CHAPTER I: BASIC FACTS ABOUT RINGS AND MODULES

§1: RINGS

(1.1) Definition: Let R be a ring. Define:

(a) $R^* = \{a \in R \mid \exists\ b \in R \text{ with } ab = 1\}$ the set of units of R

(b) $NZD(R) = \{a \in R \mid \forall\ b \in R-(0) : ab \neq 0\}$ the set of non zero divisors (NZD) of R

(c) $ZD(R) = R - NZD(R) = \{a \in R \mid \exists\ b \in R-(0) \text{ with } ab = 0\}$ the set of zero divisors (ZD) of R

(d) $Nil(R) = \{a \in R \mid \exists\ n \in \mathbb{N} : a^n = 0\}$ the nil radical of R (i.e. the set of nilpotent elements of R).

(1.2) Remark: (a) If R is not the nullring, $(R^*, \cdot)$ is an abelian group.

(b) $NZD(R)$ is a multiplicative semigroup.

(c) If $a \in NZD(R)$ and $b, c \in R$ with $ab = ac$ then $b = c$.

(d) $Nil(R)$ is an ideal of R.

(e) $(0) \subseteq Nil(R) \subseteq ZD(R) \subseteq R - R^*$ and $\{1\} \subseteq R^* \subseteq NZD(R) = R - ZD(R) \subseteq R - Nil(R)$.

Proof: (d) Let $a, b \in Nil(R)$ with $a^n = 0 = b^m$ for some $n, m \in \mathbb{N}$. Use the binomial formula to verify that $(a+b)^{n+m} = 0$.

(1.3) Examples: (a) $R = \mathbb{Z}$: $\mathbb{Z}^* = \{\pm 1\}$; $NZD(\mathbb{Z}) = \mathbb{Z} - (0)$; $ZD(\mathbb{Z}) = (0)$; $Nil(\mathbb{Z}) = (0)$.

(b) $R = \mathbb{Z}/6\mathbb{Z}$: $(\mathbb{Z}/6\mathbb{Z})^* = \{[1], [-1]\} = NZD(\mathbb{Z}/6\mathbb{Z})$;
$ZD(\mathbb{Z}/6\mathbb{Z}) = \{[0], [2], [3], [4]\}$; $Nil(\mathbb{Z}/6\mathbb{Z}) = \{[0]\}$.

(c) $R = \mathbb{Z}/12\mathbb{Z}$: $(\mathbb{Z}/12\mathbb{Z})^* = \{[1], [5], [7], [11]\} = NZD(\mathbb{Z}/12\mathbb{Z})$
$ZD(\mathbb{Z}/12\mathbb{Z}) = \{[0], [2], [3], [4], [6], [8], [9], [10]\}$; $Nil(\mathbb{Z}/12\mathbb{Z}) = \{[0], [6]\}$

(d) Let R be a finite ring and $a \in R$. Then a is a unit of R if and only if a is a NZD of R. Hence $R^* = NZD(R)$. This statement is obviously false for infinite rings.

(1.4) Definition: Let R be a ring and $I \subseteq R$ an ideal. The radical of I is defined by:
$\operatorname{rad}(I) = \{a \in R \mid \exists\ n \in \mathbb{N} \text{ with } a^n \in I\}$.

(1.5) Remark: (a) $\operatorname{rad}(I)$ is an ideal of R.
(b) Let $\nu: R \longrightarrow R/I$ be the natural map. Then $\operatorname{rad}(I) = \nu^{-1}(\operatorname{nil}(R/I))$.

Proof: (a) Let $a, b \in \operatorname{rad}(I)$ with $a^n, b^m \in I$ for some $n, m \in \mathbb{N}$. By the binomial formula: $(a+b)^{n+m} \in I$.

(1.6) Definition: Let R be a ring and $I, J \subseteq R$ ideals. I and J are called comaximal if $I + J = R$.

(1.7) Remark: Let R be a ring and $I, J, K \subseteq R$ ideals.
(a) I and J are comaximal $\Longleftrightarrow \exists\ a \in I,\ b \in J$ with $a + b = 1$.
(b) If I and J are comaximal then $IJ = I \cap J$.
(c) If I and J are comaximal and I and K are comaximal then I and JK are comaximal.

Proof: (b) $I \cap J = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ \subseteq I \cap J$.
(c) I and J are comaximal $\Rightarrow \exists\ a \in I,\ b \in J$ with $a + b = 1$.
I and K are comaximal $\Rightarrow \exists\ a' \in I,\ c \in K$ with $a' + c = 1$.
Hence $1 = (a+b)(a'+c) = \underbrace{aa' + a'b + ac}_{\in I} + \underbrace{bc}_{\in JK}$ and I and JK are comaximal.

Let R be a ring and $I_1, \ldots, I_n \subseteq R$ ideals. The map

$$\varphi: R \longrightarrow \prod_{i=1}^{n} R/I_i$$
$$a \longmapsto (a + I_1, \ldots, a + I_n)$$

is a homomorphism of rings.

(1.8) Theorem: (Chinese Remainder Theorem) Assumptions as above.

(a) If $I_1, \dots, I_n$ are mutually comaximal then $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$.

(b) φ is surjective if and only if $I_1, \dots, I_n$ are mutually comaximal.

Proof: (a) By induction on n. The case $n=2$ follows from (1.7).

$n-1 \Rightarrow n$: Suppose $K = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$. By (1.7) K and I_n are comaximal. By applying (1.7) again: $\prod_{i=1}^n I_i = KI_n = K \cap I_n = \bigcap_{i=1}^n I_i$.

(b) "$\Rightarrow$": It suffices to show that I_1 and I_2 are comaximal. Since φ is surjective there is an $a \in R$ with $\varphi(a) = (1,0,\dots,0)$. Then $1 = (1-a)+a$ with $1 \equiv a \pmod{I_1}$ and $a \equiv 0 \pmod{I_2}$. Thus $1-a \in I_1$ and $a \in I_2$; I_1 and I_2 are comaximal.

"$\Leftarrow$": It is enough to show: For all $1 \le i \le n$ there is an $a_i \in R$ with $\varphi(a_i) = (0,\dots,0,1,0,\dots,0)$ (1 at the ith place). We only show: there is an $a \in R$ with $\varphi(a) = (1,0,\dots,0)$. Since $I_1 + I_j = R$ for all $2 \le j \le n$, there are $a_j \in I$, $b_j \in I_j$ for $2 \le j \le n$ with $a_j + b_j = 1$. Set $a = \prod_{j=2}^n b_j$. Then

$$a = \prod_{j=2}^n (1-a_j) = 1 - a' \quad \text{where } a \in I_j \text{ for all } 2 \le j \le n \text{ and } a' \in I_1.$$

Thus $\varphi(a) = (1,0,\dots,0)$.

(1.9) Remark: Let R be a principal ideal domain. Then R is factorial and every element $a \in R - (R^* \cup (0))$ can be written as:

$$a = u \cdot \prod_{j=1}^n p_j^{\alpha_j}$$

where p_j are mutually non-associated prime elements of R, $\alpha_j > 0$, and $u \in R^*$ a unit. Since R is a PID, the ideals $(p_j^{\alpha_j})$ are mutually comaximal. This implies that every nonzero ideal $I = (a) \neq R$ can be written as:

$$I = (a) = (p_1^{\alpha_1}) \cdots (p_n^{\alpha_n}) = (p_1^{\alpha_1}) \cap \dots \cap (p_n^{\alpha_n}) = (p_1)^{\alpha_1} \cdots (p_n)^{\alpha_n} = (p_1)^{\alpha_1} \cap \dots \cap (p_n)^{\alpha_n},$$

that is, I is a product of prime ideals. One of the objectives of the next chapters is to 'generalize' this result to certain classes of rings.

Let $(\mathcal{M}, \le)$ be a partially ordered set and $\mathcal{K} \subseteq \mathcal{M}$ a subset. $\mathcal{K}$ is called a chain

if $\mathcal{K}$ is (completely or totally) ordered, that is, if for all $k_1, k_2 \in \mathcal{K}$ either $k_1 \leq k_2$ or $k_2 \leq k_1$. An element $m \in \mathfrak{M}$ is called an upper bound of $\mathcal{K}$ if $k \leq m$ for all $k \in \mathcal{K}$.

(1.10) Zorn's Lemma: Let $\mathfrak{M}$ be a nonempty partially ordered set in which every chain $\mathcal{K} \subseteq \mathfrak{M}$ has an upper bound. Then $\mathfrak{M}$ has a maximal element.

(1.11) Definition: A partially ordered set in which every chain has an upper bound is called inductively ordered.

(1.12) Theorem: (Existence of prime ideals) Let R be a ring, $S \subseteq R$ a multiplicative set and $I \subseteq R$ an ideal with $I \cap S = \emptyset$. Then:

(a) The set $\mathfrak{M} = \{ J \subseteq R \mid J \text{ an ideal with } I \subseteq J \subseteq R - S \}$ is partially ordered by inclusion and has maximal elements.

(b) Every maximal element of $\mathfrak{M}$ is a prime ideal of R.

Proof: (a) Obviously, $\mathfrak{M} \neq \emptyset$, since $I \in \mathfrak{M}$. We have to show that $\mathfrak{M}$ is inductively ordered. Let $\mathcal{K} \subseteq \mathfrak{M}$ be a chain. Consider the set $K = \bigcup_{J \in \mathcal{K}} J$. Since $\mathcal{K}$ is a chain of ideals, K is an ideal of R. (Let $a, b \in K$. Then there are $J_1, J_2 \in \mathcal{K}$ with $a \in J_1$ and $b \in J_2$. Since $J_1 \subseteq J_2$ or $J_2 \subseteq J_1$, it follows that $a+b \in K$.) Since $I \subseteq K$ and $K \cap S = \emptyset$, $K \in \mathfrak{M}$ and K is an upper bound of $\mathcal{K}$. By Zorn's Lemma $\mathfrak{M}$ has a maximal element.

(b) Let $P \in \mathfrak{M}$ be a maximal element and $a, b \in R$ with $ab \in P$. Suppose that $a \notin P$ and $b \notin P$. Then $P \subsetneq P + (a)$ and $P \subsetneq P + (b)$ and by the maximality of P: $P + (a) \notin \mathfrak{M}$ and $P + (b) \notin \mathfrak{M}$. Hence $(P + (a)) \cap S \neq \emptyset$ and $(P + (b)) \cap S \neq \emptyset$. Let $p_1, p_2 \in P$ and $\alpha, \beta \in R$ so that:

$$s_1 = p_1 + \alpha a \in S \quad \text{and} \quad s_2 = p_2 + \beta b \in S.$$

Since S is a multiplicative set

$$s_1 s_2 = (p_1 + \alpha a)(p_2 + \beta b) = p_1 p_2 + \alpha a p_2 + \beta b p_1 + \alpha \beta a b \in S.$$

But $s_1 s_2 \in P$, a contradiction. Thus $a \in P$ or $b \in P$ and P is prime.

