Math 250A
Solutions to Homework 8

(III.3) Let $x \in R$, $x \neq 0$. We wish to show that x has an inverse in R. To this end, note that multiplication by x gives an additive map $\phi_x(r) = xr$. Furthermore, this map is k-linear since for any $c \in k$, we have $\phi_x(cr) = x(cr) = c(xr) = c \cdot \phi_x(r)$. Since R is entire, ϕ_x is injective. But an injective homomorphism of vector spaces over a field must be an isomorphism. Thus ϕ_x is surjective, and in particular we can find a $y \in R$ such that $xy = 1$.

(III.9a) Consider the set $M \times S$, under the equivalence relation:

$$(m, s) \sim (m', s') \iff \exists t \in S,\ t(s'm - sm') = 0 \ \text{ (in } M).$$

The relation is clearly reflexive and symmetric. To see it is transitive: let $(m, s) \sim (m', s')$ and $(m', s') \sim (m'', s'')$, so that there exist $t, t' \in S$, $t(s'm - sm') = t'(s''m' - s'm'') = 0$. Then we have

$$s'tt'(s''m - sm'') = t's'' \cdot t(s'm - sm') + ts \cdot t'(s''m' - s'm'') = 0.$$

Write $S^{-1}M$ for the set of equivalence classes, and write an element of $S^{-1}M$ as m/s or $\frac{m}{s}$. Now we define the following operations on $S^{-1}M$:

$$\begin{aligned} \frac{m}{s}, \frac{m'}{s'} \in S^{-1}M \quad &\implies \quad \frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \in S^{-1}M, \\ \frac{r}{s} \in S^{-1}A, \frac{m}{s'} \in S^{-1}M \quad &\implies \quad \frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'} \in S^{-1}M. \end{aligned}$$

To check that addition is well defined, suppose $\frac{m}{s} = \frac{m_0}{s_0}$ and $\frac{m'}{s'} = \frac{m_1}{s_1}$. So there exist $t, t' \in S$ such that $t(s_0m - sm_0) = t'(s_1m' - s'm_1) = 0$. Now we check that:

$$tt'[s_0s_1(s'm + sm') - ss'(s_1m_0 + s_0m_1)] = s't's_1[t(s_0m - sm_0)] + sts_0[t'(s_1m' - s'm_1)] = 0.$$

Similarly, to check multiplication is well-defined, let $\frac{r}{s} = \frac{r_0}{s_0}$ and $\frac{m}{s'} = \frac{m_1}{s_1}$. So there exist $t, t' \in S$ such that $t(s_0r - sr_0) = 0$ and $t'(s_1m - s'm_1) = 0$. Again we check:

$$tt'[s_0s_1 \cdot rm - ss' \cdot r_0m_1] = t's_1[t(s_0r - sr_0)m] + str_0[t'(s_1m - s'm_1)] = 0.$$

(III.9b) For any homomorphism $\phi : M \to N$ of A-modules, we get a homomorphism $\phi_S : S^{-1}M \to S^{-1}N$ of $S^{-1}A$-modules, via $\frac{m}{s} \mapsto \frac{\phi(m)}{s}$. Observe that this transformation $\phi \mapsto \phi_S$ is *functorial* in the sense that if $\psi : N \to P$ is another map of A-modules, then $\psi_S \circ \phi_S = (\psi \circ \phi)_S$.

Now we shall show, more generally, that if $M \xrightarrow{\phi} N \xrightarrow{\psi} P$ is exact, then so is $S^{-1}M \xrightarrow{\phi_S} S^{-1}N \xrightarrow{\psi_S} S^{-1}P$.

First note that if $\frac{m}{s} \in S^{-1}M$, then $\psi_S(\phi_S(\frac{m}{s})) = \psi_S(\frac{\phi(m)}{s}) = \frac{\psi(\phi(m))}{s} = 0$. Hence, we have the relation $\operatorname{Im}(\phi_S) \subseteq \operatorname{Ker}(\psi_S)$. Conversely, suppose $\frac{n}{s} \in \operatorname{Ker}\psi_S$, so that $\frac{\psi(n)}{s} = 0$. Then we may find a $t \in S$ such that $0 = t \cdot \psi(n) = \psi(tn)$. This gives $tn \in \operatorname{Ker}\psi = \operatorname{Im}\phi$, so that $tn = \phi(m)$ for some $m \in M$. But now we have

$$\phi\left(\frac{m}{st}\right) = \frac{\phi(m)}{st} = \frac{tn}{st} = \frac{n}{s}.$$

So we have proved the reverse inclusion $\operatorname{Ker}(\psi_S) \subseteq \operatorname{Im}(\phi_S)$.

