MA5204 Homework 1

Nguyen Ngoc Khanh - A0275047B

May 20, 2025

Problem 1 (chapter 1 problem 1)
Let x be a nilpotent element of a ring A. Show that $1+x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. Let $x \in \eta_R$, then $-x \in \eta_R$, that is $(-x)^n = 0$ for some $n > 0$. We have

$$1 = 1 - (-x)^n = (1+x)(1 + (-x) + (-x)^2 + ... + (-x)^{n-1})$$

Hence, $1+x$ is a unit. Now let $uv = 1$ for $u, v \in R$, we have

$$(u+x)(v+x) = uv + ux + xv + x^2 = 1 + (ux + xv + x^2)$$

Since η_R is an ideal, $ux + xv + x^2 \in \eta_R$, therefore, $1 + (ux + xv + x^2)$ is a unit. Let $w \in R$ be the inverse of $1 + (ux + xv + x^2)$, we have

$$(u+x)(v+x)w = 1$$

Hence, both $u+x$ and $v+x$ are units. □

Problem 2 (chapter 1 problem 2)
Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x with coefficients in A. Let $f = a_0 + a_1x + ... + a_nx^n \in A[x]$. Prove that

1. f is a unit in $A[x] \iff a_0$ is a unit in A and $a_1, ..., a_n$ are nilpotent.
2. f is nilpotent $\iff a_0, a_1, ..., a_n$ are nilpotent
3. f is a zero divisor $\iff$ there exists $a \neq 0$ in A such that $af = 0$
4. f is said to be primitive if $(a_0, a_1, ..., a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\iff f$ and g are primitive

Proof.

1. (f is a unit in $A[x] \iff a_0$ is a unit in A and $a_1, a_2, ..., a_n$ are nilpotent) The statement is true for degree zero polynomials. Suppose $n \geq 1$

   ($\implies$) Let the inverse of $f(x)$ be polynomial $g(x) = b_0 + b_1x + b_2x^2 + ...$ of degree m, that is $b_m \neq 0$ and $b_{m+1} = b_{m+2} = ... = 0$, then $f(x)g(x) = 1$ implies $a_0b_0 = 1$, hence a_0 is a unit. We will show that $a_n^{r+1}b_{m-r} = 0$ for all $r = 0, 1, ..., m$ by induction. The statement is true when $r = 0$ since $a_nb_m = 0$. When $0 < r \leq m$, assume that the statement is true for all $0, 1, ..., r-1$, that is

   $$\begin{aligned} a_nb_m &= 0 \\ a_n^2b_{m-1} &= 0 \\ &... \\ a_n^rb_{m-r+1} &= 0 \end{aligned}$$

   We want to show that $a_n^{r+1}b_{m-r} = 0$. The degree $n+m-r$ coefficient of $f(x)g(x)$ is zero, that is

   $$a_nb_{m-r} + a_{n-1}b_{m-r+1} + ... + a_0b_{m-r+n} = 0$$

Multiply both sides by a_n^r, we have

$$a_n^{r+1}b_{m-r} + a_{n-1}a_n^r b_{m-r+1} + ... + a_0 a_n^r b_{m-r+n} = 0$$

By the induction assumption, we induce that $a_n^{r+1}b_{m-r} = 0$ for all $r = 0, 1, ..., m$. Let $r = m$, then $a_n^{m+1}b_0 = 0$. Since b_0 is a unit, $a_n^{m+1} = 0$, that is, $a_n \in \eta_A$. Note that $a_n \in \eta_{A[x]}$ is also nilpotent in the ring $A[x]$. Therefore, $f(x) - a_n x^n$ is a sum of a unit and a nilpotent element which is a unit in $A[x]$. Hence, using the same proof, $a_{n-1} \in \eta_A$. Inductively, all $a_1, a_2, ..., a_n \in \eta_A$