(1.13) Corollary: Every ideal $I \subsetneq R$ is contained in a maximal ideal of R.

Proof: Apply (1.12) to I and the multiplicative set $S = \{1\}$.

(1.14) Corollary: $R^* = R - \bigcup_{m \subseteq R \text{ max}} m$

Proof: immediately from (1.13).

(1.15) Remark: Let R be a ring, $I \subseteq R$ an ideal and $\nu : R \longrightarrow R/I$ the natural map.
(a) If $P \subseteq R$ is a prime ideal with $I \subseteq P$ then $\nu(P) = P/I$ is a prime ideal of R/I.
(b) If $Q \subseteq R/I$ is a prime ideal then $\nu^{-1}(Q)$ is a prime ideal of R.
(c) (a) and (b) establish a 1-1 correspondence between the prime ideals of R which contain I and the prime ideals of R/I.

(1.16) Corollary: Let R be a ring and $I \subseteq R$ an ideal.
(a) $\text{nil}(R) = \text{rad}(0) = \bigcap_{P \subseteq R \text{ prime}} P$
(b) $\text{rad}(I) = \bigcap_{P \subseteq R \text{ prime and } I \subseteq P} P$.

Proof: (a) "$\subseteq$": $a \in \text{nil}(R) \Rightarrow a^n = 0$ for some $n \in \mathbb{N} \Rightarrow a \in P$ for every prime ideal P of R.
"$\supseteq$": Suppose $a \in P$ for all prime ideals P of R. Consider the set $S = \{1, a, \ldots, a^n, \ldots\} \subseteq R$. S is a multiplicative set of R. If $a^n \neq 0$ for all $n \in \mathbb{N}$ then $S \cap (0) = \emptyset$. (1.12) applied to (0) and S yields the existence of a prime ideal Q of R with $Q \cap S = \emptyset$, a contradiction. Thus $a^n = 0$ for some $n \in \mathbb{N}$.
(b) Let $\nu : R \longrightarrow R/I$ be the natural map. Since there is a 1-1 correspondence between the prime ideal of R which contain I and the prime ideals of R/I and since $\text{rad}(I) = \nu^{-1}(\text{nil}(R/I))$, (b) follows from (a).

(1.17) Corollary: Let R be a ring. The set of zero divisors $ZD(R)$ is the union of some suitable prime ideals of R.

Proof: $S = NZD(R)$ is a multiplicative set with $S \cap (0) = \emptyset$. By (1.12) there is a prime ideal $P \subseteq R$ with $P \cap S = \emptyset$. Set $\mathcal{H} = \{P \subseteq R \mid P \text{ a prime ideal with } P \cap S = \emptyset\}$.

Claim: $ZD(R) = \bigcup_{P \in \mathcal{H}} P$

Pf of claim: Set $T = \bigcup_{P \in \mathcal{H}} P$. Since $T \cap S = \emptyset$, $T \subseteq R - S = ZD(R)$. For the other inclusion let $a \in ZD(R)$. Then $(a) \subseteq ZD(R)$ and $(a) \cap S = \emptyset$. By (1.12) there is a prime ideal $Q \subseteq R$ with $(a) \subseteq Q$ and $Q \cap S = \emptyset$. Hence $Q \in \mathcal{H}$ and $a \in T$.

(1.18) Definition: Let R be a ring. The set of prime ideals of R:

$$\operatorname{Spec}(R) = \{P \subseteq R \mid P \text{ a prime ideal}\}$$

is called the spectrum of R.

(1.19) Theorem: Let R be a ring. Every prime ideal $P \in \operatorname{Spec}(R)$ contains a minimal prime ideal.

Proof: Let $P \in \operatorname{Spec}(R)$. Consider the set $\mathcal{H} = \{Q \in \operatorname{Spec}(R) \mid Q \subseteq P\}$. $\mathcal{H} \neq \emptyset$ and $\mathcal{H}$ is partially ordered by 'reverse' inclusion:

$$Q_1 \leq Q_2 \iff Q_2 \subseteq Q_1.$$

Claim: $\mathcal{H}$ is inductively ordered

Pf of claim: Let $\mathcal{K} \subseteq \mathcal{H}$ be a chain. The ideal $K = \bigcap_{Q \in \mathcal{K}} Q$ is a prime ideal of R. Hence $K \in \mathcal{H}$ and K is an upper bound for $\mathcal{K}$.

The statement follows with Zorn's Lemma.

(1.20) Theorem: (Prime Avoidence Lemma) Let R be a ring and $P_1, \dots, P_n \subseteq R$ ideals with $P_1, \dots, P_{n-2}$ prime if $n > 2$. If $D \subseteq R$ is a subset which is closed under addition and multiplication and with $D \subseteq \bigcup_{i=1}^{n} P_i$, then there is an $1 \leq j \leq n$

with $D \subseteq P_j$.

Proof: By induction on n. The case $n=1$ is trivial.

$n-1 \to n$: Obviously, $D \subseteq \bigcup_{i=1}^{n} P_i \iff D = \bigcup_{i=1}^{n} (P_i \cap D)$. We want to show that there is an $1 \leq j \leq n$ so that $D \cap P_j \subseteq \bigcup_{i=1, i \neq j}^{n} P_i$ (*).

Note that if (*) holds then $D = \bigcup_{i=1, i \neq j}^{n} (P_i \cap I) \subseteq \bigcup_{i=1, i \neq j}^{n} P_i$ and the statement follows by induction.

In order to show (*) assume that for all $1 \leq j \leq n$: $D \cap P_j \not\subseteq \bigcup_{i=1, i \neq j}^{n} P_i$ and take $a_j \in (D \cap P_j) - \bigcup_{i=1, i \neq j}^{n} P_i$. Put $y = a_1 + a_2 \cdots a_n \in D$.

Claim: $y \notin P_i$ for all $1 \leq i \leq n$.

Pf of claim: $i=1$: $a_1 \in P_1$ and $a_2, \ldots, a_n \notin P_1$. Thus $y \notin P_1$ if $n > 2$ and P_1 prime.

If $n = 2$ then $y \notin P_1$ and $y \notin P_2$, a contradiction.

If $n > 2$ and $2 \leq i \leq n$, then $a_1 \notin P_1$ and $a_2 - a_n \in P_i$. Thus $y \notin P_i$.

This implies, $D \not\subseteq \bigcup_{i=1}^{n} P_i$, a contradiction.

(1.21) Definition: Let R be a ring. The ideal

$$\operatorname{Jrad}(R) = \bigcap_{m \subseteq R \text{ max.}} m$$

is called the Jacobson radical of R.

(1.22) Proposition: Let R be a ring and $a \in R$. Then

$$a \in \operatorname{Jrad}(R) \iff 1 - ab \in R^* \text{ for all } b \in R.$$

Proof: "$\Rightarrow$": If $1 - ab \notin R^*$ for some $b \in R$ then there is a maximal ideal $m \subseteq R$ with $1 - ab \in m$. If $a \in m$ then $1 \in m$, a contradiction.

"$\Leftarrow$": Suppose $a \notin m$ for some maximal ideal $m \subseteq R$. Then $m + (a) = R$ and there are elements $n \in m$ and $b \in R$ with $n + ab = 1$. Then $1 - ab = n \notin R^*$, a contradiction.

(1.23) Remark: Let $\varphi: R \longrightarrow S$ be a homomorphism of rings and $P \subseteq S$ a prime ideal. The contraction $\varphi^{-1}(P) \subseteq R$ is a prime ideal.

(1.24) Example: Let R be a ring and $R[[x_1, \dots, x_n]]$ the power series ring in n variables over R.

(a) $R[[x_1, \dots, x_n]]$ is a domain $\Longleftrightarrow$ R is a domain

(b) $f \in R[[x_1, \dots, x_n]]^* \Longleftrightarrow f \in R^* + (x_1, \dots, x_n)$

(c) $1 + (x_1, \dots, x_n) \subseteq R[[x_1, \dots, x_n]]^* \Longrightarrow (x_1, \dots, x_n) \subseteq \operatorname{Jrad}(R[[x_1, \dots, x_n]])$

Thus every maximal ideal of $R[[x_1, \dots, x_n]]$ contains $(x_1, \dots, x_n)$. The natural map $\nu: R[[x_1, \dots, x_n]] \longrightarrow R[[x_1, \dots, x_n]]/(x_1, \dots, x_n) \cong R$ induces a correspondence between the maximal ideals of R and the maximal ideals of $R[[x_1, \dots, x_n]]$.

$$\{\text{max. ideals of } R[[x_1, \dots, x_n]]\} \overset{\cong}{\longleftrightarrow} \{\text{max. ideals of } R\}$$

$$m + (x_1, \dots, x_n) \longleftarrow\!\shortmid\ m$$

$$M \longmapsto M \cap R$$

In particular, if $R = k$ is a field, then $k[[x_1, \dots, x_n]]$ contains exactly one maximal ideal namely $(x_1, \dots, x_n)$.

(d) If k is a field and $x_1, \dots, x_n$ variables, then

$$\operatorname{Jrad}(k[[x_1, \dots, x_n]]) = \bigcap_{m \subseteq k[[x_1, \dots, x_n]] \text{ max}} m = (0).$$

(Proof later).

§2: NAKAYAMA'S LEMMA

(1.25) Proposition: Let R be a ring and M an R-module.

(a) $\mathrm{Hom}_R(R,M) = \{\varphi : R \longrightarrow M \mid \varphi \ R\text{-linear}\} \cong M$

(b) Let F be a free R-module and $\mathcal{B} = \{b_i\}_{i\in I}$ a basis of F. Every map $\varphi_0 : \mathcal{B} \longrightarrow M$ extends uniquely to an R-linear map $\varphi : F \longrightarrow M$.

Proof: (a) Every $\varphi \in \mathrm{Hom}_R(R,M)$ is uniquely determined by $\varphi(1)$.

(b) For $x = \sum'_{i\in I} a_i b_i \in F$ with $a_i \in R$ and all but finitely many $a_i = 0$ define: $\varphi(x) = \sum_{i\in I} a_i \varphi(b_i)$. φ is well defined and R-linear. Uniqueness is trivial.

(1.26) Proposition: (a) Every module is factor module of a free module.

(b) Let M be a finite R-module. Then $M \cong R^n/U$ for some $n \in \mathbb{N}$ and some submodule $U \subseteq R^n$.

(c) Every factor module of a finite module is finite.

(d) Let M be an R-module and $U \subseteq M$ a submodule. If U and M/U are finite then M is finite.

Proof: (d) Let $m_1, \dots, m_n \in M$ so that $m_1 + U, \dots, m_n + U \in M/U$ is a system of generators of M/U. Let $u_1, \dots, u_t \in U$ be a set of generators of U. Then $m_1, \dots, m_n, u_1, \dots, u_t$ is a set of generators of M.

