CHAPTER I: BASIC FACTS ABOUT RINGS AND MODULES

§1. RINGS

(1.1) Definition: Let A be a ring. We define the following subsets of A:

(a) $A^* = \{a \in A \mid \exists\, b \in A : ab = 1\}$ the set of units of A

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

(c) $ZD(A) = A - NZD(A) = \{a \in A \mid \exists\, b \in A-(0) : ab = 0\}$ the set of zero divisors (ZD) of A

(d) $Nil(A) = \{a \in A \mid \exists\, n \in \mathbb{N} : a^n = 0\}$ the nilradical of A (the set of nilpotent elements of A)

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

(b) $NZD(A)$ is a multiplicative semigroup of A.

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

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

(e) $(0) \subseteq Nil(A) \subseteq ZD(A) \subseteq A \setminus A^*$

$\{1\} \subseteq A^* \subseteq NZD(A) = A - ZD(A) \subseteq A - Nil(A)$.

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

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

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

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

(d) Let A be a finite ring and $a \in A$. Then a is a unit in $A \iff a$ is a NZD of A. Thus $A^* = NZD(A)$. This statement is false for infinite rings.

(1.4) <u>Definition</u>: Let A be a ring and $I \subseteq A$ an ideal. The <u>radical</u> of I is defined by: $\operatorname{rad}(I) = \{a \in A \mid \exists\, n \in \mathbb{N} : a^n \in I\}$.

(1.5) <u>Remark</u>: (a) $\operatorname{rad}(I)$ is an ideal of A.
(b) Let $\varepsilon : A \longrightarrow A/I$ be the canonical map. Then $\operatorname{rad}(I) = \varepsilon^{-1}(\operatorname{nil}(A/I))$.

<u>Proof</u>: (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) <u>Definition</u>: Let A be a ring and $I, J \subseteq A$ ideals. I and J are called <u>comaximal</u> if $I + J = A$.

(1.7) <u>Remark</u>: Let A be a ring and $I, J, K \subseteq A$ ideals.
(a) I and J are comaximal $\Longleftrightarrow$ $\exists\, a \in I$ and $b \in J$ 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 comaximal then I and JK are comaximal.

<u>Proof</u>: (b) $I \cap J = A(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ \subseteq I + J$.
(c) I and J comaximal $\Rightarrow$ $\exists\, a \in I$ and $b \in J$ with $a + b = 1$.
I and K comaximal $\Rightarrow$ $\exists\, a' \in I$ and $c \in K$ with $a' + c = 1$.

$$\Rightarrow 1 = (a+b)(a'+c) = \underbrace{aa' + a'b + ac}_{\in I} + \underbrace{bc}_{\in JK}$$

Thus I and JK are comaximal.

Let A be a ring and $I_1, \ldots, I_n$ ideals of A. The map:

$$\varphi : A \longrightarrow \prod_{i=1}^{n} A/I_i$$
$$a \longmapsto (a + I_1, a + I_2, \ldots, a + I_n)$$

defines a homomorphism of rings.

(1.8) <u>Theorem</u>: (Chinese Remainder Theorem) Assumptions as above.

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

(b) φ is surjective $\iff I_1, \_\_, I_n$ are mutually comaximal.

<u>Proof</u>: (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.
Applying (1.7) again: $\prod_{i=1}^{n} I_i = K.I_n = K \cap I_n = \bigcap_{i=1}^{n} I_i$.
(b) "$\Rightarrow$": We only show the I_1 and I_2 are comaximal. Since φ is surjective there is an $a \in A$ with $\varphi(a) = (\bar{1}, 0, \_\_, 0)$. 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. Similar arguments show that $I_1, \_\_, I_n$ are mutually comaximal.
"$\Leftarrow$": It is enough to show: $\forall\ 1 \leq i \leq n\ \exists\ a_i \in A$ with $\varphi(a_i) = (0, \_, 0, 1, 0, \_, 0)$ (1 at the ith place). We only show: $\exists\ a \in A$ with $\varphi(a) = (1, 0, \_\_, 0)$.
Since $I_1 + I_j = A\ \forall\ 2 \leq j \leq n$, $\exists\ a_j \in I_1$ and $b_j \in I_j$ $(2 \leq j \leq n)$ with

$$a_j + b_j = 1.$$

Put

$$a = \prod_{j=2}^{n} b_j .$$

Then

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

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

(1.9) <u>Remark</u>: Let A be a principal ideal domain. Then A is factorial and every ideal $I \subseteq A$ is generated by one element: $I = (a)$ for some $a \in A$. Then

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

where p_j are mutually non-associated prime elements of A, $\alpha_j > 0$, and

and $u \in A^*$ a unit. Since A is a PID, the ideals $(p_j^{\alpha_j})$ are mutually comaximal. Thus $I = (a) = (p_1^{\alpha_1}) \cdots (p_n^{\alpha_n}) = (p_1^{\alpha_1}) \cap \ldots \cap (p_n^{\alpha_n})$.