Remark: as a consequence, we have $S^{-1}(\operatorname{Ker}\phi) = \operatorname{Ker}\phi_S$ for any homomorphism $\phi : M \to N$ of A-modules. Indeed, from the exact sequence $0 \longrightarrow \operatorname{Ker}\phi \longrightarrow M \xrightarrow{\phi} N$, we get the exact sequence $0 \longrightarrow S^{-1}(\operatorname{Ker}\phi) \longrightarrow S^{-1}M \xrightarrow{\phi_S} S^{-1}N$, and hence the result follows. Similarly, we can show $S^{-1}(\operatorname{Im}\phi) = \operatorname{Im}\phi_S$.

(III.10a) Write ϕ for the map $M \to \prod_{\mathfrak{p}} M_{\mathfrak{p}}$ and let $m \in \operatorname{Ker}\phi$. Let $\mathfrak{a} = \{x \in A \mid xm = 0 \text{ in } M\}$. It is easy to show that $\mathfrak{a} \subseteq A$ is an ideal. We claim that $\mathfrak{a} = A$.

If not, then $\mathfrak{a}$ must be contained in some maximal ideal $\mathfrak{p}$. Since the image of x in $M_\mathfrak{p}$ is zero, there exists some $s \in A - \mathfrak{p}$ such that $sx = 0 \in M$. But this means that $s \in \mathfrak{a} \subseteq \mathfrak{p}$ which is a contradiction! Hence, we must have $\mathfrak{a} = A$. Since $1 \in \mathfrak{a}$, we have $x = 0$.

(III.10b) More generally, we shall show that a sequence $M \xrightarrow{\phi} N \xrightarrow{\psi} P$ is exact if and only if the sequence $M_\mathfrak{p} \xrightarrow{\phi_\mathfrak{p}} N_\mathfrak{p} \xrightarrow{\psi_\mathfrak{p}} P_\mathfrak{p}$ is exact for all maximal ideals $\mathfrak{p}$. The forward direction ($\Rightarrow$) follows from Ex III.9b.

For the converse, we shall use the remark towards the end of Ex III.9b. First, let $P' = \operatorname{Im}(\psi \circ \phi) \subseteq P$. Then for any maximal ideal $\mathfrak{p}$,

$$P'_\mathfrak{p} = (\operatorname{Im}(\psi \circ \phi))_\mathfrak{p} = \operatorname{Im}((\psi \circ \phi)_\mathfrak{p}) = \operatorname{Im}(\psi_\mathfrak{p} \circ \phi_\mathfrak{p}) = 0.$$

Since $P'_\mathfrak{p} = 0$ for all maximal ideals $\mathfrak{p}$, by part (a), $P' = 0$. So $\operatorname{Im}\phi \subseteq \operatorname{Ker}\psi$. Now let $N' = \operatorname{Ker}\psi / \operatorname{Im}\phi$. Again, localizing at each maximal ideal $\mathfrak{p}$, we get

$$N'_\mathfrak{p} = (\operatorname{Ker}\psi / \operatorname{Im}\phi)_\mathfrak{p} = (\operatorname{Ker}\psi)_\mathfrak{p} / (\operatorname{Im}\phi)_\mathfrak{p} = \operatorname{Ker}(\psi_\mathfrak{p}) / \operatorname{Im}(\phi_\mathfrak{p}) = 0.$$

By part (a) again, $N' = 0$ so that $\operatorname{Ker}\psi = \operatorname{Im}\phi$.

(III.10c) We shall show that, in fact, $M \to S^{-1}M$ is injective for any multiplicative set S not containing 0. Indeed, suppose $m \in M$ is in the kernel of $M \to S^{-1}M$. Then $\frac{m}{1} = 0$ so there exists $s \in S$, $sm = 0$. Note that $s \neq 0$. Since M is torsion-free, this can only happen if $m = 0$.

Remark: Hence when A is entire, it is natural to look at M as a subset of $S^{-1}M$. In fact, any $S^{-1}M$ can be considered as a subset of $T^{-1}M$, where $T = A - \{0\}$. For convenience, we often write the image of $m \in M$ in $S^{-1}M$ as m as well. This interplay between elements of M and $S^{-1}M$ will be heavily exploited in the next question.

(III.11) M is a given finitely generated torsion-free module over the Dedekind ring $\mathfrak{o}$. Following the hint, for any prime ideal $\mathfrak{p}$, the module $M_\mathfrak{p}$ is finitely generated over $\mathfrak{o}_\mathfrak{p}$ (just take the image of the generators of M). We note that it is torsion-free. Indeed if $\frac{r}{s} \in \mathfrak{o}_\mathfrak{p}$, $\frac{m}{s'} \in M_\mathfrak{p}$, $\frac{rm}{ss'} = 0$; then $t \cdot rm = 0$ for some $rt \in \mathfrak{o} - \mathfrak{p}$. Since $rt \neq 0$, we have $m = 0$.

