Solutions #9

1. (a) Let $R$ be Noetherian and let $I \subset R$ be an ideal. Prove that $R/I$ is Noetherian.
   (b) Prove that $\mathbb{Z}[\sqrt{-5}]$ is Noetherian. In particular it is a Noetherian ring which is not a Unique Factorization Domain.

   Solution. (a) Set $\overline{R} := R/I$. By the Fourth Isomorphism Theorem, the ideals $\overline{I}$ of $\overline{R}$ are in a bijection with the intermediate ideals $I \subset J \subset R$. Given $\overline{J} \subset \overline{R}$, consider the corresponding $J \subset R$. Since $R$ is Noetherian, $J$ is finitely generated, i.e., $J = (a_1, a_2, \ldots, a_n)$ for some $a_i \in R$. Then clearly $\overline{J} = (\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n)$ where $\overline{a}_i = a_i + I \subset \overline{R}$. This proves that $\overline{J}$ is finitely generated.

   (b) We first establish that $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2 + 5)$. Indeed, define $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-5}]$ by $\varphi(f) := f(\sqrt{-5})$. It is clear that $\varphi$ is a surjective homomorphism. Let $f \in \mathbb{Z}[x]$. Divide $f$ by $x^2 + 5$:

   \[ f(x) = q(x)(x^2 + 5) + r(x), \quad \text{where} \quad r(x) = \alpha x + \beta. \]

   Then

   \[ f \in \text{Ker } \varphi \iff f(\sqrt{-5}) = 0 \iff r(\sqrt{-5}) = 0 \iff \alpha \sqrt{-5} + \beta = 0 \iff r = 0 \iff f \in (x^2 + 5), \]

   i.e., $\text{Ker } \varphi = (x^2 + 5)$. Thus $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2 + 5)$. Since $\mathbb{Z}$ is Noetherian (being a PID), so is $\mathbb{Z}[x]$ and part (a) implies that $\mathbb{Z}[\sqrt{-5}]$ is Noetherian as well. The fact that $\mathbb{Z}[\sqrt{-5}]$ is not a Unique Factorization Domain was discussed in class. \( \square \)

2. Let $\mathbb{F}$ be a field. The ring of polynomials of infinitely many variables $x_1, x_2, x_3, \ldots$ over $\mathbb{F}$ is by definition

   \[ \mathbb{F}[x_1, x_2, x_3, \ldots] := \bigcup_{n \in \mathbb{Z}_{>0}} \mathbb{F}[x_1, x_2, \ldots, x_n] \]

   where $\mathbb{F}[x_1, x_2, \ldots, x_k]$ is considered as a subring of $\mathbb{F}[x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n]$ for $k < n$ by

   \[ \mathbb{F}[x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n] = \mathbb{F}[x_1, x_2, \ldots, x_k][x_{k+1}, \ldots, x_n]. \]

   (a) Prove that $\mathbb{F}[x_1, x_2, x_3, \ldots]$ is a Unique Factorization Domain.
   (b) Prove that the ideal $I$ of $\mathbb{F}[x_1, x_2, x_3, \ldots]$ generated by $x_1, x_2, x_3, \ldots$ is not finitely generated. In particular $\mathbb{F}[x_1, x_2, x_3, \ldots]$ is not Noetherian.

   Solution. (a) Set $R_n := \mathbb{F}[x_1, x_2, \ldots, x_n]$ for $n \in \mathbb{Z}_{>0}$ and $R := \mathbb{F}[x_1, x_2, x_3, \ldots]$. Since $R_{n+1} = R_n[x]$ and $R_0$ is a field, we conclude that, for every $n$, $R_n$ is a UFD. Let $f \in R_n$ then one checks immediately the following statements:

   • $f$ is a unit if and only if $f \in \mathbb{F}^\times \subset R_0$;
   • If $m > n$ then $f$ is irreducible in $R_n$ if and only if $f$ is irreducible in $R_m$.

