some projection.

($\Leftarrow$) Let $A: R^n \to R^n$ be a projection. We claim that $R^n = \text{img}(A) \oplus \ker(A)$.
If $a \in \text{img}(A) \cap \ker(A)$, then $a = A(b)$ for some b, and we have $0 = A(a) = A^2(b) = A(b) = a$.
So $\text{img}(A) \cap \ker(A) = 0$.
Also, if $a \in R^n$, then $a = (a - A(a)) + A(a)$, where $a - A(a) \in \ker(A)$, and $A(a) \in \text{img}(A)$,
so $R^n = \text{img}(A) + \ker(A)$. Thus we conclude by part (b) that $\text{img}(A)$ is projective.

($\Rightarrow$) Suppose M is projective. By part (b), we know $M \oplus N = R^n$ ← We can assume finitely generated because M is f.g., so $R^n \twoheadrightarrow M$ for finite $n \Rightarrow R^n = M \oplus N$ as proven in part (b).
Take $A: M \oplus N \to M \oplus N$ as $A(m,n) = A(m,0)$.

3. (January 2013 Problem 3) We say that a ring R is *Von Neumann regular* if, for every $a \in R$ there exists an $x \in R$ such that $a = axa$. The element x is called a weak inverse of a. In particular, every division algebra is von Neumann regular (just take $x = 0$ if $a = 0$ and $x = a^{-1}$ otherwise).

(a) Give an example of a commuatative von Neumann regular ring which is not a field.

In a commutative ring, the condition is equivalent to $a = a^2x$. In $\mathbb{Z}/6\mathbb{Z}$, we have $0 = 0^2 \cdot x$, $1 = 1^2 \cdot 1$, $2 = 2^2 \cdot 2$, $3 = 3^2 \cdot 1$, $4 = 4^2 \cdot 1$, $5 = 5^2 \cdot 5$. Thus $\mathbb{Z}/6\mathbb{Z}$ is von Neumann regular.

(b) Let R be $M_2(\mathbb{C})$ and let a be the nilpotent matrix e_{12} which ends e_1 to 0 and e_2 to e_1. Give a weak inverse for a.

We are solving $E_{12} = E_{12}XE_{12}$. If $X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}$, we compute $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & x_2 \\ 0 & 0 \end{bmatrix}$, so $x_2 = 1$, so let $X = \begin{bmatrix} * & 1 \\ * & * \end{bmatrix}$

More complicated way to think about it, but also more general (like part c)

Alternatively, we can think more abstractly:
We have $a: e_1 \mapsto 0$, $e_2 \to e_1$. We want aXa: $e_1 \xrightarrow{a} 0 \xrightarrow{X} ? \xrightarrow{a} 0$, $e_2 \xrightarrow{a} e_1 \xrightarrow{X} ? \xrightarrow{a} e_1$
Since a kills e_1, X can send e_1 anywhere.
We need X to send e_1 to a vector which a sends to e_1. This vector could be e_2.
So let X be the matrix sending $e_1 \mapsto e_2$, and e_2 anywhere

(c) Prove that if V is a vector space over a field k, the ring of endomorphisms $End_k V$ is von Neumann Regular.

Let $A \in End_k(V)$. We want to solve $AXA = A$.
Let $\{b_\alpha\}$ be a basis for $\ker(A)$. This completes to a basis for V, $\{b_\alpha\} \cup \{c_\beta\}$. By the Rank-Nullity Theorem, $\{b_\alpha\} \cup \{A(c_\beta)\}$ is also a basis of V.

Rank-Nullity Theorem:
If $T: V \to W$ is a linear map of vector spaces, then
$\dim(\text{im}(T)) + \dim(\ker(T)) = \dim V$
and $V/\ker T \cong \text{im} T$

To define $X: V \to V$, we only need to define it on the basis. For each b_α, we want $AXA(b_\alpha) = A(b_\alpha) = 0$, and this will be true for any endomorphism X. For each c_β, we want $AXA(c_\beta) = A(c_\beta)$, so define $X(A(c_\beta)) = c_\beta$. Thus we have defined X on the basis $\{b_\alpha\} \cup \{A(c_\beta)\}$, and this extends to a map $X: V \to V$ with $AXA = A$.

