Lecture Notes in Commutative Algebra

Ashish Kujur

Last Updated: August 23, 2022

Introduction

This is a set of lecture notes which I took for reviewing stuff that I typed after taking class from *Dr. Viji Z Thomas*. All the typos and errors are of mine.

Contents

§1 Lecture 1 — 10th August 2022 — Local Rings, Semilocal rings, Chinese Remainder Theorem

We will be assuming the following things before proceeding in the course:

- A ring A is a commutative ring with unity.

- Existence of maximal ideals in a commutative ring with unity (this follows immediately from Zorn's Lemma)
- Definition of ring morphism.
- Definition of prime and maximal ideals and the facts that
  - P is a prime ideal of A iff A/P is an integral domain and
  - M is a maximal ideal of A iff A/P is a field

§1.1 Basic Definitions — Local Rings, Semilocal rings and few other results

Definition §1.1.1 (local ring)**.** Let A be a ring. A is said to be a *local ring* if A has a unique maximal ideal M. A local ring is often denoted by (A, M).

Definition §1.1.2 (semilocal ring)**.** Let A be a ring. A is said to be *semilocal ring* if A has only fintiely many maximal ideals.

How does one come up with a semilocal ring with exactly m maximal ideals? Here's an example:

Example §1.1.3 (A ring with m distinct maximal ideals)**.** Let $A = \mathbb{Z}/n\mathbb{Z}$. It is fairly easy to show that all the ideals of A are of the form $\left(\overline{k}\right)$ where $k \in \mathbb{N}$ and $k \mid n$ and also that if $k, j \mid n$ and $\left(\overline{k}\right) \subset \left(\overline{j}\right)$ iff $j \mid k$. (See Sepanski Exercise 3.47 and 3.48) Now let $p_1, p_2, \ldots, p_m$ be m distinct primes. Define $n = p_1 p_2 \cdots p_m$. It is easy to see from the aforementioned facts that $A = \mathbb{Z}/n\mathbb{Z}$ has m distinct maximal ideals.

Example §1.1.4 (A standard example of a local ring?)**.** Let A be a ring, M be a maximal ideal of A and $n \in \mathbb{N}$. Observe that M^n is a ideal of A (See Sepanski Exercise 3.51). We claim that A/M^n has only prime ideal namely M/M^n. Let $\mathcal{P}$ be a prime ideal of A/M^n. Then by the correspondence theorem, $\mathcal{P} = P/M^n$ where P is a prime ideal of A containing M^n. Then $P \supset M^n$ which further implies that $P \supset M$ (due to Lemma §1.1.7. Since M is a maximal ideal, we have that $P = M$. This completes the proof of the claim. Also, note that since every maximal ideal is prime, we have that A/M^n is a local ring.

Fact §1.1.5. *Let A be ring, B be an integral domain, $f : A \to B$ be a ring morphism and Q be a prime ideal of B. Then $\ker(f)$ is a prime ideal of A.*

Proof of the fact. Suppose that $ab \in \ker(f)$. Then $f(ab) = 0$ which further implies $f(a)f(b) = 0$ and hence $a \in \ker(f)$ or $b \in \ker(f)$ since B is an integral domain. □

Lemma §1.1.6. *Let A, B be rings, $f : A \to B$ be a ring morphism and Q be a prime ideal in B. Then $f^{-1}(Q)$ is a prime ideal of A.*

Proof. Let $p : B \to B/Q$ be the canonical homomorphism. Consider the map $p \circ f : A \to B/Q$. We show that $\ker(p \circ f) = f^{-1}(Q)$. The lemma will follows from fact §1.1.5, if we show that $\ker(p \circ f) = f^{-1}(Q)$ as B/Q is an integral domain. So consider the following:

$$\begin{aligned} x \in \ker(p \circ f) &\Leftrightarrow p(f(x)) = Q \\ &\Leftrightarrow f(x) + Q = Q \\ &\Leftrightarrow f(x) \in Q \\ &\Leftrightarrow x \in f^{-1}(Q) \end{aligned}$$

□

Lemma §1.1.7. *Let A be a ring, let I, J be ideals of A and P be a prime ideal of A. If $P \supset IJ$ then either $P \supset I$ or $P \supset J$.*

Proof. Suppose that $P \not\supset I$. Then there is some $i \in I \setminus P$. We show that $J \subset P$. Let $j \in P$. Then $ij \in IJ$ and hence $ij \in P$. Since P is a prime ideal, we must have that either $i \in P$ or $j \in P$. But the former is not possible by assumption, therefore, $j \in P$. Since j was arbitrary, the proof is complete. □

Remark §1.1.8. Let A be a ring, I be any ideal of A. Then there is a maximal ideal M of A containing A. The proof of this remark is fairly straightforward. Consider the ring A/I. Since every ring has a maximal ideal, so there must be some maximal ideal $\mathcal{M}$ of A/I. By the correspondence theorem, $\mathcal{M} = M/I$ for some ideal M of A. This ideal M of A must be maximal again by the correspondence theorem and this completes the proof of the remark.