   Using the fact that every factorization in $R$ happens in some $R_n$, we conclude that for $f \in R$ we have

   • $f$ is a unit if and only if $f \in \mathbb{F}^\times \subset R_0$;
   • If $f \in R_n$ then $f$ is irreducible in $R$ if and only if $f$ is irreducible in $R_n$. 

   \[ \text{MATH 893: page 1 of 4} \]
Existence of factorization. Let \( f \in R \setminus \mathbb{F} \). Then \( f \in R_n \) for some \( n \) and since \( R_n \) is a UFD, \( f \) factors into a product of irreducibles in \( R_n \). By the remarks above, this is also a factorization into irreducibles in \( R \).

Uniqueness of factorization. Assume that
\[
 f = g_1 g_2 \ldots g_k = h_1 h_2 \ldots h_l
\]
be two factorizations of \( f \) into irreducibles in \( R \). There is an integer \( n \) such that all \( f, g_i, h_j \) belong to \( R_n \). Then the factorizations above are factorizations of \( f \) into irreducibles in \( R_n \). Since \( R_n \) is a UFD, we conclude that \( k = l \) and (after relabeling) \( f_i \) and \( g_i \) are associates.

(b) Assume, to the contrary, that \( I = (f_1, f_2, \ldots, f_k) \) is finitely generated and let \( n \) be an integer such that \( f_i \in R_n = \mathbb{F}[x_1, x_2, \ldots, x_n] \). Then, for \( m > n \), we have \( R_m = R_n[\{x_{n+1}, \ldots, x_m\}] \) and, as we have seen in class, the ideal of \( R_m \) generated by \( I \) equals \( I[\{x_{n+1}, \ldots, x_m\}] \). Our assumption implies that \( x_{n+1} \in I \), i.e.,
\[
 x_{n+1} = g_1 f_1 + g_2 f_2 + \ldots + g_k f_k.
\]
Let \( m > n \) be such that \( g_i \in R_m \) for every \( 1 \leq i \leq k \). Then the equation above shows that \( x_{n+1} \) belongs to the ideal of \( R_m \) generated by \( I \). Since the latter ideal equals \( I[\{x_{n+1}, \ldots, x_m\}] \) we conclude that \( x_{n+1} \in I[\{x_{n+1}, \ldots, x_m\}] \). This implies that \( 1 \in I \) which is a contradiction.

3. Let \( R \) be a Principal Ideal Domain and let \( Q \) be its field of fractions. Assume \( g \in R \) factors as
\[
 g = p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}
\]
where \( p_1, p_2, \ldots, p_k \) are primes in \( R \), no two of which are associates, and \( l_i \in \mathbb{Z}_{>0} \).

(a) Prove that, for any \( f \in R \) we have a decomposition
\[
 \frac{f}{g} = \frac{h_1}{p_1^{l_1}} + \frac{h_2}{p_2^{l_2}} + \ldots + \frac{h_k}{p_k^{l_k}}
\]
for some \( h_i \in R \).

(b) If \( R = \mathbb{F}[x] \) and \( \deg f < \deg g \), prove that there is a unique choice for \( h_i \) such that \( \deg h_i \leq \deg p_i^{l_i} \).

Solution. (a) Let \( g_i := \frac{g}{p_i^{l_i}} \in R \). Then \( \text{GCD}(g_1, g_2, \ldots, g_k) = 1 \) and hence \( (g_1, g_2, \ldots, g_k) = R \). In particular there exist \( u_1, u_2, \ldots, u_k \in R \) such that
\[
 u_1 g_1 + u_2 g_2 + \ldots + u_k g_k = 1.
\]
Then
\[
 f = u_1 g_1 f + u_2 g_2 f + \ldots + u_k g_k f
\]
and
\[
 \frac{f}{g} = \frac{u_1 g_1 f}{g} + \frac{u_2 g_2 f}{g} + \ldots + \frac{u_k g_k f}{g} = \frac{u_1 f}{p_1^{l_1}} + \frac{u_2 f}{p_2^{l_2}} + \ldots + \frac{u_k f}{p_k^{l_k}} = \frac{h_1}{p_1^{l_1}} + \frac{h_2}{p_2^{l_2}} + \ldots + \frac{h_k}{p_k^{l_k}}.
\]
where \( h_i := u_i f \).