Rank-Nullity for Endomorphisms:
If $T: V \to V$, then $V \cong \ker(T) \oplus \text{im}(T)$.

4. (January 2004 Problem 5) Let R be a ring with 1 and let V be a left R-module. Suppose that $V = X \oplus Y$ is the internal direct sum of the two non-zero submodules X and Y.

   (a) Show that $0, X, Y$, and V are the only R-submodules of V if and only if X and Y are non-isomorphic simple R-modules.

($\Leftarrow$) Assume X and Y are non-isomorphic simple submodules of V, and let U be any other submodule of V. Since X is simple, $U \cap X = 0$.

Intersection of submodules is a submodule

We also know that $U + X = V$, since Y is simple and therefore cyclic.

An element of U has the form (x, y) for $y \neq 0$, and any such y generates Y

Thus we have

$$Y = V/X = (U+X)/X \cong U/(U \cap X) = U/0 = U$$

The same argument shows that $X = U$, which contradicts the assumption that $X \ncong Y$.

Simple Modules:
The simple modules over a ring R are the modules over R that have no nonzero proper submodules.

Equivalently, a module M is simple if and only if every cyclic submodule generated by a nonzero element of M equals M.

Second Isomorphism Theorem for Modules:
Let M be a module, and let S and T be submodules of M. Then

$$\frac{S+T}{T} \cong \frac{S}{S \cap T}$$

($\Rightarrow$) Assume $0, X, Y$, and V are the only submodules of V. Then X and Y must be simple, since any submodule of X or Y is a submodule of V.

Suppose $X \cong Y$, and let $\varphi : X \to Y$ be an isomorphism. Define $U = \{x - \varphi(x)\}$. U is a nonzero submodule of V which is not X, Y, or V. This is a contradiction, so we conclude that $X \ncong Y$.

$X \cap U = 0$, since $x - \varphi(x) \in X \Rightarrow \varphi(x) \in X \Rightarrow x = \varphi(x) = 0$

   (b) If X and Y are non-isomorphic simple R-modules, prove that $End_R(V)$, the ring of R-endomorphisms of V, is isomorphic to the direct sum of two division rings.

Since X and Y are simple, Schur's Lemma tells us that any nonzero map $X \to Y$ is an isomorphism. But $X \ncong Y$, so we have $\mathrm{Hom}_R(X, Y) = 0$, and similarly $\mathrm{Hom}_R(Y, X) = 0$.

If $V = X \oplus Y$ for R-modules V, X, Y, then

$$\mathrm{End}_R(V) = \mathrm{End}_R(X) \oplus \mathrm{End}_R(Y) \oplus \mathrm{Hom}_R(X, Y) \oplus \mathrm{Hom}_R(Y, X)$$

Thus we have $\mathrm{End}_R(V) = \mathrm{End}_R(X) \oplus \mathrm{End}_R(Y)$.
Again by Schur's lemma, any nonzero endomorphism of X must be an isomorphism, and is therefore invertible.
Thus $\mathrm{End}_R(X)$ and similarly $\mathrm{End}_R(Y)$ are both division rings.

The endomorphism ring of a simple module is a division ring.

sometimes this is the statement of Schur's

Schur's Lemma (for Modules):
If M and N are two simple modules over a ring R, then any homomorphism $f : M \to N$ of R-modules is either invertible or zero.

Division Ring:
A division ring, also called a skew field, is a nonzero ring in which every nonzero element has a multiplicative inverse. They differ from fields only in that they are not required to be commutative.

5. (August 2008 Problem 5) Let R be a subring of the ring $M_n(\mathbb{C})$ of all complex $n \times n$ matrices, and suppose that R is finitely generated as a module over the integers $\mathbb{Z}$. Let $M \in R$.