($\Longleftarrow$) If a_0 is a unit and $a_1, ..., a_n \in \eta_A$, then a_0 is also a unit in $A[x]$ and $a_1 x, ..., a_n x^n \in \eta_{A[x]}$. Therefore, $f(x) = a_0 + a_1 x + ... + a_n x^n$ is a sum of a unit and a nilpotent element which is a unit in $A[x]$

2. (f is nilpotent $\iff$ $a_0, a_1, ..., a_n$ are nilpotent)

   ($\Longrightarrow$) If $f(x)$ is nilpotent, $1 + f(x) = (1 + a_0) + a_1 x + a_2 x^2 + ...$ is a unit. Then, $1 + a_0$ is a unit and $a_1, ..., a_n \in \eta_A$. Moreover, $f(x)^m = 0$ for some $m > 0$. That implies $a_0^m = 0$ for some $m > 0$. Hence, a_0 is also nilpotent.

   ($\Longleftarrow$) If $a_0, a_1, ..., a_n \in \eta_A$, then $a_0^m = a_1^m = ... = a_n^m = 0$ for some $m > 0$. $f(x)^{(n+1)m}$ is a sum of terms, where each term is a product of $(n+1)m$ elements from the set

$$\{a_0, a_1 x, ..., a_n x^n\}$$

   By pigeonhole principle, for every term, there is an element appearing at least m times. Hence, $f(x)^{(n+1)m}$ is a zero polynomial, that is, $f(x) \in \eta_{A[x]}$

3. (f is a zero divisor $\iff$ there exists $a \neq 0$ in A such that $af = 0$)

   ($\Longrightarrow$) Let $g(x) = b_0 + b_1 x + b_2 x^2 + ... \in A[x]$ such that $f(x)g(x) = 0$. The degree zero term of $f(x)g(x)$ is zero, that is, $a_0 b_0 = 0$, we will show that $a_r b_0^{r+1} = 0$ for all r by induction. Suppose the statement is true for all $0, 1, ..., r-1$, that is

$$a_0 b_0 = 0$$
$$a_1 b_0^2 = 0$$
$$...$$
$$a_{r-1} b_0^r = 0$$

   We want to show that $a_r b_0^{r+1} = 0$. The degree r coefficient of $f(x)g(x)$ is zero, that is

$$a_0 b_r + a_1 b_{r-1} + ... + a_r b_0 = 0$$

   Multiply both sides by b_0^r, we have

$$a_0 b_0^r b_r + a_1 b_0^r b_{r-1} + ... + a_r b_0^{r+1} = 0$$

   By the induction assumption, we induce that $a_r b_0^{r+1} = 0$ for all r. Then, $f(x) b_0^{n+1} = 0$

   ($\Longleftarrow$) by the premise

4. (if $f, g \in A[x]$, then fg is primitive $\iff$ f and g are primitive)

($\Longrightarrow$) Let $g(x) = b_0 + b_1x + ... + b_mx^m$. If $f(x)g(x)$ is primitive, then

$$1 = c_0(a_0b_0) + c_1(a_0b_1 + a_1b_0) + c_2(a_0b_2 + a_1b_1 + a_2b_0) + ... + c_{n+m}(a_nb_m)$$

for some $c_0, c_1, ..., c_{n+m} \in A$. Hence, 1 can be written as a linear combination of the finite set $\{a_0, a_1, ..., a_n\}$ with coefficients in A, that is $f(x)$ is primitive. Similarly, $g(x)$ is also primitive.

($\Longleftarrow$) Suppose $f(x)g(x)$ is not primitive, let the maximal ideal containing the ideal generated by coefficients of $f(x)g(x)$ be $\mathfrak{m}$. Then, in $(A/\mathfrak{m})[x]$, $0 = \overline{f(x)g(x)} = \overline{f(x)}\ \overline{g(x)}$. Since $\mathfrak{m}$ is maximal that is prime, $A/\mathfrak{m}$ is a domain, then $(A/\mathfrak{m})[x]$ is a domain. On the other hand, $f(x)$ is primitive, then the coefficients of $f(x)$ generate the whole ring A, therefore, there exists an $a_i \notin \mathfrak{m}$, if not $A = (a_0, a_1, ..., a_n) \subseteq \mathfrak{m}$. Hence, $\overline{f(x)} \neq 0$ in $(A/\mathfrak{m})[x]$. Similarly, $\overline{g(x)} \neq 0$ in $(A/\mathfrak{m})[x]$. This contradicts with $(A/\mathfrak{m})[x]$ being a domain.

