Commutative Algebra Homework 4

Michael Nelson

Problem 1

Exercise 1. Let R be an integral domain. Show that the following conditions are equivalent.

1. Every R-module is free.
2. Every R-module is projective.
3. Every R-module is injective.
4. R is a field.

Solution 1. (1 implies 2) Suppose every R-module is free and let P be any R-module. We want to show that P is projective. Let $\varphi\colon M \to N$ be a surjective R-module homomorphism and let $\psi\colon P \to N$ be any R-module homomorphism. Let $\{e_\lambda\}_{\lambda\in\Lambda}$ be a basis for P as a free R-module. For each $\lambda \in \Lambda$, choose $u_\lambda \in M$ such that $\varphi(u_\lambda) = \psi(e_\lambda)$ (such a choice is possible as φ is surjective). Define $\widetilde{\psi}\colon P \to M$ to be the unique R-module homomorphism such that $\widetilde{\psi}(e_\lambda) = u_\lambda$ for all $\lambda \in \Lambda$. Then for all $\lambda \in \Lambda$ we have

$$\begin{aligned}(\varphi \circ \widetilde{\psi})(e_\lambda) &= \varphi(\widetilde{\psi}(e_\lambda)) \\ &= \varphi(u_\lambda) \\ &= \psi(e_\lambda).\end{aligned}$$

It follows that $\varphi \circ \widetilde{\psi} = \psi$. Therefore P is projective. Since P was arbitrary, it follows that every R-module is projective.

(2 implies 3) Suppose every R-module is projective. Let E be an R-module and let

$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{1}$$

be a short exact sequence of R-modules. Then since N is a projective R-module, the short exact sequence (5) splits. It follows that E is an injective R-module (see Appendix for equivalent criteria for an R-module to be injective). Since E was arbitrary, it follows that every R-module is injective.

(3 implies 4) Suppose every R-module is injective. We want to show R is a field. Assume for a contradiction that R is not a field. Choose a nonzero nonunit element in R, say $x \in R$. Then the multiplication map $\mathrm{m}_x\colon R \to R$, given by

$$\mathrm{m}_x(a) = ax$$

for all $a \in R$, splits since it is an injective map (as R is a domain) and since R is injective as an R-module over itself. Thus there exists an R-linear map $\varphi\colon R \to R$ such that $\varphi \mathrm{m}_x = 1_R$. Note that φ is completely determined by where it maps 1. Indeed, if $\varphi(1) = y$, then R-linearity of φ implies $\varphi = \mathrm{m}_y$. Thus we have $\mathrm{m}_y\mathrm{m}_x = 1_R$. In particular, $yx = 1$, which implies x is a unit. This is a contradiction. Thus R must be a field.

(4 implies 1) Suppose R is a field. Then an R-module is just an R-vector space. A standard argument using Zorn's Lemma tells us that every vector space has a basis (see Appendix for proof), and hence every vector space is free.

Problem 2

Exercise 2. Let P and Q be projective R-modules. Show that $P \otimes_R Q$ is projective also.

Solution 2. It suffices to show that $\mathrm{Hom}_R(P \otimes_R Q, -)$ is exact. Let

$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence of R-modules. Then since Q is projective, the induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(Q, M_1) \longrightarrow \mathrm{Hom}_R(Q, M_2) \longrightarrow \mathrm{Hom}_R(Q, M_3) \longrightarrow 0$$

is exact. Then since P is projective, the induced sequence

$$0 \to \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_1)) \to \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_2)) \to \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_3)) \to 0$$

is exact. By tensor-hom adjointness, we have a commutative diagram[1]

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_1)) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_2)) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, M_3)) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_1) \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_2) \arrow[r] & \mathrm{Hom}_R(P \otimes_R Q, M_3) \arrow[r] & 0
\end{tikzcd}$$

where the columns are isomorphisms and where the top row is exact. It follows from the 3×3 lemma that the bottom row is exact too.

Problem 3

Exercise 3. Prove that every overring of a valuation domain is a localization.

