III.11. Let M be a finitely generated torsion-free module over $\mathfrak{o}$. Prove that M is projective.

Proof. Given a prime ideal $\mathfrak{p}$, the localized module $M_\mathfrak{p}$ is generated over $\mathfrak{o}_\mathfrak{p}$ by any generating set of M over $\mathfrak{o}$, hence is finitely generated. If $\frac{a}{s}m = 0$ for some $m \in M_\mathfrak{p}$, then multiplication by s gives that $am = 0$. Thus, since M is torsion free, $a = 0$ or $m = 0$, so $M_\mathfrak{p}$ is also torsion free. $\mathfrak{o}_\mathfrak{p}$ is a principal ideal domain by the combination of exercises 15 and 16: there is a unique prime ideal $\mathfrak{q}$ of $\mathfrak{o}_\mathfrak{p}$, so every ideal factors as $\mathfrak{q}^k$ for some k; but there is some $t \in \mathfrak{q} \setminus \mathfrak{q}^2$, hence $\mathfrak{q} = (t)$ is principal, and so every ideal is principal of the form (t^k). By Theorem 7.3, $M_\mathfrak{p}$ is free and therefore projective.

Let F be finite free over $\mathfrak{o}$ and $f : F \to M$ surjective. f extends naturally to a homomorphism $f_\mathfrak{p} : F_\mathfrak{p} \to M_\mathfrak{p}$ by $f_\mathfrak{p}(\frac{a}{s}x) = \frac{a}{s}f(x)$ for $s \notin \mathfrak{p}$, which is surjective because every element of $M_\mathfrak{p}$ is of the form $\frac{a}{s}m$ for some $m \in M$. So the sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker} f_\mathfrak{p} \arrow[r] & F_\mathfrak{p} \arrow[r, "f_\mathfrak{p}"'] & M_\mathfrak{p} \arrow[l, bend right, "g_\mathfrak{p}"'] \arrow[r] & 0 \end{tikzcd}$$

is exact, hence it yields a splitting homomorphism $g_\mathfrak{p}$.

As a homomorphism of $\mathfrak{o}_\mathfrak{p}$-modules, $g_\mathfrak{p}$ is naturally a homomorphism of $\mathfrak{o}$-modules as well. Since it is a right inverse for $f_\mathfrak{p}$, it is injective, hence gives an embedding $g_\mathfrak{p}(M)$ of M into $F_\mathfrak{p}$ (as an $\mathfrak{o}$-module). This embedding has a finite generating set $\{m_1, \ldots, m_n\}$, and for each i there is some $c_i \notin \mathfrak{p}$ for which $c_i m_i \in F$. Let $c_\mathfrak{p}$ be the product of all the c_i. We know $c_\mathfrak{p} \notin \mathfrak{p}$ since $\mathfrak{p}^c$ is multiplicative, and that $c_\mathfrak{p} m_i \in F$ for all i. Thus $c_\mathfrak{p} g_p(M) \subseteq F$.

Consider the ideal $\mathfrak{a}$ generated by $\{c_\mathfrak{p} : \mathfrak{p} \subseteq \mathfrak{o} \text{ is prime}\}$. If $\mathfrak{a} \neq \mathfrak{o}$, then $\mathfrak{a}$ is contained in some maximal (hence prime) ideal $\mathfrak{q}$. But $c_\mathfrak{q} \notin \mathfrak{a}$ contradicts that $c_\mathfrak{q} \in \mathfrak{a} \subseteq \mathfrak{q}$. So we must have $\mathfrak{a} = \mathfrak{o}$. So there are some finite collections $\{c_{\mathfrak{p}_i}\}$ and $\{x_i\} \subseteq \mathfrak{o}$ for which $\sum x_i c_{\mathfrak{p}_i} = 1$. Letting $g = \sum x_i c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}$, we have $g : M \to F$ and

$$f \circ g(m) = \sum x_i f(c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}(m)) = \sum x_i f_{\mathfrak{p}_i}(c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}(m)) = \sum x_i c_{\mathfrak{p}_i} f_{\mathfrak{p}_i} \circ g_{\mathfrak{p}_i}(m) = m \sum x_i c_{\mathfrak{p}_i} = m$$

for any $m \in M$. Thus $f \circ g = \mathrm{id}_M$. This means that the sequence

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow F \longrightarrow M \longrightarrow 0$$

splits, thus $F = \operatorname{Ker} f \oplus M$. So M is a direct summand of a free module, hence projective. $\square$