(a) Show that M is contained in a commutative subring S of $M_n(\mathbb{C})$ that is finitely generated as a $\mathbb{Z}$-module.

Noetherian Module
A module is Noetherian if one of the following equivalent conditions hold:
- Every submodule is finitely generated
- Every ascending chain of submodules is eventually constant
- Every nonempty set of submodules contains a maximal element.

Noetherian Ring
A ring is said to be Noetherian if it is a Noetherian module over itself. Note the submodules in this case are just the ideals.

Let $S = \mathbb{Z}[M] = \{a_0 + a_1 M + \cdots + a_n M^n \mid a_i \in \mathbb{Z}\}$. Clearly S is commutative.
Since R is finitely generated over $\mathbb{Z}$, and $\mathbb{Z}$ is Noetherian, S must be finitely generated.

If R is a Noetherian ring, then every finitely generated R-module is Noetherian.

(b) Deduce that there is a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(M) = 0$.

Integral Ring Extension
Let S be a commutative ring with 1, and let R be a subring. We call $R \subseteq S$ a ring extension.
An element $s \in S$ is called is called integral over R if there exists a monic polynomial $f \in R[x]$ such that $f(s) = 0$. If every $s \in S$ is integral over R, then S is said to be integral over R.

Theorem
Let $R \subseteq S$ be a ring extension, and let $s \in S$. The following are equivalent:
(a) s is integral over R
(b) $R[s]$ is finitely generated as an R-module.
(c) There exists a ring extension $R[s] \subseteq S'$ such that S' is finitely generated as an R-module

Since $\mathbb{Z}[M]$ is finitely generated over $\mathbb{Z}$, s is integral over $\mathbb{Z}$, and so by definition of integral, there is a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(M) = 0$.

Without applying theorem:

proof that (b) $\Rightarrow$ (a) in theorem

Let $\mathbb{Z}[M]$ be generated by $g_1, \ldots, g_n$. For each g_i, $Mg_i \in \mathbb{Z}[M]$, and so for each i, we are $Mg_i = a_{1i} g_1 + a_{2i} g_2 + \cdots + a_{ni} g_n$ where $a_{ij} \in \mathbb{Z}$. This can be written as the matrix ation

$$Mg = Ag, \quad \text{where } A = (a_{ij}), \text{ and } g = \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix}$$

Note that the vector space we are considering here is $\mathbb{Z}[M]^n$

Then $(MI_n - A)g = 0$. This does not immediately imply $\det(MI_n - A) = 0$ because we are not working over a field.

Let $B = \operatorname{adj}(MI_n - A)$. Then
$$0 = B(MI_n - A)g = \det(M_n I_n - A) I_n g = \det(MI_n - A)g$$

This implies that $\det(MI_n - A)\,\mathbb{Z}[M] = 0$, since the entries of g generate $\mathbb{Z}[M]$. Thus $\det(MI_n - A) = 0$. Now $\det(MI_n - A)$ is a monic polynomial in M of degree n with coefficients in $\mathbb{Z}$.

Laplace's Formula
If A is an $n \times n$ matrix over a ring R, then we have
$$A \operatorname{adj}(A) = \operatorname{adj}(A) A = \det(A) I_n,$$
where $\operatorname{adj}(A)$ is the adjugate of A, that is, the transpose of the cofactor matrix of A.

(c) Prove that $tr(M)$, the matrix trace of M, is an algebraic integer.

The trace induces map of $\mathbb{Z}$-modules $tr: \mathbb{Z}[M] \to \mathbb{C}$. The image must be finitely generated as a $\mathbb{Z}$-module since $\mathbb{Z}[M]$ is. Thus the ring extension $\mathbb{Z} \subseteq \text{im}(tr)$ is a finitely generated extension of commutative rings, which implies $\text{im}(tr)$ is integral over $\mathbb{Z}$.