Solution 3. Let R be a valuation domain and let A be an overring of R. We will show A is a localization of R. Let $S = \{y \in R \mid 1/y \in A\}$. Observe that S is a multiplicatively closed subset of R since $1 \in S$ and if $y_1, y_2 \in S$, then $y_1 y_2 \in S$ since

$$1/(y_1 y_2) = (1/y_1)(1/y_2) \in A.$$

Since $R \subseteq A$, we see that any $x/y \in R_S$ is an element of A, thus $R_S \subseteq A$. To show the reverse inclusion, let $x/y \in A$ where $x, y \in R \backslash \{0\}$. Since R is a valuation domain, we have either $x \mid y$ or $y \mid x$. If $x \mid y$, then $ax = y$ for some $a \in R$. In this case,

$$\frac{x}{y} = \frac{x}{ax} = \frac{1}{a}.$$

In particular, we see that $a \in S$. Thus $x/y = 1/a \in R_S$. On the other hand, if $y \mid x$, then $x = by$ for some $b \in R$. In this case,

$$\frac{x}{y} = \frac{by}{y} = \frac{b}{1}.$$

Clearly $b/1 \in R_S$, thus $x/y = b/1 \in R_S$. In either case, we see that $x/y \in R_S$. It follows that $A \subseteq R_S$.

Problem 4

Definition 0.1. We say that the integral domain R is a **Prüfer** domain if $R_{\mathfrak{p}}$ is a valuation domain for all prime ideals $\mathfrak{p}$ in R. They are the "global" analog of valuation domains.

Exercise 4. Show that any overring of a Prüfer domain is a Prüfer domain.

Solution 4. Let R be a Prüfer domain and let A be an overring of R. We will show A is a Prüfer domain. Let $\mathfrak{q}$ be any prime ideal in A. Then $\mathfrak{p} = R \cap \mathfrak{q}$ is a prime ideal in R. Since R is a Prüfer domain, we see that $R_{\mathfrak{p}}$ is a valuation domain. Furthermore, note that $A_{\mathfrak{q}}$ is an overring of $R_{\mathfrak{p}}$. Indeed, if $x/y \in R_{\mathfrak{p}}$, then $x \in R$ implies $x \in A$, and $y \notin \mathfrak{p}$ implies $y \notin \mathfrak{q}$, thus $x/y \in A_{\mathfrak{q}}$. Thus by problem 3, we see that $A_{\mathfrak{q}}$ is a localization of $R_{\mathfrak{p}}$. A localization of a valuation domain is a valuation domain (see Appendix for proof of this), thus $A_{\mathfrak{q}}$ is a valuation domain. Since $\mathfrak{q}$ was arbitrary, it follows that A is a Prüfer domain.

[1] Note how we need naturality in the third argument to get a commutative diagram.

Problem 5

Exercise 5. Show that if v is a valuation on K then the set of elements with nonnegative value (and 0) form a valuation domain.

Solution 5. Let $(\Gamma, \geq)$ be a totally ordered abelian group and let $v\colon K^\times \to \Gamma$ be a valuation on K. Set $A = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$. We will show A is a valuation domain. Suppose $a, b \in A \backslash \{0\}$, and without loss of generality, assume that $v(b) \geq v(a)$. Then

$$\begin{aligned} v(ba^{-1}) &= v(b) - v(a) \\ &\geq 0 \end{aligned}$$

implies $ba^{-1} \in A$. In particular, this implies $a \mid b$. It follows that A is a valuation domain.

Problem 6

Definition 0.2. Let $(A_1, \leq_1)$ and $(A_2, \leq_2)$ be totally ordered abelian groups. We order the group $A_1 \oplus A_2$ by declaring $(a_1, a_2) \leq (a_1', a_2')$ if $a_1 \leq_1 a_1'$ or $a_1 = a_1'$ and $a_2 \leq_2 a_2'$. This ordering is called the **lexicographical ordering**.

Remark 1. Note that lexicographical ordering is translate invariant in the sense that if $(a_1, a_2) \leq (a_1', a_2')$ implies $(a_1 + a_1'', a_2 + a_2'') \leq (a_1' + a_1'', a_2' + a_2'')$.

Exercise 6. Construct valuation domains with value groups $\mathbb{Z} \oplus \mathbb{R}$ and $\mathbb{R} \oplus \mathbb{Z}$ ordered lexicographically.