III.12. (a) Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Show that there is an isomorphism of $\mathfrak{o}$-modules

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{o} \oplus \mathfrak{ab}.$$

Proof. We may choose a $c \in K$ such that $\mathfrak{a} + c\mathfrak{b} = \mathfrak{o}$. Consider the surjective $\mathfrak{o}$-linear map $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{a} + c\mathfrak{b}$ given by $a + b \mapsto a + cb$. Its kernel is the set of pairs $(-cb, b)$ for which $cb \in \mathfrak{a}$, which is isomorphic simply to $c\mathfrak{b} \cap \mathfrak{a}$. Since these are relatively prime, we know this equals $c\mathfrak{ab}$, which as an $\mathfrak{o}$-module is isomorphic to $\mathfrak{ab}$. Thus we have an exact sequence

$$0 \longrightarrow \mathfrak{ab} \longrightarrow \mathfrak{a} \oplus \mathfrak{b} \longrightarrow \mathfrak{o} \longrightarrow 0.$$

Clearly, $\mathfrak{o}$ is finitely generated and torsion-free over itself (it is an integral domain, generated over itself by 1). By the previous exercise, $\mathfrak{o}$ is projective. Hence, the above sequence splits, giving us $\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{o} \oplus \mathfrak{ab}$. $\square$

(b) Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals, and let $f : \mathfrak{a} \to \mathfrak{b}$ be an isomorphism (of $\mathfrak{o}$-modules). Then f has an extension to a K-linear map $f_K : K \to K$. Let $c = f_K(1)$. Show that $\mathfrak{b} = c\mathfrak{a}$ and that f is given by the mapping $m_c : x \to cx$.

Proof. If $f = 0$, we must have $\mathfrak{a} = \mathfrak{b} = 0$. In this case, $f_K(1)$ is not defined, but we can take $c = 0$ and still have $\mathfrak{b} = c\mathfrak{a}$ with $f = m_c$. So assume $f \neq 0$, and let $a \in \mathfrak{a}$ such that $f(a) \neq 0$. Then $c = f_K(1) = a^{-1}f(a)$, and for any $x \in \mathfrak{a}$ we have $f(x) = xf_K(1) = cx$, thus $f = m_c$. Since $\mathfrak{b}$ is the image of f, $\mathfrak{b} = c\mathfrak{a}$. □

(c) Let $\mathfrak{a}$ be a fractional ideal. For each $b \in \mathfrak{a}^{-1}$ the map $m_b : \mathfrak{a} \to \mathfrak{o}$ is an element of the dual $\mathfrak{a}^\vee$. Show that $\mathfrak{a}^{-1} = \mathfrak{a}^\vee = \operatorname{Hom}_\mathfrak{o}(\mathfrak{a}, \mathfrak{o})$ under this map, and so $\mathfrak{a}^{\vee\vee} = \mathfrak{a}$.

Proof. Consider $\mathfrak{a}^{-1} \to a^\vee$ given by $b \mapsto m_b$, which is clearly injective. If $f \in \mathfrak{a}^\vee$, then by the argument in (b) we know $f = m_c$ where $c = a^{-1}f(a)$. Since $\mathfrak{a}^{-1}$ is an $\mathfrak{o}$-module, and $f(a) \in \mathfrak{o}$, we have $c \in \mathfrak{a}^{-1}$. So we have an isomorphism $\mathfrak{a}^{-1} \cong a^\vee$. Therefore, $\mathfrak{a} = (\mathfrak{a}^{-1})^{-1} \cong \mathfrak{a}^{\vee\vee}$. □

III.13. (a) Let M be a projective finite module over the Dedekind ring $\mathfrak{o}$. Show that there exist free modules F and F' such that $F \supseteq M \supseteq F'$, and F, F' have the same rank, which is called the rank of M.

Proof. Let S be a generating set for M that is as small as possible, and let $|S| = n$. The free $\mathfrak{o}$-module F on S surjects onto M; since M is projective, then, M is a direct summand of F. Thus $M \subseteq F$.

Let $\mathfrak{a}$ be an ideal of $\mathfrak{o}$. We showed in the previous homework that $\mathfrak{a}$ is finitely generated. Since $\mathfrak{o}$ is an integral domain, $\mathfrak{a}$ is torsion free. Thus, by exercise 11, $\mathfrak{a}$ is projective. Also, if $\mathfrak{a} \neq 0$ and a is one of the generators of $\mathfrak{a}$, then $\mathfrak{a}$ contains the free $\mathfrak{o}$-module on a. Thus, $\mathfrak{a}$ contains a free module of rank 1. Clearly, if $\mathfrak{a} = 0$ then it contains the free module on 0 generators.