Now let F be a finite free $\mathfrak{o}$-module, and $f : F \to M$ be a surjective map. For any prime ideal $\mathfrak{p}$, localize to get $f_\mathfrak{p} : F_\mathfrak{p} \to M_\mathfrak{p}$, which is surjective by Exercise 10(b). Now $M_\mathfrak{p}$ is a finitely generated torsion-free module over $\mathfrak{o}_\mathfrak{p}$. $\mathfrak{o}_\mathfrak{p}$ is principal (see Ex II.15), and so by Theorem III.7.3, $M_\mathfrak{p}$ is free and $f_\mathfrak{p} : F_\mathfrak{p} \to M_\mathfrak{p}$ has a splitting $g_\mathfrak{p} : M_\mathfrak{p} \to F_\mathfrak{p}$ such that $f_\mathfrak{p} \circ g_\mathfrak{p} = \mathrm{id}_{M_\mathfrak{p}}$. Let $\{m_1, \ldots, m_r\}$ be a set of generators for $M_\mathfrak{p}$ over $\mathfrak{o}_\mathfrak{p}$. For each m_i, $g_\mathfrak{p}(m_i) \in F_\mathfrak{p}$, so we can find a $c_i \in \mathfrak{o} - \mathfrak{p}$ such that $c_i \cdot g_\mathfrak{p}(m_i) \in F$. Then $c_\mathfrak{p} = c_1 c_2 \ldots c_r \in \mathfrak{o} - \mathfrak{p}$ satisfies $c_\mathfrak{p} g_\mathfrak{p}(M) \subseteq F$.

Next, we prove that the set of $c_\mathfrak{p}$'s generate the unit ideal. Indeed, let this ideal be $\mathfrak{a}$. If $\mathfrak{a} \neq \mathfrak{o}$, then $\mathfrak{a} \subseteq \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$. In particular, $c_\mathfrak{p} \in \mathfrak{p}$. But by our construction, $c_\mathfrak{p} \in \mathfrak{o} - \mathfrak{p}$ which produces a contradiction. So $(c_\mathfrak{p})$ generates (1).

Now we can find finitely many $c_{\mathfrak{p}_i}$'s and elements $x_i \in \mathfrak{o}$ such that $\sum_i x_i c_{\mathfrak{p}_i} = 1$. Let $g : M \to F$ be a map defined by

$$g(m) = \sum_i x_i c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}(m) = \sum_i g_{\mathfrak{p}_i}(x_i c_{\mathfrak{p}_i} m).$$

Since for each i, $c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}(M) \subseteq F$, we see that g is indeed a map from M to F.

Finally, we need to show $f \circ g = \mathrm{id}_M$. Let $m \in M$, so that $f(g(m)) = \sum_i f(g_{\mathfrak{p}_i}(x_i c_{\mathfrak{p}_i} m))$. But $f_{\mathfrak{p}_i} \circ g_{\mathfrak{p}_i} = \mathrm{id}_{M_{\mathfrak{p}_i}}$. Hence $f(g(m)) = \sum_i x_i c_{\mathfrak{p}_i} m = m$, and M is a direct summand of the free module F.

Remark. A closer inspection of the proof reveals that we've proven something stronger: if M is a finitely

generated module over a Noetherian ring A, and $M_\mathfrak{p}$ is projective over $A_\mathfrak{p}$ for each prime ideal $\mathfrak{p}$, then M is projective over A. The converse is true as well (and quite easy to prove): if M is a projective module over any ring A, then $S^{-1}M$ is projective over $S^{-1}A$.

(III.12b) Let $S = \mathfrak{o} - \{0\}$, so that the field of fractions K is equal to $S^{-1}\mathfrak{o}$. The isomorphism $f : \mathfrak{a} \to \mathfrak{b}$ of $\mathfrak{o}$-modules then extends to an isomorphism $f_K : S^{-1}\mathfrak{a} \to S^{-1}\mathfrak{b}$ of K-vector spaces. The injection $\mathfrak{a} \hookrightarrow K$ of $\mathfrak{o}$-modules then extends to an injection $S^{-1}\mathfrak{a} \hookrightarrow S^{-1}K$ of K-vector spaces. Clearly we have a natural isomorphism $S^{-1}K \cong K$ (of K-vector spaces), so this gives $S^{-1}\mathfrak{a} \hookrightarrow K$. Since $\mathfrak{a} \neq 0$, $S^{-1}\mathfrak{a}$ must have positive dimension over K. Thus $S^{-1}\mathfrak{a} \cong K$. This gives a K-linear map $f_K : K \to K$.

Finally, for any $r \in \mathfrak{a}$, we have $f(r) = f_K(r) = r \cdot f_K(1) = rc$. Thus, $f = m_c$ and $\mathfrak{b} = f(\mathfrak{a}) = m_c(\mathfrak{a}) = c\mathfrak{a}$.