(1.27) Theorem: (Nakayama's Lemma) Let M be a finite R-module and $I \subseteq R$ an ideal. If $IM = M$, then there is an $i \in I+1$ with $aM = 0$. In particular if $M = IM$ and $I \subseteq \mathrm{rad}(R)$ then $M = 0$.

Proof: By assumption $M = Rx_1 + \dots + Rx_n$. Since $M = IM$ there is an $n \times n$-matrix A with entries in I so that

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Thus $(1_{n\times n} - A)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$ where $1_{n\times n}$ is the $n\times n$ identity matrix. This implies:

$(\mathrm{adj}(1_{n\times n} - A))(1_{n\times n} - A)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$ and hence $\det(1_{n\times n} - A)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$.

Since all entries of A are in I, $\det(1_{n\times n} - A) \in 1 + I$.

(1.28) Corollary: Let M be an R-module and $N \subseteq M$ a submodule with M/N a finite R-module. Let $I \subseteq \mathrm{Jrad}(R)$ be an ideal with $M = N + IM$. Then $M = N$.

Proof: $I(M/N) \cong (IM+N)/N = M/N$. By (1.27) $M/N = 0$.

(1.29) Remark: Let $\varphi: M \longrightarrow N$ be an R-linear map and $K \subseteq M$, $L \subseteq N$ submodules with $\varphi(K) \subseteq L$. By the 1st isomorphism theorem there is an R-linear map $\overline{\varphi}: M/K \longrightarrow N/L$ so that the diagram

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \text{nat.}\downarrow & & \downarrow\text{nat.} \\ M/K & \xrightarrow{\overline{\varphi}} & N/L \end{array}$$

commutes.

$\overline{\varphi}$ is called the (by φ) induced map.

(1.30) Corollary: Let $\varphi: M \longrightarrow N$ be an R-linear map with $\mathrm{coker}(\varphi) = N/\mathrm{im}(\varphi)$ a finite R-module. If $I \subseteq \mathrm{Jrad}(R)$ is an ideal such that the induced map $\overline{\varphi}: M/IM \longrightarrow N/IN$ is surjective, then φ is surjective.

Proof: Since $\overline{\varphi}$ is surjective, $N = \mathrm{im}(\varphi) + IN$. By (1.28): $N = \mathrm{im}(\varphi)$.

(1.31) Definition: Let M be an R-module. A generating set W of M is minimal if no proper subset of W is a generating set of M.

(1.32) Definition: A ring R is called local if R has exactly one maximal ideal (or equivalently, if $\mathrm{Jrad}(R)$ is a maximal ideal of R). Notation: (R, m, k) where $m \subseteq R$ is

the maximal ideal of R and $k = R/m$ is the residue class field of R.

(1.33) Theorem: Let (R, m, k) be a local ring and M a finite R-module.
(a) $\{x_1, \dots, x_n\}$ is a minimal generating set of M if and only if $\{x_1 + mM, \dots, x_n + mM\} = \{\overline{x_1}, \dots, \overline{x_n}\}$ is a basis of the $k = R/m$-vector space M/mM. In particular, all minimal generating sets of M have the same length.
(b) If $\{x_1, \dots, x_n\}$, $\{y_1, \dots, y_n\}$ are minimal generating sets of M then there is an invertible $n \times n$-matrix $A \in M_{n,n}(R)$ with $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Proof: (a) "$\Leftarrow$": By assumption $M/mM = k\overline{x_1} + \dots + k\overline{x_n}$. Hence $M = Rx_1 + \dots + Rx_n + mM$. Since M is finite and $m = \operatorname{Jrad}(R)$, by (1.28) $M = Rx_1 + \dots + Rx_n$. Obviously, $\{x_1, \dots, x_n\}$ is minimal.
"$\Rightarrow$": $\{\overline{x_1}, \dots, \overline{x_n}\}$ is a generating set of M/mM. If $\{\overline{x_1}, \dots, \overline{x_n}\}$ is not minimal, by "$\Leftarrow$" a proper subset of $\{x_1, \dots, x_n\}$ generates M.
(b) There is an $n \times n$ matrix A with $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Then $\begin{pmatrix} \overline{y_1} \\ \vdots \\ \overline{y_n} \end{pmatrix} = \overline{A} \begin{pmatrix} \overline{x_1} \\ \vdots \\ \overline{x_n} \end{pmatrix}$ and $\{\overline{x_1}, \dots, \overline{x_n}\}$, $\{\overline{y_1}, \dots, \overline{y_n}\}$ are k-bases of M/mM. Hence $\overline{A}$ is invertible $\Rightarrow \det \overline{A} \neq 0 \Rightarrow \overline{\det A} \neq 0 \Rightarrow \det A \notin m \Rightarrow \det A \in R^*$. A is invertible.

(1.34) Definition: Let (R, m, k) and M be as above. The cardinality of a minimal set of generators of M is denoted by $\mu(M)$ and called the minimal number of generators of M.

(1.35) Corollary: (R, m, k) and M as above. Then

$$\mu(M) = \dim_k (M/mM).$$

(1.36) Theorem: Let R be a ring, M a finite R-module and $\varphi: M \longrightarrow M$ a surjective R-linear map. Then φ is injective. Moreover, $\varphi^{-1} = f(\varphi)$ for some $f \in R[x]$.

Proof: Consider M as a finite $R[x]$-module via the scalar product $f(x)\cdot m = [f(\varphi)](m)$ for all $m \in M$. Since φ is surjective, $M = xM = (x)M$ and by (1.27) there is an $f(x) \in R[x]$ with $(1 - f(x)x)M = 0$. Thus for all $m \in M$: $m = [f(\varphi)\varphi](m)$ and $f(\varphi)\varphi = \varphi f(\varphi) = id_M$.

§3 : LOCALIZATION

Let R be a commutative ring with identity, $S \subseteq R$ a multiplicative set, and M an R-module (including the case $M=R$). On the set $M \times S = \{(m,s) \mid m \in M \text{ and } s \in S\}$ consider the relation: $(m_1,s_1) \sim (m_2,s_2) \iff \exists\, t \in S : t(s_1 m_2 - s_2 m_1) = 0$.

(1.37) Remark: "$\sim$" is an equivalence relation on $M \times S$.

Proof: Suppose that $(m_1,s_1) \sim (m_2,s_2) \iff t_1(s_1 m_2 - s_2 m_1) = 0$ for some $t_1 \in S$
and $(m_2,s_2) \sim (m_3,s_3) \iff t_2(s_2 m_3 - s_3 m_2) = 0$ for some $t_2 \in S$.
Then $0 = (t_2 s_3) t_1 (s_1 m_2 - s_2 m_1) + (t_1 s_1) t_2 (s_2 m_3 - s_3 m_2) = (t_1 t_2 s_2)(s_1 m_3 - s_3 m_1)$.
Since $t_1 t_2 s_2 \in S$, $(m_1,s_1) \sim (m_3,s_3)$.

(1.38) Definition and Remark: For an R-module M define
$$NZD(M) = \{t \in R \mid tm \neq 0 \text{ for all } m \in M-(0)\}.$$
An element $t \in NZD(M)$ is called a regular element or a non zero divisor of M.
Accordingly, $ZD(M) = R - NZD(M)$ is the set of zero divisors or non regular elements of M.
Let $S \subseteq NZD(M)$, then (*) $(m_1,s_1) \approx (m_2,s_2) \iff s_1 m_2 - s_2 m_1 = 0$
is exactly the equivalence relation "$\sim$" on $M \times S$. However, if $S \not\subseteq NZD(M)$, (*) fails to define an equivalence relation on $M \times S$.
The set of all equivalence classes $M \times S/\sim$ is denoted by $S^{-1}M$ and the equivalence class of an element (m,s) is denoted by $\frac{m}{s}$ or m/s. $S^{-1}M$ is called the localization of M by the multiplicative set S.

(1.39) Proposition: (a) $S^{-1}R$ is a commutative ring with identity under the operations:
$\forall\, a_1,a_2 \in R;\ s_1,s_2 \in S$: $(a_1/s_1) + (a_2/s_2) = (s_2 a_1 + s_1 a_2)/(s_1 s_2)$ and $(a_1/s_1)(a_2/s_2) = (a_1 a_2)/(s_1 s_2)$.
(b) $S^{-1}M$ is an $S^{-1}R$-module under the operations:
$\forall\, m_1,m_2 \in M;\ s_1,s_2 \in S;\ a \in R$: $(m_1/s_1) + (m_2/s_2) = (s_2 m_1 + s_1 m_2)/(s_1 s_2)$ and $(a/s_2)(m_1/s_1) = (a m_1)/(s_1 s_2)$.

Proof: We only show that addition is well defined. Suppose that $(m_1,s_1)\sim(n_1,t_1)$ and $(m_2,s_2)\sim(n_2,t_2)$. Then there are $u_1,u_2\in S$ with $u_1(s_1n_1-t_1m_1)=0$ and $u_2(s_2n_2-t_2m_2)=0$.

Hence: $(u_1s_1)n_1=(u_1t_1)m_1$ and $(u_2s_2)n_2=(u_2t_2)m_2$

$$\Rightarrow\quad (t_1t_2u_1u_2)(s_2m_1+s_1m_2)=(t_1t_2u_1u_2s_2)m_1+(t_1t_2u_1u_2s_1)m_2$$
$$=(t_2u_1u_2s_1s_2)n_1+(t_1u_1u_2s_1s_2)n_2$$
$$=(u_1u_2s_1s_2)(t_2n_1+t_1n_2)$$

and $(s_2m_1+s_1m_2,\ s_1s_2)\sim(t_2n_1+t_1n_2,\ t_1t_2)$.

Note that the zero element of $S^{-1}M$ is $0/1$ and the identity element of $S^{-1}R$ is $1/1$.

(1.40) Remark: (a) The map $i_{R,S}:R\longrightarrow S^{-1}R$ defined by $i_{R,S}(a)=a/1$ is a homomorphism of rings.

(b) $S^{-1}M$ is an R-module via $i_{R,S}$. The map $i_{M,S}:M\longrightarrow S^{-1}M$ defined by $i_{M,S}(m)=m/1$ is R-linear.

(c) $S\subseteq NZD(R)\iff i_{R,S}$ is injective

$S\subseteq NZD(M)\iff i_{M,S}$ is injective.

(d) $i_{R,S}(S)\subseteq(S^{-1}R)^*$

(e) $0\in S\iff S^{-1}R=0$

(1.41) Theorem: (Universal property of $S^{-1}R$) Let R be a ring, $S\subseteq R$ a multiplicative set and $\varphi:R\longrightarrow T$ a homomorphism of rings with $\varphi(S)\subseteq T^*$. Then there is a unique homomorphism of rings $\psi:S^{-1}R\longrightarrow T$ such that the diagram:

$$\begin{array}{ccc} R & \xrightarrow{\ \varphi\ } & T \\ {\scriptstyle i_{R,S}}\downarrow & \nearrow_{\psi} & \\ S^{-1}R & & \end{array}$$

commutes, i.e. $\psi\, i_{R,S}=\varphi$.