Solution 6. We first construct a valuation domain with value group $\mathbb{R} \oplus \mathbb{Z}$. Let K be any field and define $K[\mathbb{R} \oplus \mathbb{Z}]$ to be the set of elements of the form

$$\sum_{i=0}^{\infty} a_{\beta_i, n_i} X^{\beta_i} Y^{n_i} \tag{2}$$

where $a_{\beta_i, n_i} \in K$ and where $\{(\beta_i, n_i)\}_{i=0}^{\infty}$ is a linearly ordered subset of $\mathbb{R} \oplus \mathbb{Z}$ where we are viewing $\mathbb{R} \oplus \mathbb{Z}$ as a totally ordered abelian group with respect to the lexicographical ordering. To simplify our notation, we sometimes omit the subscripts in the sum (2) and simply write $\sum a_{\beta,n} X^\beta Y^n$ with the understanding that the sum is over a linearly ordered subset of $\mathbb{R} \oplus \mathbb{Z}$ with a least element. Addition in $K[\mathbb{R} \oplus \mathbb{Z}]$ is defined pointwise

$$\sum a_{\beta,n} X^\beta Y^n + \sum b_{\beta,n} X^\beta Y^n = \sum (a_{\beta,n} + b_{\beta,n}) X^\beta Y^n,$$

and multiplication in $K[\mathbb{R} \oplus \mathbb{Z}]$ is defined by

$$\left(\sum a_{\beta,n} X^\beta Y^n\right) \left(\sum b_{\beta,n} X^\beta Y^n\right) = \sum_{\beta,n} \left(\sum_{\substack{\beta' + \beta'' = \beta \\ n' + n'' = n}} a_{\beta',n'} b_{\beta'',n''} \right) X^\beta Y^n. \tag{3}$$

We simplify our notation again by omitting the subscpricts in the coefficient on the right hand side of (3) and simply write $\sum a_{\beta',n'} b_{\beta'',n''}$ with the understanding that the sum is over all $\beta' + \beta'' = \beta$ and $n' + n'' = n$. Alternatively, we can express multiplication in $K[\mathbb{R} \oplus \mathbb{Z}]$ as

$$\left(\sum_{i=0}^{\infty} a_{\alpha_i, m_i} X^{\alpha_i} Y^{m_i}\right) \left(\sum_{j=0}^{\infty} b_{\beta_j, n_j} X^{\beta_j} Y^{n_j}\right) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_{\alpha_i, m_i} b_{\beta_{k-i}, n_{k-i}}\right) X^{\beta_k} Y^{n_k}.$$

It is straightforward to check that addition and multiplication defined in this way give $K[\mathbb{R} \oplus \mathbb{Z}]$ the structure of a ring. The proof is nearly identical to the power series case. For instance, we have left distributivity of addition with respect to multiplication:

$$\begin{aligned}
\left(\sum a_{\beta,n}X^{\beta}Y^{n}\right)\left(\sum b_{\beta,n}X^{\beta}Y^{n}+\sum c_{\beta,n}X^{\beta}Y^{n}\right) &= \left(\sum a_{\beta,n}X^{\beta}Y^{n}\right)\left(\sum (b_{\beta,n}+c_{\beta,n})X^{\beta}Y^{n}\right)\\
&= \sum_{\beta,n}\left(\sum a_{\beta',n'}(b_{\beta'',n''}+c_{\beta'',n''})\right)X^{\beta}Y^{n}\\
&= \sum_{\beta,n}\left(\sum (a_{\beta',n'}b_{\beta'',n''}+a_{\beta',n'}c_{\beta'',n''})\right)X^{\beta}Y^{n}\\
&= \sum_{\beta,n}\left(\sum (a_{\beta',n'}b_{\beta'',n''}+a_{\beta',n'}c_{\beta'',n''})\right)X^{\beta}Y^{n}\\
&= \sum_{\beta,n}\left(\sum a_{\beta',n'}b_{\beta'',n''}+\sum a_{\beta',n'}c_{\beta'',n''}\right)X^{\beta}Y^{n}\\
&= \sum_{\beta,n}\left(\sum a_{\beta',n'}b_{\beta'',n''}\right)X^{\beta}Y^{n}+\sum_{\beta,n}\left(\sum a_{\beta',n'}c_{\beta'',n''}\right)X^{\beta}Y^{n}\\
&= \left(\sum a_{\beta,n}X^{\beta}Y^{n}\right)\left(\sum b_{\beta,n}X^{\beta}Y^{n}\right)+\left(\sum a_{\beta,n}X^{\beta}Y^{n}\right)\left(\sum c_{\beta,n}X^{\beta}Y^{n}\right).
\end{aligned}$$

