1 Let $R = F[x_1, \ldots, x_n]$, where F is an infinite field (or characteristic zero or algebraically closed). An element $P(x_1, \ldots, x_n) \in R$ is said to be homogeneous of degree r if

$$\lambda^r P(x_1, \ldots, x_n) = P(\lambda x_1, \ldots, \lambda x_n).$$

a. Show that any element P in R is a sum of homogeneous elements of degree $0, 1, 2, \ldots$.

b. An ideal I is homogeneous of I is generated by homogeneous elements. Suppose I is generated by homogeneous elements $f_1, \ldots, f_k$. Show that any homogeneous $g \in I$ can be expressed as

$$g = \sum_i g_i f_i,$$

where the $g_i \in R$ are homogeneous.

Solution a. Each term of $P(x_1, \ldots, x_n)$ is of the form $a x_1^{k_1} \cdots x_n^{k_n}$. It's easy to see that this is homogeneous of order $k_1 + \cdots + k_n$.

b. Let $g \in I$ be homogeneous. From part (a), we know that g is a sum of homogeneous elements. In fact, these elements must have the same order of homogeneity as g, since they are of the form above, i.e., they have the same power.

Now consider all the terms of g which are divisible by f_i. We collect them and set their sum as g_i. g_i must also be homogeneous, or else $g_i f_i$ will not be. This gives us the desired expression for g.

---

2 Let F be a field of characteristic zero. Suppose G is a finite subgroup of $\mathrm{GL}(n, F)$. Then $\mathrm{GL}(n, F)$ acts on $R = F[x_1, \ldots, x_n]$ be linear substitution as follows: Let A be an invertible $n \times n$ matrix and $P \in R$. We can define a new polynomial P_A by linear substitution. So for $n = 4$,

$$P_A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = P \left[A^{-1} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \right]$$

We get $\tau(A) \colon R \to R$, $\tau(A)(P) = P_A$.

Let $S \subseteq F[x_1, \ldots, x_n]$ be the ring of invariant polynomials under the action of G, i.e., $P \in S$ means that

$$P(x_1, \ldots, x_n) = P(g^{-1}(x_1, \ldots, g_n))$$

for all $g \in G$. Let M be the ideal of S generated by all homogeneous elements of S of positive degree. Let $\varphi \colon R \to R$ be defined by

$$\varphi(P) = \frac{1}{|G|} \sum_{g \in G} P(g^{-1}(x_1, \ldots, x_n)).$$

a. Show τ is a group homomorphism: $\tau(AB) = \tau(A)\tau(B)$.

b. Show any element of S can be written as a sum of homogeneous elements of S.

c. Show that you can find $f_1, \ldots, f_k \in S$ so that the f_i are homogeneous and the f_i generate the ideal MR of R. MR is the ideal of R generated by the elements of S.

d. Show $\varphi \colon R \to S$ and that φ restricted to S is the identity.

e. Show that if $P \in R$ and $P = \sum g_i f_i$, then $\varphi(P) = \sum \varphi(g_i) f_i$.

f. Show any element P of S is a polynomial in $f_1, \ldots, f_k$.

Solution a. Notice that we can write $\tau(A)(P) = P \circ A^{-1}$. Then

$$\tau(AB) = P \circ B^{-1} \circ A^{-1} = \tau(B) \circ A^{-1} = \tau(A) \circ \tau(B),$$

so τ is a group homomorphism.

b. We will prove this by induction on the power of P.

Base step: $n = 0$

If P is a constant, then the action of G does not change this constant, and the constant is homogeneous of order 0, so the base case holds.

Inductive step:

Now suppose P has degree n. By subtracting off lower order terms, get a sum of higher order term $\sum ax_1^{k_1} \cdots x_n^{k_n}$, where $k_1 + \cdots + k_n$ add up to the degree of P. This term must be invariant under the action of G because it is P minus the lower order terms, which is invariant under G. Moreover, this term is homogeneous, since all the terms have the order power. Hence, the inductive step holds.

c. MR is an ideal of R, and by Hilbert's basis theorem, MR is finitely generated by, say, $g_1, \ldots, g_s$. By definition, each g_i is a finite linear combination of elements of M, say $g_i = \sum_j a_{i,j} s_{i,j}$, where $s_{i,j} \in M \subseteq S$. Then the $s_{i,j}$ generate MR. Indeed, if $f \in MR$, then

$$f = \sum_i r_i g_i = \sum_i r_i \sum_j a_{i,j} s_{i,j} = \sum_{i,j} r_i a_{i,j} s_{i,j},$$

which finishes this part.

d. We just need to show that $\varphi(P)$ is invariant under the action of G. Let $h \in G$. Then

$$\varphi(P)(h^{-1}(x_1, \ldots, x_n)) = \frac{1}{|G|} \sum_{g \in G} P(h^{-1} g^{-1}(x_1, \ldots, x_n)).$$

But the action of multiplication by h^{-1} simply permutes G, so if we set $g' = gh$ for each g, the right-hand side is

$$\frac{1}{|G|} \sum_{g' \in G} P((g')^{-1}(x_1, \ldots, x_n)) = \varphi(P),$$

since we sum over all of G. Hence, φ maps R to S.

