Lang's Algebra Chapter 3 Solutions

Amanuel Tewodros

September 15, 2025

(1) By the second isomorphism theorem, we have

$$\frac{U}{U \cap W} \cong \frac{U+W}{W}.$$

For two vector spaces, $X \supseteqq Y$ over a field K, we have $\dim X/Y = \dim X - \dim Y$. Thus $\dim U - \dim U \cap W = \dim U + W - \dim W$.

(2) Let M be a module over a commutative ring R. Let I be a maximal ideal of R. We first show that for any proper ideal $\mathfrak{a}$ of R and basis set $\{x_1, x_2, \dots\}$, of M,

Lemma 1.

$$\frac{M}{\mathfrak{a}M} \cong \bigoplus_i \frac{A}{\mathfrak{a}}(x_i + \mathfrak{a}x_i).$$

Proof. $\mathfrak{a}M$ is submodule of M because $\mathfrak{a}M \subseteqq M$ by R-closure property of $\mathfrak{a}$. It immedietly follows that $\mathfrak{a}M = \bigoplus_i \mathfrak{a}x_i$. By linear independence of x_i, $\left(\sum_i r_i x_i\right) \mod \mathfrak{a}x_j = (r_j \mod \mathfrak{a})x_j + \sum_{i \neq j} r_i x_i$. Therefore, $M/\mathfrak{a}M = \bigoplus_i Ax_i/\mathfrak{a}x_i$. By the isomorphism $x_i \mapsto 1_A \mapsto (x_i + \mathfrak{a}x_i)$, $Ax_i/\mathfrak{a}x_i \cong A/\mathfrak{a} \cong A/\mathfrak{a}(x_i + \mathfrak{a}x_i)$. $\square$

Taking $\mathfrak{a}$ as a maximal ideal of R in the above lemma, we see that $M/\mathfrak{a}M$ is a direct product of vector spaces over the field $A/\mathfrak{a}$ and thus admit a basis of the same cardinality as that of M. Because the dimension of a vector space is independent of the basis choice, M also has a fixed dimension.

(3) Let $\{x_1, \dots, x_m\}$ form the basis set of R over k and let $1_R = k_1 x_1 + \dots k_m x_m$ for $k_i \in k$. For any element $a \in R$, define the sequences $\{y_1, \dots, y_m\} \subseteqq k$, $\{f_1, f_2, \dots, f_m\} \subseteqq R$ as:

$$f_1 = a, \quad y_1 = w_{1,1}^{-1} k_1$$

$$f_{i+1} = f_i y_i - k_i x_i, \quad y_i = k_i w_{i,i}^{-1},$$

,where $f_i = \sum_j w_{i,j} x_j$. By construction, $a^{-1} = \sum_i y_i x_i$. Thus R is a field.

(4) **Direct Sums**

(a) First, we show the equivalence of the two statements of the theorem. Suppose there is φ such that $g \circ \varphi = \mathrm{id}$. By the injectivness of the composition, $\operatorname{Im} \varphi \cap \ker g = \{0\}$. But by exactness, $\ker g = \operatorname{Im} f$. We can unambiguously define $\psi(u)$ to be the inverse image of $f^{-1}(u')$ where $u' \equiv u \mod \operatorname{Im} \varphi$ and $u' = f(x)$ for some $x \in M'$ because if $f(x) = f(y) \mod \operatorname{Im} \varphi$, $f(x-y) \in \operatorname{Im} \varphi$ and by injectivity of f, $x = y$.Since $M/\operatorname{Im} f \cong M'' = \operatorname{Im} \varphi$, ψ is defined in all of M. Similarly, if the second statement is true, $\ker \psi \cap \operatorname{Im} f = \{0\}$ because $\psi \circ f$ is injective. By exactness, $\operatorname{Im} f = \ker g$. We can then define $\varphi(u) = u'$ where $u' = y \mod \ker \psi$ and $g(y) = u$ for some y. φ is well-defined because if $g(y_1) = g(y_2)$ for $y_1 \neq y_2$, then $y_1 \neq y_2 \mod \ker \varphi$.

Now suppose $x \in M$. $x - \varphi(u) \in \operatorname{Im} f$ for exactly one u by the argument mentioned previously. Thus we can express $x = r + s$ where $r = \varphi(u) \in \operatorname{Im} \varphi$ and $s = x - \varphi(u) \in \operatorname{Im} f$. This implies $M = \operatorname{Im} f \oplus \operatorname{Im} \varphi$. By bijectivness of $g \circ \varphi$, $\operatorname{Im} \varphi \cong M''$. By contrast, if $M = \operatorname{Im} f \oplus N$ for some N, with isomorphism $t : N \to M''$. We can define $g : M \to M''$ as $g(u) = u'$ such that there is $u = y \mod N$ and $t^{-1}(u') = y$. This definition is unambiguous because $N \cap \operatorname{Im} f = \{0\}$. Since $g \circ t^{-1} = \mathrm{id}$, the sequence splits.

Finally, we complete the details of proposition 3.2. We have just shown $M = \text{Im } f \circ \text{Im } \varphi$. By exactness, $\text{Im } f = \ker g$. Also, $\text{Im } f \cong M'$ and $\text{Im } \varphi \cong M''$ by injectivness of f and φ resp. This proves $M \cong M' \oplus M''$. We can write $x \in M$ as $f(u) + x - f(u)$ where $x - f(u) \in \ker \psi$. u is then uniquely determined by x as $\ker \psi \cap \text{Im } f = \{0\}$ by bijectivness of $\psi \circ f$. This shows $M = \text{Im } f \oplus \ker \psi$.

(b) First, we note that φ_i is injective because othewise the composition $\psi_i \circ \varphi_i$ wouldn't be injectice, a contradiction. This implies, for every valid i, there is a submodule $E_i' = \text{Im } \varphi_i$ of E that is isomorphic to E_i. Moreover, if $c \in \text{Im } \varphi_i \cap \text{Im } \varphi_j$ for $i \neq j$, then $\psi_i(c) = \psi_j(c) = 0$, forcing c to be 0. These statements prove

$$\bigoplus_{i=1}^{n} E_i' \subseteqq E.$$

The inverse inclusion follows as follows. Let $x \in E$, then $x = \sum_{i=1}^{n} \varphi_i(\psi_i(x))$, but $\varphi_i(\psi_i(x)) \in E_i'$. Therefore $x \in \bigoplus_i E_i'$.

Let $x = x_1 + \cdots + x_m$ where $x_i \in E_i'$. The map definied by $x \mapsto (\psi x_i)_{1 \leq i \leq m}$ is therefore an isomorphism and the inverse map is given by $(\psi x_i)_i \mapsto \sum_i x_i$.

(5) Let $v_m' = a_1 v_1 + \cdots + a_m v_m$. Since $a_m \neq 0$, v_m', and by the assumption that $\{v_i\}$ is linearly independent over $\mathbb{R}$, the set $\{v_1, \ldots, v_{m-1}, v_m'\}$ is linearly indepenedent over $\mathbb{Z}$. We also note that, $v_m' - \sum_{i=1}^{m-1} a_i v_i \in A$, thus we can safely assume $a_1 = \cdots = a_{m-1} = 0$.

To show, the set spans A, we consider A/A_0. Suppose, there is $av_m \in A/A_0$ such that $av_m \neq nv_m'$ for all $n \in \mathbb{Z}$. Let r, s be two integers such that $|ra_m + sa| < a_m$. Since contradicts minimality of a_m, it must be the case that $a_m \mid a$.. Therfore $A/A_0 = \mathbb{Z}v_m'$.

(6) We induct on the size of S.

First assume that $S = \{w\}$. Then $\mathbb{Z}\langle S \rangle = \{n[w] : n \in \mathbb{Z}\}$. If M is a subgroup of $\mathbb{Z}\langle S \rangle$, then $M = \mathbb{Z}\langle a[w] \rangle$ for some $a \in \mathbb{Z}$. Here we pick $y_w = a[w]$ which is G-linear.