For each $\alpha \in \text{im}(tr)$, we have the extension $\mathbb{Z}[\alpha] \subseteq \text{im}(tr)$, and so we can use (c) $\Rightarrow$ (a) in the theorem to conclude α is integral over $\mathbb{Z}$.

Since $\alpha \in \text{im}(tr)$ is integral over $\mathbb{Z}$, in particular $tr(M)$ is integral over $\mathbb{Z}$, i.e. $tr(M)$ is an algebraic integer.

Algebraic Integer:
An algebraic integer is a complex number that is a root of some monic polynomial with coefficients in $\mathbb{Z}$, i.e. an element of $\mathbb{C}$ which is integral over $\mathbb{Z}$.

Alternatively, by part (b), there is a monic polynomial $f \in \mathbb{Z}[x]$ with $f(M) = 0$. If p is the minimal polynomial of M, then p must divide f.

The minimal polynomial has coefficients in $\mathbb{C}$.

Thus the roots of p, which are the eigenvalues of M, are also roots of f.
So we can say that each eigenvalue λ is algebraic, since $f(\lambda) = 0$.
Since $tr(M)$ is the sum of the eigenvalues of M, we conclude that $tr(M)$ is algebraic.

2. (January 2014 Problem 4) Recall that a module M for a commutative ring R is called *torsion* if, for each $m \in M$, there exists a non-zero-divisor element of r such that $rm = 0$, and M is called *torsion-free* if $rm = 0$ implies that r is a zero divisor or $m = 0$.

   (a) If M and N are torsion modules, prove that $M \otimes_R N$ is torsion. If M and N are torsion-free modules, on the other hand, $M \otimes_R N$ need not be torsion free. For example, let I be the ideal (x, y) in the ring $R = \mathbb{C}[x, y]$, which is torsion-free because R is an integral domain. Prove that $I \otimes_R I$ is not torsion free by means of the following two steps:

If N and M are torsion, then any simple tensor $n \otimes m$ is torsion, $rn = 0 \Rightarrow r(n \otimes m) = 0$.
Since any element of $M \otimes N$ can be written as $\sum_{i=1}^{n} a_i \otimes b_i$, we can take $r = r_1 \cdots r_n$, where $r_i(a_i \otimes b_i) = 0$, r_i is not a zero-divisor. Then $r \sum_{i=1}^{n} a_i \otimes b_i = 0$, and r is not a zero-divisor.
Thus $M \otimes N$ is torsion.

   (b) Show that $x \otimes y - y \otimes x \in I \otimes_R I$ is a torsion element;

We have $xy(x \otimes y - y \otimes x) = xy \otimes xy - xy \otimes xy = 0$.

   (c) Show that $x \otimes y - y \otimes x \neq 0$.

Note that we are considering $\mathbb{C}$ to be an R-module, with $fa = f(0,0) \cdot a$ for $f \in R$, $a \in \mathbb{C}$.

Define $\varphi : I \times I \to \mathbb{C}$ by $\varphi(f, g) = f_x(0,0) g_y(0,0)$.
Clearly $\varphi(f_1 + f_2, g) = \varphi(f_1, g) + \varphi(f_2, g)$, and $\varphi(f, g_1 + g_2) = \varphi(f, g_1) + \varphi(f, g_2)$.
We want to show that $p\varphi(f, g) = \varphi(pf, g) = \varphi(f, pg)$ for $p \in R$.
We have

$$\varphi(pf, g) = [(pf)_x g_y](0,0) = [p_x f g_y + p f_x g_y](0,0) = [p f_x g_y](0,0) = p\varphi(f, g)$$

($f(0,0) = g(0,0) = 0$ since $f, g \in I = (x, y)$)

$$\varphi(f, pg) = [f_x (pg)_y](0,0) = [f_x p_y g + f_x p g_y](0,0) = [f_x p g_y](0,0) = p\varphi(f, g).$$

So φ is R-bilinear, and thus induces a map $I \otimes_R I \to \mathbb{C}$.
We have $\varphi(x \otimes y - y \otimes x) = 1 \cdot 1 - 0 \cdot 0 = 1$. This implies that $x \otimes y - y \otimes x \neq 0$.