Lemma §1.1.9. *Let A be a ring, I, J, K be ideals of A. Furthermore, assume that I, J are comaximal and I, K are comaximal. Then $I + JK = A$. (Recall that two ideals I, J are said to be comaximal if $I + J = A$.)*

Proof. Suppose that $I + JK \subsetneq A$. Then by Remark §1.1.8, we have that there is some maximal (and hence prime) ideal P containing $I + JK$. Thus, we have that $I \subset P$ and $JK \subset P$.

From $JK \subset P$, we can conclude that $J \subset P$ or $K \subset P$ from Lemma §1.1.7. But in the either case, we have that $I + J \subset P \subsetneq A$. A contradiction and hence $I + JK = A$. □

Example §1.1.10. Let $A = \mathbb{Z}$. Note that the ideal $(3, 4)$ generated by 3 and 4 and the ideal $(3, 5)$ generated by 3 and 5 are exactly $\mathbb{Z}$. Thus, the ideal $(3, 20) = A$ by Lemma §1.1.9.

§1.2 Chinese Remainder Theorem

Theorem §1.2.1 (Chinese Remainder Theorem)**.** *Let A be a ring, $I_1, I_2, \ldots, I_n$ be ideals of A. Consider the canonical map $\varphi : A \to A/I_1 \times A/I_2 \times \cdots A/I_n$ given by $\varphi(x) = (x + I_1, \ldots, x + I_n)$. Then the following holds:*

1. *If I_p, I_q are comaximal for all $1 \le p < q \le n$ then $I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \ldots \cap I_n$*
2. *φ is injective iff $\ker \varphi = I_1 \cap I_2 \cap \ldots \cap I_n = \{0\}$*

3. If φ is surjective iff I_m, I_n are comaximal for all $1 \leq m < n \leq n$

Proof of (1). We proceed by induction on n. Suppose that $n = 2$. Consider the ideals I_1, I_2 satisfying $I_1 + I_2 = A$. We show that $I_1 I_2 = I_1 \cap I_2$.

It is fairly easy to see that $I_1 I_2 \subset I_1 \cap I_2$. if $i_1 \in I_1$ and $i_2 \in I_2$ then $i_1 i_2 \in I_1$ and $i_1 i_2 \in I_2$ as I_1 and I_2 are both ideals of A. Hence, $i_1 i_2 \in I_1 \cap I_2$. To see the reverse inclusion, we use the comaximality of I_1 and I_2. Since $I_1 + I_2 = A$, $1 = i_1 + i_2$ for some $i_1 \in I_1$ and some $i_2 \in I_2$. Let $c \in I_1 \cap I_2$. Then $c = i_1 c + c i_2$. Clearly $i_1 c \in I_1 I_2$ and $c i_2 \in I_1 I_2$ and hence $c \in I_1 I_2$.

Suppose that (1) holds true for any $n-1$ ideals of A where $n > 2$. Let $I_1, I_2, \ldots, I_n$ be ideals of A. Define $J = I_1 I_2 \cdots I_{n-1}$ and $I = I_n$. We show that $I + J = A$.

It is easy to see that $I + J \subset A$. Now we use that comaximality of I_{n-1} and I_n. By the comaximality, we have $1 = i_{n-1} + i_n$ for some $i_{n-1} \in I_{n-1}$ and some $i_n \in I_n$. Let $a \in A$. Then $a = a i_{n-1} + a i_n$. Clearly, $a i_n \in I_n$ as I_n is an ideal and $a i_{n-1} \in I_{n-1}$. Since $I_{n-1} \subset I$, we are done.