For the induction step, suppose the statement is true for S, $0 \leq |S| \leq m - 1$. We shall prove the statement is true for S with m elements. Fix on element $w \in S$, and consider projection map $\pi : \mathbb{Z}\langle S \rangle \to \mathbb{Z}\langle G \cdot w \rangle$. By correspondence, $\pi(M)$ is a subgroup of $\mathbb{Z}\langle G \cdot w \rangle$ with basis $\{\bar{y}_{gw}\}_{w \in G}$ which satisfy the property for $\sigma \in G$, $\sigma \bar{y}_{gw} = \bar{y}_{\sigma g w}$. We then lift the basis of $\mathbb{Z}\langle \pi(M) \rangle$ to $\mathbb{Z}\langle S \rangle$ by picking a representatives $\mathfrak{R} = \{y_w\}$ in M for $\bar{y}_w$. The y_w are linearly indepndenent thus form part of the basis for M. Again by hypothesis, $M \cap \mathbb{Z}\langle S - G \cdot w \rangle$ has basis $\mathfrak{B} = \{y_w\}_{w \in S - G \cdot w}$ that satisfy the given property. We finally combine $\mathfrak{R}$ and $\mathfrak{B}$ to get the basis of rank m for M.

(7) For convenience, we identify the properties of a semi-norm as follows

SN-1 $|v| \geq 0$

SN-2 $|nv| = |n||v|$

SN-3 $|u + v| \leq |u| + |v|$

(a) Let $a, b \in M_0$. Then by SN-2 and SN-3, $|u - b| \leq |a| + |b| = 0$. By SN-1, we have $|a - b| \geq 0$, this $a - b \in M_0$. By SN-2, $|0| = |2 \cdot 0| = 2|0|$. This implies $0 \in M_0$. Hence M_0 is a subgroup of M.

(b) If $M_0 \neq \{0\}$, we can make the transformation $x \mapsto x + M_0$ without loss of generality as such map preserves the linear independence of $\{v_i\}$. Thus, we can assume $M_0 = \{0\}$.

Let $N = \langle v_1, \ldots, v_r \rangle$. Since M has rank r, the exponent e of M/N is finite and thus eM is a subgroup of N. Moreover, N/eM is torsion group with finite number of elements. Therefore, we can pick the smallest positive integers $n_{i,j}$ such that

$$\sum_{j=1}^{i} n_{i,j} v_j = dw_i \quad \text{for some } w_i \in M$$

The linear independence follows immediately. Picking $n_{j,k}$ in the range $[0, d - 1]$,

$$d|w_i| = |dw_i| \leq \sum_{j=1}^{i} n_{i,j} |v_j| \leq d \sum_{j=1}^{i} |v_j|.$$

(8) (a) SN-1 follows immediately because $\log \geq 0$ for all $\mathbb{Z}^+$. Since, $h(x^{-1}) = h(x)$, it suffices to prove SN-2 for $n \geq 0$ in which case $h(x^n) = \log\max(|a^n|, |b^n|) = \log\max(|a|, |b|)^n = n\log\max(|a|, |b|) = nh(x)$. Finally, if $y = c/d$, $h(xy) = h(ac/bd)$. Let $e = \gcd(a, d)$ and $f = \gcd(c, b)$. Then

$$\begin{aligned} h(xy) &= \log\max(|\frac{ac}{ef}|, |\frac{bd}{ef}|) \\ &= \log\big(\frac{1}{|ef|}(\max(|ac|, |bd|))\big) \\ &= \log\max(|ac|, |bd|) - \log|ef| \\ &\leq \log\max(|ac|, |bd|) \\ &\leq \log\max(|a|, |b|) + \log\max(|c|, |d|) \end{aligned}$$

Hence SN-3 is satisfied. $\log\max(|a|, |b|) = 0$ if and only if $|a| = |b| = 1$, which makes the kernel of $\ker h = \{\pm 1\}$.

(b) For a given rational number $x = a/b$, since there are finitely many prime divisors of p, q such that $p|a$ and $q|b$, M can be generated by the set $\{-1, 1\} \cup \{p, 1/q \in \mathbb{Q}^* : p|\text{the numerator of } x_1 \cdots x_m, q|\text{the denominator of } x_1 \cdots x_m\}$. From this we can set upper bound on the norm as

$$h(y) \leq \sum_p \log p$$

where the sum is over all primes p (not necassarily distinct) that divides the numerator or denominator of x_i for some i.

(9) (a) $S^{-1}M$ can be defined as a subset of $M \times S$ for a commutative ring A, a multiplicative subset S and A-module M such that

$$(m_1, s_1) \sim (m_2, s_2)$$

, if there is a an element $s \in S$ that satisfy the equation $s(s_2m_1 - s_1m_2) = 0$. As with $S^{-1}A$, we can denote (m, s) with m/s. Since $S^{-1}A$ is a commutative ring, we can define the action of $S^{-1}A$ on $S^{-1}M$ as

$$\frac{a}{s'} \cdot \frac{m}{s} = \frac{a \cdot m}{s's}.$$

With this definition of the action of $S^{-1}A$ on $S^{-1}M$, we can show that $S^{-1}M$ is an $S^{-1}A$-module. Let $a_1/b_1, a_2/b_2 \in S^{-1}A$ and let $m_1/s_1, m_2/s_2 \in S^{-1}M$. Then we have

$$\begin{aligned} \frac{a_1}{b_1} \cdot \left(\frac{m_1}{s_1} + \frac{m_2}{s_2}\right) &= \frac{a_1}{b_1} \cdot \left(\frac{m_1s_2 + m_2s_1}{s_1s_2}\right) \\ &= \frac{a_1b_1}{b_1b_1} \cdot \left(\frac{m_1s_2 + m_2s_1}{s_1s_2}\right) \\ &= \frac{a_1b_1s_2m_1 + a_1b_1s_1m_2}{b_1s_1b_1s_2} \\ &= \frac{a_1m_1}{b_1s_1} + \frac{a_1m_1}{b_1s_2} \\ &= \frac{a_1}{b_1} \cdot \frac{m_1}{s_1} + \frac{a_1}{b_1} \cdot \frac{m_2}{s_2}. \end{aligned}$$

and

$$
\begin{aligned}
\left(\frac{a_1}{b_1}+\frac{a_2}{b_2}\right)\cdot\frac{m_1}{s_1} &= \left(\frac{a_1b_2+a_2b_1}{b_1b_2}\right)\cdot\frac{m_1}{s_1}\\
&= \left(\frac{a_1b_2+a_2b_1}{a_1a_2}\right)\cdot\frac{m_1s_1}{s_1s_1}\\
&= \frac{a_1b_2m_1s_1+a_2b_1m_1s_1}{s_1b_1s_2b_2}\\
&= \frac{a_1m_1}{b_1s_1}+\frac{a_2m_1}{b_2s_1}\\
&= \frac{a_1}{b_1}\cdot\frac{m_1}{s_1}+\frac{a_2}{b_2}\cdot\frac{m_1}{s_1}.
\end{aligned}
$$

(b) Let

$$0 \to M' \xrightarrow{f} M \xrightarrow{f''} M'' \to 0$$

be exact. Then we have the induced sequence,

$$0 \to S^{-1}M' \xrightarrow{g} S^{-1}M \xrightarrow{g''} S^{-1}M'' \to 0,$$

where g is defined as $g(m/s) = f(m)/s$ and g'' is defined as $g''(m/s) = f''(m)/s$. $\ker g = \{m/s : f(m)/s = 0\}$. Since f is injective, $f(m) = 0$ iff $m = 0$,i.e., $\ker g = \{0\}$.
By exactness $\operatorname{Im} f = \ker f''$. Evaluating g'' on $\operatorname{Im} g$, $g''(g(m/s)) = g''(f(m)/s) = f''(f(m))/s = 0/s = 0$. This shows $\operatorname{Im} g \subseteqq \ker g''$. Let $g''(x/s) = f''(x)/s = 0$. This implies $f''(x) = 0$ for some x. By exactness, $\ker f \subseteqq \operatorname{Im} f''$, implying $x = f(y)$ for some $y \in M'$. This proves $\operatorname{Im} g \supseteqq \ker g''$.
Finally, let $x/s \in S^{-1}M''$. Since $x \in M''$, $x = f''(y)$ for some $y \in M$ by exactness of the first sequence. But then $x/s = f''(y)/s = g''(y/s)$ making g'' surjective.