Proof: Set $\psi(a/s)=\varphi(a)\,\varphi(s)^{-1}$.

(i) ψ is well defined. Suppose $a_1/s_1=a_2/s_2$. Then there is an $t\in S$ with $ts_1a_2=ts_2a_1$. Hence $\varphi(t)\varphi(s_1)\varphi(a_2)=\varphi(t)\varphi(s_2)\varphi(a_1)$ and since $\varphi(t),\varphi(s_1),\varphi(s_2)\in T^*$: $\varphi(a_2)\varphi(s_2)^{-1}=\varphi(a_1)\varphi(s_1)^{-1}$.

(ii) ψ is a homomorphism of rings:

$$\psi((a_1/s_1)(a_2/s_2)) = \varphi(a_1a_2)\varphi(s_1s_2)^{-1} = \varphi(a_1)\varphi(s_1)^{-1}\varphi(a_2)\varphi(s_2)^{-1} = \psi(a_1/s_1)\psi(a_2/s_2)$$

$$\psi((a_1/s_1)+(a_2/s_2)) = \varphi(s_2a_1+s_1a_2)\varphi(s_1s_2)^{-1} = (\varphi(s_2)\varphi(a_1)+\varphi(s_1)\varphi(a_2))\varphi(s_1)^{-1}\varphi(s_2)^{-1}$$

$$= \varphi(a_1)\varphi(s_1)^{-1} + \varphi(a_2)\varphi(s_2)^{-1} = \psi(a_1/s_1) + \psi(a_2/s_2).$$

$\psi(1/1) = \varphi(1)\varphi(1)^{-1} = 1_T$.

(iii) $\psi\, i_{R,S}(a) = \psi(a/1) = \varphi(a)\varphi(1)^{-1} = \varphi(a)$

(iv) Uniqueness: Let $\tau: S^{-1}R \longrightarrow T$ be a homomorphism with $\tau\, i_{R,S} = \varphi$. Then

$$\tau(a/s) = \tau(\tfrac{a}{1})\tau(1/s) = \tau(a/1)\tau((s/1)^{-1}) = \tau(a/1)\tau(s/1)^{-1} = \varphi(a)\varphi(s)^{-1} = \psi(a/s).$$

Similarly to Theorem (1.41) one can show:

(1.42) Proposition: Let M be an R-module, N an $S^{-1}R$-module and $\varphi: M \longrightarrow N$ an R-linear map. Then there is a unique $S^{-1}R$-linear map $\psi: S^{-1}M \longrightarrow N$ so that the diagram

$$\begin{array}{ccc} M & \xrightarrow{i_{M,S}} & S^{-1}M \\ {\scriptstyle\varphi}\downarrow & \swarrow{\scriptstyle\psi} & \\ N & & \end{array}$$

commutes, i.e. $\varphi = \psi\, i_{M,S}$. This property characterizes $S^{-1}M$ up to natural isomorphisms of $S^{-1}R$-modules.

Proof: Homework

(1.43) Remark: (a) If $S \subseteq R^*$ then $i_{R,S}$ and $i_{M,S}$ are isomorphisms for every R-module M.

(b) If R is a domain and $S = R - (0)$ then $S^{-1}R = Q(R)$ is the field of quotients of R. Using (1.41) one can show that $Q(R)$ is the smallest field containing R (up to isomorphisms).

(c) In general, $S^{-1}R$ is called the localization of R at S and $S^{-1}M$ is the localization of M at S. If $P \in \operatorname{Spec}(R)$ is a prime ideal we write $R_P = S^{-1}R$ where $S = R - P$. R_P is called the localization of R at P. Similarly, $M_P = S^{-1}M$ for $S = R - P$ is called the localization of M at P.

(1.44) Proposition: Let $\varphi: M \longrightarrow N$ be an R-linear map and $S \subseteq R$ a multiplicative set. There is a unique $S^{-1}R$-linear map $S^{-1}\varphi: S^{-1}M \longrightarrow S^{-1}N$ such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle i_{M,S}}\downarrow & & \downarrow{\scriptstyle i_{N,S}} \\ S^{-1}M & \xrightarrow{S^{-1}\varphi} & S^{-1}N \end{array}$$

commutes.

Proof: By (1.42). Note that $S^{-1}\varphi\,(m/s) = (1/s)\,\varphi(m)$ for all $m \in M, s \in S$.

(1.45) Corollary: (a) If $id_M : M \longrightarrow M$ is the identity of M, then $S^{-1}id_M : S^{-1}M \longrightarrow S^{-1}M$ is the identity of $S^{-1}M$: $S^{-1}id_M = id_{S^{-1}M}$.

(b) If $\varphi: M \longrightarrow N$ and $\psi: N \longrightarrow L$ are R-linear maps, then $S^{-1}(\psi\varphi) = (S^{-1}\psi)(S^{-1}\varphi)$.

Localization is a covariant functor from the category of R-modules into the category of $S^{-1}R$-modules.

(1.46) Proposition: Let $S' \subseteq S$ be multiplicative subsets of R and M an R-module. Then

$$(i_{M,S'}(S))^{-1}\,(S'^{-1}M) \overset{\varphi}{\cong} S^{-1}M$$

where $\varphi((m/s')/(s/1)) = m/(ss')$ for all $m \in M, s' \in S', s \in S$.

Proof: By (1.42) there are unique maps λ, φ, ψ so that the diagram

$$\begin{array}{ccccc} M & \xrightarrow{i_{M,S'}} & S'^{-1}M & \xrightarrow{i_{S'^{-1}M,S}} & (i_{M,S'}(S))^{-1}(S'^{-1}M) \\ & {\scriptstyle i_{M,S}}\searrow & \downarrow{\scriptstyle \lambda} & \overset{\varphi}{\underset{\psi}{\rightleftarrows}} & \\ & & S^{-1}M & & \end{array}$$

commutes. By uniqueness: $\varphi\psi = id$ and $\psi\varphi = id$.

(1.47) Definition: Let $S \subseteq R$ be a multiplicative set.

(a) S is called saturated if whenever $a \cdot b \in S$ then $a \in S$ and $b \in S$ or, equivalently,

$$S = R - \bigcup_{P \in \operatorname{Spec}(R),\, P \cap S = \emptyset} P.$$

(b) The set $\widetilde{S} = \{a \in R \mid ab \in S \text{ for some } b \in R\}$ is called the saturation of S in R.

(1.48) Remark: $\widetilde{S}$ is a multiplicative set.

(1.49) Proposition: Let $S \subseteq R$ be a multiplicative set and $i_{R,S}: R \longrightarrow S^{-1}R$ the natural map. Then

$\widetilde{S}$ = the smallest saturated multiplicative set of R containing S

$= R - \bigcup_{P \in Spec(R),\, P \cap S = \emptyset} P$

$= i_{R,S}^{-1}\left((S^{-1}R)^*\right)$

= the biggest multiplicative set S' of R containing S so that the natural map $S^{-1}R \longrightarrow S'^{-1}R$ is an isomorphism.

Proof: Homework

(1.50) Corollary: If $S \subseteq R$ is a multiplicative set, $\widetilde{S} \subseteq R$ its saturation, and M an R-module, then the natural map $S^{-1}M \longrightarrow \widetilde{S}^{-1}M$ is an isomorphism.

§4: PROPERTIES OF THE LOCALIZATION

A sequence of R-modules and R-linear maps

$$\cdots \longrightarrow M_i \xrightarrow{\alpha_i} M_{i+1} \xrightarrow{\alpha_{i+1}} M_{i+2} \longrightarrow \cdots$$

is called exact if $\operatorname{im}(\alpha_i) = \ker(\alpha_{i+1})$ for all $i \in \mathbb{Z}$. An exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

is called a short exact sequence, that is, α is injective, $\operatorname{im}(\alpha) = \ker(\beta)$, and β is surjective.

(1.51) Theorem: (Localization is exact) Let R be a ring, $S \subseteq R$ a multiplicative set and

$$M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$$

an exact sequence of R-modules and R-linear maps. The induced sequence

$$S^{-1}M_1 \xrightarrow{S^{-1}\alpha} S^{-1}M_2 \xrightarrow{S^{-1}\beta} S^{-1}M_3$$

is an exact sequence of $S^{-1}R$-modules and $S^{-1}R$-linear maps.

Proof: Since $(S^{-1}\beta)(S^{-1}\alpha) = S^{-1}(\beta\alpha) = S^{-1}0 = 0$, $\operatorname{im}(S^{-1}\alpha) \subseteq \ker(S^{-1}\beta)$. For the other inclusion let $m/s \in \ker(S^{-1}\beta)$. Then $S^{-1}\beta(m/s) = \beta(m)/s = 0$ in $S^{-1}M_3$ and there is a $t \in S$ with $t\beta(m) = 0$ in M_3. Hence $\beta(tm) = 0$ and $tm \in \ker(\beta) = \operatorname{im}(\alpha)$. Therefore there is an $n \in M_1$ with $\alpha(n) = tm$ and $S^{-1}\alpha(n/(st)) = \alpha(n)/st = (tm)/st = m/s$.

(1.52) Corollary: Let U be a submodule of M. $S^{-1}U$ is (isomorphic to) a submodule of $S^{-1}M$ and $S^{-1}(M/U) \cong S^{-1}M/S^{-1}U$.

Proof: Apply (1.51) to the exact sequence $0 \longrightarrow U \longrightarrow M \longrightarrow M/U \longrightarrow 0$.

Let R be a ring, $I \subseteq R$ an ideal, and $S \subseteq R$ a multiplicative set. Considering R as an R-module and I as a submodule, the embedding $\varepsilon: I \longrightarrow R$ is R-linear. By (1.44) ε induces an $S^{-1}R$-linear map $S^{-1}\varepsilon: S^{-1}I \longrightarrow S^{-1}R$. By (1.51) $S^{-1}\varepsilon$ is injective and we may consider $S^{-1}I = \{a/s \mid a \in I, s \in S\}$ as a subset of $S^{-1}R$. $S^{-1}I$ is an ideal of $S^{-1}R$.

(1.52) Proposition: Let R be a ring, $I \subseteq R$ an ideal, $P \subseteq R$ a prime ideal, and $S \subseteq R$ a multiplicative set:

(a) $S^{-1}I = S^{-1}R \iff S \cap I \neq \emptyset$

(b) If $P \cap S = \emptyset$ then $S^{-1}P$ is a prime ideal of $S^{-1}R$ with $i_{R,S}^{-1}(S^{-1}P) = P$.

(c) If $J \subseteq S^{-1}R$ is an ideal then $K = i_{R,S}^{-1}(J)$ is an ideal of R with $S^{-1}K = J$.