We can even show $K[\mathbb{R}\oplus\mathbb{Z}]$ is a field with the proof being similar to the power series case. Indeed, let $f = \sum_{i=0}^{\infty} a_{\alpha_i,m_i}X^{\alpha_i}Y^{m_i}$ be a nonzero element in $K[\mathbb{R}\oplus\mathbb{Z}]$ with $a_{\alpha_0,m_0}\neq 0$. To construct an inverse of f, let us first assume that an inverse exists and see what conditions it needs to satisfy. Let $g=\sum_{j=0}^{\infty} a_{\beta_j,n_j}X^{\beta_j}Y^{n_j}$ and suppose $fg=0$. Then we obtain a sequence of equations

$$\begin{aligned}
1 &= a_{\alpha_0,m_0}b_{\beta_0,n_0}\\
0 &= a_{\alpha_0,m_0}b_{\beta_1,n_1}+a_{\alpha_1,m_1}b_{\beta_0,n_0}\\
&\vdots\\
0 &= \sum_{i=0}^{k} a_{\alpha_i,m_i}b_{\beta_{k-i},n_{k-i}}\\
&\vdots
\end{aligned}$$

Then $a_{\alpha_0,m_0}\neq 0$ forces $b_{\beta_0,n_0}=1/a_{\alpha_0,m_0}$. Similarly, $a_{\alpha_0,m_0}\neq 0$ forces $b_{\beta_1,n_1}=-a_{\alpha_1,m_1}b_{\beta_0,n_0}/a_{\alpha_0,m_0}$. More generally, in the kth step, we obtain

$$b_{\beta_k,n_k} = -\frac{1}{a_{\alpha_0,m_0}}\sum_{i=1}^{k} a_{\alpha_i,m_i}b_{\beta_{k-i},n_{k-i}}. \tag{4}$$

Conversely, any such g whose coefficients are defined inductively by (**??**) is easily seen to be an element of $K[\mathbb{R}\oplus\mathbb{Z}]$ which is an inverse to f.

Finally, we can define a valuation on $K[\mathbb{R}\oplus\mathbb{Z}]^{\times}$ with value group $\mathbb{R}\oplus\mathbb{Z}$ as follows: suppose $f\in K[\mathbb{R}\oplus\mathbb{Z}]^{\times}$. Express it as $f=\sum_{i=0}^{\infty} a_{\alpha_i,m_i}X^{\alpha_i}Y^{m_i}$ where $a_{\alpha_0,m_0}\neq 0$. Then we set $v(f)=(\alpha_0,m_0)$. We claim that v is a valuation on $K[\mathbb{R}\oplus\mathbb{Z}]^{\times}$. It clearly lands surjectively onto $\mathbb{R}\oplus\mathbb{Z}$. The fact that it is a group homomorphism follows from translation invariance of the lexicographical ordering. Finally, suppose $f=\sum_{i=0}^{\infty} a_{\alpha_i,m_i}X^{\alpha_i}Y^{m_i}$ and $g=\sum_{j=0}^{\infty} b_{\beta_j,n_j}X^{\beta_j}Y^{n_j}$ are two elements in $K[\mathbb{R}\oplus\mathbb{Z}]^{\times}$ with $a_{\alpha_0,m_0}\neq 0\neq b_{\beta_0,n_0}$. Assume without loss of generality that $v(f)\leq v(g)$. Thus $(\beta_0,n_0)\geq(\alpha_0,m_0)$. In this case, we clearly have $v(f+g)\geq v(f)=\min\{v(f),f(g)\}$. If $v(f)\neq v(g)$, then $(\beta_0,n_0)>(\alpha_0,m_0)$, which implies $v(f+g)=v(f)$. Thus v is a valuation on $K[\mathbb{R}\oplus\mathbb{Z}]^{\times}$ with value group $\mathbb{R}\oplus\mathbb{Z}$. An analagous construction shows that $\mathbb{Z}\oplus\mathbb{R}$ is a value group as well. Namely, we define $K[\mathbb{Z}\oplus\mathbb{R}]$ to be the set of elements of the form

$$\sum_{i=0}^{\infty} a_{n_i,\beta_i}X^{n_i}Y^{\beta_i} \tag{5}$$

where $a_{n_i,\beta_i}\in K$ and where $\{(n_i,\beta_i)\}_{i=0}^{\infty}$ is a linearly ordered subset of $\mathbb{Z}\oplus\mathbb{R}$ where we are viewing $\mathbb{Z}\oplus\mathbb{R}$ as a totally ordered abelian group with respect to the lexicographical ordering. Then if $f\in K[\mathbb{Z}\oplus\mathbb{R}]^{\times}$, we express it as $f=\sum_{i=0}^{\infty} a_{n_i,\beta_i}X^{n_i}Y^{\beta_i}$ with $a_{n_0,\beta_0}\neq 0$ and we set $v(f)=(n_0,\beta_0)$. Then v is a valuation on $K[\mathbb{Z}\oplus\mathbb{R}]^{\times}$ with value group $\mathbb{Z}\oplus\mathbb{R}$.