By the $n = 2$, it follows that $IJ = I \cap J$. Now our result follows from the induction hypothesis:

$$\begin{aligned}
I_1 \ldots I_{n-1} I_n &= JI \\
&= J \cap I \\
&= I_1 \ldots I_{n-1} \cap I_n \\
&= I_1 \cap \ldots \cap I_{n-1} \cap I_n
\end{aligned}$$

Observe that the third equality follows from the induction hypothesis.

□

§2 Lecture 2 — 12th August 2022 — Chinese Remainder Theorem continued. . .

§2.1 Proof of Chinese Remainder Theorem continued . . .

Proof of (2) and (3). Observe the following:

$$\begin{aligned}
a \in \ker \varphi &\iff \varphi(a) = (I_1, I_2, \ldots, I_n) \\
&\iff (a + I_1, a + I_2, \ldots, a + I_n) = (I_1, I_2, \ldots, I_n) \\
&\iff a \in I_1 \cap I_2 \cap \ldots \cap I_n
\end{aligned}$$

Hence $\ker \varphi = I_1 \cap I_2 \cap \ldots \cap I_n$. So it is easy to see now that (2) follows immediately from what we just proved.

Now, we proceed to prove (3). We first prove ($\Leftarrow$) direction. Suppose that I_p and I_q are comaximal for $1 \leq p < q \leq n$. Let us denote e_i $(1 \leq i \leq n)$ for $e_i = (I_1, I_2, \ldots, 1 + I_i, \ldots, I_n)$.

We first show that $I_1 + I_2 \cdots I_n = A$. We show this by induction. Clearly, $I_1 + I_2 = A$ by assumption. Now suppose that $I_1 + I_2 \cdots I_{n-1} = A$. It then follows from Lemma §1.1.9 and $I_1 + I_n = A$ that $I_1 + I_2 \cdots I_n = A$.

Now, $1 = x + y$ for some $x \in I_1$ and $y \in I_2 \cdots I_n$. It follows from part (1) of this theorem that $I_2 \cdots I_n = I_2 \cap \ldots \cap I_n$. Thus $y \in I_2 \cap \ldots \cap I_n$. Thus

$$\begin{aligned}\varphi(y) &= (y + I_1, \ldots, y + I_n)\\ &= (1 - x + I_1, y + I_2, \ldots, y + I_n)\\ &= (1 + I_1, I_2, \ldots, I_n)\\ &= e_1\end{aligned}$$

This shows that e_1 is in the image of φ. Similarly, it can be shown that e_i is in the image of φ for each i.

Now, we can finally show that φ is actually surjective. Let $(a_1 + I_1, \ldots, a_n + I_n)$ be in the codomain of φ. Since we have shown that each e_i is in the image of the φ, $\varphi(y_i) = e_i$ for some $y_i \in A$.

Now observe that

$$\begin{aligned}\varphi\left(\sum_{i=1}^{n} a_i y_i\right) &= \sum_{i=1}^{n} \varphi(a_i)\varphi(y_1)\\ &= \sum_{i=1}^{n} (a_i + I_1, \ldots, a_i + I_i, \ldots, a_i + I_n)(I_1, \ldots, 1 + I_i, \ldots, I_n)\\ &= \sum_{i=1}^{n} (I_1, I_2, \ldots, a_i + I_i, \ldots, I_n)\\ &= (a_1 + I_1, a_2 + I_2, \ldots, a_n + I_n)\end{aligned}$$

This shows that φ is surjective.

We proceed to prove the ($\Rightarrow$) direction of (3). Suppose that φ is surjective. We just show that $I_1 + I_2 = A$. The others follow similarly. To prove that $I_1 + I_2 = A$, it suffices to show that $1 \in I_1 + I_2$. Following the convention in the previous direction, there is some $x \in X$ such that $\varphi(x) = e_1$. So $(x + I_1, \ldots, x + I_n) = (1 + I_1, \ldots, I_n)$. Then $1 - x \in I_1$ and $x \in I_2$. Hence $1 = (1 - x) + x \in I_1 + I_2$. This completes the proof. $\square$

Lemma §2.1.1 (Prime Avoidance Lemma)**.** *Let $I, P_1, P_2, \ldots, P_n$ be ideals of a ring A. Furthermore, assume that P_i is prime for each i. If $I \subset P_1 \cup P_2 \cup \ldots \cup P_n$ then there is some j such that $I \subset P_j$.*

§3 Lecture 3 — 17th August, 2022 — Proof of Prime Avoidance, Jacobson Radical, Modules

§3.1 Proof of Prime Avoidance Lemma

Proof of §2.1.1. We prove that the following equivalent statement that:

If for all j, $I \not\subset P_j$ for all j, there is some element $x \in I$ such that $x \notin P_j$ for all j. ($\star$)

We prove this theorem by assuming that all but 2 of the P_i are prime ideals. (Note : this is a slightly weaker assumption!)