(d) There is a 1–1 correspondence between the prime ideals of $S^{-1}R$ and the prime ideals P of R with $P \cap S = \emptyset$

Proof: "$\Rightarrow$": $1/1 \in S^{-1}I \Rightarrow 1/1 = a/s$ for some $a \in I, s \in S \Rightarrow \exists\, t \in S$ with $t(s-a) = 0$ $\Rightarrow ts = at \in I \cap S$. "$\Leftarrow$": $s \in I \cap S \Rightarrow 1/s = s/s \in S^{-1}I$ and $S^{-1}I = S^{-1}R$.

(b) Suppose $a_1, a_2 \in R$; $s_1, s_2 \in S$ with $(a_1/s_1)(a_2/s_2) \in S^{-1}P$. Then there are $p \in P$, $s \in S$ with $(a_1a_2)/(s_1s_2) = p/s$ and there is a $t \in S$ with $t(sa_1a_2 - s_1s_2p) = 0$ and $tsa_1a_2 = ts_1s_2p \in P$. Since $S \cap P = \emptyset$ and P prime, $a_1 \in P$ or $a_2 \in P$ and hence $a_1/s_1 \in S^{-1}P$ or $a_2/s_2 \in S^{-1}P$. Obviously, $P \subseteq i_{R,S}^{-1}(S^{-1}P)$. Let $q \in i_{R,S}^{-1}(S^{-1}P)$. Then $i_{R,S}(q) = q/1 = p/s$ for some $p \in P$, $s \in S$. There is a $t \in S$ with $t(sq - p) = 0$ and $tsq = tp \in P$. Since $P \cap S = \emptyset$ and P prime, $q \in P$.

(d) If $Q \subseteq S^{-1}R$ is a prime ideal then $i_{R,S}^{-1}(Q) = P$ is a prime ideal of R and by (b) $S^{-1}P = Q$. The maps

$$\{P \subseteq R \mid P \text{ a prime ideal with } P \cap S = \emptyset\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{Q \subseteq S^{-1}R \mid Q \text{ a prime ideal}\}$$

defined by $\Phi(P) = S^{-1}P$ and $\Psi(Q) = i_{R,S}^{-1}(Q)$ are inverse to each other, i.e. $\Psi\Phi = \mathrm{id}$ and $\Phi\Psi = \mathrm{id}$.

(1.53) Remark: If $I \subseteq R$ is any ideal then in general $i_{R,S}^{-1}(S^{-1}I) \neq I$.

Example: $R = \mathbb{Z}$, $I = (15)$ and $S = R - (3)$. Then $S^{-1}((15)) = S^{-1}((3))$ and $i_{\mathbb{Z},S}(S^{-1}(3)) = (3) \supsetneq (15)$.

(1.54) Proposition: (a) Let $\varphi: R \longrightarrow T$ be a homomorphism of rings and $S \subseteq R$ a multiplicative set. Then $\varphi(S) \subseteq T$ is a multiplicative set and φ induces a

homomorphism of rings $\psi: S^{-1}R \longrightarrow \varphi(S)^{-1}T$ defined by $\psi(a/s) = \varphi(a)/\varphi(s)$.

(b) Let R be a ring, $I \subseteq R$ an ideal, $\nu: R \longrightarrow R/I$ the natural map, and $S \subseteq R$ a multiplicative set. Then $S^{-1}R/S^{-1}I \cong (\nu(S))^{-1}(R/I) \cong S^{-1}(R/I)$ where $S^{-1}(R/I)$ denotes the localization of the R-module R/I. Moreover, $S^{-1}(R/I)$ is a ring and isomorphic to the ring $(\nu(S))^{-1}(R/I)$.

Proof: (a) $\varphi(S)^{-1}T$ is (naturally) a $S^{-1}R$-module. By (1.42) there is a $S^{-1}R$-linear map ψ so that the diagram:

$$\begin{array}{ccccc} R & \xrightarrow{\varphi} & T & \xrightarrow{i_{T,\varphi(S)}} & \varphi(S)^{-1}T \\ {\scriptstyle i_{R,S}}\downarrow & & & \nearrow_{\psi} & \\ S^{-1}R & & & & \end{array}$$

commutes. ψ is also a homomorphism of rings.

(b) By (a) there is a homomorphism of rings $\psi: S^{-1}R \longrightarrow \nu(S)^{-1}(R/I)$ so that the diagram

$$\begin{array}{ccccc} R & \xrightarrow{\nu} & R/I & \xrightarrow{i} & \nu(S)^{-1}(R/I) \\ {\scriptstyle i}\downarrow & & & \nearrow_{\psi} & \\ S^{-1}R & & & & \end{array}$$

commutes.

Let $\nu(a)/\nu(s) \in \nu(S)^{-1}(R/I)$. Then $\psi(a/1) = \nu(a)/1$ and $\psi(s/1) = \nu(s)/1$ and hence $\psi(a/s) = \psi(a/1)\psi((s/1)^{-1}) = \psi(a/1)\psi(s/1)^{-1} = \nu(a)/\nu(s)$ and ψ is surjective. Obviously, $S^{-1}I \subseteq \ker(\psi)$. Let $\psi(a/s) = \nu(a)/\nu(s) = 0$. Then there is a $t \in S$ so that $\nu(t)\nu(a) = \nu(at) = 0$ in R/I and hence $at \in I$ and $a/s = (at)/(st) \in S^{-1}I$. ψ induces an isomorphism of rings $S^{-1}R/S^{-1}I \cong \nu(S)^{-1}(R/I)$. By (1.52) there is an isomorphism of $S^{-1}R$-modules $\tau: S^{-1}(R/I) \cong S^{-1}R/S^{-1}I$. τ is also a homomorphism of rings.

(1.55) Remark: Let R be a ring. R has exactly one maximal ideal if and only if $R - R^*$ is an ideal of R.

(1.56) Proposition: Let R be a ring and $P \in \operatorname{Spec}(R)$ a prime ideal. The ring R_P is local with maximal ideal PR_P.

Proof: By (1.52)(b) PR_P is a prime ideal of R_P and by (1.52)(d) PR_P is the only maximal ideal of R_P.

(1.57) Example: Let $R=\mathbb{Z}$, $p\in\mathbb{Z}$ a prime number and $P=(p)\in \operatorname{Spec}(\mathbb{Z})$. Then

$$\mathbb{Z}_P = \mathbb{Z}_{(p)} = \{ m/n \in \mathbb{Q} \mid m,n\in\mathbb{Z} \text{ and } p\nmid n \}.$$

$\mathbb{Z}_{(p)}$ is a PID with exactly two prime ideals: $\operatorname{Spec}(\mathbb{Z}_{(p)}) = \{(0), p\mathbb{Z}_{(p)}\}$.
Note that the ring $\mathbb{Z}_{(p)}$ is different from the ring $\mathbb{Z}_P$ which is defined by

$$\mathbb{Z}_P = \{ m/n \in \mathbb{Q} \mid m,n\in\mathbb{Z} \text{ and } n=p^e \text{ for some } e\in\mathbb{N} \}.$$

$\mathbb{Z}_P = S^{-1}\mathbb{Z}$ where S is the multiplicative set $\{1, p, p^2, \dots\}$.

(1.58) Proposition: Let R be a ring and $P\subseteq R$ a minimal prime ideal. Then $P\subseteq ZD(R)$.

Proof: Let $P\subseteq R$ be a minimal prime ideal. By (1.52) the ring PR_P has exactly one prime ideal PR_P. By (1.16): $\operatorname{nil}(R_P) = PR_P$. Let $a\in P-(0)$. Then $a/1 \in \operatorname{nil}(R_P)$ and there is an $n\in\mathbb{N}$ with $(a/1)^n = 0$. Let n be minimal. Then there is a $t\in S-R$ so that $ta^n = 0$ and $ta^{n-1}\neq 0$. Hence $a\in ZD(R)$.

(1.59) Definition: A ring R is called reduced if $\operatorname{nil}(R)=0$.

(1.60) Corollary: Let R be a reduced ring. Then $ZD(R) = \bigcup_{P\subseteq R \text{ min. prime}} P$.

Proof: By (1.58) "$\supseteq$". For the other inclusion suppose $a\in ZD(R)$ and $a\notin \bigcup_{P \text{ min.}} P$. Then there is a $b\in R-(0)$ with $ab=0$ and $ab\in P$ for all $P\in\operatorname{Spec}(R)$. Thus $b\in P$ for all minimal prime ideals $P\subseteq R$. Thus $b\in \operatorname{nil}(R) = (0)$, a contradiction.

(1.61) Remark: Let R be a ring and $S\subseteq R$ a multiplicative set.
(a) If R is a PID, $S^{-1}R$ is a PID.
(b) If R is factorial, $S^{-1}R$ is factorial.

(c) If R is reduced, $S^{-1}R$ is reduced.

(1.62) Remark: Let R be a ring and $P \subseteq R$ a prime ideal. The residue class ring $k(P) = R_P / PR_P$ is isomorphic to the field of quotients $Q(R/P)$.

Proof: The natural map $\nu: R \longrightarrow R/P$ maps $S = R - P$ into $R/P - (0)$. The statement follows by (1.54).

(1.63) Theorem: Let M be an R-module. The following are equivalent:

(a) $M = (0)$

(b) $M_m = (0)$ for all maximal ideals $m \subseteq R$.

Proof: (b) $\Rightarrow$ (a): Suppose $M \neq 0$. We want to show that there is at least one maximal ideal $m \subseteq R$ with $M_m \neq 0$. Let $n \in M - (0)$ and consider the submodule $N = Rn \subseteq M$. Since $N_m \subseteq M_m$ for all maximal ideals m of R it suffices to show that $N_m \neq 0$ for some maximal ideal $m \subseteq R$. $N = Rn \cong R/I$ for some ideal $I \subseteq R$ and it suffices to show that $(R/I)_m \neq 0$ for some maximal ideal m. Since $I \neq R$, there is a maximal ideal $m \subseteq R$ with $I \subseteq m$ and $I_m \neq R_m$ since $I \cap (R - m) = \emptyset$. Thus $(R/I)_m \cong R_m / I_m \neq 0$.

(1.64) Corollary: Let $\varphi: M \longrightarrow N$ be an R-linear map. The following are equivalent:

(a) φ is injective (or surjective, bijective).

(b) φ_m is injective (or surjective, bijective) for all maximal ideals $m \subseteq R$.

Proof: (a) $\Rightarrow$ (b): Apply (1.51) to $0 \longrightarrow M \xrightarrow{\varphi} N$ or/and $M \xrightarrow{\varphi} N \longrightarrow 0$.