□

Problem 3 (chapter 1 problem 8)
Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with respect to inclusion.

Proof. The collection of prime ideals of A is a partially ordered set with respect to inclusion. Moreover, given any chain of prime ideals $\{\mathfrak{p}_i : i \in I\}$ under inclusion, the intersection $\mathfrak{p} = \bigcap_{i \in I} \mathfrak{p}_i$ is a prime ideal and a lowerbound (note that, this is only true for arbitrary collection of prime ideals. (2) and (3) are prime in $\mathbb{Z}$ but $(6) = (2) \cap (3)$ is not prime). Suppose, $xy \in \mathfrak{p}$ but $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$. Let $x \notin \mathfrak{p}_x$ and $y \notin \mathfrak{p}_y$. Since the collection is a chain, without loss of generality, assume $\mathfrak{p}_x \subseteq \mathfrak{p}_y$. Therefore, both $x, y \notin \mathfrak{p}_x$ but $xy \in \mathfrak{p} \subseteq \mathfrak{p}_x$. Contradiction. Thus, $\mathfrak{p}$ is prime. By Zorn lemma, there is a minimal prime ideal. □

Problem 4 (chapter 1 problem 10)
Let A be a ring, η_A is its nilradical. Show that the following are equivalent:

1. A has exactly one prime ideal
2. every element of A is either a unit or nilpotent.
3. A/η_A is a field

Proof.
$(1 \implies 2)$ If A has exactly one prime ideal, namely η_A the intersection of all prime ideals. Since any maximal ideal is prime, η_A is the unique maximal ideal in A. Therefore, any element $x \in A$, if $x \in \eta_A$ then x is nilpotent, if $x \notin \eta_A$ and x is a not unit then x is contained in a maximal ideal other than η_A. Contradiction.
$(2 \implies 3)$ If $\bar{x} \in A/\eta_A$ is non-zero for some $x \in A$, then $x \notin \eta_A$, thus x is a unit, hence $\bar{x}$ is a unit. Therefore, A/η_A is a field.
$(3 \implies 1)$ A/η_A is a field, then η_A is maximal. Since η_A is the intersection of all prime ideals, but it is maximal, it can not be a proper subset of any ideal. Hence, η_A is the unique prime ideal of A □

Problem 5 (chapter 1 problem 12)
A local ring contains no idempotent $\neq 0, 1$

Proof. Let A be a local ring with $\mathfrak{m}$ be its unique maximal ideal. Suppose $a \neq 0, 1$ such that $a^2 = a$, then $a(a-1) = a^2 - a = 0$, that is, a and $a-1$ are zero divisors. Since a and $a-1$ are not a unit, $a, a-1 \in \mathfrak{m}$ but $1 = a - (a-1) \notin \mathfrak{m}$ which is a contradiction. $\square$

Problem 6 (chapter 1 problem 15 - Zariski topology)
Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E. Prove that

1. if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$
2. $V(0) = X, V(1) = \varnothing$
3. if $(E_i)_{i \in I}$ is any family of subsets of A, then
$$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i)$$
4. $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A

Proof.

1. (if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$)

   Since $E \subseteq \mathfrak{a}$, $V(E) \supseteq V(\mathfrak{a})$. By definition of ideal generated by set, $\mathfrak{a}$ is the smallest ideal containing E, therefore any prime ideal containing E must contain $\mathfrak{a}$, hence $V(E) \subseteq V(\mathfrak{a})$.

