

# Lang's Algebra Chapter 3 Solutions

Amanuel Tewodros

August 23, 2025

- (1) By the second isomorphism theorem, we have

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

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

- (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  $\mathfrak{a}M \subseteq M$  by  $R$ -closure property of  $\mathfrak{a}$ . It immediately follows that  $\mathfrak{a}M = \bigoplus_i \mathfrak{a}x_i$ . By linear independence of  $x_i$ ,  $(\sum_i r_i x_i) \bmod \mathfrak{a}x_j = (r_j \bmod \mathfrak{a})x_j + \sum_{i \neq j} r_i x_i$ . Therefore,  $M/\mathfrak{a}M = \bigoplus_i \mathfrak{a}x_i/\mathfrak{a}x_i$ . By the isomorphism  $x_i \mapsto 1_A \mapsto (x_i + \mathfrak{a}x_i)$ ,  $\mathfrak{a}x_i/\mathfrak{a}x_i \cong A/\mathfrak{a} \cong A/\mathfrak{a}(x_i + \mathfrak{a}x_i)$ .  $\square$

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  $\{y_1, \dots, y_m\} \subseteq k$ ,  $\{f_1, f_2, \dots, f_m\} \subseteq R$  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  $\varphi$  such that  $g \circ \varphi = \text{id}$ . By the injectiveness of the composition,  $\text{Im } \varphi \cap \ker g = \{0\}$ . But by exactness,  $\ker g = \text{Im } f$ . We can unambiguously define  $\psi(u)$  to be the inverse image of  $f^{-1}(u')$  where  $u' \equiv u \bmod \text{Im } \varphi$  and  $u' = f(x)$  for some  $x \in M'$  because if  $f(x) = f(y) \bmod \text{Im } \varphi$ ,  $f(x - y) \in \text{Im } \varphi$  and by injectivity of  $f$ ,  $x = y$ . Since  $M/\text{Im } f \cong M'' = \text{Im } \varphi$ ,  $\psi$  is defined in all of  $M$ . Similarly, if the second statement is true,  $\ker \psi \cap \text{Im } f = \{0\}$  because  $\psi \circ f$  is injective. By exactness,  $\text{Im } f = \ker g$ . We can then define  $\varphi(u) = u'$  where  $u' = y \bmod \ker \psi$  and  $g(y) = u$  for some  $y$ .  $\varphi$  is well-defined because if  $g(y_1) = g(y_2)$  for  $y_1 \neq y_2$ , then  $y_1 \neq y_2 \bmod \ker \varphi$ .

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

- (b) First, we note that  $\varphi_i$  is injective because otherwise the composition  $\psi_i \circ \varphi_i$  wouldn't be injective, 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

$$\bigoplus_{i=1}^n E'_i \subseteq E.$$

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  $x = x_1 + \dots + x_m$  where  $x_i \in E'_i$ . The map defined 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  $v'_m = a_1 v_1 + \dots + a_m v_m$ . Since  $a_m \neq 0$ ,  $v'_m$ , and by the assumption that  $\{v_i\}$  is linearly independent over  $\mathbb{R}$ , the set  $\{v_1, \dots, v_{m-1}, v'_m\}$  is linearly independent 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  $a_1 = \dots = a_{m-1} = 0$ .

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  $a_m \mid a$ . Therefore  $A/A_0 = \mathbb{Z}v'_m$ .

- (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  $\pi : \mathbb{Z}\langle S \rangle \rightarrow \mathbb{Z}\langle G \cdot w \rangle$ . 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  $\sigma \in G$ ,  $\sigma \bar{y}_{gw} = \bar{y}_{\sigma gw}$ . 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 independent 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

$$\text{SN-1 } |v| \geq 0$$

$$\text{SN-2 } |nv| = |n||v|$$

$$\text{SN-3 } |u+v| \leq |u| + |v|$$

- (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  $N = \langle v_1, \dots, v_r \rangle$ . 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