Next, if P is invariant under the action of G, then $P(g^{-1}(x_1, \ldots, x_n)) = P(x_1, \ldots, x_n)$ for any $g \in G$. Thus,

$$\varphi(P) = \frac{1}{|G|} \sum_{g \in G} P(g^{-1}(x_1, \ldots, x_n)) = \frac{1}{|G|} \sum_{g \in G} P(x_1, \ldots, x_n) = \frac{1}{|G|} \cdot |G| P = P,$$

so $\varphi|_S$ is the identity.

e. Let $P = \sum g_i f_i$. Because the f_i are invariant under the action of G, for each summand, we have

$$\begin{aligned} \varphi(g_i f_i) &= \frac{1}{|G|} \sum_{g \in G} g_i(g^{-1}(x_1, \ldots, x_n)) f_i(g^{-1}(x_1, \ldots, x_n)) \\ &= \left(\frac{1}{|G|} \sum_{g \in G} g_i(g^{-1}(x_1, \ldots, x_n)) \right) f_i((x_1, \ldots, x_n)) \\ &= \varphi(g_i) f_i. \end{aligned}$$

Summing them, we get $\varphi(P) = \sum \varphi(g_i) f_i$, as required.

f. Let $P = \sum g_i f_i \in S \subseteq MR$. Then by (d), $P = \varphi(P) = \sum \varphi(g_i) f_i$. Since each $\varphi(g_i) \in S \subseteq MR$, we can further write this as a linear combination of the f_i. Since the f_i have positive degree (by definition of M), each coefficient in this representation of $\varphi(g_i)$ has strictly smaller degree. Thus, we may repeat this process until we finally get a representation of P in terms of the f_i and polynomials of degree 0, i.e., elements of F. This shows that $P \in F[f_1, \ldots, f_k]$.

3 Let R be a Noetherian commutative ring and let I be an ideal. An ideal J is defined to be good with respect to I if $I \subseteq J$ and J is prime. An ideal J is very good with respect to I whenever K is a good ideal with respect to I and whenever $K \subseteq J$, then $K = J$. That is, J is minimal with respect to the property of being good with respect to I. Show that there are only a finite number of very good ideals with respect to a given ideal I.

Solution Consider the poset $S \coloneqq \{I \subseteq R \mid I \text{ is an ideal s.t. } I \text{ has infinitely many very good ideals}\}$ ordered by inclusion.

Suppose otherwise, and that there exists an ideal I so that there exist infinitely many very good ideals, i.e., $S \neq \emptyset$.

Now let $\mathcal{C} \subseteq S$ be a chain of S. Because R is Noetherian, $\bigcup \mathcal{C}$ is an upper bound for $\mathcal{C}$. Indeed, it is an ideal because it is a union of a nested set of ideals, and it is in $\mathcal{C}$ because it is finitely generated. Indeed, each of its generators must be contained in some ideal in $\mathcal{C}$ and because of total ordering, there is an ideal that contains all of them.

Hence, every chain in S has an upper bound, and S is nonempty, so it has a maximal element I with respect to inclusion. By assumption, I has infinitely many very good ideals.

I cannot be prime, or else it would be a very good ideal of itself, hence the only very good ideal of itself. Thus, there exist $a_1, a_2 \in R$ so that $a_1a_2 \in I$ but $a_1, a_2 \notin I$.

Since R is Noetherian, I is finitely generated, say by $r_1, \dots, r_n$. Now consider the two ideals $J_1 \coloneqq (r_1, \dots, r_n, a_1)$ and $J_2 \coloneqq (r_1, \dots, r_n, a_2)$.

Now let $K \supseteq I$ be a very good ideal of I. In particular, K is prime. Since $a_1a_2 \in I \subseteq K$, we have $a_1 \in K$ or $a_2 \in K$, which means that $J_1 \subseteq K$ or $J_2 \subseteq K$. Without loss of generality, assume that $J_1 \subseteq K$. Then K is a prime ideal containing J_1. Thus, K is a very good ideal of J_1, and the same argument holds in the case that $K \subseteq J_2$. But J_1 and J_2 both have only finitely many very good ideals, which implies that I has finitely many very good ideals, a contradiction. Hence, $S = \emptyset$, which proves the theorem.