(III.12c) We have a map $\mathfrak{a}^{-1} \to \mathfrak{a}^\vee = \mathrm{Hom}_\mathfrak{o}(\mathfrak{a}, \mathfrak{o})$, given by $(b \mapsto m_b = (x \mapsto bx))$. To show that this map is injective, suppose $b \in \mathfrak{a}^{-1}$, $m_b = 0$. Then $b\mathfrak{a} = 0$, and since $\mathfrak{a} \neq 0$, $b = 0$.

To show that the map is surjective, suppose $\phi \in \mathfrak{a}^\vee$, i.e. $\phi : \mathfrak{a} \to \mathfrak{o}$ is a homomorphism of $\mathfrak{o}$-modules. Suppose further $\phi \neq 0$. We now claim that ϕ is injective. Indeed, if not, we can find $x, y \in \mathfrak{a}$ such that $\phi(x) = 0$, $\phi(y) \neq 0$. Multiplying x and y by some element of $\mathfrak{o}$, we may assume they lie in $\mathfrak{o}$. Then $\phi(yx) = y\phi(x) = 0$ but $\phi(xy) = x\phi(y) \neq 0$, which is a contradiction.

Hence, $\mathrm{Im}(\phi)$ is an ideal of $\mathfrak{o}$ which is isomorphic to $\mathfrak{a}$. By part (b), $\phi : \mathfrak{a} \to \mathrm{Im}(\phi)$ must be multiplication by some element $c \in K$. The fact that $c\mathfrak{a} \subseteq \mathfrak{o}$ then implies that $c \in \mathfrak{a}^{-1}$. So we have an isomorphism $\mathfrak{a}^{-1} \cong \mathfrak{a}^\vee$. Finally,

$$\mathfrak{a}^{\vee\vee} \cong (\mathfrak{a}^{-1})^\vee = (\mathfrak{a}^{-1})^{-1} = \mathfrak{a}.$$

Remark: a closer inspection of the proof tells us that $\mathfrak{a}^{-1} = \mathfrak{a}^\vee$ for any ideal $\mathfrak{a}$ of an entire ring $\mathfrak{o}$. However, we need the fact that $\mathfrak{o}$ is Dedekind in order to conclude $\mathfrak{a}^{\vee\vee} = \mathfrak{a}$.

(III.13a) Let $S = \mathfrak{o} - \{0\}$, and $K = S^{-1}\mathfrak{o}$ be its field of fractions. Since M is finitely generated over $\mathfrak{o}$, $V = S^{-1}M$ is a vector space over K of finite dimension n. Since M is projective, it is torsion-free and thus the map $M \to S^{-1}M$ is injective.

Now pick a basis of V. Multiplying by a nonzero constant if necessary, we may assume this basis $\{m_1, \ldots, m_n\}$ is a subset of M. Let $F' \subseteq M$ be the submodule generated by the m_i's. Now $\{m_i\}$ freely generates F' since it is linearly independent over K. This gives us the construction of $F' \subseteq M$.

On the other hand, M has a finite generating set $\{m'_1, \ldots, m'_t\}$. Each m'_i can be written as a linear combination of m_i's with coefficients in K. Multiplying throughout by a common term, we see that for some $s_i \in S$, $s_i m'_i \in \oplus_i \mathfrak{o} m_i = F'$. Let $s = \prod s_i$. Then $m'_i \in s^{-1}F'$ for each i, and so $M \subseteq s^{-1}F'$. Hence we have $F := s^{-1}F' \supseteq M \supseteq F'$, where F and F' are both free of rank n.

Remark: observe that F' (resp. F) has a basis $\{m_1, \ldots, m_n\}$ (resp. $\{\frac{m_1}{s}, \ldots, \frac{m_n}{s}\}$). The rank n is then the dimension of $S^{-1}M$ over $S^{-1}\mathfrak{o} = K$.

(III.13b) Let $F_0 \subseteq F$ be the submodule generated by $\frac{m_1}{s}$. And let $M_0 = M \cap F_0$, $F'_0 = F' \cap F_0$. Hence we have $F_0 \supseteq M_0 \supseteq F'_0$. Now the map $\phi : F_0 \to \mathfrak{o}$ which takes $r \cdot \frac{m_1}{s} \mapsto r$ is an isomorphism of $\mathfrak{o}$-modules. Under this map, $\mathfrak{a} = \phi(M_0)$ is then an ideal of $\mathfrak{o}$. Hence, we get an exact sequence of $\mathfrak{o}$-modules:

$$0 \to \mathfrak{a} \to M \to M/M_0 \to 0.$$

Next, we claim that M/M_0 is projective. By Ex 11, it suffices to show M/M_0 is torsion-free. But this is clear, because we have an injective map $M/M_0 = M/F_0 \cap M \hookrightarrow F/F_0$. Since M/M_0 is isomorphic to a

submodule of $F/F_0 \cong \mathfrak{o}$ which is torsion-free, M/M_0 must be torsion-free as well.