Let $(\mathcal{M}, \leq)$ be a partially ordered set and $\mathcal{K} \subseteq \mathcal{M}$ a subset. $\mathcal{K}$ is called a <u>chain</u> of $\mathcal{M}$ if $\mathcal{K}$ is (completely) 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 $m \in \mathcal{M}$ is called an <u>upper bound</u> of $\mathcal{K}$ if $k \leq m$ for all $k \in \mathcal{K}$.

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

<u>Definition</u>: A partially ordered set in which every chain has an upper bound is called <u>inductively ordered</u>.

(1.10) <u>Theorem</u>: (Existence of prime ideals) Let A be a ring, $S \subseteq A$ a multiplicative set and $I \subseteq A$ an ideal with $S \cap I = \emptyset$. Then:
(a) The set $\mathcal{M} = \{ J \subseteq A \mid J \text{ an ideal with } I \subseteq J \subseteq A - S \}$ is partially ordered by inclusion and has maximal elements.
(b) Every maximal element of $\mathcal{M}$ is a prime ideal of A.

<u>Proof</u>: (a) Since $I \in \mathcal{M}$, $\mathcal{M} \neq \emptyset$. We have to show that $\mathcal{M}$ is inductively ordered. Let $\mathcal{K} \subseteq \mathcal{M}$ be a chain. Consider the set:

$$K = \bigcup_{J \in \mathcal{K}} J$$

and note that K is an ideal of A. 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 $\mathcal{K}$ is a chain $J_1 \subseteq J_2$ or $J_2 \subseteq J_1$. Thus $a + b \in K$.

$I \subseteq K$ and $K \cap S = \emptyset$, thus $K \in \mathfrak{M}$ and K is an upper bound of $\mathfrak{K}$. By Zorn's Lemma $\mathfrak{M}$ has a maximal element P.

(b) Let $P \in \mathfrak{M}$ be a maximal element and let $a, b \in A$ 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 $P+(b) \notin \mathfrak{M}$. This implies:

$$(P+(a)) \cap S \neq \emptyset \quad \text{and} \quad (P+(b)) \cap S \neq \emptyset.$$

Let $p_1, p_2 \in P$ and $\alpha, \beta \in A$ 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:

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

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

(1.11) <u>Corollary</u>: Every ideal $I \subsetneq A$ is contained in a maximal ideal of A.

<u>Proof</u>: Apply (1.10) to I and the multiplicative set $S = \{1\}$.

(1.12) <u>Corollary</u>:
$$A^* = A - \bigcup_{m \subseteq A \text{ maximal ideal}} m$$

<u>Proof</u>: immediately from (1.10).

(1.13) <u>Remark</u>: Let A be a ring, $I \subseteq A$ an ideal and $\varepsilon: A \longrightarrow A/I$ the canonical map.

(a) If $P \subseteq A$ is a prime ideal with $I \subseteq P$ then $\varepsilon(P) = P/I$ is a prime ideal of A/I.

(b) If $Q \subseteq A/I$ is a prime ideal then $\varepsilon^{-1}(Q)$ is a prime ideal of A.

(c) (a) and (b) establishes a 1-1 correspondence between the prime ideals of A which contain I and the prime ideals of A/I.

(1.14) <u>Corollary</u>: Let A be a ring and $I \subseteq A$ an ideal.

(a) $$\operatorname{nil}(A) = \operatorname{rad}(0) = \bigcap_{P \subseteq A \text{ prime}} P$$

(b) $$\operatorname{rad}(I) = \bigcap_{P \subseteq A \text{ prime and } I \subseteq P} P$$

<u>Proof</u>: (a) "$\subseteq$": $a \in \operatorname{nil}(A) \Rightarrow a^n = 0$ for some $n \in \mathbb{N} \Rightarrow a \in P$ for every prime ideal P of A.
"$\supseteq$": Suppose $a \in P$ for all prime ideals P of A. Consider the set $S = \{1, a, \dots, a^n, \dots\} \subseteq A$. S is a multiplicative set of A. If $a^n \neq 0$ for all $n \in \mathbb{N}$ then $S \cap (0) = \emptyset$. (1.10) applied to (0) and S yields the existence of a prime ideal Q of A with $Q \cap S = \emptyset$, a contradiction. Thus $a^n = 0$ for some $n \in \mathbb{N}$.
(b) Let $\varepsilon : A \longrightarrow A/I$ be the canonical map. Since there is a 1-1 correspondence between the prime ideals of A which contain I and the prime ideals of A/I and since $\operatorname{rad}(I) = \varepsilon^{-1}(\operatorname{nil}(A/I))$, (b) follows from (a).

(1.15) <u>Corollary</u>: Let A be a ring. The set of zero divisors $ZD(A)$ is the union of some suitable prime ideals of A.

<u>Proof</u>: $S = NZD(A)$ is a multiplicative set with $S \cap (0) = \emptyset$. By (1.10) there is a prime ideal $P \subseteq A$ with $P \cap S = \emptyset$. Set $\mathcal{X} = \{P \subseteq A \mid P \text{ a prime ideal with } P \cap S = \emptyset\}$.