---

4 Let R be a Noetherian integral domain. If f and g are in R and $f, g \neq 0$, we define a new set

$$(f) : (g) \coloneqq \{h \in R \mid hg \in (f)\}.$$

a. Show $(f) : (g)$ is an ideal.
b. Show that if R is a UFD, then $(f) : (g)$ is principal.
c. Show that if $(f) : (g)$ is principal for all f and g in R, then R is a UFD.

Solution a. If $a, b \in (f) : (g)$, then $ag, bg \in (f) \implies (a + b)g = ag + bg \in (f)$. If $r \in R$, then $(ra)g = r(ag) \in (f)$, so the set is an ideal.

b. Since R is a UFD, we may write f and g as a product of irreducible elements of R. Let d be the product of the factors of f which are not factors of g, counting multiplicities. We claim that $(d) = (f) : (g)$.

It's easy to see that $(d) \subseteq (f) : (g)$, since dg is divisible by f, by definition of d. Now let $h \in (f) : (g)$. By definition, there exists $b \in R$ such that $hg = bf \coloneqq c$. Then $f \mid c$ and $g \mid c$, so $d \mid c = hg$. By definition, $d \nmid g$, so $d \mid h \implies h \in (d)$. Hence, $(d) = (f) : (g)$, as required.

c. Recall that in a Noetherian ring, any element can be written as a product of irreducible elements. Hence, to show that R is a UFD, it suffices to show that irreducible elements are prime, since the existence of a prime decomposition for every element implies that R is a UFD.

Let $f \in R$ be irreducible and assume that $f \mid ab$. Now suppose $f \nmid a$, and consider $(f) : (a)$. By assumption, this is principal, so it is equal to (g) for some $g \in R$. Note that $fa \in (f)$, so $f \in (f) : (a) = (g) \implies g \mid f$.

Since f is irreducible, it follows that g is a unit or $g \approx f$. In the first case, $(f) : (a) = (1) = R$, but this means that $1 \cdot a \in (f) : (a) \implies f \mid a$, but this is impossible by assumption. In the second case, $(f) : (a) = (f)$. By assumption, $ba \in (f) \implies b \in (f) : (a) = (f) \implies f \mid b$, as required.

Hence, irreducibles are primes, so R is a UFD.

5 Let R be an integral domain and $I \subseteq R$ be an ideal. Let M be an R-module and let $U \subseteq R$ be a multiplicatively closed set: If f and g are in U, then so is fg. Consider the set of pairs of the form (m, u), where $m \in M$ and $u \in U$. Define an equivalence relation $\sim$ on these pairs:

$$(m, u) \sim (m', u') \iff \exists v \in U \text{ such that } v(u'm - um') = 0.$$

Let $U^{-1}M$ be the set of equivalence classes.

a. Define a structure of a module on $U^{-1}M$ so $U^{-1}M$ is a module over R.

b. Show that if $M \to N$ is a homomorphism of R-modules, then there is a natural extension

$$U^{-1}M \to U^{-1}N.$$

c. If

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is a short exact sequence of R modules, show

$$0 \longrightarrow U^{-1}M' \longrightarrow U^{-1}M \longrightarrow U^{-1}M'' \longrightarrow 0$$

is a short exact sequence.

Solution a. For $(m, u), (m', u') \in U^{-1}M$ and $r \in R$, set $(m, u) + (m', u') = (u'm + um', uu')$ and $r \cdot (m, u) = (rm, u)$. We now need to verify that this indeed gives an R-module structure. First, we need to check that this is well-defined. If we have $(m, u) \sim (m', u')$ and $(n, v) \sim (n', v')$, then

$$(m, u) + (n, v) = (vm + un, uv)$$
$$(m', u') + (n', v') = (v'm' + u'n', u'v').$$

Then

$$uv(v'm' + u'm') - u'v'(vm + un) = vv'(um' - u'm) + uu'(vm' - v'n).$$

Since $(m, u) \sim (m', u')$ and $(n, v) \sim (n', v')$, we can find a, b so that ab will send the above term to 0. This shows that $(vm + un, uv) \sim (v'm' + u'n', u'v')$, so addition is well-defined.

It's easy to see that $U^{-1}M$ is closed under $+$.

Next, notice that for $u, u' \in U$,

$$u' \cdot 0 - u \cdot 0 = 0,$$

so $(0, u) \sim (0, u')$. This gives us a well-defined identity under $+$, as

$$(m, u) + (0, u') = (u' \cdot m + u \cdot 0, uu') = (u'm, uu').$$

Then

$$(uu')m - u(u'm) = 0 \iff (m, u) \sim (u'm, uu'),$$

which shows that $(0, u)$ is the identity. It's also easy to verify that the inverse of (m, u) is $(-m, u)$. Lastly, the operation is commutative, since R is commutative.