Having established the fact that M/M_0 is projective, we now know the above exact sequence splits, and $M \cong \mathfrak{a} \oplus (M/M_0)$. But we have $F/F_0 \supseteq M/M_0 \supseteq F'/F_0'$. If $n = 1$, then all these modules are 0, and the proof is complete. Otherwise, the endterms are free of rank $n-1$. Now apply induction on n.

(III.13c) We know that $M \cong \oplus \mathfrak{a}_i$ for some ideals $\mathfrak{a}_i$ of $\mathfrak{o}$. Now repeatedly apply Ex III.12a (or HW 7, problem 7):

$$\begin{aligned} M &\cong (\mathfrak{a}_1 \oplus \mathfrak{a}_2) \oplus \mathfrak{a}_3 \oplus \cdots \oplus \mathfrak{a}_n \cong (\mathfrak{o} \oplus \mathfrak{a}_1\mathfrak{a}_2) \oplus \mathfrak{a}_3 \oplus \cdots \oplus \mathfrak{a}_n \\ &\cong \mathfrak{o} \oplus (\mathfrak{o} \oplus \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3) \oplus \cdots \oplus \mathfrak{a}_n \cdots \cong \mathfrak{o}^{n-1} \oplus (\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n). \end{aligned}$$

Let us define a map $K_0(\mathfrak{o}) \to \mathrm{Pic}(\mathfrak{o})$, which takes $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a} \mapsto \mathfrak{a}$. The hard part is show that this map is well-defined. For this, let us suppose modules M and M' have the same image in $K_0(\mathfrak{o})$. Hence there are finite free modules F and F' such that $F \oplus M \cong F' \oplus M'$. Writing $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a}$ and $M' \cong \mathfrak{o}^{n'-1}\mathfrak{a}'$, we get $\mathfrak{o}^{m-1} \oplus \mathfrak{a} \cong \mathfrak{o}^{m-1} \oplus \mathfrak{a}'$ (where m is the rank of both sides).

Localizing at $S = \mathfrak{o} - \{0\}$, we get an isomorphism of vector spaces $K^m \cong K^m$. Write this map as an $m \times m$ matrix M with coefficients in K. By assumption, we have $M(\mathfrak{o}^{m-1} \oplus \mathfrak{a}) = \oplus_{i=1}^m N_i$, where $N_1 \cong \cdots \cong N_{m-1} \cong \mathfrak{o}$ and $N_m \cong \mathfrak{a}'$. Perform elementary row operations to reduce the matrix M to a diagonal matrix and observe that the operations have the following effect on the image $M(\mathfrak{o}^{m-1} \oplus \mathfrak{a})$:

(i) *Multiply column i by $c \in K^*$*: replace N_i by cN_i.
(ii) *Swap columns i and j* : swap N_i and N_j.
(iii) *Add columns i to columns j* : no effect on the image of M.

Hence, we have a diagonal matrix M which takes $\mathfrak{o}^{m-1} \oplus \mathfrak{a} \xrightarrow{\cong} \mathfrak{o}^{m-1} \oplus \mathfrak{a}'$. But this means $\mathfrak{a} = c\mathfrak{a}'$ for some $c \in K^*$, so $\mathfrak{a}$ and $\mathfrak{a}'$ have the same image in $\mathrm{Pic}(\mathfrak{o})$.

The map is clearly injective and surjective. It is a homomorphism of groups, since the direct sum of $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a}$ and $M' \cong \mathfrak{o}^{n'-1} \oplus \mathfrak{a}'$ is $\mathfrak{o}^{n+n'-2} \oplus \mathfrak{a} \oplus \mathfrak{a}' \cong \mathfrak{o}^{n+n'-1} \oplus \mathfrak{a}\mathfrak{a}'$. Hence, we have an isomorphism of groups $K_0(\mathfrak{o}) \cong \mathrm{Pic}(\mathfrak{o})$.

(III.15) Let us label the horizontal maps of the diagram:

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{\phi_1} & M_2 & \xrightarrow{\phi_2} & M_3 & \xrightarrow{\phi_3} & M_4 & \xrightarrow{\phi_4} & M_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ N_1 & \xrightarrow{\psi_1} & N_2 & \xrightarrow{\psi_2} & N_3 & \xrightarrow{\psi_3} & N_4 & \xrightarrow{\psi_4} & N_5 \end{array}$$

