2 Modules

2.7 Noetherian modules and UFD

1. Let $M = Rm_1 + \cdots + Rm_r$, then $R^r \xrightarrow{\varphi} M \to 0$, $\varphi(a_1, \cdots, a_r) = \sum a_i m_i$, is a epimorphism. For any submodule N of M, $\varphi^{-1}(N)$ is a submodule of R^r. If R^r is a Northerian ring, then $\varphi^{-1}(N)$ is finitely generated, thus $N = \varphi(\varphi^{-1}(N))$ is finitely generated, hence M is a Noetherian ring. We will proof that R^r is a Noetherian ring as follows. For any two Noetherian rings M_1, M_2, we have $0 \longrightarrow M_1 \xrightarrow{\iota} M_1 \oplus M_2 \xrightarrow{\pi} M_2 \longrightarrow 0$. For any submodule L of $M_1 \oplus M_2$, then $\pi(L) = Rx_1 + \cdots + Rx_p$, take $y_i \in L$ satisfy $\pi(y_i) = x_i$. While $Ker(\pi|_L) = L \cap M_1 \leqslant M_1$, there are $z_1, \cdots, z_q \in L \cap M_1$ such that $L \cap M_1 = Rz_1 + \cdots + Rz_q$. For any $m \in L$, assume $\pi(m) = \sum a_i x_i$, then $\pi(m - \sum a_i y_i) = 0$, thus $m - \sum a_i y_i \in L \cap M_1$, therefore $m = \sum a_i y_i + \sum b_j z_j \in Ry_1 + \cdots + Ry_p + Rz_1 + \cdots + Rz_q \subseteq L$, then L is finitely generated. Hence R^r is a Noetherian ring.

2. Assume $I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is an ascending chain on left ideals, then it is also an ascending chain of left R-module. While $M_n(R) \cong R^{n^2}$ as left R-module. According to Exercise 2.7.1, R^{n^2} is a Noetherian ring, then there is n such that $I_n = I_{n+k}, \forall k \geq 0$, hence $M_n(R)$ is a Noetherian ring.

3. $\forall \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in R$, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & c-c' \end{pmatrix} \in R$ and $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \in R$, thus R is a subring. If J is right ideal of R, according to $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}$, then J_1, J_2 are right ideals of $\mathbb{Z}$ where $J = \begin{pmatrix} J_1 & J_3 \\ 0 & J_2 \end{pmatrix}$. If $a \neq 0$, then $J_3 = \mathbb{Q}$; if $a = 0$, then $J_3 = \mathbb{Q}$. If J is a right ideal, then J can be $\begin{pmatrix} I_1 & \mathbb{Q} \\ 0 & I_2 \end{pmatrix}$ or $\begin{pmatrix} 0 & \mathbb{Q} \\ 0 & I_2 \end{pmatrix}$ where I_1, I_2 are ideals of $\mathbb{Z}$. If J is a left ideal, then J can be $\begin{pmatrix} I_1 & \mathbb{Q} \\ 0 & I_2 \end{pmatrix}$ or $\begin{pmatrix} I_1 & A \\ 0 & 0 \end{pmatrix}$ where I_1, I_2 are ideals of $\mathbb{Z}$ and $(A, +) \leqslant (\mathbb{Q}, +)$. Thus R satisfies ascending chain condition on right ideals, while $I_n = \begin{pmatrix} 0 & \frac{1}{2^n}\mathbb{Z} \\ 0 & 0 \end{pmatrix}$ is a ascending chain on left ideals. Hence R is a right Noetherian ring but not a left Noetherian ring.

4. $\Rightarrow$: If R is left Artinian and J is a Jacobson radical, then $J^n = 0$ and $R/J \cong M_{n_1}(D_1) + \cdots + M_{n_r}(D_r)$ where D_i are divisions, then R/J are Noetherian. While J^r/J^{r+1} is a R/J-module, then J^r/J^{r+1} is semisimple and an Artinian R/J-module, thus J^r/J^{r+1} is Noetherian, hence R is Noetherian.($0 = J^n \leqslant J^{n-1} \leqslant \cdots \leqslant J \leqslant R$ and $J^r/J^{r+1}, R/J$ are Noetherian, then R is Noetherian)

$\Leftarrow$: If R is left Noetherian, $J^n = 0$, R/J is semisimple, then R/J is Artinian. While J^r/J^{r+1} is a finitely generated R/J-module, J^r/J^{r+1} are Artinian. Hence R is Artinian.