Appendix

Problem 1

Equivalent Criteria for an R-module to be Injective

Proposition 0.1. *Let E an R-module. The following statements are equivalent;*

1. *E is an injective R-module;*
2. *Every short exact sequence of the form*

$$0 \longrightarrow E \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{6}$$

   splits.

3. *If E is a submodule of an R-module M, then E is a direct summand of M.*

Proof. ($2 \implies 1$) Assume that any short exact sequence of the form (5) splits. This means, equivalently, that any injective R-linear map out of E splits. Let $\varphi\colon M \to N$ be an injective R-linear map and let $\psi\colon M \to E$ be any R-linear map. We need to construct a map $\widetilde{\psi}\colon N \to E$ such that $\widetilde{\psi}\varphi = \psi$. To do this, consider the pushout module

$$E +_M N = (E \times N)/\{(\psi(u), -\varphi(u)) \mid u \in M\}$$

together its natural maps $\iota_1\colon E \to E +_M N$ and $\iota_2\colon N \to E +_M N$, given by

$$\iota_1(v) = [v, 0] \qquad \text{and} \qquad \iota_2(w) = [0, w]$$

for all $v \in E$ and $w \in N$ where $[v, w]$ denotes the equivalence class in $E +_M N$ with (v, w) as one of its representatives. Observe that

$$\begin{aligned} \iota_1(\psi(u)) &= [\psi(u), 0] \\ &= [0, \varphi(u)] \\ &= \iota_2(\varphi(u)) \end{aligned}$$

for all $u \in M$. Therefore, we have a commutative diagram

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N \arrow[d, "\iota_2"] \\ E \arrow[r, "\iota_1"'] & E +_M N \end{tikzcd}$$

We claim that ι_1 is injective. Indeed, suppose $v \in \ker \iota_1$. Then $[v, 0] = [0, 0]$ implies if $(v, 0) = (\psi(u), -\varphi(u))$ for some $u \in M$. Then $\varphi(u) = 0$ implies $u = 0$ since φ is injective, and therefore

$$\begin{aligned} v &= \psi(u) \\ &= \psi(0) \\ &= 0. \end{aligned}$$

Thus ι_1 is injective. Therefore by hypothesis the map $\iota_1\colon E \to E +_M N$ splits, say by $\lambda\colon E +_M N \to E$, where $\lambda\iota_1 = 1_E$. Finally, we obtain a map $\widetilde{\psi}\colon N \to E$ by setting $\widetilde{\psi} := \lambda\iota_2$. Then

$$\begin{aligned} \widetilde{\psi}\varphi &= \lambda\iota_2\varphi \\ &= \lambda\iota_1\psi \\ &= \psi, \end{aligned}$$

shows that $\widetilde{\psi}$ has the desired property.

($1 \implies 2$) Assume that E is an injective R-module. Let $\varphi\colon E \to M$ be an injective homomorphism. Since E is an injective R-module and since $1_E\colon E \to E$ is an injective R-module homomorphism, there exists an R-linear map $\widetilde{\varphi}\colon M \to E$ such that $\widetilde{\varphi} \circ \varphi = 1_E$. That is, $\widetilde{\varphi}$ splits $\varphi\colon E \to M$.