(a) Suppose f_1 is surjective and f_2, f_4 are injective. Suppose $m_3 \in M_3$, $f_3(m_3) = 0$. Then $f_4 \circ \phi_3(m_3) = \psi_3 \circ f_3(m_3) = 0$ and since f_4 is injective, $\phi_3(m_3) = 0$. So, $m_3 = \phi_2(m_2)$ for some $m_2 \in M_2$. Now $\psi_2 \circ f_2(m_2) = f_3 \circ \phi_2(m_2) = f_3(m_3) = 0$. Hence $f_2(m_2) \in \mathrm{Ker}\,\psi_2 = \mathrm{Im}\,\psi_1$, and $f_2(m_2) = \psi_1(n_1)$ for some $n_1 \in N_1$. But f_1 is surjective, so $n_1 = f_1(m_1)$ for some $m_1 \in M_1$. This gives $f_2(m_2) = \psi_1 \circ f_1(m_1) = f_2 \circ \phi_1(m_1)$. Since f_2 is injective, we get $m_2 = \phi_1(m_1) \implies m_3 = \phi_2 \circ \phi_1(m_1) = 0$. Thus, f_3 is injective.

(b) Now suppose f_5 is injective and f_2, f_4 are surjective. Let $n_3 \in N_3$. Since f_4 is surjective, there exists an $m_4 \in M_4$, $f_4(m_4) = \psi_3(n_3)$. Now $f_5 \circ \phi_4(m_4) = \psi_4 \circ f_4(m_4) = \psi_4 \circ \psi_3(n_3) = 0$, and since f_5 is injective, $\phi_4(m_4) = 0$. Thus, $m_4 \in \mathrm{Ker}\,\phi_4 = \mathrm{Im}\,\phi_3$, and we can write $m_4 = \phi_3(m_3)$, $m_3 \in M_3$. Let $n_3' = f_3(m_3)$. Then $\psi_3(n_3') = \psi_3 \circ f_3(m_3) = f_4 \circ \phi_3(m_3) = f_4(m_4) = \psi_3(n_3)$, and so $n_3 - n_3' \in \mathrm{Ker}\,\psi_3 = \mathrm{Im}\,\psi_2$. Write $n_3 - n_3' = \psi_2(n_2)$, $n_2 \in N_2$. Since f_2 is surjective, $n_2 = f_2(m_2)$ for some $m_2 \in M_2$. Then $f_3(m_3 + \phi_2(m_2)) = f_3(m_3) + \psi_2 \circ f_2(m_2) = n_3' + \psi_2(n_2) = n_3$. Hence f_3 is surjective.

Remark. I know the above looks really confusing. The process, called diagram-chasing, is more easily under-

stood through a live demonstration on a chalkboard.

(III.17a) For any integers $m \geq n \geq 0$, we have $p^m\mathbb{Z} \subseteq p^n\mathbb{Z}$. Hence, this gives a surjection $p_{m,n} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. For any $m \geq n \geq n'$, the inclusion $p^m\mathbb{Z} \subseteq p^n\mathbb{Z} \subseteq p^{n'}$ shows that we have $p_{n,n'} \circ p_{m,n} = p_{m,n'}$. Hence, the abelian groups $A_n = \mathbb{Z}/p^n\mathbb{Z}$ form a projective system.

An element of the inverse limit $\mathbb{Z}_p$ consists of an infinite-tuple $(\ldots, c_2, c_1, c_0)$, where each $c_i \in \mathbb{Z}$ and $c_{i+1} \equiv c_i \pmod{p^i}$. If $\overline{c} \in \mathbb{Z}/p^i\mathbb{Z}$ with $c \in \mathbb{Z}$, then the element $(\ldots, \overline{c}, \overline{c}, \overline{c})$ maps onto $\overline{c}$. Hence $\mathbb{Z}_p \to A_i$ is surjective for each i. Note that this gives an injection $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$.

Next, suppose $(c_i), (d_i) \in \mathbb{Z}_p$ are non-zero elements. Then there exist indices m, n such that $c_m \neq 0$, $d_n \neq 0$. This means c_m is not a multiple of p^m. Since $c_{m+n} \equiv c_m \pmod{p^m}$, we also know that c_{m+n} is not a multiple of p^m. Likewise, d_{m+n} is not a multiple of p^n. But this means that $c_{m+n}d_{m+n}$ is not a multiple of p^{m+n}, and hence $(c_i)(d_i) \neq 0$.

Now, $p \in \mathbb{Z}_p$ is not a unit. Indeed, if $p \cdot (d_i) = 1$, then in particular $p \cdot d_1 \equiv 1 \pmod{p}$ which is impossible. On the other hand, we shall prove that if (c_i) is not divisible by p, then (c_i) is a unit in $\mathbb{Z}_p$. For this, we note that $c_i \equiv c_1 \pmod{p}$ for all $i \geq 1$. Since each c_i is coprime to p, we can find a d_i such that $c_i d_i \equiv 1 \pmod{p^i}$. Since $c_{i+1}d_{i+1} \equiv 1 \equiv c_i d_i \pmod{p^i}$ and $c_{i+1} \equiv c_i \pmod{p^i}$ for each $i \geq 1$, we have $d_{i+1} \equiv d_i \pmod{p^i}$. Hence (d_i) is an element of $\mathbb{Z}_p$ and $(c_i)(d_i) = 1$. We have thus proven that any element of $\mathbb{Z}_p$, which is not divisible by p, is a unit. So $\mathbb{Z}_p$ is a local ring with maximal ideal (p).