5. For any $a, b \in \sqrt{I}$, $(a-b)^{n+m} = \sum\limits_{k=0}^{m+n} C_{m+n}^{k} a^{m+n-k}(-b)^k \in I$ where $a^n, b^m \in I$. For any $r \in R$, $(ar)^n = a^n r^n \in I$. Hence $\sqrt{I}$ is an ideal of R.

6. For any ideal J of $R[S^{-1}]$, let $I = \{r \in R | \frac{r}{s} \in J \ for \ some \ s \in S\}$, then $\frac{r_1}{s_1} \cdot \frac{r}{s} = \frac{r_1 r}{s_1 s}$, thus $r_1 r \in I$. $\frac{r_1 - r_2}{s_1 s_2} = \frac{r_1}{s_1} \cdot \frac{1}{s_2} - \frac{r_2}{s_2} \cdot \frac{1}{s_1} \in J$, then $r_1 - r_2 \in I$. Hence I is an ideal of R. Consider $\varphi : I \otimes_R R[S^{-1}] \to J$, $\varphi(\sum r_i \otimes_R \frac{a_i}{s_i}) = \sum \frac{r_i a_i}{s_i} = \sum \frac{r_i}{s_i} \cdot \frac{a_i s_i}{t_i} \in J$. It is obvious that φ is epimorphic. Since I is finitely generated, $I = x_1 R + \cdots + x_n R$, then $I \otimes_R R[S^{-1}] = x_1 R[S^{-1}] + \cdots + x_n R[S^{-1}]$ is finitely generated, thus $R[S^{-1}]$ is a Noetherian ring.

7. $\Rightarrow$: Let E_i is a injective R-module and for any I is a left ideal of R. Consider
$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "\lambda"] \arrow[d, "\forall f"'] & R \\ & \sum\limits_{i \in J} \oplus E_i & \end{tikzcd}$$
. Since I is finitely generated, $Imf \subseteq \sum\limits_{i \in J'} \oplus E_i$ where $J' \subseteq J$ is a finite subset. As $\sum\limits_{i \in J'} \oplus E_i$ is injective, there is $\widetilde{f} : R \to \sum\limits_{i \in J'} \oplus E_i \subseteq \sum\limits_{i \in J} \oplus E_i$ such that $\widetilde{f} \circ \lambda = f$.

$\Leftarrow$: For any ascending chain on left ideals of R $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, take injective module E_i such that $R/I_i \subseteq E_i$. Let $I = \bigcup\limits_{n=1}^{\infty} I_n$, define $f : I \to \bigoplus\limits_{i=1}^{\infty} E_i$, $f(a) = (a + I_i)_{i=1}^{\infty}$, then there is $\varphi : R \to \bigoplus\limits_{i=1}^{\infty} E_i$ such that $\varphi|_I = f$, thus $\varphi(a) = a\varphi(1)$ for any $a \in I$. Assume $\varphi(1) \in \bigoplus\limits_{i=1}^{n} E_i$, then $Imf \subseteq \bigoplus\limits_{i=1}^{n} E_i$. While $f(a) = (a + I_i)_{i=1}^{\infty}$, then $a + I_i = 0$ where $i \geq n+1$, that is $a \in I_i$, thus $\bigcup\limits_{n=1}^{\infty} I_n \subseteq I_{n+k}$ where $k \geq 1$, therefore $I_{n+1} = I_{n+1+k}$ for any $k \geq 1$. Hence R is left Noetherian.

8. Since $\sqrt{(x^2, y)} = (x, y)$ is a maximal ideal of $F[x, y]$, (x^2, y) is a primary ideal of $F[x, y]$.

9. (1) Since $x^2 \in (x) \cap (x^2, y)$ and $(xy) \in (x) \cap (x^2, y)$, $(x^2, xy) \subseteq (x) \cap (x^2, y)$. For any $xf(x, y) \in (x) \cap (x^2, y)$, $xf(x, y) = x^2 g_1(x, y) + y g_2(x, y)$, then $x | g_2(x, y)$, that is $g_2(x, y) = x\widetilde{g_2}(x, y)$, thus $xf(x, y) = x^2 g_1(x, y) + xy\widetilde{g_2}(x, y) \in (x^2, xy)$. Hence $(x^2, xy) = (x) \cap (x^2, y)$.

(2) Since $x^2 \in (x) \cap (x^2, x+y)$ and $xy = x(x+y) - x^2 \in (x) \cap (x^2, x+y)$, $(x^2, xy) \subseteq (x) \cap (x^2, x+y)$. For any $xf(x,y) \in (x) \cap (x^2, x+y)$, $xf(x,y) = x^2 g_1(x,y) + (x+y)g_2(x,y)$, then $x | g_2(x,y)$, that is $g_2(x,y) = xg_3(x,y)$, thus $xf(x,y) = x^2(g_1(x,y)+g_3(x,y)) + xyg_3(x,y) \in (x^2, xy)$. Hence $(x^2, xy) = (x) \cap (x^2, x+y)$.