($2 \implies 3$) Assume that any short exact sequence of the form (5) splits. Let M be an R-module such that $E \subseteq M$. Then the short exact sequence

$$0 \longrightarrow E \xrightarrow{\iota} M \xrightarrow{\pi} M/E \longrightarrow 0$$

splits, where $\iota\colon E \to M$ denotes the inclusion map and $\pi\colon M \to M/E$ denotes the quotient map. Therefore we may choose a $\widetilde{\pi}\colon M/E \to M$ such that $\pi\widetilde{\pi} = 1_{M/E}$. We claim that

$$M = E \oplus \widetilde{\pi}(M/E).$$

Indeed, they are both submodules of M. Furthermore, observe that we have $E \cap \widetilde{\pi}(M/E) = \{0\}$. Indeed, suppose $u \in E \cap \widetilde{\pi}(M/E)$. Then $u \in E$ implies $\pi(u) = 0$. Also $u \in \widetilde{\pi}(M/E)$ implies $u = \widetilde{\pi}(\overline{v})$ for some $\overline{v} \in M/E$. Therefore

$$\begin{aligned}
0 &= \widetilde{\pi}(0) \\
&= \widetilde{\pi}\pi(u) \\
&= \widetilde{\pi}\pi\widetilde{\pi}(\overline{v}) \\
&= \widetilde{\pi}(\overline{v}) \\
&= u.
\end{aligned}$$

Finally, note that if $u \in M$, then we can write

$$u = u - \widetilde{\pi}\pi(u) + \widetilde{\pi}\pi(u),$$

where $\widetilde{\pi}\pi(u) \in \widetilde{\pi}(M/E)$ and where $u - \widetilde{\pi}\pi(u) \in E$ since

$$\begin{aligned}
\pi(u - \widetilde{\pi}\pi(u)) &= \pi(u) - \pi\widetilde{\pi}\pi(u) \\
&= \pi(u) - \pi(u) \\
&= 0
\end{aligned}$$

implies $u - \widetilde{\pi}\pi(u) \in \ker \pi = E$. This implies $M = E + \widetilde{\pi}(M/E)$.

($3 \implies 2$) Assume that E satisfies the property that if E is a submodule of an R-module M, then it must be a direct summand of M. We show that any short exact sequence of the form (5) splits by showing that any injective R-linear map out of E splits.

Step 1: Before we show that any injective R-linear map out of E splits, we need to show that if $\varphi\colon E \to F$ is an isomorphism of R-modules, then F satisfies the same property as E; namely if N is an R-module such that $F \subseteq N$, then F is a direct summand of N. Let $\varphi\colon E \to F$ be an isomorphism, let $\psi\colon F \to E$ denote its inverse, and let N be an R-module such that $F \subseteq N$. We define an R-module $\psi(N)$, where as a set we have

$$\psi(N) = E \cup \{\psi(v) \mid v \in N \backslash F\},$$

where $\psi(v)$ is understood to be a formal symbol if $v \in N\backslash F$ and is understood to be an element in E if $v \in F$. Here, E is *literally* a subset of $\psi(N)$. We extend the R-linear structure on E to an R-linear structure on $\psi(N)$ by defining addition and scalar multiplication by

$$\psi(v_1) + \psi(v_2) = \psi(v_1 + v_2) \quad \text{and} \quad a\psi(v) = \psi(av).$$

for all $v, v_1, v_2 \in N\backslash F$ and $a \in R$. Defining the R-linear structure on $\psi(N)$ in this way makes it so that $\psi\colon F \to E$ and $\varphi\colon E \to F$ extends to an isomorphism $\psi\colon N \to \psi(N)$ with corresponding inverse $\varphi\colon \psi(N) \to N$.

With this construction in place, we see that E is *literally* a submodule of $\psi(N)$. Therefore $\psi(N)$ is an internal direct sum, say

$$\psi(N) = E \oplus K,$$

where K is another submodule of $\psi(N)$ such that $E \cap K = \{0\}$ and $E + K = \psi(N)$. Then since $\varphi\colon \psi(N) \to N$ is an isomorphism, we see that

$$\begin{aligned}
N &= \varphi(E) \oplus \varphi(K) \\
&= F \oplus \varphi(K).
\end{aligned}$$

Step 2: Now we will show that any injective R-linear map out of E splits. Let $\varphi\colon E \to M$ be any injective R-linear map. We claim that $\varphi\colon E \to M$ splits if and only if $\iota\colon \varphi(E) \to M$ splits, where ι denotes the inclusion map. Indeed, denote $\varphi^{-1}\colon E \to \varphi(E)$ to be the inverse of $\varphi\colon E \to \varphi(E)$. If $\varphi\colon E \to M$ splits, then there exists an R-linear map $\widetilde{\varphi}\colon M \to E$ such that $\widetilde{\varphi}\varphi = 1_E$. Then $\varphi\widetilde{\varphi}\colon M \to \varphi(E)$ splits $\iota\colon \varphi(E) \to M$ since