Finally to wrap things up, we want to show that $\mathbb{Z}_p$ is factorial. Let $(c_i) \in \mathbb{Z}_p$ be non-zero. Then there is a maximal index m such that $c_m = 0$. Note that since $c_0 = 0$ we always have $m \geq 0$. Now, for any $i \geq 0$, c_{m+i} is divisible by p^m but not by p^{m+1}. So we can write $c_{m+i} = p^m \cdot d_i$, for a unique d_i modulo p^i. Since $c_{m+i+1} \equiv c_{m+i} \pmod{p^{m+i}}$ we have $d_{i+1} \equiv d_i \pmod{p^i}$, and (d_i) is an element of $\mathbb{Z}_p$. Furthermore, $p^m \cdot (c_i) = (d_i)$ and (d_i) is a unit since $d_1 \not\equiv 0 \pmod{p}$. Hence, every nonzero (c_i) is a unit multiplied by some p^m and $\mathbb{Z}_p$ is factorial.

Remark. For the last paragraph, it actually suffices just to show $\mathbb{Z}_p$ is noetherian. But that doesn't seem much easier than proving directly $\mathbb{Z}_p$ is factorial.

(III.17b) We shall define maps $\phi : \varprojlim \mathbb{Z}/(a) \to \prod_p \mathbb{Z}_p$ and $\psi : \prod_p \mathbb{Z}_p \to \varprojlim \mathbb{Z}/(a)$.

Let p be prime. For each $i \geq 0$, let $a' = p^i$ and we have a map $\phi_i : \varprojlim \mathbb{Z}/(a) \to \mathbb{Z}/(a') = \mathbb{Z}/(p^i)$. By the universal property of inverse limits, we obtain a map $\varprojlim \mathbb{Z}/(a) \to \mathbb{Z}_p$. Since p can be any prime, by the universal property of direct products, we get a map $\phi : \varprojlim \mathbb{Z}/(a) \to \prod_p \mathbb{Z}_p$.

For the reverse map, let a be a positive integer. For any prime p, let $\nu = \nu_p(a)$ be the highest power of p dividing a. We get an isomorphism of rings $\mathbb{Z}/(a) \cong \prod_p \mathbb{Z}/(p^{\nu_p(a)})$. Compose this with the map $\prod_p \mathbb{Z}_p \to \prod_p \mathbb{Z}/(p^{\nu_p(a)})$ to get $\prod_p \mathbb{Z}_p \to \mathbb{Z}/(a)$. By the universal property of inverse limits, this induces a map $\psi : \prod_p \mathbb{Z}_p \to \varprojlim \mathbb{Z}/(a)$.

By construction, the two maps are mutually inverse to each other. Hence, we have an isomorphism of rings $\varprojlim \mathbb{Z}/(a) \cong \prod_p \mathbb{Z}_p$.

(III.18a) Denote the maps in the inverse system $\{M_n\}$ by $\phi_n^M : M_n \to M_{n-1}$. An element of $\varprojlim M_n$ can be written in the form (m_n), $m_n \in M_n$ such that $\phi_n^M(m_n) = m_{n-1}$ for all n. Likewise, we write $(a_n) \in \varprojlim A_n$, $\phi_n^A(a_n) = a_{n-1}$. We can then define the product to be: $(a_n)(m_n) = (a_n m_n)$. Then

$$\phi_n^M(a_n m_n) = \phi_n^A(a_n)\phi_n^M(m_n) = a_{n-1}m_{n-1}$$

by the commutative diagram in the problem.

(III.18b) First, we give the definition of $T_p(M)$. For each $n \geq 0$, let $M_n = M[p^n] = \{m \in M \mid p^n m = 0\}$. Then multiplication by p gives a map $M_n \to M_{n-1}$ for each n. We define the group $T_p(M)$ to be the inverse limit of $\{M_n\}$.

For each n, since $p^n M_n = 0$ we can view M_n as a module over $\mathbb{Z}/p^n\mathbb{Z}$. Now the following diagram is commutative:

$$\begin{array}{ccccc} \mathbb{Z}/p^{n+1}\mathbb{Z} & \times & M[p^{n+1}] & \longrightarrow & M[p^{n+1}] \\ \downarrow & & \downarrow p & & \downarrow p \\ \mathbb{Z}/p^n\mathbb{Z} & \times & M[p^n] & \longrightarrow & M[p^n] \end{array}$$

and so by part (a), $T_p(M) = \varprojlim M_n$ is a module over $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

(III.18c) Let $P = M \oplus N$ and M_n, N_n, P_n be as above. The inclusion $M_n \hookrightarrow P_n$ for each n induces a map $T_p(M) \to T_p(P)$. Likewise, we have a map $T_p(N) \to T_p(P)$. By the universal property of products (finite direct sums are identical to finite direct products), we get a map $T_p(M) \oplus T_p(N) \to T_p(P)$.