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

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 necessarily 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 an element  $s \in S$  that satisfy the equation  $s(s_2 m_1 - s_1 m_2) = 0$ . 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

$$\begin{aligned}
 \frac{a_1}{b_1} \cdot \left( \frac{m_1}{s_1} + \frac{m_2}{s_2} \right) &= \frac{a_1}{b_1} \cdot \left( \frac{m_1 s_2 + m_2 s_1}{s_1 s_2} \right) \\
 &= \frac{a_1 b_1}{b_1 b_1} \cdot \left( \frac{m_1 s_2 + m_2 s_1}{s_1 s_2} \right) \\
 &= \frac{a_1 b_1 s_2 m_1 + a_1 b_1 s_1 m_2}{b_1 s_1 b_1 s_2} \\
 &= \frac{a_1 m_1}{b_1 s_1} + \frac{a_1 m_2}{b_1 s_2} \\
 &= \frac{a_1}{b_1} \cdot \frac{m_1}{s_1} + \frac{a_1}{b_1} \cdot \frac{m_2}{s_2}.
 \end{aligned}$$

and

$$\begin{aligned}
\left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) \cdot \frac{m_1}{s_1} &= \left(\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}\right) \cdot \frac{m_1}{s_1} \\
&= \left(\frac{a_1 b_2 + a_2 b_1}{a_1 a_2}\right) \cdot \frac{m_1 s_1}{s_1 s_1} \\
&= \frac{a_1 b_2 m_1 s_1 + a_2 b_1 m_1 s_1}{s_1 b_1 s_2 b_2} \\
&= \frac{a_1 m_1}{b_1 s_1} + \frac{a_2 m_1}{b_2 s_1} \\
&= \frac{a_1}{b_1} \cdot \frac{m_1}{s_1} + \frac{a_2}{b_2} \cdot \frac{m_1}{s_1}.
\end{aligned}$$

(b) Let

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

be exact. Then we have the induced sequence,

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

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  $\text{Im } f = \ker f''$ . Evaluating  $g''$  on  $\text{Im } g$ ,  $g''(g(m/s)) = g''(f(m)/s) = f''(f(m))/s = 0/s = 0$ . This shows  $\text{Im } g \subseteq \ker g''$ . Let  $g''(x/s) = f''(x)/s = 0$ . This implies  $f''(x) = 0$  for some  $x$ . By exactness,  $\ker f \subseteq \text{Im } f''$ , implying  $x = f(y)$  for some  $y \in M'$ . This proves  $\text{Im } g \supseteq \ker g''$ .

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

(b) Let  $f : M'' \rightarrow M$  and  $\hat{f} : M''_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}}$ . 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  $0 \rightarrow M'_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} \rightarrow M''_{\mathfrak{p}}$  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  $g f(x) = n$ . 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  $\text{Im } f \subseteq \ker g$ . 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  $r_{\mathfrak{p}}y \in \text{Im } f$  for all prime  $\mathfrak{p}$ . Since  $M/\text{Im } f$  is also an  $A$ -module, it implies  $r_{\mathfrak{p}}(x + \text{Im } f) = 0$  for all  $\mathfrak{p}$  implying  $x + \text{Im } f = 0 + \text{Im } f$  or in other words,  $x \in \text{Im } f$ . This proves  $\text{Im } f = \ker g$ .

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,  $y \in \text{Im } g$ , proving the exactness of the first sequence.

(c) Let  $\phi : M \rightarrow M_{\mathfrak{p}}$  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

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

such that

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

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

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

where  $l_{\mathfrak{p}} : M \rightarrow M_{\mathfrak{p}}$  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

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

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

- (12) (a) Define a map  $\mathfrak{a} \oplus \mathfrak{b} \rightarrow \mathfrak{o}$  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 inclusion 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  $\mathfrak{a}\mathfrak{b} \rightarrow c\mathfrak{a}\mathfrak{b}$  is bijective, and  $\mathfrak{o}$  is finitely 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  $\mathfrak{o}$ -linearity  $f$  and by commutativity 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 extension 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 additive subgroup of  $\mathfrak{o}$ . For  $a, b \in \mathfrak{a}$ , by properties of  $\mathfrak{o}$ -homomorphism  $\phi$ ,  $\phi(\phi(a)b) = \phi(a)\phi(b) \in \phi(\mathfrak{a})$ . Finally, for  $c \in \mathfrak{o}$ ,  $c\phi(\mathfrak{a}) = \phi(c\mathfrak{a}) \subseteq \phi(\mathfrak{a})$  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-unique, a contradiction in Dedekind domains.

(13) (a)