(10) (a) The natural map under consideration is the map

$$f = x \mapsto (x/1, \dots).$$

If $x/s' \sim 0/1$, for some $s' \in A - \mathfrak{p}$ and $x \in M$, then it means $sx = 0$ for some $s \in A - \mathfrak{p}$. Therefore, the kernel of f is the set $\{x : sx = 0,$ for some $s \in A - \mathfrak{p}$ for all maximal ideals $\mathfrak{p}\}$. If $x \in \ker f$, then $\operatorname{Ann}(x)$ is not contained in any maximal ideal $\mathfrak{p}$, implying $\operatorname{Ann}(x) = A \implies x = 0$.

(b) Let $f : M'' \to M$ and $\hat{f} : M''_{\mathfrak{p}} \to M_{\mathfrak{p}}$. Define g and $\hat{g}$ similarly for the second halves of the sequences.

($\implies$) This directly follows from part (b) of exercise 9.

($\impliedby$) Suppose $0 \to M'_p \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}}$ is exact sequence for all primes $\mathfrak{p}$.
Let $f(x) = 0$, then $\hat{f}(x/s) = f(x)/s = 0/1$ for all $s \in \mathfrak{p}$. By exactness, $\hat{f}$ is injective. thus $x/s = 0$. By similar reasoning as part (a) of this problem $x = 0$. Hence f is injective.
Now let $gf(x) = n$. By definition, $\hat{g}\hat{f}(x/s) = n/s$. By exactness, the left-hand side is 0. Thus $s'n = 0$ for $s' \in \mathfrak{p}$ for all prime $\mathfrak{p}$. Again, by similar reasoning as part (a), n has to be 0 and $\operatorname{Im} f \subseteqq \ker g$.
To see the converse, suppose $g(y) = 0$. Consequently, $\hat{g}(y/s) = g(y)/s = 0$ for all $s \in \mathfrak{p}$ and by exactness, $y/1 = \hat{f}(x/t_{\mathfrak{p}}) = f(x)/t_{\mathfrak{p}}$ for some $t_{\mathfrak{p}}$ depending on $\mathfrak{p}$. This implies $s_{\mathfrak{p}}(f(x) - t_{\mathfrak{p}}y) = 0$ or equivalently $f(s_{\mathfrak{p}}x) = r_{\mathfrak{p}}y$ for some $x \in M'_{\mathfrak{p}}$ and $r_{\mathfrak{p}} = s_{\mathfrak{p}}t_{\mathfrak{p}}$ implying $r_{\mathfrak{p}}y \in \operatorname{Im} f$ for all prime $\mathfrak{p}$. Since $M/\operatorname{Im} f$ is also an A-module, it implies $r_{\mathfrak{p}}(x + \operatorname{Im} f) = 0$ for all $\mathfrak{p}$ implying $x + \operatorname{Im} f = 0 + \operatorname{Im} f$ or in other words, $x \in \operatorname{Im} f$. This proves $\operatorname{Im} f = \ker g$.
Finally, suppose $y \in M''$. By surjectivity of $\hat{g}$, $y/1 = \hat{g}(x/s) = g(x)/s$ for some $x \in M$. By definition, $s_{\mathfrak{p}}(g(x) - t_{\mathfrak{p}}y) = 0$. By similar argument as above, $y \in \operatorname{Im} g$, proving the exactness of the first sequence.

(c) Let $\phi : M \to M_{\mathfrak{p}}$ be the natural map in question. Then $\phi(x) = x/1$. If $\phi(x) = 0$, then $sx = 0$ for some $s \in A - \mathfrak{p}$. This contradicts the assumption M is torsion-free and since $0 \notin A - \mathfrak{p}$, $x = 0$.

Projective modules over Dedekind rings

(11) Let $\mathfrak{o}$ be a Dedekind domain, and let M be a finitely generated torsion-free $\mathfrak{o}$-module. For each prime ideal $\mathfrak{p}$, consider the localization $\mathfrak{o}_\mathfrak{p}$ and the localized module $M_\mathfrak{p}$.

Since $\mathfrak{o}_\mathfrak{p}$ is a Dedekind domain with only one prime ideal $S^{-1}\mathfrak{p}$, by the result from the previous chapter it is a PID. Finite generation and torsion-freeness of $M_\mathfrak{p}$ follow from the corresponding properties of M, and Theorem 7.3 then implies that $M_\mathfrak{p}$ is a free $\mathfrak{o}_\mathfrak{p}$-module (and hence projective).

Now let F be a free $\mathfrak{o}$-module, and suppose there is a surjective homomorphism

$$f : F \twoheadrightarrow M.$$

Localizing at $\mathfrak{p}$, we obtain a surjective map

$$f_\mathfrak{p} : F_\mathfrak{p} \twoheadrightarrow M_\mathfrak{p}.$$

Since $M_\mathfrak{p}$ is projective, there exists a homomorphism

$$g_\mathfrak{p} : M_\mathfrak{p} \to F_\mathfrak{p}$$

such that

$$f_\mathfrak{p} \circ g_\mathfrak{p} = \mathrm{id}_{M_\mathfrak{p}}.$$

Because M is finitely generated, say by $m_1, \dots, m_r$, each $g_\mathfrak{p}(m_i/1) \in F_\mathfrak{p}$ can be written with a denominator not in $\mathfrak{p}$. Let $c_\mathfrak{p} \in \mathfrak{o} \setminus \mathfrak{p}$ be the product of all these denominators for $i = 1, \dots, r$. Then

$$c_\mathfrak{p}\, g_\mathfrak{p}\big(l_\mathfrak{p}(M)\big) \subseteq F,$$

where $l_\mathfrak{p} : M \to M_\mathfrak{p}$ is the localization map.

We claim that the set $\{c_\mathfrak{p} : \mathfrak{p} \text{ prime}\}$ generates the unit ideal (1). Indeed, if this ideal were proper, it would be contained in some maximal ideal $\mathfrak{m}$; but then $c_\mathfrak{m} \in \mathfrak{m}$, contradicting $c_\mathfrak{m} \notin \mathfrak{m}$. Thus there exist primes $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ and elements $x_1, \dots, x_n \in \mathfrak{o}$ such that

$$\sum_{i=1}^{n} x_i\, c_{\mathfrak{p}_i} = 1.$$

Define

$$g := \sum_{i=1}^{n} x_i\, c_{\mathfrak{p}_i} \cdot g_{\mathfrak{p}_i} \circ l_{\mathfrak{p}_i} : M \to F.$$

This is well-defined since each $c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}(l_{\mathfrak{p}_i}(M)) \subseteq F$.

For $m \in M$, we have

$$f(g(m)) = \sum_{i=1}^{n} x_i\, c_{\mathfrak{p}_i}\, f(g_{\mathfrak{p}_i}(m/1)) = \sum_{i=1}^{n} x_i\, c_{\mathfrak{p}_i}\,(m/1) = \left(\sum_{i=1}^{n} x_i\, c_{\mathfrak{p}_i}\right) m = 1 \cdot m = m.$$

Thus $f \circ g = \mathrm{id}_M$, showing that M is a direct summand of F and hence projective.