Next, we need to show that $\cdot$ is well-defined. Let $r \in R$ and $(m, u) \sim (m', u')$. Then

$$r \cdot (m, u) = (rm, u) \quad \text{and} \quad r \cdot (m, u) = (rm', u').$$

Then

$$u'(rm) - u(rm') = r(u'm - um').$$

By definition of the equivalence class, we can find a which annihilates the term in the parentheses. By commutativity of R, this annihilates the entire term above, so multiplication is well-defined.

The multiplication axioms are inherited from the module structure of M, so we get an R-module structure on $U^{-1}M$.

b. Let $\varphi\colon M \to N$ be a homomorphism of R-modules. Then $\overline{\varphi}(m,u) = (\varphi(m),u)$ is a natural extension. We just need to check that this is well-defined, so let $(m,u) \sim (m',u')$. Then φ is an R-module homomorphism,

$$u'\varphi(m) - u\varphi(m') = \varphi(u'm - um').$$

We can annihilate the inside term, by definition of the equivalence class. This allows us to annihilate the entire thing, so $\overline{\varphi}$ is well-defined.

c. Let $\varphi\colon M' \to M$ and $\psi\colon M \to M''$ be homomorphisms which make the sequence exact. We'll show that $\overline{\varphi}$ and $\overline{\psi}$ will make the next sequence exact.

Exactness at $U^{-1}M'$:

We just need to show that $\overline{\varphi}$ is injective.

Suppose $\overline{\varphi}(m,u) = (0,u)$. Then $\varphi(m) = 0$, so by injectivity of φ, $m = 0$, so $(m,0) = 0$, as required.

Exactness at $U^{-1}M$:

Let $(m,u) \in \operatorname{im}\overline{\varphi}$, so that there is $(m',u) \in U^{-1}M'$ such that $\overline{\varphi}(m',u) = (m,u)$. Then $\overline{\psi}(m,u) = ((\psi \circ \varphi)(m'),u) = (0,u)$, because $\psi \circ \varphi = 0$, by exactness. Hence, $\operatorname{im}\overline{\varphi} \subseteq \ker\overline{\psi}$.

On the other hand, let $(m,u) \in \ker\overline{\psi}$, i.e., $(\psi(m),u) = 0$. Since $\operatorname{im}\varphi = \ker\psi$, there exists $m' \in M'$ so that $\varphi(m') = m$. Hence, $\overline{\varphi}(m',u) = (\varphi(m'),u) = (m,u)$. Thus, $\operatorname{im}\overline{\varphi} \supseteq \ker\overline{\psi}$, as required.

Exactness at $U^{-1}M''$:

We only need to show surjectivity of $\overline{\psi}$ here.

Let $(m'',u) \in U^{-1}M''$. Since ψ is surjective, there exists $m \in M$ so that $\psi(m) = m''$. Then $\overline{\psi}(m,u) = (m'',u)$, so $\overline{\psi}$ is surjective.

---

6 Suppose $f_1, \ldots, f_k \in R$ and let M be an R-module. Suppose

$$(f_1, \ldots, f_k) = R.$$

a. For any N a positive integer, show that there are r_i so that

$$\sum_i r_i f_i^N = 1.$$

b. Let $U(f) \coloneqq (1, f, f^2, f^3, \ldots)$, and let

$$\begin{aligned} M_i &= U(f_i)^{-1}M \quad \text{and} \\ M_{i,j} &= U(f_i f_j)^{-1}M. \end{aligned}$$

Find a natural sequence

$$0 \longrightarrow M \longrightarrow \bigoplus_i M_i \longrightarrow \bigoplus_{i<j} M_{i,j}$$

and show that this sequence is exact.

Solution a. We prove this by strong induction on N. The base case holds by assumption, so we just need to show the inductive step.

Suppose $(f_1^M, \ldots, f_k^M) = R$ for $1 \leq M \leq N-1$. We wish to show that $(f_1^N, \ldots, f_k^N) = R$ also. By assumption, there exist $r_1, \ldots, r_k$ so that

$$\sum_i r_i f_i^{N-1} = 1.$$

So, for each i, there exist s_j^i so that

$$r_i = \sum_j s_j^i f_i.$$

If we substitute these for r_i, we get a sum with terms with f_i^N, which are fine, and terms of the form $s_j^i f_1 \cdots f_{i-1} f_i^{N-1} f_{i+1} \cdots f_k$. But we can repeat the process, which raises the power of the f_i each time. This process must terminate after finitely many steps, so we eventually end up with

$$\sum_i t_i f_i^N = 1,$$

where the t_i may have some f_j factors.

b. Send $m \in M$ to $(m/1, \ldots, m/1)$ via φ, and send $(m_1/f_1^{n_1}, \ldots, m_k/f_i^{n_k}) \in \bigoplus_i M_i$ to $(m_i/f_i^{n_i} - m_j/f_j^{n_j})_{ij}$ via ψ. It's clear that $\operatorname{im}\varphi \subseteq \ker\psi$ and that φ is injective.