We will now induct on n (the least possible size of a generating set for M) to show that if $M \subseteq \mathfrak{o}^n$ then $M = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ for some nonzero ideals $\mathfrak{a}_i$ of $\mathfrak{o}$. This is clear if $n = 0$, since then $M \cong (0)$ is the empty sum. If $n = 1$, then M is, by definition, a nonzero ideal of $\mathfrak{o}$. Supposing this holds for $n - 1$, if $M \subseteq \mathfrak{o}^n$ we can take the projection map π of $\mathfrak{o}^n$ onto its first coordinate, and consider its restriction to M. The image of M is a submodule of the image of $\mathfrak{o}^n$, which is $\mathfrak{o}$. Therefore, the image of M is an ideal $\mathfrak{a}_n$, which is also projective. The kernel lies within the last $n - 1$ summands of $\mathfrak{o}^n$, hence by induction equals $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_{n-1}$. Since $\mathfrak{a}_n$ is projective, the exact sequence

$$0 \longrightarrow \operatorname{Ker} \pi \mid_M \longrightarrow M \longrightarrow \operatorname{Im} M \longrightarrow 0$$

which is the same as

$$0 \longrightarrow \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_{n-1} \longrightarrow M \longrightarrow \mathfrak{a}_n \longrightarrow 0$$

splits, giving us $M = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$. We have already argued that each $\mathfrak{a}_i$ contains a rank 1 submodule M_i. Therefore, $F' = M_1 \oplus \cdots \oplus M_n$ is a free module of rank n contained in M. □

(b) Prove that there exists a basis $\{e_1, \ldots, e_n\}$ of F and ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ such that $M = \mathfrak{a}_1 e_1 + \cdots + \mathfrak{a}_n e_n$, or in other words, $M \cong \oplus \mathfrak{a}_i$.

Proof. We have just shown this in part (a). We know $M \cong \oplus \mathfrak{a}_i$, so M has a generating set $e_1, \ldots, e_n$ such that $M = \oplus \mathfrak{a}_i e_i$. Thus, $\mathfrak{o}\langle\{e_1, \ldots, e_n\}\rangle$ is a free module F of rank n that contains M (since M is projective). □

(c) Prove that $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a}$ for some ideal $\mathfrak{a}$, and that the association $M \mapsto \mathfrak{a}$ induces an isomorphism of $K_0(\mathfrak{o})$ with the group of ideal classes $\operatorname{Pic}(\mathfrak{o})$.

Proof. Using associativity of the direct sum, part (a) of exercise 12 extends to $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n \cong \mathfrak{o}^{n-1} \oplus (\mathfrak{a}_1 \cdots \mathfrak{a}_n)$ for any n. By the previous result, we have $M \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n \cong \mathfrak{o}^{n-1} \oplus (\mathfrak{a}_1 \cdots \mathfrak{a}_n)$, hence $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Note that if $M \neq 0$ can be written as $\mathfrak{o}^{n-1} \oplus 0$, then $n \geq 2$ and so it can also be written as $\mathfrak{o}^{n-2} \oplus \mathfrak{o}$. For the remainder of this proof, we will always take the latter form if this ambiguous case arises, so that the righthand summand is never 0 unless $M = 0$.

Since any finite projective module M over $\mathfrak{o}$ can be written as $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a}$ for some nonzero ideal $\mathfrak{a}$, we would like to define a map $K_0(\mathfrak{o}) \to \mathrm{Pic}(\mathfrak{o})$ by $[\mathfrak{o}^{n-1} \oplus \mathfrak{a}] \mapsto [\mathfrak{a}]$; however, it is not immediately evident that this is well-defined. Specifically, we need to verify that if $[\mathfrak{o}^{n-1} \oplus \mathfrak{a}] = [\mathfrak{o}^{m-1} \oplus \mathfrak{b}]$ in $K_0(\mathfrak{o})$ (for some $\mathfrak{a}$ and $\mathfrak{b}$ nonzero), then $[\mathfrak{a}] = [\mathfrak{b}]$ in $\mathrm{Pic}(\mathfrak{o})$.