$$\begin{aligned}(\varphi\widetilde{\varphi}\iota)(\varphi(u)) &= \varphi\widetilde{\varphi}(\varphi(u)) \\ &= \varphi(\widetilde{\varphi}\varphi(u)) \\ &= \varphi(u)\end{aligned}$$

for all $\varphi(u) \in \varphi(E)$. Similarly, if $\iota\colon \varphi(E) \to M$ splits, then there exists an R-linear map $\widetilde{\iota}\colon M \to \varphi(E)$ such that $\widetilde{\iota}\iota = 1_{\varphi(E)}$. Then $\varphi^{-1}\widetilde{\iota}\colon M \to E$ splits $\varphi\colon E \to M$ since

$$\begin{aligned}(\varphi^{-1}\widetilde{\iota}\varphi)(u) &= (\varphi^{-1}\widetilde{\iota})(\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota})(\iota\varphi(u)) \\ &= (\varphi^{-1}\widetilde{\iota}\iota)(\varphi(u)) \\ &= (\varphi^{-1})(\varphi(u)) \\ &= u\end{aligned}$$

for all $u \in E$.

Thus, to show that $\varphi\colon E \to M$ splits, it suffices to show that $\iota\colon \varphi(E) \to M$ splits. In this case, $\varphi(E)$ is a submodule of M, and by step 1, we see that M is an internal direct sum, say

$$M = \varphi(E) \oplus K$$

for some R-module $K \subseteq M$. The projection map $\pi_1\colon M \to \varphi(E)$ is easily seen to split the inclusion map $\iota\colon \varphi(E) \to M$. □

Every Vector Space has a Basis

Proposition 0.2. *Every vector space has a basis.*

Proof. Let K be a field and let V be a K-vector space. We will show V has a basis over K. Let S be the set of all linearly independent sets in V. Note that for any nonzero $v \in V$, the singleton $\{v\}$ is a linearly independent set. Thus $S \neq \emptyset$. For two linearly independent sets L and L' in V, we say $L \leq L'$ if $L \subseteq L'$. This is the partial ordering on S by inclusion. Let us show that every totally ordered subset of S is bounded. Let $(L_\alpha)_{\alpha \in A}$ be a totally ordered subset of S. We claim that $L = \bigcup_{\alpha \in A} L_\alpha$ is an upper bound of (L_α). Indeed, clearly we have $L_\alpha \subseteq L$ for all $\alpha \in A$. It remains to check that L is a linearly independent set. Let $v_1, \dots, v_n \in L$. Then for each $1 \leq i \leq n$ there exists $\alpha_i \in A$ such that $v_i \in L_{\alpha_i}$. Since the L_α's are totally ordered, one of the sets $L_{\alpha_1}, \dots, L_{\alpha_n}$ contains the others. Thus $v_1, \dots, v_n$ all belong to a common L_α. In particular, they are linearly independent.

Thus by Zorn's Lemma, S contains a maximal element, say $\mathcal{B} \in S$. We claim that $\mathcal{B}$ is a basis for V. Indeed, since $\mathcal{B} \in S$, we see that $\mathcal{B}$ is linearly independent. Thus it suffices to show that $\operatorname{span}\mathcal{B} = V$. To see this, assume for a contradiction that $\operatorname{span}\mathcal{B} \neq V$. Choose $v \in V \backslash \operatorname{span}\mathcal{B}$. Then $\mathcal{B} \cup \{v\}$ is a linearly independent set. By maximality of $\mathcal{B}$, we must have $\mathcal{B} = \mathcal{B} \cup \{v\}$. Hence $v \in \mathcal{B}$, a contradiction. Thus $\operatorname{span}\mathcal{B} = V$, and hence $\mathcal{B}$ is a basis for V. □

Problem 4

Localization of Valuation Domain is a Valuation Domain

Proposition 0.3. *Let R be a valuation domain and let S be a multiplicatively closed subset of R. Then R_S is a valuation domain.*

Proof. Let a/s and b/t be two nonzero elements in R_S, so $a, b \in R \backslash \{0\}$ and $s, t \in S$. Since R is a valuation domain, either $a \mid b$ or $b \mid a$. Without loss of generality, say $a \mid b$, so $b = ax$ for some $x \in R$. Then observe that

$$\frac{b}{t} = \frac{ax}{t} = \frac{a}{s}\frac{sx}{t}$$

implies $a/s \mid b/t$. It follows that R_S is a valuation domain. □