(3) Since $x^2 \in (x) \cap (x^2, xy, y^2)$, $(x^2, xy) \subseteq (x) \cap (x^2, xy, y^2)$. For any $xf(x,y) \in (x) \cap (x^2, xy, y^2)$, $xf(x,y) = x^2 g_1(x,y) + xyg_2(x,y) + y^2 g_3(x,y)$, then $x | g_3(x,y)$, that is $g_3(x,y) = xg_4(x,y)$, thus $xf(x,y) = x^2 g_1(x,y) + xy(g_2(x,y) + yg_4(x,y)) \in (x^2, xy)$. Hence $(x^2, xy) = (x) \cap (x^2, xy, y^2)$.

Since (x) is a prime ideal of $F[x,y]$, (x) is a primary ideal of $F[x,y]$. Since $\sqrt{(x^2, y)} = (x, y)$ and $\sqrt{(x^2, xy, y^2)} = (x, y)$ is a maximal ideal, (x^2, y) and (x^2, xy, y^2) is a primary ideal. Since $\sqrt{(x^2, x+y)} \supseteq (x, x+y) = (x, y)$, $\sqrt{(x^2, x+y)} = (x, y)$, then $(x^2, x+y)$ is a primary ideal.

10. (a) $\Rightarrow$: If C is a primary submodule of D, if $rx \in f^{-1}(C)$ where $r \in R$ and $x \in B$, then $rf(x) \in C$, thus $f(x) \in C$ or $r^n(D/C) = 0$, therefore $x \in f^{-1}(C)$ or $f^{-1}(r^n D) = r^n f^{-1}(D) = r^n B \subseteq f^{-1}(C)$, hence $f^{-1}(C)$ is a primary submodule of B.

$\Leftarrow$: If $rx \in C$ where $r \in R$ and $x \in D$, then $f^{-1}(rx) = rf^{-1}(x) \in f^{-1}(C)$, thus $f^{-1}(x) \in f^{-1}(C)$ or $r^n B \subseteq f^{-1}(C)$, therefore $x \in C$ or $r^n f(B) = r^n D \subseteq f(f^{-1}(C)) = C$, hence C is a primary submodule of D.

(b)

$$
\begin{aligned}
r_C &= \{r \in R | r^n(D/C) = 0\} \\
&= \{r \in R | r^n D \subseteq C\} \\
&= \{r \in R | r^n B \subseteq f^{-1}(C)\} \\
&= r_{f^{-1}(C)}.
\end{aligned}
$$

11. (a) $A[S^{-1}] = A \otimes_R R[S^{-1}] \subseteq B \otimes_R R[S^{-1}]$, consider

$$
0 \to A \otimes_R R[S^{-1}] \longrightarrow B \otimes_R R[S^{-1}] \longrightarrow B/A \otimes_R R[S^{-1}] \to 0 .
$$

If $P \cap S \neq \emptyset$, then there is $r \in P \cap S$, since $P = \{r \in R | r^n(B/A) = 0\} = \{r \in R | r^n B \subseteq A\}$, $a \otimes b = a \otimes r^n(br^{-n}) = ar^n \otimes br^{-n} = 0, \forall a \in B/A, \forall b \in R[s^{-1}]$, then $B/A \otimes_R R[S^{-1}] = 0$. Thus $A[S^{-1}] = B[S^{-1}]$.

(b) For any $\frac{r}{s} \in R[S^{-1}]$ and any $\frac{x}{t} \in B[S^{-1}]$, if $\frac{r}{s} \cdot \frac{x}{t} = \frac{rx}{st} \in A[S^{-1}]$, then $\frac{rx}{st} = \frac{y}{u}$ where $y \in A, u \in S$, thus there is $v \in S$ such that $v(urx - sty) = 0$, therefore $(uvr)x = (vst)y \in A$. Hence $x \in A$ or $(uvr)^n B \subseteq A$, then $(uvr)^n B[S^{-1}] \subseteq A[S^{-1}]$. Hence $A[S^{-1}]$ is a primary submodule of $B[S^{-1}]$. It is obvious that $P[S^{-1}] \subseteq r_{A[S^{-1}]}$. For any $\frac{r}{s} \in r_{A[S^{-1}]} \backslash P[S^{-1}]$, we have $r \notin P$ and $\frac{r^n}{s^n} B[S^{-1}] \subseteq A[S^{-1}]$, then there is $x_n \in B$ such that $r^n x_n \notin A$ and $\frac{r^n}{s^n} \cdot \frac{x_n}{t_n} = \frac{y}{u} \in A[S^{-1}]$ for any $\frac{x_n}{t_n} \in B[S^{-1}]$, thus there is $v \in S$ such that $v(r^n ux_n - t_n s^n y) = 0$, therefore $r^n vux_n \in A$. Since $r^n x_n \notin A$, $uv \in P \cap S$, it is a contradiction. Hence $P[S^{-1}] = r_{A[S^{-1}]}$.