To verify this, suppose that $[\mathfrak{o}^{n-1} \oplus \mathfrak{a}] = \mathfrak{o}^{m-1} \oplus \mathfrak{b}]$. Because the equivalence relation defining the classes of $K_0(\mathfrak{o})$ equates two ideals that are isomorphic up to adding a free module, we can simply assume that $\mathfrak{o}^{n-1} \oplus \mathfrak{a} \cong \mathfrak{o}^{m-1} \oplus \mathfrak{b}$ (since adding free modules does nothing but increase the values of n and m, which are already arbitrary). Tensoring over $\mathfrak{o}$ with its field of fractions K gives us

$$(\mathfrak{o}^{m-1} \oplus \mathfrak{b}) \otimes K = (\mathfrak{o} \otimes K)^{m-1} \oplus (\mathfrak{b} \otimes K)$$

We have "extended the base" of $\mathfrak{o}$ and of $\mathfrak{b}$ to produce vector spaces over K. Lang's Proposition 4.1 in the chapter on the tensor product states that $\mathfrak{o} \otimes K$ is a 1-dimensional vector space over K.

For the righthand term, we know $\mathfrak{b} \otimes K \subseteq \mathfrak{o} \otimes K$, thus $\mathfrak{b} \otimes K$ has dimension at most 1. If it had dimension 0, this would mean that the only $\mathfrak{o}$-bilinear map from $\mathfrak{b} \times K$ to a given $\mathfrak{o}$-module is 0. However, $(b, k) \mapsto bk$ is bilinear, and is nonzero unless $\mathfrak{b} = 0$, which we know is not the case. Therefore, $\mathfrak{b} \otimes K$ has dimension 1 as well, proving that $m = n$.

We will now show by induction on n that if $\mathfrak{o}^{n-1} \oplus \mathfrak{a} \cong \mathfrak{o}^{n-1} \oplus \mathfrak{b}$, then $\mathfrak{a} \cong \mathfrak{b}$. This is clear for $n = 1$, but consider $n = 2$, i.e. $f : \mathfrak{o} \oplus \mathfrak{a} \to \mathfrak{o} \oplus \mathfrak{b}$ is an isomorphism. Suppose first that $f^{-1}((1, 0)) = (0, \alpha) \in 0 \oplus \mathfrak{a}$. Then $f^{-1}(\mathfrak{o} \oplus 0) \subseteq 0 \oplus \langle \alpha \rangle$. If $\mathfrak{a} \neq \langle \alpha \rangle$, then there is some $\beta \in \mathfrak{a} \setminus \langle \alpha \rangle$. Since f is injective, we must have $f((0, \beta)) \in 0 \oplus \mathfrak{b}$, hence $f(0 \oplus \langle \beta \rangle) \subseteq 0 \oplus \mathfrak{b}$. However, $\alpha\beta \in \langle \alpha \rangle \cap \langle \beta \rangle$, thus $f((0, \alpha\beta)) \in (\mathfrak{o} \oplus 0) \cap (0 \oplus \mathfrak{a}) = 0$. This means $\alpha\beta = 0$, a contradiction ($\alpha \neq 0$ because $f((0, \alpha)) \neq 0$, $\beta \neq 0$ because $\beta \notin \langle \alpha \rangle$, and $\mathfrak{o}$ is an integral domain so $\alpha\beta \neq 0$).

We now know that either $\mathfrak{a}$ is principal and $f(0 \oplus \mathfrak{a}) = \mathfrak{o} \oplus 0$, or $f^{-1}((1, 0)) \in \mathfrak{o} \oplus 0$. The first case implies that $f(\mathfrak{o} \oplus 0) = 0 \oplus \mathfrak{b}$, meaning that $\mathfrak{b} \cong \mathfrak{o} \cong \mathfrak{a}$, as desired. So assume the second case, meaning $f^{-1}((1, 0)) = (x, 0)$ for some nonzero x. If $f((1, 0)) = (a, b)$, then $(1, 0) = f((x, 0)) = xf((1, 0)) = (xa, xb)$, so a is a unit and $b = 0$. Thus $f((1, 0))$ generates $\mathfrak{o} \oplus 0$, so $f(\mathfrak{o} \oplus 0) = \mathfrak{o} \oplus 0$. Thus the restriction of f to $0 \oplus \mathfrak{a}$ gives an isomorphism $\mathfrak{a} \cong \mathfrak{b}$, as desired.