Conversely, suppose $m_i/f_i^{n_i} - m_j/f_j^{n_j} = 0$ for all $i < j$. Let $N_1 \in \mathbb{N}$ be the largest of the n_i. We can then replace m_i with $m_i' \coloneqq m_i f_i^n / f_i^n$ for some n so that we can write

$$(m_1/f_1^{n_1}, \ldots, m_k/f_k^{k_1}) = (m_1'/f_1^{N_1}, \ldots, m_k'/f_k^{N_1}).$$

Thus, we have

$$\frac{m_i'}{f_i^{N_1}} - \frac{m_j'}{f_j^{N_1}} = \frac{f_j^{N_1} m_i' - f_i^{N_1} m_j'}{f_i^{N_1} f_j^{N_1}} = 0$$

for all $i < j$. By definition of $M_{i,j}$ and $U(f_i f_j)$, there exists $(f_i f_j)^{N_2}$ so that

$$(f_i f_j)^{N_2}(f_j^{N_1} m_i' - f_i^{N_1} m_j') = f_i^{N_1} f_j^{N_1+N_2} m_i' - f_i^{N_1+N_2} f_j^{N_2} m_j' = 0 \implies f_i^{N_1} f_j^{N_1+N_2} m_i' = f_i^{N_1+N_2} f_j^{N_2} m_j'$$

Now set

$$m = \sum_i r_i f_i^{N_1+N_2} m_i'.$$

Then by part (a) and our previous calculation,

$$\begin{aligned}
f_i^{N_2} m_i' &= f_i^{N_2} \cdot 1 \cdot m_i' \\
&= f_i^{N_2} \left(\sum_j r_j f_j^{N_1+N_2} \right) m_i' \\
&= \sum_j r_j f_j^{N_1+N_2} f_i^{N_2} m_i' \\
&= \sum_j r_j f_j^{N_2} f_i^{N_1+N_2} m_j' \\
&= \left(\sum_j r_j f_j^{N_2} m_i' \right) f_i^{N_1+N_2} \\
&= f_i^{N_1+N_2} m.
\end{aligned}$$

This shows that

$$f_i^{N_2}\left(m_i' - f_i^{N_1} m\right) = 0 \iff m_i'/f_i^{N_1} = m,$$

by definition of the equivalence relation. This shows that $\ker\psi \supseteq \operatorname{im}\varphi$, as required.

7 Let R be a Noetherian ring and M be an R-module. An R-module M is said to be primitive if M has no submodules other than 0 and M. M is a small R-module if there is a finite sequence

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_N = M$$

so that M_k/M_{k-1} are primitive.

a. Show that if M', M, and M'' are in an exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

then if any two of M', M, and M'' are small, then so is the third.

b. Show that if

$$0 = M_0' \subseteq M_1' \subseteq M_2' \subseteq \cdots \subseteq M_P' = M$$

so that M_k'/M_{k-1}' are primitive, then $N = P$.

Solution a. We will show that being both Noetherian and Artinian is equivalent to being a small module.

" $\implies$ "

Let M_1 be a non-trival submodule of M. If M has none, then $M/0$ is simple, and M has a trivial composition chain. Now consider $S_1 = \{N \subseteq R \mid N > M\}$. Such a set is non-empty, since $M \in S_1$. Because R is Artinian, this set has a minimal element with respect to $\subseteq$. We set that to be M_2. Then M_1/M_2 is simple: By the correspondence principle, M_1/M_2 corresponds to a submodule of M_1 containing M_2. But there are only trivial ones, so there are only trivial submodules in M_1/M_2.

Continuing this process by induction, we get a sequence of submodules

$$M_1 \subseteq M_2 \subseteq \cdots$$

Since R is Noetherian, this chain must stabilize. In fact, this chain must stabilize to M, or else we can find a module in between the maximum and M, which cannot happen. Thus, there exists $n \geq 1$ so that

$$0 \coloneqq M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M,$$

and by induction, M_k/M_{k-1} are all simple.

" $\impliedby$ "

Suppose that M is not Noetherian. Then there is an infinite chain of submodules of M:

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M.$$

But this allows us to find an infinitely long chain of submodules with M_k/M_{k-1} all primitive, which contradicts part (b). Hence, M must be Noetherian. Similarly, we can show that M is Artinian using the same argument, but with an infinite descending chain of submodules of M.