<u>Claim</u>: $$ZD(A) = \bigcup_{P \in \mathcal{X}} P$$

<u>Pf of claim</u>: Set $T = \bigcup_{P \in \mathcal{X}} P$.
(a) $T \cap S = \emptyset \Rightarrow T \subseteq A - S = ZD(A) \Rightarrow T \subseteq ZD(A)$
"$\leq$": Let $a \in ZD(A) \Rightarrow (a) \subseteq ZD(A)$ and $(a) \cap S = \emptyset$. By (1.10) there is a prime ideal $Q \subseteq A$ with $(a) \subseteq Q$ and $Q \cap S = \emptyset \Rightarrow Q \in \mathcal{X}$ and $a \in T$.

(1.16) <u>Definition</u>: Let A be a ring. The set of prime ideals of A:

$$\mathrm{Spec}(A) = \{P \subseteq A \mid P \text{ a prime ideal}\}$$

is called the <u>spectrum</u> of A.

(1.17) <u>Theorem</u>: Let A be a ring. Every prime ideal $P \in \mathrm{Spec}(A)$ contains a minimal prime ideal.

<u>Proof</u>: Let $P \in \mathrm{Spec}(A)$. Consider the set:

$$\mathcal{H} = \{Q \in \mathrm{Spec}(A) \mid Q \subseteq P\}.$$

$\mathcal{H} \neq \emptyset$ and $\mathcal{H}$ is partially ordered by 'reverse' inclusion.

$$Q_1 \leq Q_2 \longleftrightarrow Q_2 \subseteq Q_1.$$

<u>Claim</u>: $\mathcal{H}$ is inductively ordered.

<u>Pf</u>: Let $\mathcal{K} \subseteq \mathcal{H}$ be a chain. The ideal $K = \bigcap_{Q \in \mathcal{K}} Q$ is a prime ideal of A. Therefore $K \in \mathcal{H}$ and K is an upper bound for $\mathcal{K}$. The statement follows with Zorn's Lemma.

(1.18) <u>Proposition</u>: Let A be a ring and $P_1, \ldots, P_n, I \subseteq A$ ideals with $P_1, \ldots, P_{n-2}$ prime ideals if $n > 2$. If $I \subseteq \bigcup_{i=1}^{n} P_i$

then there is an $1 \leq j \leq n$ such that $I \subseteq P_j$.

<u>Proof</u>: By induction on n. The case $n = 1$ is trivial.

$n-1 \Rightarrow n$: Obviously: $I \subseteq \bigcup_{i=1}^{n} P_i \iff I = \bigcup_{i=1}^{n} (P_i \cap I)$.

We want to show: There is an $1 \leq j \leq n$ so that $I \cap P_j \subseteq \bigcup_{\substack{i=1 \\ i \neq j}}^{n} P_i$. $(*)$.

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

In order to show $(*)$ assume $\forall\ 1 \leq j \leq n:\ I \cap P_j \nsubseteq \bigcup_{\substack{i=1 \\ i \neq j}}^{n} P_i$ and take

$$a_j \in (I \cap P_j) - \bigcup_{\substack{i=1 \\ i \neq j}}^{n} P_i . \quad \text{Put} \quad y = a_1 + \prod_{k=2}^{n} a_k \in I .$$

<u>Claim</u>: $y \notin P_i\ \forall\ 1 \leq i \leq n$.

<u>Pf</u>: $i=1$: $a_1 \in P_1$ and $a_2, \ldots, a_n \notin P_1 \implies y \notin P_1$. In particular, if $n=2$ then $y \notin P_1$ and $y \notin P_2$, a contradiction.

If $n > 2$, then $a_1 \notin P_i$ and $\prod_{k=2}^{n} a_k \in P_i\ \forall\ 2 \leq i \leq n$.

Thus $y \notin P_i\ \forall\ 2 \leq i \leq n$.

Since P_1 is prime $\prod_{k=2}^{n} a_k \notin P_1$ and also $y \notin P_1$, a contradiction.

(1.19) <u>Definition</u>: Let A be a ring. The ideal

$$\operatorname{Jrad}(A) = \bigcap_{m \subseteq A \text{ a max. ideal}} m$$

is called the <u>Jacobson radical</u> of A.

(1.20) <u>Proposition</u>: Let A be a ring and $a \in A$. Then

$$a \in \operatorname{Jrad}(A) \iff 1 - ab \in A^*\ \forall\ b \in A.$$

<u>Proof</u>: "$\Rightarrow$": If $1-ab \notin A^*$ for some $b \in A$ then there is a maximal ideal m with $1-ab \in m$. Since $a \in m$ we have $1 \in m$, a contradiction.

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

(1.21) <u>Remark</u>: Let $\varphi: A \longrightarrow B$ be a homomorphism of rings and $P \subseteq B$ a prime ideal. The contraction $\varphi^{-1}(P) \subseteq A$ is a prime ideal.

§2: NAKAYAMA'S LEMMA

(1.22) Proposition: Let A be a ring and M an A-module.