   Since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, $V(\mathfrak{a}) \supseteq V(\sqrt{\mathfrak{a}})$. We want to show the other direction $V(\mathfrak{a}) \subseteq V(\sqrt{\mathfrak{a}})$, that is any prime ideal containing $\mathfrak{a}$ must contain $\sqrt{\mathfrak{a}}$. Let $\mathfrak{b} \supseteq \mathfrak{a}$ be a prime ideal, for any element, $x \in \sqrt{\mathfrak{a}}$, $x^n \in \mathfrak{a} \subseteq \mathfrak{b}$ for some $n > 0$.Then, $xx^{n-1} \in \mathfrak{b}$ therefore, either $x \in \mathfrak{b}$ or $x^{n-1} \in \mathfrak{b}$. The induction argument on n implies $x \in \mathfrak{b}$. Hence, $\mathfrak{b} \supseteq \sqrt{\mathfrak{a}}$

2. ($V(0) = X, V(1) = \varnothing$)

   Every prime ideal contains 0, hence $V(0) = X$. Every prime ideal is proper, hence it cannot contain 1, then $V(1) = \varnothing$

3. ($V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i)$)

   Let $\mathfrak{a}$ be an ideal. Then,

   $\mathfrak{a} \in V\left(\bigcup_{i \in I} E_i\right) \iff \mathfrak{a} \supseteq E_i$ for all $i \in I \iff \mathfrak{a} \in V(E_i)$ for all $i \in I \iff \mathfrak{a} \in \bigcap_{i \in I} V(E_i)$

4. ($V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A)

   Note that, if $E, F \subseteq A$, then $E \subseteq F \implies V(E) \supseteq V(F)$. Since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$, then
   $$V(\mathfrak{a}\mathfrak{b}) \supseteq V(\mathfrak{a} \cap \mathfrak{b}) \supseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$$

   We will show that $V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$. Suppose $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$ but $\mathfrak{p} \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$. $\mathfrak{p} \notin V(\mathfrak{a})$ implies there exists $a \in \mathfrak{a}$ such that $a \notin \mathfrak{p}$. $\mathfrak{p} \notin V(\mathfrak{b})$ implies there exists $b \in \mathfrak{b}$ such that $b \notin \mathfrak{p}$. But $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. This is a contradiction since $\mathfrak{p}$ is prime.

$\square$

Problem 7 (chapter 1 problem 17 - a basis for Zariski topology)
For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \operatorname{Spec} A$. The set X_f are open. Show that they form a basis of open sets for the Zariski topology, and that

1. $X_f \cap X_g = X_{fg}$
2. $X_f = \varnothing \iff f$ is nilpotent
3. $X_f = X \iff f$ is a unit
4. $X_f = X_g \iff \sqrt{(f)} = \sqrt{(g)}$
5. X is quasi-compact
6. each X_f is quasi-compact
7. an open subset of X is quasi-compact if and only if it is a finite union of set X_f

Proof.
(X_f form a basis for Zariski topology) Given any ideal I, the open set $X - V(I)$ can be written as a union of X_f

$$X - V(I) = X - \bigcap_{f \in I} V(f) = \bigcup_{f \in I} (X - V(f)) = \bigcup_{f \in I} X_f$$

1. ($X_f \cap X_g = X_{fg}$)

$$\begin{aligned} X_f \cap X_g &= (X - V(f)) \cap (X - V(g)) \\ &= X - (V(f) \cup V(g)) \\ &= X - (V((f)) \cup V((g))) \\ &= X - V((fg)) \\ &= X - V(fg) \\ &= X_{fg} \end{aligned}$$

2. ($X_f = \varnothing \iff f$ is nilpotent)

$$X_f = \varnothing \iff V(f) = X \iff f \in \mathfrak{p} \text{ for every prime ideal } \mathfrak{p} \iff f \in \eta_A$$

3. ($X_f = X \iff f$ is a unit)

$$X_f = X \iff V(f) = \varnothing \iff f \notin \mathfrak{m} \text{ for every maximal ideal } \mathfrak{m} \iff f \text{ is a unit}$$

   The last $\iff$ is true because f is a unit implies f is not in any maximal ideal and f is not a unit implies f is contained in some maximal ideal.