Now, assume that M' and M'' are small. Then they are Noetherian and Artinian, by what we just proved. Also, let φ and ψ be the homomorphisms that make the sequence exact.

Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ be an ascending chain of submodules in M. Notice that $\varphi^{-1}(M_i)$ and $\psi(M_i)$ are both ascending chains of submodules in M' and M'', respectively. Take N large enough so that both of these chains stabilize. We want to show that M_i stabilizes to M_N also.

Notice that

$$0 \longrightarrow \varphi^{-1}(M_k) \longrightarrow M_k \longrightarrow \psi(M_k) \longrightarrow 0$$

is exact; it inherits it from the exact sequence given in the problem.

Let $x \in M_{N+i}$, for $i \geq 0$. Then $\psi(x) \in \psi(M_N)$ and $\varphi^{-1}(x) \in \varphi^{-1}(M_N)$. Thus, there exists $y \in M_N$ so that $\psi(y) = \psi(x) \implies \psi(x - y) = 0$, so $x - y \in \ker \psi = \operatorname{im} \varphi = M_k$. Because M_N is a module,

$$x = (x - y) + y \in M_N,$$

so $M_{N+i} \subseteq M_N$, which shows that the sequence stabilizes.

A similar argument works to show that M_N is additionally Artinian.

By the equivalence we proved at the beginning, this shows that M_N is small, as required.

b. For a module M, let $\ell(M)$ be the least length of the chain, which exists as long as M is small, by well-ordering.

Let $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_P = M$ be the chain with the least length.

For a strictly smaller submodule $N < M$, we" show that $\ell(N) < \ell(M)$. We have, by the second isomorphism theorem, that

$$(N \cap M_i)/(N \cap M_{i-1}) = (N \cap M_i)/((N \cap M_{i-1}) \cap M_i) \simeq (M_i \oplus N \cap M_{i-1})/M_i,$$

which is a submodule of M_{i+1}/M_i. Since it is simple, it follows that $(N \cap M_i)/(N \cap M_{i-1})$ is also simple, which means that

$$0 = N \cap M_0 \subseteq N \cap M_1 \subseteq \cdots \subseteq N \cap M_P = N$$

is a chain of the right form, so N is also small. This shows that $\ell(N) \leq \ell(M)$, since the shortest chain of N has length at most $\ell(N)$.

Now suppose that $\ell(N) = \ell(M)$, i.e., each quotient is different from the previous one. Thus, by the isomorphism we showed,

$$M_i \oplus N \cap M_{i-1} = M_i,$$

since this cannot be trivial, or else we get a repetition in the sequence. Next, notice that $N \cap M_i = M_i$. We prove this by induction:

Base step:

$N \cap M_0 = 0 = M_0$, so the base step holds.

Inductive step:

We have

$$N \cap M_k = N \cap (M_k \oplus N \cap M_{k-1}) = N \cap M_k \oplus N \cap M_{k-1} = M_{k-1} \oplus N \cap M_k = M_k,$$

by our previous observation. Hence, the inductive step holds.

In particular, this property holds for $k = P$, which means that $N = N \cap M_P = M$, but this contradicts our assumption that $N < M$. Hence, there must have been a repetition somewhere, i.e., $\ell(N) < \ell(M)$, as desired.

Now consider a sequence of the right form

$$0 = M_0' \subseteq M_1' \subseteq \cdots \subseteq M_N' = M.$$

By our previous claim, we have

$$\ell(M) > \ell(M_N') > \cdots > \ell(M_0)' > 0,$$

which means that $\ell(M) \geq N$. But by definition of ℓ, $\ell(M) \leq N$. Hence, $\ell(M) = N$, which completes the problem.

8 Suppose I is an ideal of a Noetherian ring R. Let I be an ideal maximal with respect to the property that R/I is not small. So if $I \subsetneq J$ is an ideal, then R/J is small. Show I is prime.

Solution By a lemma in the previous problem, R/I not small means that R/I is not Artinian or not Noetherian.

Assume that I is not prime, so that there are $J_1, J_2 \supsetneq I$ strictly larger ideals such that $J_1 J_2 \subseteq I$. By maximality of I, R/J_1 and R/J_2 are small, hence Noetherian and Artinian.

By the third isomorphism theorem, regarding $R/J_1 J_2$ as a submodule of R/J_2, we get

$$(R/J_1 J_2)/(R/J_2) \simeq J_2/J_1 J_2.$$

Consider the sequence

$$0 \longrightarrow J_2/J_1 J_2 \xrightarrow{\varphi} R/J_1 J_2 \xrightarrow{\psi} R/J_2 \longrightarrow 0,$$

where $j_2 + J_1 J_2$ embeds via $j_2 + J_1 J_2$ and $r + J_1 J_2 \mapsto r + J_2$. Then $\psi \circ \varphi = 0$. Moreover, if $\psi(r) = r + J_2 = J_2$, then $r \in J_2 \implies r = \varphi(r + J_1 J_2)$, so $\operatorname{im} \varphi = \ker \psi$.