**Remark.** In the assignment the problem was stated for a Unique Factorization Domain \( R \). Unfortunately, the statement is not correct in that case. Indeed, \( \mathbb{Z}[x] \) is a Unique Factorization Domain but \( \frac{1}{x} \) cannot be decomposed as \( \frac{f}{z} + \frac{g}{x} \) for any \( f, g \in \mathbb{Z}[x] \).

**(b)** Let

\[
\frac{f}{g} = \frac{h_1}{p_1^{l_1}} + \frac{h_2}{p_2^{l_2}} + \ldots + \frac{h_k}{p_k^{l_k}}
\]

be a decomposition obtain in (a) and let

\[
h_i = q_i p_i^{l_i} + r_i, \quad \text{where} \quad \deg r_i < \deg p_i^{l_i}.
\]

Then we have

\[
\frac{f}{g} = (q_1 + q_2 + \ldots + q_k) + \frac{r_1}{p_1^{l_1}} + \frac{r_2}{p_2^{l_2}} + \ldots + \frac{r_k}{p_k^{l_k}}
\]

and, setting \( q := q_1 + q_2 + \ldots + q_k \), we have

\[
f = q g + r_1 g_1 + r_2 g_2 + \ldots + r_k g_k.
\]

Noting that \( \deg f < \deg g \) and

\[
\deg(r_ig_i) = \deg r_i + \deg g_i = \deg r_i + \deg g - \deg p_i^{l_i} < \deg g,
\]

we conclude that \( \deg q g < \deg g \) which implies that \( q = 0 \) and hence

\[
\frac{f}{g} = \frac{r_1}{p_1^{l_1}} + \frac{r_2}{p_2^{l_2}} + \ldots + \frac{r_k}{p_k^{l_k}}
\]

is the desired decomposition. Note that this decomposition, i.e., the one for which \( \deg r_i < \deg p_i^{l_i} \), is unique. \( \square \)

#### 4. Consider \( f := \det \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in \mathbb{Z}[x, y, z, t] \). Prove that

**(a)** \( (f) \) is a prime ideal.

**(b)** \( \mathbb{Z}[x, y, z, t]/(f) \) is not a Unique Factorization Domain.

**Solution.** (a) It is sufficient to prove that \( f \) is irreducible and consider it as an element of \( \mathbb{Z}[x, y, z][t] \). Assume not. Since \( z \) is a polynomial of \( t \) of degree 1, it decomposes as

\[
f = \alpha(x, y, z)(\beta(x, y, z)t + \gamma(x, y, z))
\]