We now start the proof using induction.

We first consider the case when $n = 2$. Let I be an ideal and P_1 and P_2 be prime ideals of A such that $I \not\subset P_1$ and $I \not\subset P_2$. So, there are some element $x \in I \setminus P_1$ and $y \in I \setminus P_2$.

If $x \notin P_2$ then we are done. Likewise if $y \notin P_1$ then we are again done. So, we may assume that $x \in P_2$ and $y \in P_1$.

Now consider $x + y$. Undoubtedly, $x + y \in I$. If it were the case that $x + y \in P_1$ then $x \in P_1$ which is not possible by choice of x. Likewise if it were the case that $x + y \in P_2$ then $y \in P_2$ as $x \in P_2$ which again is not possible by choice of y. Therefore, we have that $x + y \in I$, $x + y \notin P_1$ and $x + y \notin P_2$ and this ends our verification of the base case.

Now, suppose that the $(\star)$ is true when the number of prime ideals is equal to $n-1$ where $n \geq 3$.

Let I be an ideal and $P_1, P_2, \ldots, P_n$ be prime ideals such that $I \not\subset P_j$ for $1 \leq j \leq n$.

By using the induction hypothesis, there is an element $x \in I$ such that $x \notin P_j$ for $1 \leq j \leq n - 1$.

If $x \notin P_n$ then our proof is complete! So, we assume that $x \in P_n$.

Furthermore, we may assume that for $i \neq j$, it is not the case that $P_i \subset P_j$ or $P_j \subset P_i$, that is, there are no inclusions among the prime ideals. Since $n \geq 3$ and all but 2 of the P_j are prime ideals, we may assume that P_n is a prime ideal.

We claim that $IP_1P_2 \ldots P_{n-1} \not\subset P_n$. Suppose not then $IP_1P_2 \ldots P_{n-1} \subset P_n$. It follows by induction and Lemma §1.1.7 that $I \subset P_n$ or $P_i \subset P_n$ for some $1 \leq j \leq n - 1$. Note that the latter part of the 'or' cannot hold by our assumption in the previous paragraph. Thus $I \subset P_n$. But then again this is a contradiction! So, we have that $IP_1P_2 \ldots P_{n-1} \not\subset P_n$.

Now select a $y \in IP_1 \ldots P_{n-1}$ but $y \notin P_n$.

Now, we finish the proof by showing that $x + y \in I$ but $x + y \notin P_i$ for all $1 \leq i \leq n$. It is evident that $x + y \in I$. If $x + y \in P_n$ then $y \in P_n$ which is not possible by choice of y. Note that $y \in IP_1 \ldots P_{n-1}$ implies $y \in P_i$ for all $1 \leq i \leq n - 1$. Now if $x + y \in P_i$ for some $1 \leq i \leq n - 1$ then $x \in P_i$. But that cannot happen by choice of x. Thus we have found an element which is in I but not in any of P_i and this completes the proof!

□

§3.2 Jacobson Radical & Local Rings revisited

Notation §3.2.1. *Let A be a ring. We will use max-spec(A) to denote the set of all maximal ideals of A.*

Definition §3.2.2 (Jacobson Radical)**.** Let A be a ring. The Jacobson radical $\mathcal{J}(A)$ is defined to by the intersection of all maximal ideals of A. In other words,

$$\mathcal{J}(A) := \bigcap \{m : m \in \text{max-spec}(A)\}$$

Lemma §3.2.3. *Let A be a ring. Then $x \in \mathcal{J}(A)$ iff $1 - xy$ is a unit for all $y \in A$.*

Proof. ($\Longrightarrow$) Suppose that $x \in \mathcal{J}(A)$. Suppose that $1-xy$ is not a unit for some $y \in A$. Then there is some maximal ideal m of A containing $1 - xy$. (Just consider the ideal generated by $1 - xy$ and Remark §1.1.8)

Since $x \in \mathcal{J}(A)$, $x \in m$. So $xy \in m$ as m is an ideal. Then $1 = (1 - xy) + xy \in m$ but this is not possible as maximal ideals are not the entire ring by definition! Hence $1 - xy$ is a unit for all $y \in A$.