If we can show that $J_2/J_1 J_2$ is small, then we're done: $R/J_1 J_2$ is not small because $J_1 J_2 \subseteq I$, and R/I is not small. On the other hand, R/J_2 and $J_2/J_1 J_2$ are both small. By the previous problem, this implies that $R/J_1 J_2$ is small, a contradiction. Hence, I must be prime.

However, I don't know how to show that $J_2/J_1 J_2$ is small.

9 If $A, B\colon V \to V$, then define

$$[A, B] = AB - BA.$$

We consider 4-tuples (V, H, X, Y), where V is a finite dimensional complex vector space and $H, X, Y\colon V \to V$ are linear. We also assume

$$[H, X] = 2X,\ [H, Y] = -2Y,\ [X, Y] = H.$$

Now suppose V is finite dimensional and that H is diagonalizable. So, we can write

$$V = \bigoplus_{\alpha} V_\alpha,$$

where the α's are the eigenvalues of H and $v \in V_\alpha$ if and only if $Hv = \alpha v$. So, the V_α's are the eigenspaces of H. (V, H, X, Y) are called irreducible if there is no non-trivial subspace $W \subseteq V$ which is invariant under X, Y, and H. For this problem, assume (V, H, X, Y) is irreducible.

a. Show that $X\colon V_\alpha \to V_{\alpha+2}$ and $Y\colon V_\alpha \to V_{\alpha-2}$ by considering $HX(v)$ and $HY(v)$ for $v \in V_\alpha$.

b. Let α_0 be one of the eigenvalues of H and suppose V is irreducible. Let

$$U = \bigoplus_{k\in\mathbb{Z}} V_{\alpha_0+2k}.$$

Show U is invariant under X, Y, and H. Show that all of the eigenvalues of H are of the form $\alpha_0 + 2n$ for $n \in \mathbb{Z}$.

c. Let n be the largest integer so that $V_{\alpha_0+2n} \neq \{0\}$ and let $v \in V_{\alpha_0+2n}$. Let $r = \alpha_0 + 2n$. Show that $XY(v) = rv$. More generally,

$$XY^k(v) = k(r - k + 1)Y^{k-1}v.$$

d. Let m be the largest integer so that $Y^m(v) \neq 0$, using the v from part (c). Show that the span U' of $v, Yv, Y^2v, \ldots, Y^m v$ is invariant under each of X, Y, H, and that U' has dimension $m + 1$. Further, $v, Yv, Y^2v, \ldots, Y^m v$ are linearly independent.

e. Show all the eigenvalues of H are integers.

f. Suppose (V, H', X', Y') satisfy the same commutation relations, (V, H', X', Y') is also irreducible, and H' is diagonalizable. Show (V, H, X, Y) and (V, H', X', Y') are isomorphic after giving a definition of isomorphism in this context.

Solution a. Let $v \in V_\alpha$. Then

$$HX(v) = (HX(v) - XH(v)) + XH(v) = 2X(v) + \alpha X(v) = (\alpha + 2)X(v),$$

so $X(v)$ is an eigenvector with eigenvalue $\alpha + 2$. Similarly,

$$HY(v) = (HY(v) - YH(v)) + YH(v) = -2Y(v) + \alpha Y(v) = (\alpha - 2)Y(v),$$

so $Y(v)$ is an eigenvector with eigenvalue $\alpha - 2$.

b. Let $v = \sum c_k v_{\alpha_0+2k} \in U$. Then by linearity of X, Y, and H,

$$\begin{aligned}
X(v) &= \sum_{k\in\mathbb{Z}} c_k X(v_{\alpha_0+2k}) \in \bigoplus_{k\in\mathbb{Z}} V_{\alpha_0+2(k+1)} = U\\
Y(v) &= \sum_{k\in\mathbb{Z}} c_k Y(v_{\alpha_0+2k}) \in \bigoplus_{k\in\mathbb{Z}} V_{\alpha_0+2(k-1)} = U\\
H(v) &= \sum_{k\in\mathbb{Z}} c_k(\alpha_0 + 2k)v_{\alpha_0+2k} \in \bigoplus_{k\in\mathbb{Z}} V_{\alpha_0+2k} = U,
\end{aligned}$$

so U is invariant under these operators. Since V is irreducible, this implies that $U = \{0\}$ or $U = V$. Clearly $U \neq \{0\}$, since H has eigenvectors, so $U = V$. Hence, all the eigenvalues of V are of the given form.