(12) (a) Define a map $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{o}$ as

$$(a, b) \mapsto ca + b,$$

where c is as defined in question 19 of chapter II. Since $c\mathfrak{a}$ and $\mathfrak{b}$ are coprime the image of this map is $\mathfrak{o}$. The kernel of this map which is given by $c\mathfrak{a} \cap \mathfrak{b} \supseteq c\mathfrak{a}\mathfrak{b}$ also satisfies the reverse inclustion because for $d \in c\mathfrak{a} \cap \mathfrak{b}$, we can write $d = d(ca + b) = ca \cdot d + d \cdot a \in c\mathfrak{a}\mathfrak{b}$. Therefore, kernel is $c\mathfrak{a}\mathfrak{b}$. Since the map $\mathfrak{a}ib \to c\mathfrak{a}\mathfrak{b}$ is bijective, and $\mathfrak{o}$ is fintely generated and torsion-free (thus free), it follows that

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{o} \oplus \mathfrak{a}\mathfrak{b}$$

(b) First we show that $f = m_c$ for some $c \in K$. Let $a_1, a_2 \in \mathfrak{a}$. For fixed elements, a_1, a_2, we can assume $f(a_1) = c_1 a_1$ and $f(a_2) = c_2 a_2$ for $c_1, c_2 \in K$ since both $\mathfrak{a}$ and $\mathfrak{b}$ are contained in the field K. By the definition of fractional ideals, there is an element $c \in \mathfrak{o}$ such that $ca_1, ca_2 \in \mathfrak{o}$ and $ca_1 a_2 \in \mathfrak{a}$. By the $\mathfrak{o}$-linearlity f and by commuitivity of K, $f(ca_1 a_2) = ca_1 f(a_2) = ca_2 f(a_1) \implies c_1 = c_2$. Thus $f = m_c$. This also proves $\mathfrak{b} = c\mathfrak{a}$ for some $c \in K$.

We can define an extension of f, f_K, in K as $f_K(x) = f_K(a^{-1}ax) = a^{-1}x f_K(a) = a^{-1} f(a) x = cx$. f_K is clearly K-linear and agrees with f on $\mathfrak{a}$.

Remark 2. Lang takes for granted that the assumption that there exists a K-linear map f_K. This is not obvious and we have just proved that in fact there exists a K-linear map that is an extenstion of f.

(c) The assertion that m_b is an element of $\mathfrak{a}^\vee$ follows directly from the inclusion $b\mathfrak{a} \subseteq \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$. This implies $\mathfrak{a}^{-1} \subseteq \mathfrak{a}^\vee$. We show the reverse inclusion holds.

Let $\phi \in \mathfrak{a}^\vee$. By the previous subproblem, it suffices to show that $\phi(\mathfrak{a})$ is an ideal of $\mathfrak{o}$. Since $\phi(\mathfrak{a})$ is a $\mathfrak{o}$-submodule of $\mathfrak{o}$, $\phi(\mathfrak{a})$ is an additve subgroup of $\mathfrak{o}$. For $a, b \in \mathfrak{a}$, by properties of $\mathfrak{o}$-homomorphism ϕ, $\phi(\phi(a)b) = \phi(a)\phi(b) \in \phi(\mathfrak{a})$. Finally, for $c \in \mathfrak{o}$, $c\phi(\mathfrak{a}) = \phi(c\mathfrak{a}) \subseteq \phi(a)$ where the last inclusion followed from the definition of fractional ideals.

Thus, we have $\phi(\mathfrak{a}) = c\mathfrak{a}$ where $c = \phi_K(1)$. c has to be a member of $\mathfrak{a}^{-1}$ because otherwise $c\mathfrak{o} + \mathfrak{a}^{-1}$ would be an inverse of $\mathfrak{a}$ making $\mathfrak{a}^{-1}$ non-unqiue, a contradiction in Dedekind domains.

(13) (a) M should be torsion-free. Otherwise, by projectivity of M, for some free module $F \supseteq M$ and any surjective $\mathfrak{o}$-homomorphism $f : F \to M$, there is a correspoding $g : M \to F$ such that $f \circ g = \mathrm{id}_M$. If non-zero $x \in M$ is a torision element, say with exponent $a \in \mathfrak{o}$, then $0 = g(ax) = ag(x) \in F$ implying either $a = 0$ or $g(x) = 0$. Since $f(g(x)) = x \neq 0$, it follows $a = 0$, proving M is torsion free.

Localizing M at any prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, we see that the module $M_\mathfrak{p}$ is a PID that is torsion-free and finity generted. This makes $M_\mathfrak{p}$ free. Let $M_\mathfrak{p} = \bigoplus_{i=1}^n \mathfrak{o}_\mathfrak{p} m_i$. By finiteness of m_i, there is an element $c \in \mathfrak{o}$ such that $cm_i \in M$ for all i. We then find F' as

$$F' = \bigoplus_{i=1}^n \mathfrak{o}(cm_i) \subseteq M.$$

Now, let $\{v_1, \ldots, v_k\}$ be the generators of M and let

$$v_i = \sum_{j=1}^n r_j^{(i)} m_i.$$

Pick $d \in \mathfrak{o}$ such that $dr_j^{(i)} \in \mathfrak{o}$ which exists by the finiteness of $r_j^{(i)}$. It follows that $dM \subseteq \bigoplus_{i=1}^n \mathfrak{o} m_i$ and that

$$M \subseteq \bigoplus_{i=1}^n \mathfrak{o}(\frac{1}{d} m_i) = F.$$

The equality $\operatorname{rank} F = \operatorname{rank} F'$ immediately follows.

(b) Let $\frac{1}{d} m_i = e_i$ in the proof of (b). We prove the statement by inducting on the number of basis elements, n.

When $n = 1$, then define $\mathfrak{a}_1 = \{a : ae_1 \in M\}$. This subset of $\mathfrak{o}$ is an ideal of $\mathfrak{o}$ because if $m = ae_1$ for some a, then $rae_1 = rm \in M$ for any $r \in \mathfrak{o}$.

For the induction step, suppose N is a submodule of M spanned by $e_1, \ldots .e_{n-1}$. By induction hypothesis, $N = \bigoplus_{i=1}^{n-1} \mathfrak{a}_i e_i$. Consider the exact sequence

$$0 \to N \to M \to M/N \to 0.$$

Since $\operatorname{rank} M/N = \operatorname{rank} M - \operatorname{rank} N = 1$, and by the projectivity of M/N, the induction follows.

(c) The statement that $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a}$ for some ideal $\mathfrak{a}$ follows immediately from part (b) of this problem and part (a) of problem 12.

Let $F : K_o(\mathfrak{o}) \to \mathrm{Pic}(\mathfrak{o})$ be the given association. First, we show that this association is a group homomorphism. By the linear independece of F (as defined in (a)), the 'decomposition' of M in terms of $\mathfrak{a}_i$ is unique. Thus, $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ is uniquely determined by M, making F a well-defined mapping.

Consider M, N are two finite projective modules. Then $F(M) + F(N) = \mathfrak{o}^{n-1} \oplus \mathfrak{a} \oplus \mathfrak{o}^{m-1} \oplus \mathfrak{b} = \mathfrak{o}^{n-m-2} \oplus \mathfrak{a} \oplus \mathfrak{b} = \mathfrak{o}^{n-m+1} \oplus \mathfrak{a}\mathfrak{b} = F(M \oplus N)$. Thus F is a group homomorphism.

Let $M \in \ker F$. Then, $F(M) = \mathfrak{o}$. This implies $M = \mathfrak{o}^n$ is free which is a single equivalence class in $K_0(A)$. Therefore, $M = [0]$. Finally, taking M as any ideal $\mathfrak{a}$ of $\mathfrak{o}$ as $\mathfrak{o}$-module, we see that $F(M) = \mathfrak{a}$, making F surjective and thus an isomorphism.

A few snakes

(14) Let $M' \xrightarrow{\phi'} M \xrightarrow{\phi} M'' \to 0$ and let $0 \to N' \xrightarrow{\psi'} N \xrightarrow{\psi} N''$ be the two exact sequence in the diagram.