Finally, consider the general case $\mathfrak{o}^{n-1} \oplus \mathfrak{a} \cong \mathfrak{o}^{n-1} \oplus \mathfrak{b}$. We have $\mathfrak{o}^{n-2} \oplus (\mathfrak{o} \oplus \mathfrak{a}) \cong \mathfrak{o}^{n-2} \oplus (\mathfrak{o} \oplus \mathfrak{b})$, thus $\mathfrak{o} \oplus \mathfrak{a} \cong \mathfrak{o} \oplus \mathfrak{b}$ by induction. Having reduced the problem to the $n = 2$ case, we know $\mathfrak{a} \cong \mathfrak{b}$. By part (b) of the previous exercise, $\mathfrak{a} = c\mathfrak{b}$ for some $c \in K$, therefore $\mathfrak{a}\mathfrak{b}^{-1} = (c)$ is principal; thus $[\mathfrak{a}] = [\mathfrak{b}]$ in $\mathrm{Pic}(\mathfrak{o})$. This proves that the map $K_0(\mathfrak{o}) \to \mathrm{Pic}(\mathfrak{o})$ given by $[\mathfrak{o}^{n-1} \oplus \mathfrak{a}] \mapsto [\mathfrak{a}]$ is well-defined.

Now, suppose $[\mathfrak{o}^{n-1} \oplus \mathfrak{a}]$ is in the kernel. Then $\mathfrak{a}$ is principal, meaning that $\mathfrak{a} \cong \mathfrak{o}$. But then $\mathfrak{o}^{n-1} \oplus \mathfrak{a} \cong \mathfrak{o}^{n} \sim 0$, so $[\mathfrak{o}^{n-1} \oplus \mathfrak{a}] = [0]$. So the map is injective. Next, consider any ideal $\mathfrak{a}$ of $\mathfrak{o}$. Since $\mathfrak{a}$ is projective, so is $\mathfrak{o}^{n-1} \oplus \mathfrak{a}$. Thus $[\mathfrak{o}^{n-1} \oplus \mathfrak{a}] \mapsto [\mathfrak{a}]$, so this map is surjective as well. Every class contains some ideal as a representative, so to see that the map is a homomorphism we can just check the property on ideals:

$$[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a} \oplus \mathfrak{b}] = [\mathfrak{o} \oplus \mathfrak{a}\mathfrak{b}] \mapsto [\mathfrak{a}\mathfrak{b}] = [\mathfrak{a}][\mathfrak{b}].$$

The explanation for this is that the operation in $K_0(\mathfrak{o})$ is the direct sum, but we can rewrite $\mathfrak{a} \oplus \mathfrak{b}$ as $\mathfrak{o} \oplus \mathfrak{a}\mathfrak{b}$ by the previous exercise. On the right side of the arrow, the classes are elements of $\mathrm{Pic}(\mathfrak{o})$. But $\mathrm{Pic}(\mathfrak{o})$ is a quotient of the group of nonzero fractional ideals of $\mathfrak{o}$ under ideal multiplication, therefore the $[\mathfrak{a}\mathfrak{b}] = [\mathfrak{a}][\mathfrak{b}]$. So this map is an isomorphism $K_0(\mathfrak{o}) \cong \mathrm{Pic}(\mathfrak{o})$. $\square$

Exercise. Show that the functor that takes each set to its power set is not representable.

Proof. Suppose the functor is representable by some set S. Then $\mathrm{Maps}(X, \emptyset) \cong \mathcal{P}(\emptyset) = \{\emptyset\}$. If X is nonempty, then $\mathrm{Maps}(X, \emptyset) = \emptyset$, a contradiction because this has cardinality less than $\{\emptyset\}$. Thus X is the empty set (so $\mathrm{Maps}(X, \emptyset) = \{\emptyset\}$ is satisfied). But then $\mathrm{Maps}(X, \{\emptyset\}) = \emptyset \not\cong \{\emptyset, \{\emptyset\}\} = \mathcal{P}(\{\emptyset\})$. $\square$

III.15. **The five lemma.** Consider a commutative diagram of R-modules and homomorphisms such that each row is exact:

$$\begin{tikzcd} M_1 \arrow[r] \arrow[d, "f_1"'] & M_2 \arrow[r] \arrow[d, "f_2"'] & M_3 \arrow[r] \arrow[d, "f_3"'] & M_4 \arrow[r] \arrow[d, "f_4"'] & M_5 \arrow[d, "f_5"'] \\ N_1 \arrow[r] & N_2 \arrow[r] & N_3 \arrow[r] & N_4 \arrow[r] & N_5 \end{tikzcd}$$

Prove

(a) If f_1 is surjective and f_2, f_4 are monomorphisms, then f_3 is a monomorphism.