4. ($X_f = X_g \iff \sqrt{(f)} = \sqrt{(g)}$)

$$X_f = X_g \iff V(f) = V(g) \iff V((f)) = V((g))$$

By definition, $\sqrt{(f)} = \bigcap_{\mathfrak{p}\in V((f))} \mathfrak{p}$ and $\sqrt{(g)} = \bigcap_{\mathfrak{p}\in V((g))} \mathfrak{p}$, then

$$V((f)) = V((g)) \implies \sqrt{(f)} = \sqrt{(g)}$$

On the other hand,

$$\sqrt{(f)} = \sqrt{(g)} \implies V(\sqrt{(f)}) = V(\sqrt{(g)}) \implies V((f)) = V((g))$$

5. (X is quasi-compact)

   It is sufficient to prove that given any open cover by basic open sets $\{X_{f_i}\}_{i\in I}$, then there exists a finite subcover $\{X_{f_j}\}_{j\in J}$ for finite subset $J \subseteq I$. We have

   $$\bigcup_{i\in I} X_{f_i} = \bigcup_{i\in I}(X - V(f_i)) = X - \bigcap_{i\in I} V(f_i)$$

   That is, $\bigcup_{i\in I} X_{f_i} = X \iff \bigcap_{i\in I} V(f_i) = \varnothing$. Moreover,

   $$\bigcap_{i\in I} V(f_i) = \varnothing \iff \text{there is no prime ideal containing } \{f_i\}_{i\in I} \iff (f_i)_{i\in I} = A$$

   where $(f_i)_{i\in I}$ denotes the ideal generated by $\{f_i\}_{i\in I}$. The second $\iff$ is due to every prime ideal is contained is a maximal ideal. Then, $(f_i)_{i\in I} = A$ implies

   $$1 = \sum_{j\in J} a_j f_j$$

   for some finite subset $J \subseteq I$. Hence, $(f_j)_{j\in J} = A$. That implies $\bigcup_{j\in J} X_{f_j} = X$ by the same argument for index set J

6. (each X_f is quasi-compact)

   Let $\{X_{f_i}\}_{i\in I}$ be an open cover for X_f by basic open sets. We have

   $$X_f \subseteq \bigcup_{i\in I} X_{f_i} \iff V(f) \supseteq \bigcap_{i\in I} V(f_i) = V((f_i)_{i\in I})$$

   If $\bigcap_{i\in I} V(f_i) = \varnothing$, this falls back to the previous case. Suppose $V((f_i)_{i\in I}) = \bigcap_{i\in I} V(f_i) \neq \varnothing$, we have

   $$\mathfrak{p} \in V((f_i)_{i\in I}) \implies \mathfrak{p} \in V(f) \implies f \in \mathfrak{p}$$

   Therefore

   $$f \in \sqrt{(f_i)_{i\in I}} = \bigcap_{\mathfrak{p}\in V((f_i)_{i\in I})} \mathfrak{p}$$

   That is, $f^n \in (f_i)_{i\in I}$ for some $n > 0$, then

   $$f^n = \sum_{j\in J} a_j f_j$$

   for some finite subset $J \subseteq I$. As $f^n \in (f_j)_{j\in J}$, then $V(f^n) \supseteq V((f_j)_{j\in J})$, we have

   $$\mathfrak{p} \in V((f_j)_{j\in J}) \implies \mathfrak{p} \in V(f^n) \implies f^n \in \mathfrak{p}$$

Since $\mathfrak{p}$ is prime, $f^n \in \mathfrak{p} \implies f \in \mathfrak{p}$. Therefore,

$$\mathfrak{p} \in V((f_j)_{j\in J}) \implies \mathfrak{p} \in V(f^n) \implies f^n \in \mathfrak{p} \implies f \in \mathfrak{p} \implies \mathfrak{p} \in V(f)$$

Thus, $V(f) \supseteq V((f_j)_{j\in J})$, that is, X_f is covered by a finite subcollection

$$X_f \subseteq \bigcup_{j\in J} X_{f_j}$$

7. (an open subset of X is quasi-compact if and only if it is a finite union of set X_f)

   ($\impliedby$) finite union of quasi-compact sets is quasi-compact since we can pick a finite subcollection for each set, the total is still a finite subcollection.