(a) Let $g(x) = 0$. By commutitivity, $\psi(gx) = h(\phi x) = 0$. By the injectivity of h, $\phi(x) = 0$. By exactness of the top sequence, $x = \phi'(y)$ for $y \in M'$. By commutitivity of the diagram, $0 = g(\phi' y) = \psi'(fy)$. By exactness of the bottom sequence $f(y) = 0$. By the injectivity of f, then $y = 0$ and its image under ψ', x is also 0. This proves g is a mono-morphism.

(b) Let $x \in N$. Then $\psi x \in N''$. By surjectivity of h and ϕ, there is an element $y \in M$ such that $h(\phi y) = \psi x$. By commutitivity, it follows that $\psi x = \psi(gy)$ and consequently $x - gy \in \ker \psi$. By exactness, $x - gy = \psi' z$ for some $z \in N'$ and by surjectivity of f, $x - gy = \psi'(fw)$ for some $w \in M'$. By commutitivity, it follows that $x - gy = g(\phi' w)$ or $x = g(y + \phi' w)$, implying $x \in \operatorname{Im} g$ (g is surjective).

(c) If f and h are isomorphims, then g is isomporphims by (a) and (b) of this problem.

Consider g and h are isomorphims, i.e., $\ker g = \ker h = \operatorname{Coker} g = \operatorname{Coker} h = 0$. By the snake lemma, there is a map $\ker h \to \operatorname{Coker} f$ showing f is surjective. By injectivity of the map $M' \to M$, $\ker f \to \ker g$ is injective, making $\ker f = 0$. Hence, f is an isomorphism.

Now suppose f and g are isomorphisms. By the snake lemma, $\ker g \to \ker h \to \operatorname{Coker} f$ is exact. Since $\ker g = \operatorname{Coker} f = 0$, $\ker h = 0$. Similarly, by the exactness of the sequence $\operatorname{Coker} g \to \operatorname{Coker} h \to 0$, $\operatorname{Coker} h = 0$.

(15) We denote the module homomorphimsm as follows:

$$\begin{tikzcd}
M_1 \arrow[r, "\alpha"] \arrow[d, "f_1"] & M_2 \arrow[r, "\beta"] \arrow[d, "f_2"] & M_3 \arrow[r, "\gamma"] \arrow[d, "f_3"] & M_4 \arrow[r, "\delta"] \arrow[d, "f_4"] & M_5 \arrow[d, "f_5"] \\
N_1 \arrow[r, "\alpha'"] & N_2 \arrow[r, "\beta'"] & N_3 \arrow[r, "\gamma'"] & N_4 \arrow[r, "\delta'"] & N_5
\end{tikzcd}$$

We apply the snake lemma on the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \beta M_2 \arrow[r] \arrow[d, "f_3|_{\beta M_2}"] & M_3 \arrow[r] \arrow[d, "f_3"] & \gamma M_3 \arrow[r] \arrow[d, "f_4|_{\gamma M_3}"] & 0 \\
0 \arrow[r] & \beta' N_2 \arrow[r] & N_3 \arrow[r] & \gamma' N_3 \arrow[r] & 0
\end{tikzcd}$$

Exacteness of the top and bottom sequence and commutitivity of the diagram follow immediately. By the snake lemma, we have the short exact sequence:

$$0 \to \ker f_3|_{\beta M_2} \to \ker f_3 \to \ker f_4|_{\gamma M_3} \to \operatorname{Coker} f_3|_{\beta M_2} \to \operatorname{Coker} f_3 \to \operatorname{Coker} f_4|_{\beta M_3} \to 0$$

(a) By assumption $\ker f_4|_{\gamma M_3} = 0$. Thus, it suffices to show that $\ker f_3|_{\beta M_2} = 0$.

Let $x \in \ker f_3|_{\beta M_2}$. Then $x = \beta(y)$ for some $y \in M_2$. By commutitivity, we have $0 = f_3(\beta y) = \beta'(f_2 y)$, implying $f_2 y \in \ker \beta' = \alpha' N_1$ where the last equality follows from the exactness of the bottom sequence. Since f_1 is surjective, there is an element $z \in M_1$ such that $\alpha'(f_1 z) = f_2(\alpha z) = f_2 y$. By injectivity of f_2, $y = \alpha(z) \implies x = \beta(\alpha z) = 0$. Hence f_3 is injective.

(b) Let $x = \beta'(y) \in \beta' N_2$. By surjectivity of f_2, $y = f_2(z)$ for some $z \in M_2$. By commutitivity, $\beta'(y) = f_3(\beta z) \in f_3 \beta M_2 \implies \operatorname{Coker} f_3|_{\beta M_2} = 0$. Hence, it suffices to prove that $\operatorname{Coker} f_4|_{\gamma M_3} = 0$.

Now let $x = \gamma'(y)$ for some $y \in N_3$. By exactness $x \in \ker \delta'$. By surjectivity of f_4, there is $f_4(z) = x$ and by commutitivity $0 = \delta'(f_4 z) = f_5(\delta z)$. Since f_5 is injective, $\delta z = 0 \implies z \in \ker \delta = \gamma M_3$ where the last equality followed from the exactness of the top sequence. Hence $x \in f_4|_{\gamma M_3}$ and $\operatorname{Coker} f_4|_{\gamma M_3} = 0$. This proves the statement.

Remark 3. The diagram-chasing argument is more direct and arguably a better proof. I provided this proof as a practice on the application of the snake lemma.

Inverse limits

(16) Let I be a directed set and let $\{A_i\}_{i \in I}$ be a system of simple groups with surjective homomorphisms $f_{ij} : A_i \to A_j$ for every $j \leq i$. By the first isomorphism theorem we have $A_j = A_i / N$ for some nomral subgroup N of A_i. By simplicity of each A_i, it follows that either $A_i = 0$ or $A_i = A_j$ for all $j \leq i$ (or both). There are two types of such families of groups that could arise:

Case 1 : All $A_i = 0$. In this case, $\varprojlim A_i = 0$.

Case 2 : $A_i = 0$ for all $i < n$ and $A_i = A$ for all $n \leq i$ for some $n \in I$. In this case f_{ij} is an isomorphism for $j \geq n$ and the elements of $\varprojlim A_i$ have the form $(0, \dots, 0, x_n, f^{-1}_{n+1,n} x_n, \dots) \sim x_n \in A$. In other words, $\varprojlim A_i \cong A$ which is simple.

(17) (a) The set of positive integers is inherently directed by $<$. We define $f_{ij} = \pi_{ij} : A_i \to A_j$ by $\pi([x]_{p^i}) = [x]_{p^j}$. Let $k \geq j \geq i \in \mathbb{Z}^+$. Then we have $\pi_{ji} \circ \pi_{kj}(x) = [[x]_{p^j}]_{p^i} = [x]_{p^i} = \pi_{ki}(x)$ and trivially $\pi_{ii} = \text{id}$. Hence, $\mathbb{Z}/p^n\mathbb{Z}$ form a projective system under (π_{ij}).

Let $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ along with the morphisms $\psi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$. Consider the projection maps $\mu_i : \mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$. Then $\pi_{ij} \circ \mu_i(x) = \pi_{ij}([x]_{p^i}) = [x]_{p^j} = \mu_j(x)$. By universality of $\mathbb{Z}_p$, there is a unique morphism ϕ from $\mathbb{Z} \to \mathbb{Z}_p$ such that $\psi_i \circ \phi = \mu_i$. By definition, μ_i are surjective. Hence ψ_i is surjective.

We use induction to show that $\mathbb{Z}_p$ has no divisors of 0. Let $(x_1, x_2, \dots), (y_1, y_2, \dots)$ are non zero elements of $\mathbb{Z}_p$ such that their product is 0. This implies

$$x_i y_i = 0 \mod p^i \text{ for all } i.$$

For $i = 1$, then by the field properties of $\mathbb{Z}/p\mathbb{Z}$, either $x_1 = 0$ or $y_1 = 0$. With out loss of generality, let $x_1 = 0$.