12. Let $F = R[S^{-1}]$ where $S = R \setminus 0$, then F is a field. For any $f(x) \in F[x]$, then $f(x) = \frac{a}{b} f_1(x)$ where $f_1(x) = a_n x^n + \cdots + a_1 x + a_0$ and $a_i \in R$ satisfy $(a_n, \cdots, a_0) = 1$ as R is a UFD, which is called a primitive polynomial. For any $f(x) \in R[x]$, then $f(x) = \frac{a}{b} p_1(x)^{n_1} \cdots p_r(x)^{n_r}$ in $F[x]$ where $p_i(x) \in R[x]$ are primitive polynomial and are irreducible in $F[x]$, thus $p_i(x)$ are irreducible in $R[x]$. Let $f(x) = cf_1(x)$ where $f_1(x)$ is a primitive polynomial, then $f_1(x) = up_1(x)^{n_1} \cdots p_r(x)^{n_r}$ where $u \in R$ is a unit. Since R is a UFD, then $cu = q_1 \cdots q_s$ where q_i are irreducible in R, thus q_i are irreducible in $R[x]$. Therefore $f(x) = q_1 \cdots q_s p_1(x)^{n_1} \cdots p_r(x)^{n_r}$ where q_i and $p_i(x)$ are irreducible. If $f(x) = q_1 \cdots q_s p_1(x)^{n_1} \cdots p_r(x)^{n_r} = q'_1 \cdots q'_{s'} p'_1(x)^{l_1} \cdots p'_t(x)^{l_t}$ where $p_i(x)$ and $p'(x)$ are primitive polynomial and irreducible in $R[x]$. Since $F[x]$ is a UFD, $r = t$, $n_i = l_i$ and $p_i(x) = u_i p'_i(x)$(after reorder if necessary) where u_i is a unit. Then $q_1 \cdots q_s = q'_1 \cdots q'_{s'} u$ where u is a unit in R, since R is a UFD, then $s = s'$ and $q_i = q'_i$(after reorder if necessary). Hence $R[x]$ is a UFD.

13. Since $6 = 3 \times 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, hence $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

14. $\Rightarrow$: If R is a UFD and $P \neq 0$ is a prime ideal of R, then for any $a \in P$, a is not an unit and $a = p_1^{l_1} \cdots p_r^{l_r}$ where p_i are irreducible. Since P is a prime ideal, there is $p_i \in P$ such that $(p_i) \subseteq P$. For any $a, b \in R$, if $ab \in (p_i) = Rp_i$, then $p_i | ab$, thus $p_i | a$ or $p_i | b$, therefore $a \in (p_i)$ or $b \in (p_i)$, hence (p_i) is aprime ideal of R.

    $\Leftarrow$:

    (1) Let $S = \{r \in R | r\ is\ a\ unit\ or\ r\ is\ a\ product\ of\ finite\ elements\}$ and $\Omega = \{I \lhd R | I \cap S = \emptyset\}$. Since S is a multiplicatively closed set, then there is a maximal element $P \in \Omega$, which is a prime ideal of R. If $P \neq 0$, then there is a prime ideal $Rp \subseteq P$, the $p \in P \cap S$, it is a contradiction. Thus $P = 0$. Therefore, for any $0 \neq a \in R$ which is not a unit, $(a) \cap S \neq \emptyset$, then there is $ar \in S$, that is $ar = p_1 \cdots p_t$ where p_i are prime elements, thus a is a product of finite elements.

    (2) If $p = ab$ where p is a prime element and $a, b \in R$, then $p | ab$, thus $p | a$ or $p | b$. If $p | a$, then b is a unit; if $p | b$, then a is a unit. Therefore p is irreducible. Hence any element, which is a nonzero and non unit, is a product of irreducible elements.

    (3) For any $0 \neq a \in R$ is a non unit, if $a = p_1 \cdots p_r = q_1 \cdots q_s$ where p_i and q_j are irreducible. Assume $a = p'_1 \cdots p'_t$ where p'_i are prime elements, then $t = r$ and $p'_i = u_i p_i$(after reorder if necessary), $s = t$ and $q_i = v_i p'_i$(after reorder if necessary) where u_i, v_i are units. Hence R is a UFD.