Proof. Let $m_3 \in \operatorname{Ker} f_3$. The image of m_3 in N_3, and hence also in N_4, is 0. Since f_4 is injective, this means the image of m_3 in M_4 is 0. Since the top row is exact, m_3 has a preimage m_2 in M_2. m_2 maps to 0 in N_3 (since it shares the image of m_3), hence $f(m_2)$ has a preimage n_1 in N_1 by the exactness of the bottom row. Since f_1 is surjective, n_1 has a preimage m_1 in M_1. The image of m_1 in N_2 is the same as that of m_2, hence m_1 maps to m_2 by the injectivity of f_2. Thus, by the exactness of the top row, the image of m_2 in M_3 is 0. But this image is m_3 by assumption, thus f_3 is injective. $\square$

(b) If f_5 is a monomorphism and f_2, f_4 are surjective, then f_3 is surjective.

Proof. Let $n_3 \in N_3$. Some m_4 in M_4 shares an image in N_4 with n_3. By the exactness of the bottom row, n_3 maps to 0 in N_5, hence so does m_4. By the injectivity of f_5, m_4 goes to 0 in M_5. So, by the exactness of the top row, m_4 has a preimage m_3 in M_3. Now, $f_3(m_3)$ and n_3 share an image in N_4, so $n_3 - f(m_3)$ has a preimage n_2 in N_2 (by exactness of the bottom row). Let x be the image of m_2 in M_3. Since m_2 goes to $n_3 - f_3(m_3)$, we know $f_3(x) = n_3 - f_3(m_3)$. Thus, $f_3(x + m_3) = n_3$, so f_3 is surjective. $\square$

XVI.6. Let M, N be flat. Show that $M \otimes N$ is flat.

Proof. Suppose $0 \longrightarrow X \longrightarrow Y$ is exact. Since N is flat, $0 \longrightarrow N \otimes X \longrightarrow N \otimes Y$ is exact. Since M, is exact, $0 \longrightarrow (M \otimes N) \otimes X \longrightarrow (M \otimes N) \otimes Y$ where we have also applied the associativity of the tensor product. Therefore, $M \otimes N$ is flat. $\square$

XVI.7. Let F be a flat R-module, and let $a \in R$ be an element which is not a zero-divisor. Show that if $ax = 0$ for some $x \in F$ then $x = 0$.

Proof. Since a is not a zero divisor, we have an exact sequence $0 \longrightarrow R \xrightarrow{\varphi_a} (a) \longrightarrow 0$ where φ_a is multiplication by a. By Proposition 3.7, $(a) \otimes F \cong (a)F$ by the natural map, so tensoring with F yields the exact sequence $0 \longrightarrow F \xrightarrow{\overline{\varphi}_a} (a)F \longrightarrow 0$, where the induced map $\overline{\varphi}_a$ is scaling by a. Therefore, the kernel of this homomorphism is 0, which is the desired result. $\square$

XVI.9. Prove Proposition 3.2:

(i) Let S be a multiplicative subset of R. Then $S^{-1}R$ is flat over R.

Proof. Suppose $f : M \to N$ is an injection, and that the induced map $\overline{f} : S^{-1}R \otimes M \to S^{-1}R \otimes N$ takes $\frac{r}{s} \otimes m$ to 0, meaning $\frac{r}{s} \otimes f(m) = 0$. Multiplying by s gives $r \otimes f(m) = 0$. We know that the base ring R is flat, however, so the restriction of $\overline{f}$ to $R \otimes M$ must be injective. Thus, $r \otimes m = 0$. Multiplying by $\frac{1}{s}$ yields $\frac{r}{s} \otimes m = 0$, hence $\overline{f}$ is injective. $\square$

(ii) A module M is flat over R if and only if the localization $M_{\mathfrak{p}}$ is flat over $R_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of R.