c. Notice that $V_{\alpha_0+2(n+1)} = \{0\}$, so since $X(v) \in V_{\alpha_0+2(n+1)}$, $X(v) = 0$. Hence,

$$rv = H(v) = XY(v) - YX(v) = XY(v),$$

as required. We will prove the general result via induction:
Suppose $XY^{k-1}(v) = (k-1)(r-k+2)Y^{k-2}v$. Notice that

$$XY = H + YX \implies XY^k = HY^{k-1} + YXY^{k-1}.$$

Applying both sides to v, we get

$$\begin{aligned}
XY^k(v) &= HY^{k-1}(v) + YXY^{k-1}(v) \\
&= (r-2(k-1))Y^{k-1}(v) + (k-1)(r-k+2)Y^{k-1}(v) \\
&= (r-2(k-1))Y^{k-1}(v) + k(r-k+2)Y^{k-1}(v) - (r-k+2)Y^{k-1}(v) \\
&= (r-2(k-1))Y^{k-1}(v) + \left[kY^{k-1}(v) + k(r-k+1)Y^{k-1}(v)\right] - \left[Y^{k-1}(v) + (r-k+1)Y^{k-1}(v)\right] \\
&= (r-k+1)Y^{k-1}(v) + k(r-k+1)Y^{k-1}(v) - (r-k+1)Y^{k-1}(v) \\
&= k(r-k+1)Y^{k-1}(v),
\end{aligned}$$

so the inductive step holds.

d. Applying X to a vector reduces its power of Y by 1, for the terms $Y^k(v)$, $1 \leq k \leq m$. When $k = 0$, then we get $X(v) = 0$, by the same argument as before. Thus, the subspace is invariant under X.
For Y, we raise the power of Y by 1 for each $Y^k v$, for $0 \leq k \leq m-1$. When $k = m$, we get $Y^{m+1}(v) = 0$, by maximality of m. Thus, the subspace is also invariant under Y.
Lastly, each $Y^k v$ is an eigenvector of H, so applying H gives us a scalar multiple $Y^k v$, so the subspace is invariant under H as well.
If we show that the $v, Yv, \ldots, Y^m v$ are linearly independent, then this also shows that their span has dimension $m+1$. But this is easy: they all have different eigenvalues with respect to H, so they must be linearly independent.

e. If just one of the eigenvalues is not integral, then none of them must be, since they are all related by $\alpha_0 + 2n$. Thus, if one of them is not integral, then none of them can be integral.
Let r be as above, and assume that it is not integer. Then for any $k \geq 1$, (c) tells us that

$$XY^k(v) = \prod_{1 \leq j < k} j(r-j+1)v.$$

But this is non-zero, since none of the factors are 0 since r is non-integer. Thus, we have infinitely many $XY^k(v)$, each with a different eigenvalue, hence all linearly independent. But this implies that V is infinite dimensional, a contradiction. Hence, r must be integral.

f. The two 4-tuples are isomorphic if there exists a bijection $\Phi \colon V \to V$ such that $H' = \Phi H \Phi^{-1}$, $X' = \Phi X \Phi^{-1}$, and $Y' = \Phi Y \Phi^{-1}$.
By (c), we see that the eigenvalues of H and H' must be the same. Indeed, Y^{k-1} has the same eigenvalue λ for XY as $(Y')^{k-1}$ for $X'Y'$, for each $1 \leq k \leq m$, since r is determined by $m+1$.
Hence, let v' be such that $H'v' = rv'$, so that $v', Y'v', \ldots, (Y')^m v'$ form a basis for V, and set $\Phi(Y^k v) = (Y')^k v'$. This is an isomorphism since it sends a basis to another basis. For Y, we have for $0 \leq k \leq m$ that

$$\Phi Y \Phi^{-1}(Y')^k v' = \Phi Y Y^k v = (Y')^{k+1} v = Y'(Y')^k v,$$

so $\Phi Y \Phi^{-1} = Y'$, since they agree on a basis. Similarly, using the calculation we get from (c), we have

$$\Phi X \Phi^{-1}(Y')^k v' = \Phi X Y^k v = \Phi k(r-k+1)Y^{k-1} v = k(r-k+1)(Y')^{k-1} v = X'(Y')^k v',$$

so $\Phi X \Phi^{-1} = X'$ also. Lastly, by the commutation relations,

$$\Phi H \Phi^{-1} = \Phi(XY - YX)\Phi^{-1} = \left(\Phi X \Phi^{-1}\right)\left(\Phi Y \Phi^{-1}\right) - \left(\Phi Y \Phi^{-1}\right)\left(\Phi X \Phi^{-1}\right) = X'Y' - Y'X' = H',$$

so Φ is an isomorphism, as required.