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

(b) Let F be a free A-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 A-linear map $\varphi : F \longrightarrow M$.

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

(b) For $x = \sum_{i \in I}' a_i b_i \in F$ with $a_i \in A$ and all but finitely many $a_i = 0$ define:

$$\varphi(x) = \sum_{i \in I} a_i \, \varphi_0(b_i).$$

φ is well defined and A-linear. Uniqueness is trivial.

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

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

(c) Every factor module of a finitely generated module is finitely generated.

(d) Let M be an A-module and $\mathcal{U} \subseteq M$ a submodule. If $\mathcal{U}$ and $M/\mathcal{U}$ are finitely generated then M is finitely generated.

Proof: (d) Let $m_1, \ldots, m_s \in M$ such that $\overline{m}_1, \ldots, \overline{m}_s \in M/\mathcal{U}$ is a system of generators of $M/\mathcal{U}$. Let $u_1, \ldots, u_t \in \mathcal{U}$ be a system of generators of $\mathcal{U}$. Then $m_1, \ldots, m_s, u_1, \ldots, u_t$ is a system of generators of M.

(1.24) Theorem: (Nakayama's Lemma) Let A be a ring and $I \subseteq A$ an ideal. The following are equivalent:

(a) $I \subseteq \mathrm{Jrad}(A)$

(b) For every finitely generated A-module M if $IM = M$ then $M = 0$.

Proof: (a) $\Rightarrow$ (b): Let M be a finitely generated A-module with $IM = M$. If $M \neq 0$ then there is a minimal integer $n \in \mathbb{N}$ such that M is generated by n elements, thus $M = Am_1 + \dots + Am_n$ where n minimal. Then

$$M = IM = \{ \sum_{i=1}^{n} b_i m_i \mid b_i \in I \} \quad \text{and}$$

$$m_n = \sum_{i=1}^{n} b_i m_i \quad \text{for some } b_i \in I.$$

$$\Rightarrow \quad (1-b_n) m_n = \sum_{i=1}^{n-1} b_i m_i$$

Since $b_n \in \mathrm{Jrad}(A)$, $1-b_n \in A^*$. Hence M is generated by $m_1, \dots, m_{n-1}$, a contradiction.

(b) $\Rightarrow$ (a): Suppose $I \nsubseteq \mathrm{Jrad}(A)$. Then there is a maximal ideal $m \subseteq A$ with $I \nsubseteq m$ and $m + I = A$. Let $M = A/m \neq 0$. Then $IM = (I+m)/m = A/m = M$.

(1.25) Corollary: Let M be an A-module and $N \subseteq M$ a submodule so that M/N is a finitely generated A-module. Let $I \subseteq \mathrm{Jrad}(A)$ be an ideal with $M = N + IM$. Then $M = N$.

Proof: $I(M/N) \cong (IM+N)/N = M/N$. By (1.24): $M/N = 0$.

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

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\mathrm{can}"'] & N \arrow[d, "\mathrm{can}"] \\ M/K \arrow[r, "\overline{\varphi}"] & N/L \end{tikzcd}$$

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

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

Proof: Since φ is surjective, $N = im(\varphi) + IN$. By (1.25): $N = im(\varphi)$.

§3: LOCALIZATION

Let A be a commutative ring with identity 1, $S \subseteq A$ a multiplicative set, and M an A-module (special emphasis on the case $M = A$). On the set $M \times S = \{(m,s) \mid m \in M \text{ and } s \in S\}$ consider the relation:

$$(m_1, s_1) \sim (m_2, s_2) \iff \exists\, t \in S : t(s_1 m_2 - s_2 m_1) = 0.$$

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

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

(1.29) Definition and Remark: For an A-module M define

$$NZD(M) = \{ t \in A \mid tm \neq 0 \text{ for all } m \in M - (0)\}.$$

An element $t \in NZD(M)$ is called a regular element or a non zero divisor on M. Accordingly, $ZD(M) = A - NZD(M)$ is the set of zero divisors or non regular elements on M.

If $S \subseteq NZD(M)$ is a multiplicative set 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 the element (m,s) is denoted by $\frac{m}{s}$ (or m/s). $S^{-1}M$ is called the localization of M by S.

(1.30) Proposition: (a) $S^{-1}A$ is a commutative ring with identity under the operations:

$\forall\, a_1, a_2 \in A;\ \forall\, s_1, s_2 \in S$: $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2 a_1 + s_1 a_2}{s_1 s_2}$ and $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$

(b) $S^{-1}M$ is an $S^{-1}A$-module under the operations:
$\forall\, m_1, m_2, m \in M;\ s_1, s_2, t, s \in S;\ a \in A$: $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$ and $\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$

Proof: We only show that the 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 $u_1, u_2 \in S$ so that:

$u_1(s_1 n_1 - t_1 m_1) = 0$ and $u_2(s_2 n_2 - t_2 m_2) = 0$.