($\Longleftarrow$) Now suppose that $1 - xy$ is a unit for all $y \in A$. If $x \notin \mathcal{J}(A)$ then there must be some maximal ideal m of A such that $x \in A \setminus m$. Now consider the ideal $m + (x)$. Clearly $m + (x) \supsetneq m$ for otherwise $x \in m$. Hence $m + (x) = A$ as m is a maximal ideal. Thus there are some elements $z \in m$ and $y \in A$ such that $z + xy = 1$. But then $1 - xy = z \in m$. Also, $1 - xy$ is a unit, but that cannot possibly happen as maximal ideals cannot contain units! □

Lemma §3.2.4. *Let A be a ring and m be a nontrivial ideal such that every element of $A \setminus m$ is a unit. Then (A, m) is a local ring.*

Proof. Let I be any nontrivial ideal of A. To show that (A, m) is a local ring, it suffices to show that that $I \subset m$. Let $x \in I$. If $x \notin m$ then x must be a unit by hypothesis. But that is not possible as I is not trivial and hence $I \subset m$. Thus, (A, m) is a local ring. □

Lemma §3.2.5. *Let A be a ring, m be a maximal ideal. If every element of $1 + m$ is a unit then (A, m) is local.*

Proof. By lemma §3.2.4, it suffices to show that every element of $A \setminus m$ is a unit. So let $x \in A \setminus m$. Then $(x) + m = A$as m is a maximal ideal. So, there are elements $y \in A$ and $z \in m$ such that $1 = xy + z$. Then $xy = 1 - z \in 1 + m$ and hence xy is a unit. Since xy is a unit, there is some $u \in A$ such that $(xy)u = u(xy) = 1$. But by associativity and commutativity, we have that $x(yu) = (yu)x = 1$ and hence x is a unit. □

§3.3 Introduction to Modules

Definition §3.3.1. Let A be a ring. An A-module is a abelian group M with a multiplication map

$$\cdot : A \times M \to M$$

$$(a \cdot x) \mapsto ax$$

satisfying

(i) $a(x + y) = ax + ay$ for all $a \in A$ and $x, y \in M$,

(ii) $(a + b)\,x = ax + bx$ for all $a, b \in A$ and $x \in M$,

(iii) $(ab)x = a(bx)$ for all $a, b \in A$ and $x \in M$,

(iv) $1_A x = x$ for $x \in M$.

Alternatively, an A-module is an abelian group M together with a ring homomorphism $\varphi : A \to \mathrm{End}(M)$ where $\mathrm{End}(M)$ is the ring of endomorphism of the abelian group M. Recall that sum in the ring $\mathrm{End}(M)$ is given pointwise and the multiplication is given by function composition.

To check the equivalence of two definitions, let M be a A-module in the sense of Definition §3.3.1. Define a map $\varphi : A \to \text{End}(M)$ by $a \overset{\varphi}{\mapsto} \varphi_a$ where $\varphi_a : M \to M$ given by $\varphi_a(m) = am$ for every $m \in M$. It is now easily seen that φ is a ring homomorphism. Conversely, let M be a module in the sense of previous paragraph. Now, define $\cdot : A \to M \times M$ by $(a \cdot m) = (\varphi(a))(m)$. It is easy to check the properties (i)–(iv) of Definition §3.3.1.

Definition §3.3.2. A A-module M is said to be *faithful* if the map $\varphi : A \to \text{End}(M)$ is injective.

Example §3.3.3. Here are a few examples of modules:

1. Every vector space over a field k is a k-module.

2. Every abelian group is a $\mathbb{Z}$-module.

§4 Lecture 4 — 22 August, 2022 — Exact Sequences and some homological algebra?

§4.1 Review of Exact Sequences

Definition §4.1.1 (Short Exact Sequence)**.** $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is called a short exact sequence if

1. $\text{im } f = \ker g$,

2. g is surjective,

3. f is injective.

Remark §4.1.2. The sequence $0 \longrightarrow A \xrightarrow{f} B$ is an exact sequence iff f is injective. Also the sequence $A \xrightarrow{g} B \longrightarrow 0$ is exact iff g is surjective.

Definition §4.1.3. Let $f : M \to N$ be a A-module homomorphism then we define $\text{coker } f := N/\text{im } f$.