(b) $\Rightarrow$ (a): Consider the exact sequences

$$0 \longrightarrow \ker(\varphi) \longrightarrow M \xrightarrow{\varphi} N \quad \text{and} \quad M \xrightarrow{\varphi} N \longrightarrow \operatorname{coker}(\varphi) \longrightarrow 0.$$

By (1.51) for all maximal ideals $m \subseteq R$ the sequences:

$0 \to \ker(\varphi)_m \to M_m \xrightarrow{\varphi_m} N_m$ and $M_m \xrightarrow{\varphi_m} N_m \to \operatorname{coker}(\varphi)_m \to 0$ are exact. In particular, $\ker(\varphi)_m = \ker(\varphi_m)$ and $\operatorname{coker}(\varphi)_m = \operatorname{coker}(\varphi_m)$. Thus φ_m is injective for all maximal ideals $m \subseteq R \iff \ker(\varphi)_m = \ker(\varphi_m) = 0$ for all maximal ideals $m \subseteq R \iff \ker(\varphi) = 0$ (by (1.63)) $\iff \varphi$ is injective. A similar argument applied to $\operatorname{coker}(\varphi)$ yields the surjective case.

(1.65) Corollary: Let M be an R-module, $U \subseteq M$ a submodule and $x \in M$. Then $x \in U \iff i_{M,m}(x) \in U_m$ for all maximal ideals $m \subseteq R$.

Proof: Consider the R-linear map $\varphi: R \to M/U$ defined by $\varphi(a) = ax + U$. Obviously, $x \in U \iff \varphi = 0 \iff \operatorname{im}(\varphi) = 0$. Since $\operatorname{im}(\varphi)_m = \operatorname{im}(\varphi_m)$ for all maximal ideals $m \subseteq R$, the statement follows by (1.63).

(1.66) Corollary: Let R be a domain and $Q(R)$ its field of quotients. For all maximal ideals $m \subseteq R$ consider R_m a subring of $Q(R)$. Then

$$R = \bigcap_{m \subseteq R \text{ max}} R_m .$$

Proof: $U = R$ and $M = \bigcap R_m$ are R-submodules of $Q(R)$ with $R = U \subseteq M$. For all maximal ideals $m \subseteq R$: $M \subseteq R_m = U_m$ and thus $M_m \subseteq (R_m)_m = R_m$. Therefore $i_{M,m}(x) \in U_m$ for all $x \in M$ and $M = U$ by (1.65).

§4: CHAIN CONDITIONS

(1.67) Proposition: Let $(\mathcal{M}, \leq)$ be a partially ordered set. The following are equivalent:
(a) Every ascending chain $M_1 \leq M_2 \leq \dots$ of elements of $\mathcal{M}$ is stationary, that is, there is an $n \in \mathbb{N}$ such that $M_n = M_{n+k}$ for all $k \in \mathbb{N}$.
(b) Every nonempty subset of $\mathcal{M}$ has a maximal element.

Proof: (a) $\Rightarrow$ (b): Suppose that (b) is false and let $\Gamma \subseteq \mathcal{M}$ be a nonempty subset which fails to have a maximal element. Let $M_1 \in \Gamma$. M_1 is not maximal in Γ, thus there is an element $M_2 \in \Gamma$ with $M_1 \lneq M_2$. Since $M_2 \in \Gamma$ is not maximal, there is an $M_3 \in \Gamma$ with $M_2 \lneq M_3$. Continuing we obtain an infinite chain: $M_1 \lneq M_2 \lneq M_3 \lneq \dots$.
(b) $\Rightarrow$ (a): Let $M_1 \leq M_2 \leq \dots$ be an ascending chain in $\mathcal{M}$. Apply (b) to the subset: $\Gamma = \{M_1, M_2, \dots\}$.

(1.68) Proposition: Let $(\mathcal{M}, \leq)$ be a partially ordered set. The following are equivalent:
(a) Every descending chain $M_1 \geq M_2 \geq \dots$ of elements of $\mathcal{M}$ is stationary, that is, there is an $n \in \mathbb{N}$ such that $M_n = M_{n+k}$ for all $k \in \mathbb{N}$.
(b) Every nonempty subset of $\mathcal{M}$ has a minimal element.

Proof: Similar to the proof of (1.67).

(1.69) Definition: Let M be an R-module. The set $\mathcal{M} = \{N \subseteq M \mid N \text{ a submodule}\}$ of submodules of M is partially ordered by inclusion.
(a) M satisfies the ascending chain condition (acc) or M is a Noetherian R-module if $(\mathcal{M}, \leq)$ satisfies the conditions of (1.67).
(b) M satisfies the descending chain condition (dcc) or M is an Artinian R-module if $(\mathcal{M}, \leq)$ satisfies the conditions of (1.68).
(c) R is called a Noetherian (Artinian) ring if the R-module R is Noetherian (Artinian).

(1.70) Examples: (a) Every PID is Noetherian. In particular, $\mathbb{Z}$ and $K[x]$, the polynomial ring in one variable over a field K, are Noetherian.
(b) For all $n \in \mathbb{N}$ with $n \neq 0$ the ring $\mathbb{Z}/n\mathbb{Z}$ is Artinian and Noetherian.
(c) $\mathbb{Z}$ and $K[x]$ are not Artinian. For example, the descending chain of ideals:
$(2) \supseteq (4) \supseteq (8) \supseteq \ldots$ is not stationary.

Proof: (a) Let R be a PID and $(a_1) \subseteq (a_2) \subseteq \ldots$ an ascending chain of ideals of R. Their union $I = \bigcup_{i \in \mathbb{N}} (a_i)$ is an ideal of R and hence principal: $I = (a)$. Then $a \in (a_n)$ for some $n \in \mathbb{N}$ and $(a_n) = (a_{n+k})$ for all $k \in \mathbb{N}$.
(b) $\mathbb{Z}/n\mathbb{Z}$ has only finitely many ideals. Thus $\mathbb{Z}/n\mathbb{Z}$ is Artinian and Noetherian.

(1.71) Lemma: Let M be an R-module, $E \subseteq F \subseteq M$ and $N \subseteq M$ submodules of M. If $E \cap N = F \cap N$ and $(E+N)/N = (F+N)/N$, then $E = F$.

Proof: Let $f \in F$. Since $(E+N)/N = (F+N)/N$, there are elements $e \in E$ and $n_1, n_2 \in N$ such that $f + n_1 = e + n_2 \Rightarrow f - e = n_2 - n_1 \in F \cap N = E \cap N \Rightarrow f \in E$.

(1.72) Proposition: Let $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ be an exact sequence of R-modules. M is Noetherian (Artinian) if and only if M' and M'' are Noetherian (Artinian).

Proof: "$\Rightarrow$": Suppose that M is Noetherian (Artinian). Let $N \subseteq M$ be a submodule. Then N and M/N are Noetherian (Artinian). The statement follows since M' is isomorphic to a submodule N of M and M'' is isomorphic to M/N.
"$\Leftarrow$": Consider an ascending chain $M_1 \subseteq M_2 \subseteq \ldots$ of submodules of M. Identify M' with a submodule of M and M'' with the factor module M/M'. If M' and M'' are Noetherian, the chains: $M_1 \cap M' \subseteq M_2 \cap M' \subseteq \ldots$ in M' and

$$(M_1+M')/M' \subseteq (M_2+M')/M' \subseteq \ldots \quad \text{in } M'' = M/M'$$

are stationary. There is an $n \in \mathbb{N}$ with $M_n \cap M' = M_{n+k} \cap M'$ and $(M_n+M')/M' = (M_{n+k}+M')/M'$

for all $k \in \mathbb{N}$. By (1.71) $M_n = M_{n+k}$ for all $k \in \mathbb{N}$. In the Artinian case a similar argument works for a descending chain of submodules of M.

(1.73) Corollary: Let $M_1, M_2, \ldots, M_n$ be R-modules. The following are equivalent:
(a) For all $1 \leq i \leq n$ M_i is Noetherian (Artinian).
(b) $\bigoplus_{i=1}^{n} M_i$ is Noetherian (Artinian).
In particular, if R is a Noetherian (Artinian) ring, the finite free R-module R^n is Noetherian (Artinian).

Proof: By induction on n. Apply (1.72) to the exact sequence:

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_n \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0.$$

(1.74) Proposition: Let R be a Noetherian (Artinian) ring. Every finite R-module is Noetherian (Artinian).

Proof: A finite R-module M is a homomorphic image of R^n for some $n \in \mathbb{N}$.

(1.75) Corollary: Let R be a Noetherian (Artinian) ring and $I \subseteq R$ an ideal. The ring R/I is Noetherian (Artinian).

Proof: R/I is a finite R-module. Every ideal of R/I is an R-submodule of R/I.

§5: NOETHERIAN RINGS AND MODULES

(1.76) Proposition: An R-module M is Noetherian if and only if every submodule of M is finitely generated. In particular, the ring R is Noetherian if and only if every ideal of R is finitely generated.

Proof: "$\Rightarrow$": Suppose that M is Noetherian and that $N \subseteq M$ is a submodule. Consider $\Gamma = \{U \subseteq N \mid U \text{ a submodule and } U \text{ is finitely generated}\}$. Since $(0) \in \Gamma$, $\Gamma \neq \emptyset$, and Γ has a maximal element N_0. If $N \neq N_0$, let $x \in N - N_0$. Then $N_0 + Rx \in \Gamma$ and $N_0 \neq N_0 + Rx$, a contradiction.
"$\Leftarrow$": Let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of submodules of M. By assumption the submodule $N = \bigcup_{i \in \mathbb{N}} M_i$ is finitely generated. Then $N = M_n$ for some $n \in \mathbb{N}$ and $M_n = M_{n+k}$ for all $k \in \mathbb{N}$.

(1.77) Hilbert's Basis Theorem: Let R be a Noetherian ring. The polynomial ring $R[x]$ is Noetherian.

Proof: Suppose that $R[x]$ is not Noetherian and let $I \subseteq R[x]$ be an ideal which is not finitely generated. Let $f_1 \in I - (0)$ be an element of minimal degree. Then $I \neq (f_1)$ and there is an element $f_2 \in I - (f_1)$ of minimal degree. Continue to choose elements $f_n \in I$ so that $f_{i+1} \in I - (f_1, \dots, f_i)$ of minimal degree. Set $k_i = \deg f_i$ and let a_i be the leading coefficient of f_i. By construction $k_1 \leq k_2 \leq \dots$. With $J_n = (a_1, \dots, a_n) \subseteq R$ $J_1 \subseteq J_2 \subseteq \dots$ is an ascending chain of ideals of R. Since R is Noetherian, there is an $r \in \mathbb{N}$ so that $J_r = J_{r+t}$ for all $t \in \mathbb{N}$. In particular, $a_{r+1} = \sum_{i=1}^{r} a_i b_i$ for some $b_i \in R$. Consider $g = f_{r+1} - \sum_{i=1}^{r} b_i f_i x^{k_{r+1} - k_i}$. Obviously, $g \in I$, $\deg g < \deg f_{r+1}$ and $g \notin (f_1, \dots, f_r)$, a contradiction.