$\Rightarrow$ $(u_1 s_1) n_1 = (u_1 t_1) m_1$ and $(u_2 s_2) n_2 = (u_2 t_2) m_2$

$\Rightarrow$ $(t_1 t_2 u_1 u_2)(s_2 m_1 + s_1 m_2) = (t_1 t_2 u_1 u_2 s_2) m_1 + (t_1 t_2 u_1 u_2 s_1) m_2$

$= (t_2 u_1 u_2 s_1 s_2) n_1 + (t_1 u_1 u_2 s_1 s_2) n_2$

$= (u_1 u_2 s_1 s_2)(t_2 n_1 + t_1 n_2)$

$\Rightarrow$ $(s_2 m_1 + s_1 m_2,\ s_1 s_2) \sim (t_2 n_1 + t_1 n_2,\ t_1 t_2)$.

Note that the zero element of $S^{-1}M$ is $\frac{0}{1}$, and the identity element of $S^{-1}A$ is $\frac{1}{1}$.

(1.31) Remark: (a) The map $i_{A,S} : A \longrightarrow S^{-1}A$ with $i_{A,S}(a) = \frac{a}{1}$ is a homomorphism of rings.

(b) $S^{-1}M$ is an A-module via $i_{A,S}$. The map $i_{M,S} : M \longrightarrow S^{-1}M$ with $i_{M,S}(m) = \frac{m}{1}$ is A-linear.

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

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

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

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

(1.32) Theorem: (Universal property of $S^{-1}A$) Let A be a ring, $S \subseteq A$ a multiplicative subset, and $\varphi : A \to B$ a homomorphism of rings with $\varphi(S) \subseteq B^*$.

Then there is a unique homomorphism of rings $\psi : S^{-1}A \longrightarrow B$ such that the diagram :

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "i_{A,S}"'] & B \\ S^{-1}A \arrow[ur, "\psi"'] & \end{tikzcd}$$

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

<u>Proof</u>: Define $\psi(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$.

(i) ψ is well defined

Suppose $\frac{a_1}{s_1} = \frac{a_2}{s_2} \Rightarrow \exists\, t \in S,\ ts_1a_2 = ts_2a_1 \Rightarrow \varphi(t)\varphi(s_1)\varphi(a_2) = \varphi(t)\varphi(s_2)\varphi(a_1)$

$\varphi(t), \varphi(s_1), \varphi(s_2) \in B^* \Rightarrow \varphi(a_2)\varphi(s_2)^{-1} = \varphi(a_1)\varphi(s_1)^{-1}$.

(ii) ψ is a homomorphism of rings

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

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

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

$\psi(\frac{1}{1}) = \varphi(1)\varphi(1)^{-1} = 1_B$.

(iii) $\psi \circ i_{A,S}(a) = \psi(\frac{a}{1}) = \varphi(a)\varphi(1)^{-1} = \varphi(a)$

(iv) Uniqueness

Let $\tau : S^{-1}A \longrightarrow B$ be a homomorphism with $\tau \circ i_{A,S} = \varphi$. Then

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

(1.33) <u>Remark</u>: (a) If $S \subseteq A^*$ then $i_{A,S}$ is an isomorphism.

(b) If A is a domain and $S = A - (0)$ then $S^{-1}A = Q(A)$ is called the <u>field of quotients</u> of A. Using (1.32) one can show that $Q(A)$ is the smallest field containing A (up to isomorphism).

(c) In general, $S^{-1}A$ is called the <u>localization of</u> A <u>at</u> S and $S^{-1}M$ is the <u>localization</u> of M at S. If $P \in \mathrm{Spec}(A)$ is a prime ideal we write $A_P = S^{-1}A$ where $S = A - P$. A_P is called the <u>localization</u> of A at P. Similarly, $M_P = S^{-1}M$ for $S = A - P$ is called the <u>localization</u> of M at P.

(1.34) <u>Proposition</u>: Let $\varphi : M \longrightarrow N$ be an A-linear map and $S \subseteq A$ a multiplicative subset. There is a unique $S^{-1}A$-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.

<u>Proof</u>: Define $S^{-1}\varphi$ by $S^{-1}\varphi\left(\frac{m}{s}\right) = \frac{\varphi(m)}{s}$. It is easy to see that $S^{-1}\varphi$ is well defined and $S^{-1}A$-linear.

(1.35) <u>Corollary</u>: (a) If $id_M : M \longrightarrow M$ is the identity on M, then $S^{-1}id_M : S^{-1}M \longrightarrow S^{-1}M$ is the identity on $S^{-1}M$: $S^{-1}id_M = id_{S^{-1}M}$.
(b) If $\varphi : M \longrightarrow N$ and $\psi : N \longrightarrow T$ are A-linear maps, then $S^{-1}(\psi \circ \varphi) = S^{-1}\psi \circ S^{-1}\varphi$.
Localization is a covariant functor from the category of A-modules into the category of $S^{-1}A$-modules.

A sequence of A-modules and A-linear maps:

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

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

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

is called a <u>short exact sequence</u> if (a) α is injective, (b) $\operatorname{im}(\alpha) = \ker(\beta)$, and (c) β is surjective.