Proof. Localization distributes over exact sequences: Let S be a multiplicative subset of R, and denote $S^{-1}M$ by M_S. Given a sequence $Y \xrightarrow{f} X \xrightarrow{g} Z$ there is a unique induced sequence $Y_S \xrightarrow{f_S} X_S \xrightarrow{g_S} Z_S$. This is because an R-linear map on M has a unique extension to an R_S-linear map on M_S, since $sf(\frac{r}{s}m) = f(rm)$, so $f(\frac{r}{s}m) = \frac{r}{s}f(m)$. We will show the induced sequence is exact. Let $x \in \operatorname{Ker} g_S$. Then $\frac{1}{s}g_S(rx) = 0$ so $rx \in \operatorname{Ker} g = \operatorname{Im} f \subseteq \operatorname{Im} f_S$. This is an ideal, thus scaling gives $\frac{r}{s}x \in \operatorname{Im} f_S$. Now if $\frac{r}{s}x \in \operatorname{Im} f_S$ then it is the image of some $\frac{u}{v}y \in Y$. Thus $f(suy) = vrx$, so $vrx \in \operatorname{Im} f = \operatorname{Ker} g \subseteq \operatorname{Ker} g_S$. Scaling by $\frac{v}{s}$ shows that $\frac{r}{s}x \in \operatorname{Ker} g_S$. Therefore, if $M \to N$ is injective, then $0 \longrightarrow M_{\mathfrak{p}} \xrightarrow{f} N_{\mathfrak{p}}$ is exact, hence $f_{\mathfrak{p}}$ is injective.

Localization also distributes over the tensor product. $(M \otimes_R N)_S = M_S \otimes_{R_S} N_S$ since the map $(\frac{r}{s}m, \frac{u}{v}n) \mapsto \frac{ru}{sv}m \otimes n$ is obviously bilinear and induces a bijection. Also, if M is already an R_S-module, then $M_S = M$ due to the fact of S being multiplicative.

Finally, $0 \longrightarrow M \longrightarrow N$ is exact if and only if $0 \longrightarrow M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ is exact for all prime ideals $\mathfrak{p} \subseteq R$. The forward direction is trivial, since the kernel of $M \to N$ is a subset of the kernel of $M_{\mathfrak{p}} \to N_{\mathfrak{p}}$. For the converse, suppose the kernel K contains some nonzero x. Then 1 is not in the annihilator of x, hence this ideal is proper and can be embedded in some maximal (hence prime) ideal $\mathfrak{p}$. But then we cannot have $x = 0$ in $K_{\mathfrak{p}}$, since it would mean $sx = 0$ for some $s \notin \mathfrak{p}$, contradicting that the annihilator is contained in $\mathfrak{p}$. Thus $K_{\mathfrak{p}} \neq 0$.

For the main proof, suppose M is flat over R. If $0 \longrightarrow X \longrightarrow Y$ is exact (over $R_{\mathfrak{p}}$), then $0 \longrightarrow M \otimes_R X \longrightarrow M \otimes_R Y$ is exact, hence $0 \longrightarrow (M \otimes_R X)_{\mathfrak{p}} \longrightarrow (M \otimes_R Y)_{\mathfrak{p}}$ is exact for all $\mathfrak{p}$. But this sequence equals $0 \longrightarrow M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} X_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} Y_{\mathfrak{p}}$, which equals $0 \longrightarrow M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} X \longrightarrow M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} Y$ because $X_{\mathfrak{p}} = X$. Therefore, $M_{\mathfrak{p}}$ is flat over $R_{\mathfrak{p}}$ for all $\mathfrak{p}$.

Next, suppose $M_{\mathfrak{p}}$ is flat over $R_{\mathfrak{p}}$ for all $\mathfrak{p}$, and that $0 \longrightarrow X \longrightarrow Y$ is exact (over R). Then $0 \longrightarrow M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} X_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} Y_{\mathfrak{p}}$ and hence $0 \longrightarrow (M \otimes_R X)_{\mathfrak{p}} \longrightarrow (M \otimes_R Y)_{\mathfrak{p}}$ are exact for all $\mathfrak{p}$. By the previous paragraph, $0 \longrightarrow M \otimes_R X \longrightarrow M \otimes_R Y$ must be exact, so M is flat. $\square$

(iii) Let R be a principal ring. A module F is flat if and only if F is torsion free.

Proof. The forward direction is the result of the previous exercise. By Proposition 3.7, F is flat if the natural map $(a) \otimes F \to (a)F$ is an isomorphism. Clearly, it is surjective. If $a \otimes x \mapsto ax = 0$, then we must have $a = 0$ or $x = 0$ because F is torsion free. Thus the map is injective, so F is flat. $\square$