   ($\implies$) if U is an open set in X, then U can be written as $U = \bigcup_{i\in I} X_{f_i}$ since $\{X_f\}$ form a basis for X. By compactness of U, U can be cover by a finite union $U \subseteq \bigcup_{j\in J} X_{f_j} \subseteq \bigcup_{i\in I} X_{f_i} = U$. Hence, $U = \bigcup_{j\in J} X_{f_j}$

$\square$

Problem 8 (chapter 2 problem 9)
Let $0 \longrightarrow A \xhookrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$ be an exact sequence of R-modules. If A and C are finitely generated, then so is B

Proof. If $b \in \ker p = \operatorname{im} i$, since i is injective, we can write $i^{-1}(b) = r_1a_1 + r_2a_2 + ... + r_na_n$ where $\{a_1, a_2, ..., a_n\}$ generates A and $r_1, r_2, ..., r_n \in R$. Therefore,

$$b = r_1i(a_1) + r_2i(a_2) + ... + r_ni(a_n)$$

That is, $\{i(a_1), i(a_2), ..., i(a_n)\}$ generates $\ker p$. Let $\{c_1, c_2, ..., c_m\}$ generates C. Since p is surjective, pick $\{b_1, b_2, ..., b_m\} \subseteq B$ so that $p(b_i) = c_i$ for all $i = 1, 2, ..., m$. Now, if $b \in B - \ker p$, we can write

$$p(b) = s_1c_1 + s_2c_2 + ... + s_mc_m$$

for some $s_1, s_2, ..., s_m \in R$. Let

$$b' = s_1b_1 + s_2b_2 + ... + s_mb_m$$

Then, $p(b - b') = 0$, that is, $b - b' \in \ker p$, hence $b - b'$ can be written as a linear combination of $\{i(a_1), i(a_2), ..., i(a_n)\}$. Thus, the set $\{i(a_1), i(a_2), ..., i(a_n)\} \cup \{b_1, b_2, ..., b_m\}$ generates B $\square$

Problem 9 (chapter 2 problem 10)
Let A be a ring and $\mathfrak{a}$ be an ideal contained in the Jacobson radical of A. Let M be an A-module and N be finitely generated A-module, let $u : M \to N$ be a homomorphism. If the induced homomorphism $M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, then u is surjective

Proof. We will show that $N = \mathfrak{a}N + \operatorname{im} u$ so that Nakayama lemma version 2 implies $N = \operatorname{im} u$. Let $\{y_1, y_2, ..., y_n\}$ generates N, then $\{y_1 + \mathfrak{a}N, y_2 + \mathfrak{a}N, ..., y_n + \mathfrak{a}N\}$ generates $N/\mathfrak{a}N$. For each $i = 1, 2, ..., n$, since $u^* : M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, there is $x_i \in M$ such that

$$u^*(x_i + \mathfrak{a}M) = y_i + \mathfrak{a}N$$

That is, $z_i = u(x_i) - y_i \in \mathfrak{a}N$. Now, for each $y \in N$, we have

$$y = \sum_{i=1}^{n} a_i y_i = \sum_{i=1}^{n} a_i(u(x_i) - z_i)$$

for some $a_1, a_2, ..., a_n \in A$. $\mathfrak{a}N + \operatorname{im} u$ being a submodule of N and $u(x_i) - z_i \in \mathfrak{a}N + \operatorname{im} u$ implies $a_i(u(x_i) - y_i) \in \mathfrak{a}N + \operatorname{im} u$. Hence, $y \in \mathfrak{a}N + \operatorname{im} u$. Thus, $N \subseteq \mathfrak{a}N + \operatorname{im} u \subseteq N$, hence $N = \mathfrak{a}N + \operatorname{im} u$ □

Problem 10 (chapter 2 problem 12)
Let M be a finitely generated A-module and $\phi : M \to A^n$ a surjective homomorphism. Show that $\ker\phi$ is finitely generated.