(1.36) <u>Theorem</u>: (Localization is exact) Let A be a ring, $S \subseteq A$ a multiplicative subset and

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

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

Proof: We know: $S^{-1}\beta \circ S^{-1}\alpha = S^{-1}(\beta\circ\alpha) = S^{-1}0 = 0$. Therefore: $\mathrm{im}(S^{-1}\alpha) \subseteq \ker(S^{-1}\beta)$.
In order to show "$\supseteq$" let $\frac{m}{s} \in \ker(S^{-1}\beta) \Rightarrow S^{-1}\beta\left(\frac{m}{s}\right) = \frac{\beta(m)}{s} = 0$ in $S^{-1}M_3$.
$\Rightarrow \exists\, t \in S:\ t\beta(m) = 0$ in $M_3 \Rightarrow \beta(tm) = 0$ and $tm \in \ker(\beta) = \mathrm{im}(\alpha)$
$\Rightarrow \exists\, n \in M_1$ with $\alpha(n) = tm \Rightarrow S^{-1}\alpha\left(\frac{n}{st}\right) = \frac{\alpha(n)}{st} = \frac{tm}{st} = \frac{m}{s}$.

(1.37) 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 (1.36) to the exact sequence $0 \longrightarrow U \longrightarrow M \longrightarrow M/U \longrightarrow 0$.

Let A be a ring, $I \subseteq A$ an ideal, and $S \subseteq A$ a multiplicative subset. Considering A as an A-module and I as a submodule the embedding $\varepsilon: I \longrightarrow A$ (with $\varepsilon(a) = a$) is A-linear. By (1.34) ε induces an $S^{-1}A$-linear map: $S^{-1}\varepsilon: S^{-1}I \longrightarrow S^{-1}A$. By (1.36) $S^{-1}\varepsilon$ is injective and we consider $S^{-1}I = \{\frac{a}{s} \mid a \in I \text{ and } s \in S\}$ as a subset of $S^{-1}A$. $S^{-1}I$ is an ideal of $S^{-1}A$.

(1.38) Proposition: Let A be a ring, $I \subseteq A$ an ideal, $P \subseteq A$ a prime ideal, and $S \subseteq A$ a multiplicative subset.
(a) $S^{-1}I = S^{-1}A \Longleftrightarrow I \cap S = \emptyset$
(b) If $P \cap S = \emptyset$ then $S^{-1}P$ is a prime ideal of $S^{-1}A$ with $i_{A,S}^{-1}(S^{-1}P) = P$.
(c) If $J \subseteq S^{-1}A$ is an ideal then $K = i_{A,S}^{-1}(J)$ is an ideal of A with $S^{-1}K = J$.
(d) There is a 1-1 correspondence between the prime ideals of $S^{-1}A$ and the prime ideals P of A with $P \cap A = \emptyset$.

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

(b) $S^{-1}P$ is a prime ideal

Suppose $a_1, a_2 \in A$ and $s_1, s_2 \in S$ with $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2} \in S^{-1}P \Rightarrow \exists\, p \in P, s \in S$ with $\frac{a_1 a_2}{s_1 s_2} = \frac{p}{s} \Rightarrow \exists\, t \in S:\ t(s a_1 a_2 - s_1 s_2 p) = 0 \Rightarrow (ts) a_1 a_2 = t s_1 s_2 p \in P$. Since P is prime with $S \cap P = \emptyset$: $a_1 \in P$ or $a_2 \in P \Rightarrow \frac{a_1}{s_1} \in S^{-1}P$ or $\frac{a_2}{s_2} \in S^{-1}P$.

$i_{A,S}^{-1}(S^{-1}P) = P$: Obviously, $P \subseteq i_{A,S}^{-1}(S^{-1}P)$. Let $q \in i_{A,S}^{-1}(S^{-1}P)$. Then $i_{A,S}(q) = \frac{q}{1} = \frac{p}{s}$ for some $p \in P, s \in S \Rightarrow \exists\, t \in S:\ t(sq - 1p) = 0 \Rightarrow$ $tsq = tp \in P$. Since $P \cap S = \emptyset$ and P prime: $q \in P$.

(c) easy

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

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

defined by $\Phi(P) = S^{-1}P$ and $\Psi(Q) = i_{A,S}^{-1}(Q)$ are inverse to each other, i.e. $\Psi \circ \Phi = id_\Sigma$ and $\Phi \circ \Psi = id_\Lambda$.

<u>Note</u>: If $I \subseteq A$ is an ideal it in general <u>not</u> true that $i_{A,S}^{-1}(S^{-1}I) = I$. Example: $A = \mathbb{Z}$ and $I = (15)$, $S = A - (3)$. Then $S^{-1}(15) = S^{-1}(3)$ and $i_{\mathbb{Z},S}(S^{-1}(3)) = (3) \supsetneq (15)$.

(1.39) <u>Proposition</u>: (a) Let $\varphi: A \longrightarrow B$ be a homomorphism of rings and $S \subseteq A$ a multiplicative subset. Then $\varphi(S) \subseteq B$ is a multiplicative subset and φ induces a homomorphism of rings $\psi: S^{-1}A \longrightarrow \varphi(S)^{-1}B$ defined by $\psi(\frac{a}{s}) = \varphi(a)/\varphi(s)$.