where \( \alpha(x, y, z) \) and \( \beta(x, y, z)t + \gamma(x, y, z) \) are not units in \( \mathbb{Z}[x, y, z] \). Comparing coefficient we have \( x = \alpha(x, y, z)\beta(x, y, z) \). Since \( \mathbb{Z}[x, y, z]/(x) \cong \mathbb{Z}[y, z] \) is a domain, we conclude that \( (x) \subset \mathbb{Z}[x, y, z] \) is a prime ideal and hence \( x \in \mathbb{Z}[x, y, z] \) is irreducible. Thus either \( \alpha \beta \) is a unit. Having assumed that \( \alpha \) is not a unit, we conclude that \( \alpha \) is an associate of \( x \). Then the identity \( -yz = \alpha \gamma \) is impossible since \( x \) does not divide \( yz \) (why?). This completes the proof that \( (f) \) is a prime ideal.
(b) It is sufficient to show that the images \( \bar{x}, \bar{y}, \bar{z}, \bar{t} \) of \( x, y, z, t \) in \( \mathbb{Z}[x, y, z, t]/(f) \) are irreducible. Indeed, then the equation \( \bar{x}\bar{t} = \bar{y}\bar{z} \) gives two distinct decompositions of an element of \( \mathbb{Z}[x, y, z, t]/(f) \) into irreducibles. Because of symmetry, we will show that \( \bar{x} \) is irreducible. Assume, to the contrary, that \( \bar{x} = \bar{a}\bar{b} \). Then \( a\beta - x \in (f) \). Let \( a = a_0 + a_1 + \ldots + a_k \) and \( \beta = \beta_0 + \beta_1 + \ldots + \beta_l \) be the decomposition of \( a \) and \( \beta \) into homogeneous polynomials (by total degree). We may assume that \( a_i, \beta_j \not\in (f) \) unless they are equal to zero. Since \( f \) is homogeneous, each homogeneous component of \( a\beta - x \) belongs to \( (f) \). (Why?). In particular, if \( k + l > 1 \), then \( a_\ell \beta_1 \in (f) \). Since \( (f) \) is prime, either \( a_\ell \) or \( \beta_1 \) belongs to \( (f) \) which contradicts our assumption. Hence \( k + l \leq 1 \) and clearly \( k + l \neq 0 \), i.e., \( k + l = 1 \). Let \( k = 0 \) and \( l = 1 \). Then

\[
a_0(\beta_0 + \beta_1) = x \in (f).
\]

Equivalently,

\[a_0\beta_0 \in (f) \quad \text{and} \quad a_0\beta_1 = x \in (f).
\]

Since both polynomials above are homogeneous of degree smaller than the degree of \( f \), we have

\[a_0\beta_0 = 0 \quad \text{and} \quad a_0\beta_1 = x = 0.
\]

Since \( x \) is irreducible in \( \mathbb{Z}[x, y, z, t] \), we conclude that \( a_0 = \pm 1, \beta_0 = 0, \) and \( \beta_1 = \pm x \), which implies that \( \bar{a} \) is a unit in \( \mathbb{Z}[x, y, z, t]/(f) \) completing the proof that \( \bar{x} \) is irreducible.

5. An \( R \)-module \( M \) is simple if the only submodules of \( M \) are 0 and \( M \). Prove:

(a) Every simple module is cyclic.
(b) (Schur’s Lemma) If \( M \) and \( N \) are simple \( R \)-modules and \( \varphi : M \to N \) is a homomorphism of \( R \)-modules then \( \varphi = 0 \) or \( \varphi \) is an isomorphism.
(c) Prove that \( \text{End}_R(M) \) is a division ring.

Solution. (a) Recall that \( M \) is cyclic if it is generated by a single element. Let \( M \) be simple and let \( m \neq 0 \) be an arbitrary element of \( M \). The submodule \( K \) of \( M \) generated by \( m \) does not equal \( 0 \) since it contains \( m \neq 0 \). Thus \( K = M \), i.e., \( M \) is generated by \( m \). Notice that we proved a stronger statement: \( M \) is generated by any non-zero element.

(b) \( \ker \varphi \) is a submodule of \( M \). If \( \ker \varphi = M \) then \( \varphi = 0 \). Otherwise \( \ker \varphi = 0 \) and \( \text{im} \varphi \) is a nonzero submodule of \( N \), i.e., \( \text{im} \varphi = N \). Thus \( \varphi \) is an isomorphism.

(c) \( \text{End}_R(M) \) is readily a ring with identity. We only need to show that every nonzero \( \varphi \in \text{End}_R(M) \) is a unit. By (b) \( \varphi \) is an isomorphism. In particular \( \varphi \) is a bijection and the map \( \varphi^{-1} \) is well-defined. One checks easily that \( \varphi^{-1} \) is a homomorphism of \( R \)-modules, i.e., that it is \( R \)-linear. Thus the map \( \varphi^{-1} \) belongs to \( \text{End}_R(M) \) which completes the proof.