(1.78) Definition: Let R be a ring. A ring S is called a finitely generated R-algebra if

$S \cong R[x_1, \dots, x_n]/I$ where $x_1, \dots, x_n$ variables and $I \subseteq R[x_1, \dots, x_n]$ an ideal.

(1.79) Corollary: If R is Noetherian every finitely generated R-algebra is Noetherian.

(1.80) Examples of non-Noetherian rings:

(a) Let K be a field. The polynomial ring $R = K[\{x_i\}_{i \in \mathbb{N}}]$ in infinitely many variables is not Noetherian. $(x_1) \subseteq (x_1, x_2) \subseteq \dots$ is an ascending, non-stationary chain of ideals.

(b) The ring of entire functions $R = \{f : \mathbb{C} \to \mathbb{C} \mid f \text{ analytic on } \mathbb{C}\}$ is not Noetherian. Define for all $n \in \mathbb{N}$: $I_n = \{f \in R \mid f(z) = 0 \ \forall\, z \in \mathbb{N} \text{ with } z > n\}$. $I_1 \subseteq I_2 \subseteq \dots$ is an increasing, non stationary chain of ideals of R. (Weierstraß factorization theorem)

(c) The ring of continuous functions on $[0,1]$: $R = \{f : [0,1] \to \mathbb{R} \mid f \text{ continuous}\}$ is not Noetherian. For all $n \in \mathbb{N}$ set $I_n = \{f \in R \mid f(x) = 0 \ \forall\, x \in [0, 1/n]\}$. Then $I_1 \subseteq I_2 \subseteq \dots$ is an asending, non-stationary chain of ideals of R.

(1.81) Definition: Let R be a ring, M an R-module, $N, N' \subseteq M$ submodules and $I \subseteq R$ an ideal. Define:

$(N : N') = (N : N')_R := \{a \in R \mid aN' \subseteq N\}$

$(N : I) = (N : I)_M := \{x \in M \mid Ix \subseteq N\}$

$(0 : M) = (0 : M)_R = \operatorname{ann}(M)$ is called the annihilator of M. M is called a faithful R-module if $\operatorname{ann}(M) = 0$.

(1.82) Remark: $(N : N')_R$ is an ideal of R and $(N : I)_M$ is a submodule of M.

(1.83) Theorem: (Cohen): Let R be a ring. If all prime ideals of R are finitely generated then R is Noetherian.

Proof: Consider the set $\mathfrak{M} = \{I \subseteq R \mid I \text{ a non-finitely generated ideal}\}$. If R is not Noetherian, $\mathfrak{M} \neq \emptyset$ and $\mathfrak{M}$ is partially ordered by inclusion. In order to verify

that Zorn's Lemma applies, let $\mathcal{K} \subseteq \mathfrak{M}$ be a chain. The ideal $J = \bigcup_{I \in \mathcal{K}} I$ is not finitely generated (if $J = (a_1, \dots, a_n)$ then $J = I$ for some $I \in \mathcal{K}$). Hence $J \in \mathfrak{M}$ and $\mathfrak{M}$ has a maximal element I.

Claim: I is a prime ideal.

Pf of claim: If I is not prime there are elements $a, b \in R$ with $ab \in I$ and $a \notin I$, $b \notin I$. Then $I + (a) \notin \mathfrak{M}$ and $I + (b) \notin \mathfrak{M}$ and there are $u_1, \dots, u_n \in I$ with $I + (b) = (u_1, \dots, u_n, b)$. Since $I + (a) \subseteq (I : (b)) = \{x \in R \mid xb \in I\}$, also $(I : (b)) \notin \mathfrak{M}$ and $(I : (b)) = (v_1, \dots, v_m)$ for some $v_i \in R$. But then $I = (u_1, \dots, u_n, bv_1, \dots, bv_m)$. Obviously, $(u_1, \dots, u_n, bv_1, \dots, bv_m) \subseteq I$. In order to verify the other inclusion let $z \in I$. Then $z \in I + (b)$ and there are elements $d_i, y \in R$ so that $z = \sum_{i=1}^{n} d_i u_i + by$. Thus $by \in I$ and $y \in (I : (b))$. Therefore $y = \sum_{i=1}^{m} c_i v_i$ for some $c_i \in R$.

(1.84) Corollary: Let R_1 and R_2 be Noetherian rings. Their product $R_1 \times R_2$ is a Noetherian ring.

Proof: Every prime ideal of $R_1 \times R_2$ is of the form $P \times R_2$ or $R_1 \times Q$ where $P \in \operatorname{Spec}(R_1)$ and $Q \in \operatorname{Spec}(R_2)$.

(1.85) Proposition: Let R be a ring and M an R-module. If M is Noetherian, the ring $R/\operatorname{ann}(M)$ is Noetherian.

Proof: We may replace R by $R/\operatorname{ann}(M)$ and assume that M is a faithful R-module. Suppose $M = \sum_{i=1}^{n} R m_i$ and consider the map $\varphi : R \longrightarrow M^n$ defined by $\varphi(a) = (am_1, \dots, am_n)$. φ is R-linear and injective since $\operatorname{ann}(M) = 0$. Thus R is isomorphic to a submodule of the Noetherian R-module M^n. R is Noetherian.

(1.86) Theorem (Formanek): Let R be a ring and T a finite faithful R-module. Suppose that the set

$$\mathfrak{M} = \{IT \mid I \subseteq R \text{ an ideal}\}$$

satisfies the ascending chain condition when partially ordered by inclusion. Then R is a Noetherian ring.

Proof: By (1.85) it suffices to show that there is a faithful Noetherian R-module. Suppose that T is not a Noetherian R-module. Since T is finite, R is not a Noetherian ring. Consider the following subset of $\mathfrak{M}$:

$$\mathfrak{N} = \{IT \mid I \subseteq R \text{ an ideal and } T/IT \text{ not Noetherian}\}.$$

Since $(0) \in \mathfrak{N}$, $\mathfrak{N} \neq \emptyset$, by assumption $\mathfrak{N}$ has a maximal element IT, where $I \subseteq R$ is an ideal. Replace R by $R/\operatorname{ann}(T/IT)$ and T by T/IT and assume:

(*) T is a finite, non-Noetherian, faithful R-module and for every ideal $J \subseteq R$ with $J \neq (0)$ the factor module T/JT is Noetherian.

Consider the following set of submodules of T:

$$\Gamma := \{N \subseteq T \mid N \text{ a submodule and } T/N \text{ is faithful over } R\}.$$

If $T = Rb_1 + \cdots + Rb_n$, then

(**) $N \in \Gamma \iff \forall\, a \in R,\ a \neq 0 : \{ab_1, \ldots, ab_n\} \not\subseteq N$.

Since T is a faithful R-module, $(0) \in \Gamma$ and $\Gamma \neq \emptyset$. Moreover, Γ is partially ordered by inclusion. We want to show that Γ is inductively ordered. For a chain $\mathcal{K} \subseteq \Gamma$ set $N = \bigcup_{K \in \mathcal{K}} K$. N is a submodule of T. If $N \notin \Gamma$ there is an $a \in R - (0)$ with $\{ab_1, \ldots, ab_n\} \subseteq N$ by (**). But then $\{ab_1, \ldots, ab_n\} \subseteq K$ for some $K \in \mathcal{K}$ and $K \notin \Gamma$, a contradiction. By Zorn's Lemma Γ has a maximal element $N_0 \in \Gamma$. Replace T by T/N_0. Then:

(a) T is a non-Noetherian, faithful R-module. (If T is Noetherian, by (1.85) the ring R is Noetherian. But R is assumed to be not Noetherian.)

(b) By (*) for every ideal $I \subseteq R$ with $I \neq (0)$ the R-module T/IT is Noetherian.

(c) By the maximality of N_0 for every nonzero submodule $N \subseteq T$ the factor module T/N is not faithful over R.

We claim that conditions (a), (b), and (c) imply that every submodule of T is

finitely generated. This yields the contradiction that T is a Noetherian R-module. Let $N \subseteq T$ be a nonzero submodule. By (c) T/N is not faithful over R and there is an element $a \in R-(0)$ with $aT \subseteq N$. By (b) T/aT is Noetherian and N/aT is a finite R-module. Since T is a finite R-module, aT is finitely generated. Thus N is finitely generated and T is Noetherian, a contradiction.

(1.87) Theorem: (Eagin-Nagata) Let T be a Noetherian ring and $R \subseteq T$ a subring such that T is a finite R-module. Then R is a Noetherian ring.

Proof: Obviously, T is a faithful R-module and the set

$$\mathcal{M} = \{IT \mid I \subseteq R \text{ an ideal}\}$$

is a set of ideals of T. Apply (1.86).

§6: ARTINIAN RINGS AND MODULES

Let M be an R-module. A finite chain of submodules $(0)=M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n = M$ is called a normal series of M. The modules M_i/M_{i-1} are called the factors of the series. We are mostly interested in normal series of M so that the factors M_i/M_{i-1} have special properties.

(1.88) Definition: Let M be an R-module.

(a) Two normal series of M: $(0)=M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n = M$ and $(0)=N_0 \subsetneq N_1 \subsetneq \dots \subsetneq N_r = M$ are called equivalent if:

(i) $n=r$

(ii) There is a permutation $\sigma \in S_n$ so that $M_i/M_{i-1} \cong N_{\sigma(i)}/N_{\sigma(i)-1}$ for all $1 \le i \le n$.

(b) The series $(0)=P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_s = M$ is called a refinement of the series $(0)=M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n = M$ if for all $0 \le i \le n$ there is an $0 \le j \le s$ with $M_i = P_j$.

(1.89) Theorem: (Schreier) Let M be an R-module. Any two normal series of M have equivalent refinements.

Proof: MTH 818, 819

(1.90) Definition: An R-module M is called simple if M does not contain a proper submodule.

(1.91) Definition: Let M be an R-module. A normal series of M: $(0)=M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n = M$ is called a composition series if for all $1 \le i \le n$ the factor module M_i/M_{i-1} is a simple R-module.

(1.92) Remark: (a) Not every R-module admits a composition series. The $\mathbb{Z}$-module $\mathbb{Z}$ has no composition series while $\mathbb{Z}/n\mathbb{Z}$ for $n \neq 0$ has a composition series.

(b) A composition series has no proper refinement.

(1.93) Definition: An R-module M is called of finite length if M has a composition series $(0)=M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_r = M$. r is called the length of M, denoted $\ell_R(M)=r$. If M has no composition series we set $\ell_R(M)=\infty$.

(1.94) Proposition: Let M be an R-module of finite length.
(a) Any normal series of M has a refinement which is a composition series.
(b) Any two composition series of M are equivalent.