(b) Let A be a ring, $I \subseteq A$ an ideal, $\nu: A \longrightarrow A/I$ the canonical map, and $S \subseteq A$ a multiplicative set. Then:

$$S^{-1}A/S^{-1}I \underset{\text{rg iso}}{\cong} (\nu(S))^{-1}(A/I) \underset{\text{mod iso}}{\cong} S^{-1}(A/I)$$

where $S^{-1}(A/I)$ denotes the localization of the A-module A/I by S.

<u>Proof</u>: (a) By (1.32) there is a homomorphism ψ (of rings) such that the diagram:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "i_{A,S}"'] & B \arrow[r, "i_{B,\varphi(S)}"] & \varphi(S)^{-1}B \\ S^{-1}A \arrow[urr, "\psi"'] & & \end{tikzcd}$$

commutes.

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

$$\begin{tikzcd} A \arrow[r, "\nu"] \arrow[d] & A/I \arrow[r] & \nu(S)^{-1}(A/I) \\ S^{-1}A \arrow[urr, "\psi"'] & & \end{tikzcd}$$

commutes.

Let $\nu(a)/\nu(s) \in \nu(S)^{-1}(A/I)$. Then $\psi(\frac{a}{1}) = \frac{\nu(a)}{1}$ and $\psi(\frac{s}{1}) = \frac{\nu(s)}{1}$ and therefore: $\psi(\frac{a}{s}) = \psi(\frac{a}{1}) \cdot \psi((\frac{s}{1})^{-1}) = \psi(\frac{a}{1})\psi(\frac{s}{1})^{-1} = \nu(a)/\nu(s)$. ψ is surjective.

Obviously, $S^{-1}I \subseteq \ker(\psi)$. Let $\psi(\frac{a}{s}) = \nu(a)/\nu(s) = 0 \Longrightarrow \exists\, t \in S$ such that $\nu(t)\nu(a) = \nu(at) = 0$ in $A/I \Longrightarrow at \in I$ and $\frac{a}{s} = at/st \in S^{-1}I$. ψ is an isomorphism of rings.

By (1.37) there is an isomorphism of $S^{-1}A$-modules: $S^{-1}(A/I) \cong S^{-1}A/S^{-1}I$.

(1.40) <u>Remark</u>: Let A be a ring. A has exactly one maximal ideal if and only if $A - A^*$ is an ideal of A.

<u>Proof</u>: Let $n \in A$ be a maximal ideal. If n is the only maximal ideal of A then $n = A - A^*$. Conversely, if $A - A^*$ is an ideal of A then $n \subseteq A - A^*$ and therefore $n = A - A^*$.

(1.41) <u>Definition</u>: A ring A is called a <u>(quasi)</u> <u>local</u> ring if A has exactly one maximal ideal. A is called a <u>semi</u>-<u>local</u> ring if A has only finitely many maximal ideals. (Some books call a ring A local if A has exactly one maximal ideal <u>and</u> if A is Noetherian.)

<u>Recall</u>: If $P \in \mathrm{Spec}(A)$ is a prime ideal then $A_P = S^{-1}A$ where $S = A - P$.

(1.42) <u>Proposition</u>: Let A be a ring and $P \in \mathrm{Spec}(A)$ a prime ideal. The ring A_P is local with maximal ideal PA_P.

<u>Proof</u>: By (1.38)(b) PA_P is a prime ideal of A_P and by (1.38)(d) PA_P is the only maximal ideal of A_P. Alternatively, one can show: $A_P^* = A_P - PA_P$.

(1.43) <u>Example</u>: Let $A = \mathbb{Z}$, $p \in \mathbb{Z}$ a prime number and $P = (p) \in \mathrm{Spec}(\mathbb{Z})$. Then

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

$\mathbb{Z}_{(p)}$ is a PID with exactly two prime ideals: $\mathrm{Spec}(\mathbb{Z}_{(p)}) = \{0, p\mathbb{Z}_{(p)}\}$. The ring $\mathbb{Z}_{(p)}$ is different from the ring $\mathbb{Z}_p$ which is defined as follows:

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

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

(1.44) <u>Proposition</u>: Let A be a ring and $P \subseteq A$ a minimal prime ideal. Then $P \subseteq ZD(A)$.

<u>Proof</u>: Let $P \subseteq A$ be a minimal prime ideal. By (1.38) the ring PA_P has exactly one prime ideal PA_P. By (1.14): $\mathrm{nil}(A_P) = PA_P$. Let $a \in P - (0) \Rightarrow$ $\frac{a}{1} \in \mathrm{nil}(A_P)$ and there is an $n \in \mathbb{N}$ with $(\frac{a}{1})^n = 0$. Let n be chosen minimal. Then there is a $t \in S = A - P$ so that $ta^n = 0$ and $ta^{n-1} \neq 0 \Rightarrow a \in ZD(A)$.