Now suppose $x_i = 0 \mod p^i$ for all $i \leq n-1$ and $x_n \neq 0 \mod p^n$. Since $x_n y_n = 0 \mod p^n$ and $x_{n-1} = 0 \mod p^{n-1}$, $x_n = r_1 p^{n-1} \mod p^n$ for some r_1 not divisble by p. On the other hand, $y_i = s_1 p \mod p^n$ for $s_1 \neq 0 \mod p^{n-1}$ otherwise all $y_i = 0 \mod p^i$ for all $i \leq n$ and the induction step is fullfilled. Similary, we can deduce that

$$x_{2n-1} = r_1 p^{n-1} + \cdots + r_n p^{2n-1} \mod p^{2n-2} \quad \text{and} \quad y_{2n-1} = s_1 p + s_2 p^n + \cdots s_n p^{2n-2} \mod p^{2n-1}$$

Note tha we didn't assume $r_i, s_i \neq 0$ for $i \geq 2$. The product $x_{2n-2} y_{2n-2}$ reduces to $r_1 s_1 p^n \mod p^{2n-1}$. Since $x_{2n-1} y_{2n-1} = 0 \mod p^{2n-1}$, and $p \nmid r_1$ by assumptions $p^{n-1} \mid s_1$ and $y = 0 \mod p^n$ a contradiction. Thus $p \mid r_1$ and $x_n = 0 \mod p^n$.

Since $x_i = 0$ for all i by induction, it implies $(x_1, x_2, \dots) = 0$ and $\mathbb{Z}_p$ has no zero divisors itself.

Next we show that $\mathbb{Z}_p$ has a unique maxmial ideal generated by $p = (0, p, p, \dots)$. To show that the ideal $\mathfrak{a}$ generated by p is maximal consider the quotient group $\mathbb{Z}_p/\mathfrak{a}$. Since $\mathbb{Z}/p^j\mathbb{Z}/(0, p, \dots)\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$, the quotien group $\mathbb{Z}_p/\mathfrak{a}$ is (isomorphic to) a subgroup of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cdots$ that satisifes the projective system of morphisms $\pi'_{ij} = \text{id}$. Therefore, by surjectivity of ψ_i, $\mathbb{Z}_p/\mathfrak{a}$ is isomorphic to $\mathbb{F}_p$ which is a field and thus $\mathfrak{a}$ is maximal.

To see that $\mathfrak{a}$ is unique, note that if $(x_1, x_2, \dots) \in \mathfrak{b}$ for some proper ideal $\mathfrak{b}$ of $\mathbb{Z}_p$ and if $x_1 \neq 0$, then $x = (x_1, x_2, \dots)$ is a unit whose inverse is $(x_1^{p-2}, x_2^{p^2-p-1}, \dots)$. Therefore, any proper ideal of $\mathbb{Z}_p$ should have its first component of its elements equal to 0. This implies $x_i = px$ for all $i \geq 2$ which implies $\mathfrak{b} = 0 \mod \mathfrak{a}$ implying $\mathfrak{a}$ is unique.

Finally, to see that $\mathbb{Z}_p$ is a factorial ring, we show that it is a PID. Let $\mathfrak{b}$ be an ideal of $\mathbb{Z}_p$. Then every component of $\mathfrak{b}$ must be an ideal in its domain. But ideals in $\mathbb{Z}/p^n\mathbb{Z}$ are PIDs say with generators y_n (resp.). Then $\mathfrak{b}$ is generated by $(y_1, y_2, \dots)$. p is the only prime of $\mathbb{Z}_p$ because otherwise an ideal generated by another prime in PID is maximal which contradicts the uniqueness of $p\mathbb{Z}_p$.

(b) By the chinese remainder theorem, there is a homomorhism $k : \prod_p \mathbb{Z}_p \to \varprojlim \mathbb{Z}/a\mathbb{Z}$ such that a-th component of $y = k(x)$ is the solutions for equation $y_a = x_n \mod p^n$ for all $p^n \mid a$ and $p^{n+1} \nmid a, n \geq 1$. $y = 0$ iff $y_p = 0 \mod p$ for all p which is impossible. Hence k is injective. By the uniquness of the solution y_a given the projective system, k is also surjective. Hence k is an isomorphism.

(18) (a) Trivially, we define the action of $\varprojlim A_i$ on $\varprojlim M_i$ as the component-wise action of A_i on M_i. This action is well-defined by the commutitivity of the diagram. The module properties $\varprojlim M_i$ as a $\varprojlim A_i$-module follow directly from the module properties of M_i as an A_i-module.

(b) By section chapter I, §10, $T_p(M) = \varprojlim_i \ker p^n_M$ where $p_M : M \to M$ is the multiplication by p mapping from M onto itself. We can define the action of $\mathbb{Z}/p^{i+1}\mathbb{Z}$ on M by multiplication of $[x]_{p^{i+1}}$. We also note that for some $m \in M$, $[x]_{p^i} m = [x]_{p^i} m + k p^i_M m = [x]_{p^i} m + k p^i m = [x]_{p^{i+1}} m$. Therefore, if we take $A_i = \mathbb{Z}/p^i\mathbb{Z}$ in part (a) of this question, the diagram commutes and $T_p(M)$ is a module over $\varprojlim \mathbb{Z}/p^i\mathbb{Z} = \mathbb{Z}_p$.

(c) By (a) and (b) and the distrbutivity of mulriplication by p, $T_p(M \oplus N)$ is a $\mathbb{Z}_p$-module and so is $T_p(M) \oplus T_p(N)$. There is a homomorphism between the former and the later defined by $(m_1 + n_1, \dots) \mapsto (m_1, \dots) + (n_1, \dots)$.

Direct limits

(19) By definition, if $a_k = 0$ for all k, the $a \sim 0$ which implies $f_{ij}(a) = f_{kj}(0) = 0$ for all $j \geq n$ for some $n \in I$.

(20) Let $\{f_{(a,b),(c,d)}\}_{(a,b),(c,d) \in I \times I}$ be the given $I \times I$-indexed direct family of morphisms. Let $f_{ij}^k = f_{(k,i),(k,j)} : A_{ki} \to A_{kj}$ and $g_{ij}^k = f_{(i,k),(j,k)} : A_{ik} \to A_{jk}$. By definition $\{f_{ij}^k\}$ and $\{g_{ij}^k\}$ form a direct family of morphisms. Let $A^{(i)} = \lim_j A_{ij}$ and let $N^{(i)}$ be an ideal/normal subgroup generated by the elements

$$x_{jk} = (0, \dots, 0, x, \dots, 0, -f_{jk}^i(x), 0, \dots),$$

where x and $-f_{jk}(x)$ are the at the j-th and k-th components of x_{jk} resp. Let $[x]_i = x \mod N^i$. Define the map $\mu_{ij} : A^{(i)} \to A^{(j)}$ by

$$\mu_{ij}([x]_i) = [g_{ij}^k(x)]_j,$$

where $x \in A_{rk}$ for some r. Then $\mu_{ii}([x]_i) = [g_{ii}^k(x)]_i = [x]_i$ and for $i < m < j$

$$\begin{aligned} \mu_{ij}([x]_i) &= [g_{ij}^k(x)]_j \\ &= [g_{mj}^k \circ g_{im}^k(x)]_j \\ &= \mu_{mj}([g_{im}^k(x)]_m) \\ &= \mu_{mj} \circ \mu_{im}([x]_i). \end{aligned}$$

Hence $\{\mu_{ij}\}$ form a direct family of morphism and $\lim_i \lim_j A_{ij}$ exists. By symmetry $\lim_j \lim_i A_{ij}$ also exists.