Proof. Since $\phi : M \to A^n$ is surjective, the first row is exact

$$\begin{tikzcd}
0 \arrow[r] & \ker\phi \arrow[r, hook] & M \arrow[r, two heads, "\phi"] & A^n \arrow[r] & 0 \\
 & & & A^n \arrow[u, "1_{A^n}"'] \arrow[ul, dashed, "\psi"] &
\end{tikzcd}$$

A^n is projective since it is free, hence the map $1_{A^n} : A^n \to A^n$ factors through the surjective map $M \to A^n$ by a map $\psi : A^n \to M$. In particular, let $e_1, e_2, ..., e_n$ be the canonical basis for A^n, for each e_i pick $u_i \in M$ such that $\phi(u_i) = e_i$. Define the map $\psi : A^n \to M$ by

$$\psi : A^n \to M$$
$$e_i \mapsto u_i$$

so that $\phi\psi = 1_{A^n}$. Thus, the sequence splits, by Five lemma, there is an isomorphism $f : M \to \ker\phi \oplus A^n$. Both M and A^n being finitely generated, so is $\ker\phi$.
Indeed, if $f : M \to N \oplus P$ is an isomorphism with M and N being finitely generated. Let $\{x_1, x_2, ..., x_m\}$ generate M and $\{y_1, y_2, ..., y_n\}$ generate N. For each $i = 1, 2, ..., m$, then

$$f(x_i) = \left(\sum_{j=1}^{n} a_j y_j, p_i \right)$$

for some $a_1, a_2, ..., a_n \in A$ and $p_i \in P$. Let $p \in P$, then there are some $b_1, b_2, ..., b_m \in A$ such that

$$f\left(\sum_{i=1}^{m} b_i x_i \right) = (0, p)$$

Then,

$$(0, p) = f\left(\sum_{i=1}^{m} b_i x_i \right) = \sum_{i=1}^{m} b_i f(x_i) = \sum_{i=1}^{m} b_i \left(\sum_{j=1}^{n} a_j y_j, p_j \right) = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} b_i a_j y_j, \sum_{i=1}^{m} b_i p_i \right)$$

Thus, $\{p_1, p_2, ..., p_m\}$ generates P. □

Problem 11 (chapter 3 problem 5)
Let A be a ring. Suppose that for each prime ideal $\mathfrak{p}$, the local ring $A_\mathfrak{p}$ has no nilpotent element $\neq 0$. Show that A has no nilpotent element $\neq 0$. If each $A_\mathfrak{p}$ is an integral domain, is A necessarily an integral domain?

Proof.

(A has no nilpotent element $\neq 0$) Suppose $x \in A$ such that $x \neq 0$ and $x^n = 0$ for some $n > 0$. The ideal $(\{a \in A : ax = 0\})$ is proper since if $r_1a_1 + r_2a_2 + ... + r_ma_m = 1$, then $0 = r_1a_1x + r_2a_2x + ... + r_ma_mx = x$. Let $\mathfrak{p}$ be the maximal ideal of A containing $(\{a \in A : ax = 0\})$. For any $s \in A - \mathfrak{p}$, $\frac{x}{s}$ is nilpotent in $A_\mathfrak{p}$ since

$$\left(\frac{x}{s}\right)^n = \frac{x^n}{s^n} = \frac{0}{s^n} = \frac{0}{1} = 0$$

Moreover, $\frac{x}{s} \neq 0$ in $A_\mathfrak{p}$ since if $\frac{x}{s} = 0$ in $A_\mathfrak{p}$, then there exists $t \in A - \mathfrak{p}$ so that $tx = 0$, by construction of $\mathfrak{p}$, this is a contradiction.