(1.45) <u>Definition</u>: A ring A is called <u>reduced</u> if $\mathrm{nil}(A) = (0)$.

(1.46) <u>Corollary</u>: Let A be a reduced ring, then $ZD(A) = \bigcup_{P \subseteq A \text{ min. prime}} P$

<u>Proof</u>: By (1.44): "$\supseteq$"

"$\subseteq$" Suppose $a \in ZD(A)$ and $a \notin \bigcup_{P \min} P$. Then there is a $b \in A - (0)$ with $ab = 0$. $ab \in P$ for all $P \in \mathrm{Spec}(A)$ $\Rightarrow$ $b \in P$ for all minimal prime ideals $P \subseteq A$ $\Rightarrow b \in \mathrm{nil}(A) \Rightarrow b = 0$, a contradiction.

(1.47) Remark: Let A be a ring and $S \subseteq A$ a multiplicative subset.

(a) If A is a PID, $S^{-1}A$ is a PID.

(b) If A is factorial, $S^{-1}A$ is factorial.

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

(1.48) Remark: Let A be a ring and $P \subseteq A$ a prime ideal. The residue class ring A_P/pA_p is isomorphic to the field of quotients $Q(A/p)$.

Proof: The canonical map $\nu : A \longrightarrow A/P$ maps $S = A-P$ into $A/p - (0)$. The statement follows with (1.39).

(1.49) Theorem: Let M be an A-module. The following are equivalent:

(a) $M = (0)$

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

Proof: (b) $\Rightarrow$ (a): Suppose $M \neq 0$. We want to show that there is at least one maximal ideal $m \subseteq A$ with $M_m \neq 0$. Let $n \in M-(0)$ and consider the submodule $N = An$ of M. Since $N_m \subseteq M_m$ for all maximal ideals m of A it suffices to show that $N_m \neq 0$ for some maximal ideal $m \subseteq A$. The map $\varphi : A \longrightarrow N$ defined by $\varphi(a) = an \ \forall a \in A$ is A-linear and surjective. Let $I = \ker(\varphi)$. Then $N \cong A/I$. Since $N \neq 0$, $I \neq A$ and there is a maximal ideal $m \subseteq A$ with $I \subseteq m$. Then $N_m \cong (A/I)_m \cong A_m/I_m$. Since $I \cap (A-m) = \emptyset$, $I_m \neq A_m$ and $N_m \neq 0$.

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

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

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

Proof: (a) $\Rightarrow$ (b): By (1.36) applied to $0 \rightarrow M \xrightarrow{\varphi} N$ or $M \xrightarrow{\varphi} N \longrightarrow 0$, respectively.

(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 (1.36) for all maximal ideals $m \subseteq A$ the sequences:

$$0 \rightarrow \ker(\varphi)_m \longrightarrow M_m \xrightarrow{\varphi_m} N_m \quad \text{and} \quad M_m \xrightarrow{\varphi_m} N_m \longrightarrow \operatorname{coker}(\varphi)_m \longrightarrow 0$$

are exact. In particular, $\ker(\varphi)_m = \ker(\varphi_m)$ and $\operatorname{coker}(\varphi)_m = \operatorname{coker}(\varphi_m)$.
φ_m is injective for all maximal ideals $m \subseteq A \Longleftrightarrow \ker(\varphi)_m = \ker(\varphi_m) = 0$ for all maximal ideals $m \subseteq A \Longleftrightarrow \ker(\varphi) = 0$ (by (1.49)) $\Longleftrightarrow \varphi$ is injective.
A similar argument applied to $\operatorname{coker}(\varphi)$ yields the surjective case.

(1.51) Corollary: Let M be an A-module, $\mathfrak{U} \subseteq M$ a submodule and $x \in M$. Then:
$x \in \mathfrak{U} \Longleftrightarrow i_{M,m}(x) \in \mathfrak{U}_m$ for all maximal ideals $m \subseteq A$.

Proof: Consider the A-linear map $\varphi: A \longrightarrow M/\mathfrak{U}$ defined by $\varphi(a) = ax + \mathfrak{U}$.
Obviously, $x \in \mathfrak{U} \Longleftrightarrow \varphi = 0 \Longleftrightarrow \operatorname{im}(\varphi) = 0$. Since $\operatorname{im}(\varphi)_m = \operatorname{im}(\varphi_m)$ for all maximal ideals $m \subseteq A$, the statement follows from (1.49).

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

$$A = \bigcap_{m \subseteq A \text{ max. id.}} A_m$$

Proof: $\mathfrak{U} = A$ and $M = \bigcap A_m$ are A-submodules of $Q(A)$ with $A = \mathfrak{U} \subseteq M$.
For all maximal ideals $m \subseteq A$: $M \subseteq A_m = \mathfrak{U}_m$. Therefore $M_m \subseteq (A_m)_m = A_m$ for all maximal ideals $m \subseteq A$. For all $x \in M$: $i_{M,m}(x) \in \mathfrak{U}_m$ and by (1.51) : $M = \mathfrak{U}$.