Now suppose A is the group of infinite dimensional matrices $\{a_{ij}\}$ where $a_{ij} \in A_{ij}$ under component-wise group operation, and let N be the ideal generated by the matrices

$$X_{ijkl} = \begin{bmatrix} 0 & \dots & 0 & \dots & 0 & 0 & \dots \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots \\ 0 & \dots & x & \dots & 0 & 0 & \dots \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots \\ 0 & \dots & 0 & \dots & -f_{ij}^k(g_{ik}^l x) & 0 & \dots \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots \end{bmatrix}$$

where $i \leq j$ and $i \leq k$ and x is the (i,l)-th entry and $-f_{ij}^k(g_{ik}^l x) = -g_{ik}^l(f_{lj}^i x)$ is the (k,j)-th entry of X_{ijkl}. From the descrption above, it is clear that both direct limits are naturally isomorphic to A/N.

The case for inverse limits is also similar. Let $\{f_{(a,b),(c,d)}\}_{(a,b),(c,d) \in I \times I}$ be the given $I \times I$-indexed direct family of morphisms. Let $f_{ij}^k = f_{(k,i),(k,j)} : A_{ki} \to A_{kj}$ and $g_{ij}^k = f_{(i,k),(j,k)} : A_{ik} \to A_{jk}$ for all $j \leq i$. Let $A^{(i)} = \varprojlim_j A_{ij}$ with projections $\pi_j^{(i)} : A^{(i)} \to A_{ij}$, $(\dots, x_j, \dots) \mapsto x_j$. Then there are maps $\nu_{ijk} : A^{(i)} \to A_{kj}$ for some $k \leq i$ and all $j \in I$ defined by

$$\nu_{ijk}(x) = g_{ik}^j(\pi_j^{(i)}(x)).$$

By universality, there is a unique map $\nu_{ik} : A^{(i)} \to A^{(k)}$ for fixed i, k such that $\nu_{ijk} = \pi_j^{(k)} \circ \nu_{ik}$. We see that these maps are defined as

$$\nu_{ik}(x_0, x_1, \dots) \mapsto (g_{ik}^0(x_0), g_{ik}^1(x_1), \dots).$$

Since, g_{ik}^j form a directed family of morphisms, $A^{(i)}$ form a directed family and thus posses an inverse limit. By symmetry, $\varprojlim_i \varprojlim_j A_{ij}$ also exists. For fixed $i \leq k, j \leq l$, since $g_{ki}^j \circ f_{lj}^k = f_{lj}^i \circ g_{ki}^l$, the two inverse limits are naturally isomorphic.

(21) The u_i and v_i commute with the direct family of morphisms of M_i', M_i and M_i, M_i'' resp., we can define the maps between limits unambiguously as maps that send representative $[x] \mapsto [u_i(x)]$ and $[y] \mapsto [v_i(y)]$ where $x \in M_i'$ and $y \in M_i$. Let

$$0 \to \lim M' \xrightarrow{u} \lim M \xrightarrow{v} \lim M'' \to 0.$$

and let f_{ij}, g_{ij} and h_{ij} be the directed family of morphisms of M_i', M_i and M_i'' resp. If $[x] \in \ker u$, the $g_{ij}(u_i(x)) = 0$ for some i, j. By commutitivity, this implies $u_j(f_{ij}(x)) = 0$. By exactness, u_j is injective and $f_{ij}(x) = 0 \implies [x] = 0$. Thus u is injective.

Similarly, if $[x] \in \ker v$, then $h_{ij}(v_i(x)) = 0 = v_j(g_{ij}(x))$ by commutitivity. Since $\ker v_j = \operatorname{Im} u_j$, $g_{ij}(x) = u_j(y)$ for some $y \in M_j'$. It directly follows that $u([y]) = [x]$ and thus $[x] \in \operatorname{Im} u \implies \ker v \subseteq \operatorname{Im} u$. For the reverse inclusion, let $[x] = u([y])$. Then $g_{kj}(x) = u_j(f_{ij}(y))$ for some $i, k \leq j$. By exactness, $v_j(g_{kj}(x)) = 0$ or $[x] \in \ker v$.

Finally, $[x] \in \lim M''$, then $h_{ij}(x) = v_j(y)$ for some $y \in M_j''$ by surjectivity of v_j. It immediately follows $v([y]) = [x]$, proving the direct limit preserves the exactness of a sequence

(22) All constructed maps are homomorphisms inherently.

(a) Let $f \in \operatorname{Hom}(\bigoplus M_i, N)$ and let $f_i = f|_{M_i} : M_i \to N, x \mapsto f(x)$. By definition, $f = (f_i)$ and hence $f \in \prod_i \operatorname{hom}(M_i, N)$. Now, let $f_i \in \operatorname{Hom}(M_i, N)$. Define $f : \bigoplus M_i \to N$ by $f((x_i)) = \sum_i f_i(x_i)$. Therefore $\prod_i \operatorname{Hom}(M_i, N) \subseteq \operatorname{Hom}(\bigoplus M_i, N)$.

(b) Let $f \in \operatorname{Hom}(N, \prod M_i)$ and let $\pi_j : \prod M_i \to M_j$ projection map to the j-th component. By definition, $f = (f \circ \pi_i)_i \in \prod_i \operatorname{Hom}(M_i, N)$, implying the forward inclusion. Let $f_i : N \to M_i$. Similarly to the previous subproblem, define $f(x) = (f_i(x)) \in \operatorname{Hom}(N, \prod_i M_i)$.

(23) Let f_{ij} be the directed family of morphism of $\{M_i\}$. Then the induced morphism $\phi_{ij} : g \to f_{ij} \circ g$ form a directed family morphisms for $\operatorname{Hom}(N, M_i)$ because

$$\phi_{ii}(g) = f_{ii} \circ g = \mathrm{id} \circ g = g \quad \text{and}$$
$$\phi_{jk}(g) = f_{jk} \circ g = f_{ik} \circ f_{ji} \circ g = f_{ik} \circ \phi_{ji}(g) = \phi_{ik} \circ \phi_{ji}(g), k \leq i \leq j.$$

Hence, the inverse limit $\varprojlim_i \operatorname{Hom}(N, M_i)$ exists. Let $\pi_j : \varprojlim M_i \to M_j$ be the natural projection map to the j-th component.

If $(g_i) \in \varprojlim \operatorname{Hom}(N, M_i)$, then $g_i = \phi_{ji}(g_j) = f_{ij} \circ g_j$ for all $j \geq i$. This is isomorphic to a morphism in $\operatorname{Hom}(N, \varprojlim M_i)$ naturally as $(g_i)(x)$ satisfies $g_i(x) = f_{ij}(g_j(x))$ making the image of (g_i) a subset of $\varprojlim M_i$. Thus $\varprojlim_i \operatorname{Hom}(N, M_i) \subseteq \operatorname{Hom}(N, \varprojlim_i M_i)$.

Similarly, for any $f \in \operatorname{Hom}(N, \varprojlim_i M_i)$, define $f_i : N \to M_i$ by $f_i(x) = \pi_j(f(x))$. Then $(f_i)_i \in \varprojlim_i \operatorname{Hom}(N, M_i)$.

(24) Let index set I be the set of all fintely generated submodules of M orderd by inclusion. For $A, B \in I$, $\{f_{AB} : A \to B\}$ be a family of morphisms indexed by I defined by $f_{AB} = i_{AB}$, the canonical inclusion of A into B. Clearly, this family is directed and admits a direct limit. Since $M = \bigsqcup_{A \in I} A / \sim$, We can express M as a direct limit of fintely generated submodules.

(25) Let M be a fintely-generated module. Then there exists a free module F and a (potentially infinitly-generated) module of relations N such that $M = F/N$. Let $I(M)$ be the set of fintely-generated ideals of submodule of relation N of M ordered by inclusion. By the previous problem, there is a directed family of finitely-generated modules $N_A = A$ and a directed family of morphisms f_{AB} indexed by $I(M)$ admitting N as a direct limit. In other words, $M = F/\lim_A A$ where the limit is taken over all finitely-generated submodules of the relation module N.