Proof: (a) Let $(0)=M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n = M$ be a normal series and $(0)=N_0 \subsetneq N_1 \subsetneq \dots \subsetneq N_s = M$ a composition series of M. By (1.89) both series have equivalent refinements. There is no proper refinement of a composition series, and a series which is equivalent to a composition series is a composition series.
(b) immediately from (1.89)

(1.95) Proposition: Let M be an R-module and $U \subseteq M$ a submodule.
(a) $\ell_R(M) < \infty \iff \ell_R(U) < \infty$ and $\ell_R(M/U) < \infty$
(b) If $\ell_R(M) < \infty$ then $\ell_R(M) = \ell_R(U) + \ell_R(M/U)$
(c) Suppose that $\ell_R(M) < \infty$. Then $U \neq M \iff \ell_R(U) < \ell_R(M)$ and $U \neq 0 \iff \ell_R(M/U) < \ell_R(M)$.

Proof: (a) "$\Leftarrow$": Consider composition series $(0)=U_0 \subsetneq U_1 \subsetneq \dots \subsetneq U_r$ of U and $(0)=\overline{V_0} \subsetneq \overline{V_1} \subsetneq \dots \subsetneq \overline{V_s} = M/U$ of M/U. Let $\varphi: M \longrightarrow M/U$ be the natural map. For all $0 \le i \le s$ set $V_i = \varphi^{-1}(\overline{V_i})$. Then for all $0 \le i \le s$ $U \subseteq V_i$ and $V_i/U = \overline{V_i}$. Moreover, $V_i/V_{i-1} = (V_i+U)/(V_{i-1}+U) \cong ((V_i+U)/U)/((V_{i-1}+U)/U) = \overline{V_i}/\overline{V_{i-1}}$. Hence $(0)=U_0 \subsetneq U_1 \subsetneq \dots \subsetneq U_r = U = V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_s = M$ is a composition series of M.
"$\Longrightarrow$": Consider the normal series of M: $(0)=M_0 \subsetneq M_1 = U \subsetneq M$. By (1.94) this series has a refinement which is a composition series:

$$\underbrace{(0)=M_0=U_0 \subsetneq U_1 \subsetneq \dots \subsetneq U_r=M_1=U}_{(*)}=\underbrace{V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_s = M}_{(**)}.$$

$(*)$ is a composition series of U. From $(**)$ we obtain the composition series of M/U:

$$(0)=\overline{V_0}=V_0/U \subsetneq \overline{V_1}=V_1/U \subsetneq \dots \subsetneq \overline{V_s}=V_s/U=M/U.$$

(b) and (c) follow from the proof of (a).

(1.96) Corollary: Length is an additive function, i.e., let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of R-modules. Then $\ell_R(M)=\ell_R(M')+\ell_R(M'')$.

Proof: Identify M' with a submodule U of M and M'' with M/U.

(1.97) Proposition: Let R be a ring and M an R-module. Then

(a) $\ell_R(M)<\infty$

(b) M satisfies the a.c.c. and the d.c.c.

Proof: (a) $\Rightarrow$ (b): Every series of submodules of M has length $\leq \ell_R(M)$.

(b) $\Rightarrow$ (a): The a.c.c. implies that every nonempty set of submodules has a maximal element. Let $M_1 \subsetneq M$ be a maximal submodule U with $U \neq M$; then let $M_2 \subsetneq M_1$ be a maximal submodule $V \subsetneq M_1$. This yields a descending chain of submodules $M \supsetneq M_1 \supsetneq \dots$ By the d.c.c. the chain is stationary. By construction the factor modules are simple. Thus $M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$ is a composition series of M.

(1.98) Proposition: Every prime ideal of an Artinian ring R is maximal.

Proof: Let $P \subseteq R$ be a prime ideal. The ring $S=R/P$ is an Artinian domain. We want to show that S is a field. Let $b \in S-(0)$ and consider the descending chain of ideals: $(b) \supseteq (b^2) \supseteq (b^3) \supseteq \dots$. Since S is Artinian there is an $r \in \mathbb{N}$ so that $(b^r)=(b^{r+1})$. Thus there is an $a \in S$ with $b^r = ab^{r+1}$. Since S is a domain, $1=ab$.

(1.99) Proposition: An Artinian ring R has only finitely many maximal ideals.

Proof: Suppose that R has infinitely many maximal ideals. Take an infinite countable set $\{m_i\}_{i\in\mathbb{N}}$ of maximal ideals of R and consider the set of ideals:

$$\mathcal{M} = \{m_1 \cap \dots \cap m_r \mid r \in \mathbb{N}\}$$

Since R is Artinian, $\mathcal{M}$ has a minimal element $m_1 \cap \dots \cap m_r$. Then $m_1 \cap \dots \cap m_r = m_1 \cap \dots \cap m_{r+1}$ and therefore $m_{r+1} \supseteq m_1 \cap \dots \cap m_r$. Thus $m_{r+1} = m_i$ for some $1 \le i \le r$.

(1.100) Proposition: Let R be an Artinian ring. The nilradical $nil(R)$ is nilpotent, that is, there is an $n \in \mathbb{N}$ with $(nil(R))^n = (0)$.

Proof: Since R satisfies the d.c.c. there is a $k \in \mathbb{N}$ with $(nil(R))^k = (nil(R))^{k+t}$ for all $t \in \mathbb{N}$. Suppose $(nil(R))^k \neq (0)$ and set $I = (nil(R))^k$. Consider the set $\mathcal{M} = \{J \subseteq R \mid J \text{ an ideal and } JI \neq (0)\}$. Since $R \in \mathcal{M}$, $\mathcal{M} \neq \emptyset$, and $\mathcal{M}$ has a minimal element $J_0 \in \mathcal{M}$. Thus there is an $x \in J_0$ with $xI \neq (0)$ and by the minimality of J_0: $J_0 = (x)$. By assumption $I^t = I$ for all $t \in \mathbb{N}$ and therefore $(xI)I = xI^2 = xI \neq (0)$. Hence $xI = (x)$. Let $y \in I$ with $x = xy$, then $x = xy = \dots = xy^n$. By assumption $y \in nil(R)$, thus $x = 0$, a contradiction.

Let R be an Artinian ring. By (1.98) and (1.99) every prime ideal of R is maximal and R has only finitely many maximal ideals. Let $\mathcal{M} = \{m_1, \dots, m_r\} = Spec(R)$ be the set of maximal ideals of R. Then $nil(R) = \bigcap_{i=1}^r m_i = Jrad(R)$. Since $m_1, \dots, m_r$ are mutually comaximal, by the Chinese remainder theorem:

$$nil(R) = \bigcap_{i=1}^r m_i = \prod_{i=1}^r m_i.$$

By (1.100) there is a $k \in \mathbb{N}$ such that

$$nil(R)^k = \left(\prod_{i=1}^r m_i\right)^k = \prod_{i=1}^r m_i^k = (0).$$

Thus in an Artinian ring the zero ideal is a (finite) product of maximal ideals.

(1.101) Theorem: Let R be a ring in which the zero ideal is product of (finitely many) maximal ideals. Then R is Noetherian if and only if R is Artinian. In particular, every Artinian ring is Noetherian.

For the proof of (1.101) we need:

(1.102) Lemma: Let K be a field and V a K-vector space. The following are equivalent:

(a) $\dim_K V < \infty$

(b) $\ell_K(V) < \infty$

(c) V is a Noetherian K-vector space.

(d) V is an Artinian K-vector space.

Proof: Homework

Proof of (1.101) Let $m_i \subseteq R$, $1 \le i \le n$, be maximal ideals with $(0) = m_1 \cdots m_n$. Consider the chain of ideals $R \supseteq m_1 \supseteq m_1 m_2 \supseteq \cdots \supseteq m_1 \cdots m_n = (0)$. The factor modules $M_1 = R/m_1$ and $M_i = m_1 \cdots m_{i-1}/m_1 \cdots m_i$ are $K_i = R/m_i$-vector spaces. By (1.102) the K_i-modules M_i are Noetherian if and only if they are Artinian. Set $J_i = m_1 \cdots m_i$ and consider the exact sequences:

$$0 \longrightarrow J_1 \longrightarrow R \longrightarrow M_1 \longrightarrow 0$$

$$0 \longrightarrow J_2 \longrightarrow J_1 \longrightarrow M_2 \longrightarrow 0$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$0 \longrightarrow J_{r-2} \longrightarrow J_{r-1} \longrightarrow M_{r-2} \longrightarrow 0$$

$$0 \longrightarrow J_{r-1} \xrightarrow{\cong} M_{r-1} \longrightarrow 0$$

R Noetherian $\Rightarrow$ J_1, M_1 Noetherian

$\Rightarrow$ J_1, J_2, M_1, M_2 Noetherian

$\vdots$

$\Rightarrow$ $J_1, \dots, J_{r-1}, M_1, \dots, M_{r-1}$ Noetherian

$\Rightarrow$ $J_{r-1} = M_{r-1}, M_1, \dots, M_{r-2}$ Artinian

$\Rightarrow$ $\mathfrak{J}_{r-2}, \mathfrak{J}_{r-1}, M_1, \dots, M_{r-2}$ Artinian

$\vdots$

$\Rightarrow$ R Artinian.

A similar argument shows: R Artinian $\Rightarrow$ R Noetherian.

(1.103) Corollary: Let R be a ring. R is Artinian if and only if R is Noetherian and every prime ideal of R is maximal.

Proof: "$\rightarrow$": By (1.98), (1.100), and (1.101).

"$\leftarrow$": Suppose that R is Noetherian and every prime ideal of R is maximal. Then every prime ideal of R is maximal and minimal. We show in the next chapter (2.17) that a Noetherian ring has only finitely many minimal primes. Let $\mathfrak{M} = \{m_1, \dots, m_n\}$ be the set of maximal ideals of R. Then $nil(R) = \bigcap_{i=1}^n m_i = \prod_{i=1}^n m_i$. Since $nil(R)$ is finitely generated, there is a $k \in \mathbb{N}$ with $nil(R)^k = \prod_{i=1}^n m_i^k = (0)$. By (1.101) R is Artinian.

(1.104) Corollary: Every Artinian ring is isomorphic to a (finite) product of local Artinian rings.

Proof: Let R be an Artinian ring, $\mathfrak{M} = \{m_1, \dots, m_n\}$ the finite set of maximal ideals of R. There is a $k \in \mathbb{N}$ so that $\prod_{i=1}^n m_i^k = (0)$. Since the ideals $m_1^k, \dots, m_n^k$ are mutually comaximal, by the Chinese Remainder Theorem:

$$R \xrightarrow{\cong} \prod_{i=1}^n R/m_i^k.$$

The rings R/m_i^k are local Artinian with maximal ideal m_i/m_i^k.

(1.105) Remark: Apparently Artinian rings are the 'little' cousin of Noetherian rings. For modules the story is not so simple. We will see later: If R is a complete local Noetherian ring, then there is a 1-1 correspondence between Noetherian and Artinian R-modules.