Lang's Algebra Chapter 3 Solutions

Amanuel Tewodros

July 14, 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 $1_R = k_1x_1 + \dots k_mx_m$ 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 $g \circ \varphi = \text{id}$. By the injectivness 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 $u' \equiv u \mod \text{Im } \varphi$ and $u' = f(x)$ for some $x \in M'$ because if $f(x) = f(y) \mod \text{Im } \varphi$, $f(x-y) \in \text{Im } \varphi$ 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 $u' = y \mod \ker \psi$ 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 $x \in M$. $x - \varphi(u) \in \text{Im } f$ 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 bijectivness of $g \circ \varphi$, $\text{Im } \varphi \cong M''$. By contrast, if $M = \text{Im } f \oplus N$ for some N, with isomorphism $t : N \to M''$. 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 $N \cap \text{Im } f = \{0\}$. 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 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

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

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

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