(If each $A_\mathfrak{p}$ is an integral domain, is A necessarily an integral domain?) Let $A = \mathbb{Z}_6$, $\mathbb{Z}_6$ is not a domain since $2 \times 3 = 0 \mod 6$. The prime ideals of $\mathbb{Z}_6$ are $\{(2), (3)\}$, we have

$$S_2 = \mathbb{Z}_6 - (2) = \{1, 3, 5\}$$
$$S_3 = \mathbb{Z}_6 - (3) = \{1, 2, 4, 5\}$$

The zeros in $S_2^{-1}A$ are a/s where $s \in S_2$ and $a \in \mathbb{Z}_6$ such that $ta = 0 \mod 6$ for $t \in S_2$, that is

$$\left\{\frac{0}{s}, \frac{2}{s}, \frac{4}{s} : s \in S\right\}$$

The zeros in $S_3^{-1}A$ are a/s where $s \in S_3$ and $a \in \mathbb{Z}_6$ such that $ta = 0 \mod 6$ for $t \in S_3$, that is

$$\left\{\frac{0}{s}, \frac{3}{s} : s \in S\right\}$$

In $S_2^{-1}A$, if $\frac{a}{s}\frac{b}{r} = \frac{ab}{sr} = 0$, then $ab \in \{0, 2, 4\}$. Hence one of a or b must be in $\{0, 2, 4\}$. In In $S_3^{-1}A$, if $\frac{a}{s}\frac{b}{r} = \frac{ab}{sr} = 0$, then $ab \in \{0, 3\}$. Hence one of a or b must be in $\{0, 3\}$. Thus, both $S_2^{-1}A$ and $S_3^{-1}A$ are domain but A is not. □

Problem 12 (chapter 3 problem 6)
Let A be a ring $\neq 0$ and let Σ be the set of all multiplicatively closed subsets S of A such that $0 \notin S$. Show that Σ has maximal elements and that $S \in \Sigma$ is maximal if and only if $A - S$ is a minimal ideal of A.

Proof. As Σ forms a partially ordered set under inclusion and union of arbitrary number of sets in Σ is also in Σ. By Zorn lemma, Σ has a maximal element. Let $S \in \Sigma$, there is a minimal prime ideal $\mathfrak{p}_S$ in the ring $S^{-1}R$, let $\mathfrak{p}$ be the extension of $\mathfrak{p}_S$ in R so that $\mathfrak{p} \cap S = \varnothing$. Since $\mathfrak{p}$ is prime, $A - \mathfrak{p}$ is a multiplicatively closed that that contains S.

($S \in \Sigma$ is maximal $\implies$ $A - S$ is a minimal prime ideal of A)

By maximality of S, $S = A - \mathfrak{p}$. Suppose there is a prime ideal $\mathfrak{q}$ contained properly in $\mathfrak{p}$, the contraction $\mathfrak{q}^c$ of $\mathfrak{q}$ is contained (not necessarily proper) in the contraction $\mathfrak{p}^c = \mathfrak{p}_S$ of $\mathfrak{p}$. As $\phi_S : \operatorname{Spec} S^{-1}R \to \operatorname{Spec} R$ is injective, the containment is proper, $\mathfrak{q}^c \subsetneq \mathfrak{p}_S$, this contradicts the minimality of $\mathfrak{p}_S$. Hence, $\mathfrak{p} = A - S$ is minimal in A

($S \in \Sigma$ is maximal $\impliedby$ $A - S$ is a minimal prime ideal of A)

S is contained in a maximal multiplicatively closed set S_1 in Σ. Then, $A - S_1$ is a minimal prime ideal of A. Suppose S is a proper subset of S_1, then the minimal prime ideal $A - S$ contains properly a smaller prime ideal $A - S_1$, that is a contradiction. □