3. (August 2014 Problem 4) Let R be a commutative ring and M an R-module. Recall that a prime ideal P is an associated prime of M if there exists some $m \in M$ such that P consists of those f such that $fm = 0$; i.e., P is the *annihilator* of some $m \in M$.

(a) Let

$$0 \to M' \to M \to M'' \to 0$$

be an exact sequence of R-modules, and let P be an associated prime of M. Prove that P is an associated prime of either M' or M''.

Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be exact, and let P be an associated prime of M.
Then $P = \text{Ann}(m)$ for some $m \in M$. Suppose P is not associated to M'. We will show P is associated to M''.

Claim: If $a \in R - P$, then am is not in the image of f. In particular, m is not in the image of f.
proof:
First note that $\text{Ann}(m) = \text{Ann}(am)$ for $a \in R - P$, since
$b(am) = 0 \Rightarrow (ba)m = 0 \Rightarrow ba \in \text{Ann}(m) = P \Rightarrow b \in P$ ← P is prime, and $a \notin P$.
$bm = 0 \Rightarrow bam = 0 \Rightarrow b \in \text{Ann}(am)$
If $am = f(m')$ for some m', then $\text{Ann}(m') = \text{Ann}(am) = P$, which contradicts the assumption that P is not associated to M'.
Since f is injective, we can consider $M' \subseteq M$ as a submodule

We claim that $P = \text{Ann}(g(m))$, and hence P is associated to M''.
First, if $b \in P$, then $bg(m) = g(bm) = g(0) = 0$, so $b \in \text{Ann}(g(m))$.
Also, if $b \in \text{Ann}(g(m))$, then $0 = bg(m) = g(bm)$, which implies $bm \in \ker g = \text{im} f$ by exactness. The claim implies $b \in P$.

(b) Is the converse true? That is, if P is an associated prime of either M' or M'', must it be the case that P is an associated prime of M?

Consider the exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}.$$

The only associated prime of $\mathbb{Z}$ is 0.
The associated prime of $\mathbb{Z}/2\mathbb{Z}$ is $\text{Ann}(1) = (2)$
Note that $\text{Ann}(0) = \mathbb{Z}$ is not a prime ideal

Intuition
When you quotient a module, you gain torsion. So the annihilator of a given element has the chance to "get bigger".

1. (January 2015 Problem 3) Let $R = k[x]$, for k an algebraically closed field, and let M be a finitely generated R-module. Define the rank of M to be the dimension of the $k(x)$-vector space $M_{(0)}$. (Here (0) is the prime ideal in R, and the subscript denotes localization.)

   (a) Prove that the rank of M is finite.

Localization of a Module:
The localization of an R-module M is a systematic way to construct a new module $S^{-1}M$ containing algebraic fractions $\frac{m}{s}$, where the denominators s range in a given subset $S \subseteq R$.
$S^{-1}M$ consists of equivalence classes, where $\frac{m}{s} \equiv \frac{n}{t}$ if there is $u \in S$ with $u(sn - tm) = 0$.
The localization of a ring is just the localization of the ring as a module over itself.
If P is a prime ideal of R then we denote $(R-P)^{-1}M$ as M_P

Since M is finitely generated as an R-module, there is a surjection $R^n \to M$ for some finite n. Thus we have an exact sequence

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

where K is an R-module. Thus we have the exact sequence

$$0 \to K_{(0)} \to R^n_{(0)} \to M_{(0)} \to 0.$$

Localization commutes with direct sums

Localization of a module is an exact functor.

Now $R^n_{(0)} = [R_{(0)}]^n = [k[x]_{(0)}]^n = [k(x)]^n$. Thus we have a surjection $k(x)^n \to M_{(0)}$, which implies $\dim_{k(x)} M_{(0)} < n$.

   (b) If the rank of M is zero, prove that there exists a polynomial $f \in R$ such that $M_f = 0$.

