Lang's Algebra Chapter 3 Solutions

Amanuel Tewodros

July 22, 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 $x_i \mapsto 1_A \mapsto (x_i + \mathfrak{a}x_i)$, $Ax_i/\mathfrak{a}x_i \cong A/\mathfrak{a} \cong A/\mathfrak{a}(x_i + \mathfrak{a}x_i)$. □

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 $1_R = k_1x_1 + \dots k_mx_m$ 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, $\mathrm{Im}\ \varphi \cap \ker g = \{0\}$. But by exactness, $\ker g = \mathrm{Im}\ f$. We can unambiguously define $\psi(u)$ to be the inverse image of $f^{-1}(u')$ where $u' \equiv u \mod \mathrm{Im}\ \varphi$ and $u' = f(x)$ for some $x \in M'$ because if $f(x) = f(y) \mod \mathrm{Im}\ \varphi$, $f(x-y) \in \mathrm{Im}\ \varphi$ and by injectivity of f, $x = y$.Since $M/\mathrm{Im}\ f \cong M'' = \mathrm{Im}\ \varphi, \psi$ is defined in all of M. Similarly, if the second statement is true, $\ker \psi \cap \mathrm{Im}\ f = \{0\}$ because $\psi \circ f$ is injective. By exactness, $\mathrm{Im}\ f = \ker g$. 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 $x \in M$. $x - \varphi(u) \in \mathrm{Im}\ f$ for exactly one u by the argument mentioned previously. Thus we can express $x = r + s$ where $r = \varphi(u) \in \mathrm{Im}\ \varphi$ and $s = x - \varphi(u) \in \mathrm{Im}\ f$. This implies $M = \mathrm{Im}\ f \oplus \mathrm{Im}\ \varphi$. By bijectivness of $g \circ \varphi$, $\mathrm{Im}\ \varphi \cong M''$. By contrast, if $M = \mathrm{Im}\ f \oplus N$ 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 $N \cap \mathrm{Im}\ f = \{0\}$. Since $g \circ t^{-1} = \mathrm{id}$, the sequence splits.

Finally, we complete the details of proposition 3.2. We have just shown $M = \mathrm{Im}\ f \circ \mathrm{Im}\ \varphi$. By exactness, $\mathrm{Im}\ f = \ker g$. Also, $\mathrm{Im}\ f \cong M'$ and $\mathrm{Im}\ \varphi \cong M''$ 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 $\ker \psi \cap \mathrm{Im}\ f = \{0\}$ by bijectivness of $\psi \circ f$. This shows $M = \mathrm{Im}\ f \oplus \ker \psi$.

(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 $E_i' = \mathrm{Im}\ \varphi_i$ of E that is isomorphic to E_i. Moreover, if $c \in \mathrm{Im}\ \varphi_i \cap \mathrm{Im}\ \varphi_j$ 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 $x = x_1 + \cdots + x_m$ 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 $\sigma \in G$, $\sigma\bar{y}_{gw} = \bar{y}_{\sigma gw}$. 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 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

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

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

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

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 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.