Conversely, the projection maps $P \to M$ and $P \to N$ induce $T_p(P) \to T_p(M)$ and $T_p(P) \to T_p(N)$. This then gives a map $T_p(P) \to T_p(M) \oplus T_p(N)$. It is clear from the construction that the two maps are mutually inverse, so $T_p(M) \oplus T_p(N) \cong T_p(M \oplus N)$.

Additional Problems

(1) To prove the first claim about $\mathfrak{a}$, note that since $\alpha \in \mathfrak{a}$, we have $(\alpha) \subseteq \mathfrak{a}$. By Exercise (II.17a), the ideal $\mathfrak{a}$ divides (α) so $\mathfrak{a}$ is a factor of (α). Hence we can write $\mathfrak{a}$ as $\prod_{i=1}^t \mathfrak{p}_i^{e_i}$, for some $e_i \geq 0$, $e_i \leq f_i$.

Next, the existence of β follows from Chinese Remainder Theorem. To be specific, let $x_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$ for each $i = 1, 2, \ldots, t$. Such an x_i exists because the fractional ideals form a group, so if $\mathfrak{p}_i^{e_i+1} = \mathfrak{p}_i^{e_i}$, we can multiply $\mathfrak{p}_i^{-e_i}$ on both sides to obtain $\mathfrak{p}_i = \mathfrak{o}$ which is absurd. By Exercise (II.18), we can apply the Chinese Remainder Theorem to the ideals $\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_t^{e_t}$. Hence there exists a $\beta \in \mathfrak{o}$ such that $\beta \equiv x_i \pmod{\mathfrak{p}_i^{e_i+1}}$ for $i = 1, 2, \ldots, t$. Then β is divisible by all $\mathfrak{p}_i^{e_i}$ and no $\mathfrak{p}_i^{e_i+1}$.

For such a β, we have $(\alpha, \beta) = (\alpha) + (\beta) = \gcd((\alpha), (\beta))$ by Exercise II.17b. But we know that the prime factorizations of (α) and (β) are: $(\alpha) = \mathfrak{p}_1^{f_1}\mathfrak{p}_2^{f_2}\ldots\mathfrak{p}_t^{f_t}$ and $(\beta) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_t^{e_t}\mathfrak{q}_1^{e_1'}\ldots\mathfrak{q}_r^{e_r'}$, where the prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are all distinct. Since $e_i \leq f_i$ for each i, the gcd of (α) and (β) is $\mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_t^{e_t} = \mathfrak{a}$.

---

(2) The first step of the proof follows straight from page 113 of the textbook: *every irreducible element of a factorial ring is prime*. But I'll still give a proof here for completeness. Suppose $\pi \in \mathfrak{o}$ is irreducible and $x, y \in \mathfrak{o}$, $xy \in (\pi)$. Hence after factoring xy as a product of irreducibles, π (or $u\pi$ for some unit u) must occur among the irreducibles. So π must occur in the factorization of x or y, i.e. $x \in (\pi)$ or $y \in (\pi)$.

Next, suppose $a \in \mathfrak{o}$ is any non-zero element. We can then write a as a product of irreducible elements $\prod_i \pi_i^{e_i}$. By the above paragraph, each irreducible element π_i generates a prime ideal (π_i). Hence, this expresses the principal ideal (a) as a product $\prod_i (\pi_i)^{e_i}$, where each (π_i) is a *principal* prime ideal.

For the last step, we know from (1) that $\mathfrak{a}$ can be generated by two elements, i.e. $\mathfrak{a} = (a, b)$. By the previous paragraph, the principal ideal (a) (*resp.* (b)) can be written as a product of principal prime ideals $\prod_{i=1}^t (\pi_i)^{e_i}$ (*resp.* $\prod_{i=1}^t (\pi_i)^{e_i'}$), where each $e_i \geq 0$ (*resp.* $e_i' \geq 0$). Note that possibly some of the e_i or e_i' may be 0. Then $\mathfrak{a}$ is the gcd of (a) and (b) and $\mathfrak{a} = \prod_{i=1}^t (\pi_i)^{\min(e_i, e_i')} = \left(\prod_{i=1}^t \pi_i^{\min(e_i, e_i')}\right)$. Thus $\mathfrak{a}$ is principal. Since $\mathfrak{a}$ can be any non-zero ideal of $\mathfrak{o}$, $\mathfrak{o}$ must be principal.