If the rank of M is zero, then $\dim_{k(x)} M_{(0)} = 0$, and thus $M_{(0)} = 0$. $\frac{m}{s} = \frac{0}{f} \iff mf = 0$
So for each $m \in M$, there is $f \in R - (0)$ such that $fm = 0$.
Let $\{m_i\}$ be a finite set of generators of M, and let $f_i \in R - (0)$ be such that $f_i m_i = 0$.

Let $F = \prod_i f_i$. Then for any $m = \sum_i a_i m_i$ in M, we have

$$Fm = \sum_i \left(a_i \prod_{j \neq i} f_j\right) f_i m_i = 0.$$

If we consider m as an element of M_F, we have

$$m = \frac{F}{F} m = \frac{Fm}{F} = 0,$$

which implies $M_F = 0$.

If R is an integral domain, then $\frac{m}{s} = \frac{n}{t}$ iff $sn - tm = 0$. In other words, fractions work "as we expect."

(c) Consider the function $f : k \to \mathbb{Z}$ given by

$$f(a) = \dim_k M \otimes_R R/(x-a)$$

Prove that for all but finitely many $a \in k$ we have $f(a) = \operatorname{rank} M$.

Since $k[x]$ is a PID, by the structure theorem for finitely generated modules over a PID, we can say

$M = k[x]^r \oplus k[x]/Q_1 \oplus k[x]/Q_2 \oplus \cdots \oplus k[x]/Q_n$

where each Q_i is a primary ideal.

Since $k[x]$ is a PID, and since k is algebraically closed, every prime ideal of $k[x]$ has the form $(x-a)$ for $a \in k$.

In a PID, the primary ideals coincide with the powers of prime ideals → So each primary ideal Q_i has the form $Q_i = (x-a_i)^{m_i}$

Let $S = k - \{a_1, \ldots, a_n\}$. We show that for $b \in S$, $\dim_k M \otimes_R R/(x-b) = \operatorname{rank} M = r$

If $b \in S$, then $(x-b)$ and $(x-a_i)$ are relatively prime for each i, and so $R/(x-a_i)^{m_i} \otimes R/(x-b) = 0$ ← same reasoning as $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$

We conclude that

$$M \otimes_R R/(x-b) = R^r \otimes_R R/(x-b) = (R/(x-b))^r$$

(from distributing tensor over direct sum)

Thus $f(b) = \dim_k (k[x]/(x-b))^r = r$

Now we calculate $\operatorname{rank} M = \dim_{k(x)} M_{(0)}$.

We have $M_{(0)} = M \otimes_R k(x)$ ← $S^{-1}M = M \otimes_R S^{-1}R$

And so $\operatorname{rank} M = \dim_{k(x)} M \otimes_R k(x) = \dim_{k(x)} R^r \otimes k(x) = \dim_{k(x)} k(x)^r = r$.

Structure Theorem:

Invariant factor decomposition: For every finitely generated module M over a principal ideal domain R, there is a unique decreasing sequence of proper ideals $(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_n)$ such that M is isomorphic to the sum of cyclic modules:

$$M \cong \bigoplus_i R/(d_i) = R/(d_1) \oplus R/(d_2) \oplus \cdots R/(d_n)$$

The generators d_i are unique up to multiplication by a unit. The inclusion of ideals gives $d_1 | d_2 | \cdots | d_n$. The free part corresponds to $d_i = 0$, and so we may rewrite

$$M \cong R^f \oplus R/(d_1) \oplus \cdots \oplus R/(d_{n-f})$$

Primary Decomposition: For every finitely generated module M over a principal ideal domain R, we can write

$$M \cong \bigoplus_i R/(q_i)$$

where $(q_i) \neq R$ and (q_i) are primary ideals. The q_i are unique up to multiplication of units. We may also write

$$M \cong R^f \oplus \left(\bigoplus_i R/(q_i)\right)$$

where each copy of R corresponds to $q_i = 0$.