To proceed, we prove that $F/\lim_A A = \lim_A F/A$. In fact, consider the exact sequence

$$0 \to A \hookrightarrow F \overset{\bmod A}{\to} F/A \to 0.$$

Taking, $g_{AB} = \mathrm{id}_F$ and $h_{AB} = x + A \mapsto x + B$ in the proof of exercise (21), we get the exact sequence

$$0 \to \lim_A A \hookrightarrow F \to \lim_A F/A \to 0,$$

which proves the assertion $M = F/\lim_A A = \lim_A F/A$. Since F/A is fintely-presented module, the statement is proved for M finitely-generated.

If M is not finitely-generated, then by problem (24),

$$M = \lim_B B,$$

where the limit is taken over all fintely-generated submodules of M. We now define the index set

$$J = \bigcup_{\substack{B \subset M \\ B \text{ fintely-generated}}} \{(B, A) : A \in I(B)\}$$

using the ordering $(A, B) \leq (C, D)$ if and only if $A \subseteq C$ or $A = B$ and $B \leq D$. The directed family of morphisms $f_{A'B'} : A' \to B'$ indexed by $I(M)$ associated with the direct limit M, and the directed family of morphisms between finitely-presented modules $g^C_{AB} : A \to B$ for a fixed finitely-generated module C indexed by $I(C)$ naturally induce a directed family of finitely-presented submodules of the free module F directed by the index set J, with direct limit M.

(26) Let $(f_i) \in \lim \operatorname{Hom}(E, M_i)$ with the direct family of morphisms induced by $f_{ij} : M_i \to M_j$. Since $f_j = f_{ij} \circ f_i$, we can define (naturally) a map $\phi : \lim_i \operatorname{Hom}(E, M_i) \to \operatorname{Hom}(E, \lim M_i)$ defined by

$$\phi((f_i)) = e \mapsto (f_i(e)).$$

Now let $(f_i) \in \ker \phi$, i.e., $(f_i(e)) = [0]$ for all $e \in E$. If E is finitely generated, say by $(x_1, \ldots, x_m)$, then there is a $N \in I$ such that $f_i(x_j) = 0$ for all $i \geq N$ and all j. This implies $f_i = 0$ for all $i \geq N$ which implies $(f_i) = [0]$.

For the rest of the statement, first let $E = R^n$ for a ring R. Then we have $\operatorname{Hom}(R^n, \lim M_i) = \operatorname{Hom}(R, \lim M_i)^n$ and $\lim \operatorname{Hom}(R^n, M_i) = \lim \operatorname{Hom}(R, M_i)^n = (\lim \operatorname{Hom}(R, M_i))^n$. Thus, it suffices to show that ϕ is isomorphsim for $E = R$.

Let $g \in \operatorname{Hom}(R, \lim M_i)$ such that $g(1) = (e_i) \in \lim M_i$. Defining $f_i(1) = e_i$, and $f = (f_i) \in \lim \operatorname{Hom}(R, M_i)$, we see that ϕ is surjective, and thus isomorphism.

Finally, when E is finitely presented, let $\psi_k : \lim \operatorname{Hom}(F_k, M_i)$. Applying the snake lemma, we have the exact sequence

$$0 = \ker \psi_1 \to \operatorname{Coker} \phi \to \operatorname{Coker} \psi_0 = 0.$$

Hence $\operatorname{Coker} \phi = 0$, making it isomorphism for this case.

Graded Algebras

(27) Let $x \in A_i$ and $y \in A_j$ for some i, j. Let $(\cdot)$ be the binear operator associated with the $k-$algebra A. Define the natural product $(*)$

$$(x + A_{i-1}) * (y + A_{j-1}) = (x \cdot y + A_{i+j-1})$$

By this product, $\operatorname{gr}_i(A)\operatorname{gr}_j(A) \subseteq \operatorname{gr}_{i+j}(A)$.

(28) (a) Define

$$\operatorname{gr}_i(L)(x + A_{i-1}) = L(x) + B_{i-1}.$$

Since $L(A_i) \subseteq B_i$, $\operatorname{gr}_i(L)(A_i) \subseteq B_i/B_{i-1} = \operatorname{gr}_i(B)$. Similarly,

$$\begin{aligned} \operatorname{gr}_i(L)\big((c + A_{-1}) * (a + A_{i-1})\big) &= \operatorname{gr}_i(L)\big(ca + A_{i-1}\big) \\ &= L(ca) + B_{i-1} \\ &= L(c)\, L(a) + B_{i-1} \\ &= (L(c) + B_{-1}) * (L(a) + B_{i-1}) \\ &= \operatorname{gr}_0(L)(c + A_{-1}) * \operatorname{gr}_i(L)(a + A_{i-1})\,. \end{aligned}$$

(b) $\hookrightarrow$ Let $x \in A$ such that $L(x) = 0$. Let i be the smallest i such that $x \in A_i$. By definition, $\operatorname{gr}_i(L)(x + A_{i-1}) = L(x) + B_{i-1} = 0 + B_{i-1} \implies x \in A_{i-1}$ a contradiction unless $x \in A_{-1} = \{0\}$.

$\twoheadrightarrow$ Let $x \in B$. Then there is smallest i such that $x \in B_i$ and consequently, $x + B_{i-1} \in \operatorname{gr}_i B$. By surjectivness of $\operatorname{gr}_i(L)$, there is y_i such that $x - L(y_i) \in B_{i-1}$. Applying this procedure i more times, we get $x - \sum_{j=0}^{i} L(y_j) \in B_{-1} = \{0\}$. This implies $x = \sum_{j=0}^{i} L(y_j) = L\big(\sum_{j=0}^{i} y_j\big)$ showing L is surjective.

(29) (a) The given definition of $\mathfrak{n}_c$ is equivalent to

$$\mathfrak{n}_c := \{X = [x_{ij}] \in \mathfrak{n} : x_{ij} = 0 \text{ if } j - i < n - c\} \quad \text{for } 0 \leq c \leq n-1.$$

By the trivial action of component-wise addition and scalar multiplicaiton $\mathfrak{n}_c$ is a vector space over the field k. What remains is to show the standard matrix multiplication is closed under $\mathfrak{n}_c$ as it is bi-linear by definition. To see that consider the multiplication of two matrices $X = [x_{ij}], Y = [y_{ij}] \in \mathfrak{n}_c$, XY is given by the $[\sum_k x_{ik}y_{kj}]$. For an entry, $\sum_k x_{ik}y_{kj} \neq 0$, we require, $k - i \geq n - c$ and $j - k \geq n - c$ or in other words, $j - c \leq n - (2c - n)$. Hence $XY \in \mathfrak{n}_{2c-n} \subseteq \mathfrak{n}_c$. Since $2c - n < c$ for all c, $X^{c+1} = 0$.

(b) Associativity follows from associativity of standard matrix mutliplication. Since $0 \in \mathfrak{n}$, $I \in U$. Finally, for every $I + X$, by nilpotence $I + Y = \prod_{k \geq 0}(I - X^{2k})$ is a unique inverse of $I + X$ hence U satisfies all the group properties.

(c) Let $\exp(X) = I + X + \frac{1}{2!}X^2 + \cdots$ and $\log(I + Y) = Y - \frac{1}{2}Y^2 + \frac{1}{3}Y^3 - \cdots$. Injectivity of $\exp$ directly follows from the definition.

Let $Z = \exp(\log(I + Y))$, then we have

$$Z = I + \sum_{n=1}^{\infty} \frac{1}{n!} Y^n \sum_{i_1 + \cdots + i_n = k} \frac{(-1)^{k+n}}{i_1 \cdots i_n}.$$

The RHS famously evaluates to $I + Y$. Hence, $\log$ is a well-defined inverse of $\exp$ making it a bijection.