§4.2 Theorems involving exactness of Hom-functor

Proposition §4.2.1 (Left exactness of the Hom-functor)**.** *Let* $0 \longrightarrow N_1 \xrightarrow{\varphi} N_2 \xrightarrow{\psi} N_3$ *be an exact sequence of R-modules. Then*
$0 \longrightarrow Hom_R(M, N_1) \xrightarrow{\varphi^*} Hom(M, N_2) \xrightarrow{\psi^*} Hom(M, N_3)$ *is an exact sequence.*

Proof. First, we need to define the map $\varphi^* : Hom(M, N_1) \to Hom(M, N_2)$. So, let $f \in Hom(M, N_1)$. Then we may define the map $\varphi^*(f) = \varphi f$ as the folllowing diagram:

$$\begin{tikzcd} M \arrow[d, "f"'] \arrow[dr, dotted, "\varphi f"] & \\ N_1 \arrow[r, "\varphi"] & N_2 \end{tikzcd}$$

Likewise, we define $\psi^* : Hom(M, N_2) \to Hom(M, N_3)$ by $\psi^*(g) = \psi g$ for $g \in Hom(M, N_2)$ as in the following diagram:

$$\begin{tikzcd} M \arrow[d, "g"] \arrow[dr, dotted, "\psi g"] & \\ N_2 \arrow[r, "\psi"] & N_3 \end{tikzcd}$$

Now, we show that $0 \longrightarrow Hom_R(M, N_1) \xrightarrow{\varphi^*} Hom(M, N_2) \xrightarrow{\psi^*} Hom(M, N_3)$ is an exact sequence.

We first show exactness in the middle. For that, we need to show that im $\varphi^* = \ker \psi^*$.

First, we show the im $\varphi^* \subset \ker \psi^*$. Let $g \in$ im φ^*. Then $g = \varphi^*(f)$ for some $f \in Hom(M, N_1)$. Then

$$\begin{aligned} \psi^*(g) &= \psi^*(\varphi^*(f)) \\ &= \psi(\varphi f) = 0 \end{aligned}$$

Note that the last equality holds because the the original sequence is exact at N_2. (For more details, let $m \in M$. Then $\psi(\varphi(f(m))) = 0$ as im $\varphi = \ker \psi$).

(The reverse inclusion is much harder to prove, or, at least that's what he said ...) Let $f \in \ker \psi^*$. Then $\psi f = 0$.

Also, note that $\ker \psi = \varphi(N_1) \cong N_1$ since φ is injective and the original exact sequence.

We claim that (by the universal property of the kernel (N_1, φ)) there is a unique map $g : M \to N_1$ such that $g\varphi = f$.

$$\begin{tikzcd} & & M \arrow[dl, dotted, "\exists! g"'] \arrow[d, "f"] & \\ 0 \arrow[r] & N_1 \arrow[r, "\varphi"] & N_2 \arrow[r, "\psi"] & N_3 \end{tikzcd}$$

We proceed to show the existence of the map $g : M \to N_1$ that we have claimed. Let $m \in M$. Then $f(m) \in N_2$. Then $\psi(f(m)) = 0$ because $\psi f = 0$. Hence $f(m) \in \ker \psi$. But $\ker \psi =$ im ϕ, so, there is some $n_1 \in N_1$ such that $\varphi(n_1) = f(m)$. We define $g(m) = n_1$.

It is easy to see that if $g(m) = n_1$ then $\varphi g(m) = \varphi(n_1) = f(m)$. So $\varphi g = f$.

Now, we show that φ is well-defined. The only place where well-definedness is lost is when we took preimages, so, let $n_1, n_1' \in N_1$ such that $\varphi(n_1) = f(m)$ and $\varphi(n_1') = f(m)$. Now, since φ is injective, we have that $f(m) = \varphi(n_1) = \varphi(n_1')$ implies $n_1 = n_1'$. Therefore, g is well-defined.

Now, we need to prove that $g \in Hom(M, N_1)$. But this immediately follows from the facts that φ and f are homomorphisms.

Thus, we have that $\varphi^*(g) = f$ and hence $f \in$ im g^*.

We need to show that $\ker \varphi^* = \{0\}$. For that, let $f \in Hom(M, N_1)$. Then $\varphi^*(f) = 0$ implies that $\varphi f = 0$. By the original exact sequence, φ is injective. Let $m \in M$. Then $\varphi(f(m)) = 0$ and the fact that φ is injective implies that $f(m) = 0$. Since m was arbitrary, we have that $f = 0$.

□