15. Suppose that $n = p_1^{l_1} \cdots p_r^{l_r}$ where p_i are prime elements and $(p_i, p_j) = 1, (i \neq j)$, then $\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{l_1}) \oplus \cdots \oplus \mathbb{Z}/(p_r^{l_r})$. As $(a)/(p_1^{l_1})$ is a submodule of $\mathbb{Z}/(p_1^{l_1})$, assume $a = a_1 p_1^{n_1}$ where $p_1 \nmid a_1$, then $(a_1, p_1^{l_1}) = 1$, thus there exist $x, y \in \mathbb{Z}$ such that $a_1 x + p_1^{l_1} y = 1$, therefore $a_1 x + (p_1^{l_1}) = 1 + (p_1^{l_1}) = (a_1 + (p_1^{l_1}))(x + (p_1^{l_1}))$, hence $(a + (p_1^{l_1}))(x + (p_1^{l_1})) = p_1^{n_1} + (p_1^{l_1}) \in (a)/(p_1^{l_1})$. Thus $(a)/(p_1^{l_1}) = (p_1^{n_1})/(p_1^{l_1})$ where $0 < n_1 \leq l_1$. Therefore $\mathbb{Z}/(p_1^{l_1})$ is a uniserial $\mathbb{Z}$-module, hence $\mathbb{Z}/n\mathbb{Z}$ is a serial module.

16. $(f(x)) = (p_1(x)^{n_1} \cdots p_r(x)^{n_r}) = (p_1(x)^{n_1}) \cap \cdots \cap (p_r(x)^{n_r})$ and $(p_i(x)^{n_i}) + (p_j(x)^{n_j}) = F[x]$, define $\varphi : F[x]/(f(x)) \to F[x]/(p_1(x)^{n_1}) \oplus \cdots \oplus F[x]/(p_r(x)^{n_r})$, $\varphi(g(x) + (f(x))) = (g(x) + (p_1(x)^{n_1}), \cdots, g(x) + (p_r(x)^{n_r}))$, then we can testify that φ is an bijective and $\varphi(g_1(x)g_2(x)) = \varphi(g_1(x))\varphi(g_2(x))$, thus φ is an isomorphism.

17. Let $I = \{f \in End_R(M) | Imf \neq M\}$, $Imf_1, Imf_2 \leqslant M$ for any $f_1, f_2 \in I$, then $Imf_1 \leqslant Imf_2$ or $Imf_2 \leqslant Imf_1$, thus $Im(f_1 + f_2) \subseteq Imf_1 + Imf_2 \neq M$, therefore $f_1 + f_2 \in I$, hence I is an ideal of $End_R(M)$. If $f \notin I$, consider ascending chain $Kerf \subseteq Kerf^2 \subseteq \cdots \subseteq Kerf^n \subseteq \cdots$, since M is a Noetherian ring, then there is n such that $Kerf^n = Kerf^{n+k}$ for any $k \geq 1$. While $Imf^n = Imf^{n+k} = M$, then $f^n(x) = f^{2n}(x), \forall x \in M$, thus $f^n(x - f^n(x)) = 0$, therefore $x - f^n(x) \in Kerf^n$, hence $M = Kerf^n + Imf^n$. For any $y \in Kerf^n \cap Imf^n$, $y = f^n(y') \in Kerf^n$, then $0 = f^n(y) = f^{2n}(y')$, thus $y' \in Kerf^{2n} = Kerf^n$, therefore $y = 0$. Hence $M = Kerf^n \oplus Imf^n$, therefore $Kerf^n = 0$, thus f^n is invertible, then f is invertible. Hence $End_R(M)/I$ is a division. For any $f \in End_R(M)$, if f is not invertible and $Imf \neq M$, then $f \in I$, thus I is an unique maximal ideal of $End_R(M)$, hence $End_R(M)$ is a local ring.

18. Let ${}_RR = \sum\limits_{\alpha \in \Lambda} \oplus I_\alpha$ where I_α are left uniserial ideal, then $1 \in \sum\limits_{\alpha \in \Lambda} \oplus I_\alpha$, therefore ${}_RR = I_1 \oplus \cdots \oplus I_n$ where I_i are left uniserial ideal, thus $R = Re_1 \oplus \cdots \oplus Re_n$ where $I_i = Re_i$ and e_i are idempotents.($1 = e_1 + \cdots + e_n$, then $e_i = e_i e_1 + \cdots + e_i e_n$, thus $e_i = e_i^2$)