Corollary 20. If R is a Dedekind Domain then R is a P.I.D. (i.e., R has class number 1) if and only if R is a U.F.D.

Proof: Every P.I.D. is a U.F.D., so suppose that R is a U.F.D. and let P be any prime ideal in R. Then $P = Ra + Rb$ for some $a \neq 0$ and b in R by Corollary 19. We have $(a') \subseteq P$ for one of the irreducible factors a' of a since their product is an element in the prime P, and then P divides (a') in R by Proposition 17(1). It follows that $P = (a')$ is principal since (a') is a prime ideal (Proposition 12 in Section 8.3). Since every ideal in R is a product of prime ideals, every ideal of R is principal, i.e., R is a P.I.D.

Corollary 20 shows that the class number of a Dedekind domain R gives a measure of the failure of unique factorization of elements. It is a fundamental result in algebraic number theory that the class number of the ring of integers of an algebraic number field is finite. For general Dedekind Domains, however, the class number need not be finite. In fact, for any abelian group A (finite or infinite) there is a Dedekind Domain whose class group is isomorphic to A.

Modules over Dedekind Domains and the Fundamental Theorem of Finitely Generated Modules

We turn next to the consideration of modules over Dedekind Domains R. Every fractional ideal of R is an R-module and the first statement in the following proposition shows that two fractional ideals of R are isomorphic as R-modules if and only if they represent the same element in the class group of R.

Proposition 21. Let R be a Dedekind Domain with fraction field K.

(1) Suppose I and J are two fractional ideals of R. Then $I \cong J$ as R-modules if and only if I and J differ by a nonzero principal ideal: $I = (a)J$ for some $0 \neq a \in K$.

(2) More generally, suppose $I_1, I_2, \ldots, I_n$ and $J_1, J_2, \ldots, J_m$ are nonzero fractional ideals in the fraction field K of the Dedekind Domain R. Then

$$I_1 \oplus I_2 \oplus \cdots \oplus I_n \cong J_1 \oplus J_2 \oplus \cdots \oplus J_m$$

as R-modules if and only if $n = m$ and the product ideals $I_1 I_2 \cdots I_n$ and $J_1 J_2 \cdots J_n$ differ by a principal ideal:

$$I_1 I_2 \cdots I_n = (a) J_1 J_2 \cdots J_n$$

for some $0 \neq a \in K$.

(3) In particular,

$$I_1 \oplus I_2 \oplus \cdots \oplus I_n \cong \underbrace{R \oplus \cdots \oplus R}_{n-1 \text{ factors}} \oplus (I_1 I_2 \cdots I_n)$$

and $R^n \oplus I \cong R^n \oplus J$ if and only if I and J differ by a principal ideal: $I = (a)J$, $a \in K$.

Proof: Multiplication by $0 \neq a \in K$ gives an R-module isomorphism from J to $(a)J$, so if $I = (a)J$ we have $I \cong J$ as R-modules. For the converse, observe that we

may assume $J \neq 0$ and then $I \cong J$ implies $R \cong J^{-1}I$. But this says that $J^{-1}I = aR$ is principal (with generator a given by the image of $1 \in R$), i.e., $I = (a)J$, proving (1).

We next show that for any nonzero fractional ideals I and J that $I \oplus J \cong R \oplus IJ$. Replacing I and J by isomorphic R-modules aI and bJ, if necessary, we may assume that I and J are integral ideals that are relatively prime (cf. Exercise 12), so that $I + J = R$ and $I \cap J = IJ$. It is easy to see that the map from $I \oplus J$ to $I + J = R$ defined by mapping (x, y) to $x + y$ is a surjective R-module homomorphism with kernel $I \cap J = IJ$, so we have an exact sequence

$$0 \longrightarrow IJ \longrightarrow I \oplus J \longrightarrow R \longrightarrow 0$$

of R-modules. This sequence splits since R is free, so $I \oplus J \cong R \oplus IJ$, as claimed.

The first statement in (3) now follows by induction, and combining this statement with (1) shows that if $I_1 \cdots I_n = (a)J_1 \cdots J_n$ for some nonzero $a \in K$ then $I_1 \oplus \cdots \oplus I_n$ is isomorphic to $J_1 \oplus \cdots \oplus J_n$. This proves the "if" statement in (2). It remains to prove the "only if" statement in (2) since the corresponding statement in (3) is a special case. So suppose $I_1 \oplus I_2 \oplus \cdots \oplus I_n \cong J_1 \oplus J_2 \oplus \cdots \oplus J_m$ as R-modules.

Since $I \otimes_R K$ is the localization of the ideal I in K (cf. Proposition 41 in Section 15.4) it follows that $I \otimes_R K \cong K$ for any nonzero fractional ideal I of K. Since tensor products commute with direct sums, $(I_1 \oplus \cdots \oplus I_n) \otimes_R K \cong K^n$ is an n-dimensional vector space over K. Similarly, $J_1 \oplus \cdots \oplus J_m \otimes_R K \cong K^m$, from which it follows that $n = m$.

Note that replacing I_1 by the isomorphic fractional ideal $a_1^{-1}I_1$ for any nonzero element $a_1 \in I_1$ does not effect the validity of the statements in (2). Hence we may assume I_1 contains R, and similarly we may assume that each of the fractional ideals in (2) contains R. Let φ denote the R-module isomorphism from $I_1 \oplus \cdots \oplus I_n$ to $J_1 \oplus \cdots \oplus J_n$. For $i = 1, 2, \ldots, n$ define

$$\varphi((0, \ldots, 0, 1, 0, \ldots, 0)) = (a_{1,i}, a_{2,i}, \ldots, a_{n,i}) \in J_1 \oplus J_2 \oplus \cdots \oplus J_n$$

where $1 \in I_i$ on the left hand side occurs in position i. Since φ is an R-module homomorphism it follows that

$$J_j = a_{j,1}I_1 + a_{j,2}I_2 + \cdots + a_{j,i}I_i + \cdots + a_{j,n}I_n$$

for each $j = 1, 2, \ldots, n$. Taking the product of these ideals for $j = 1, 2, \ldots, n$ it follows that

$$(a_{j_1,1}a_{j_2,2} \cdots a_{j_n,n})I_1I_2 \cdots I_n \subseteq J_1J_2 \cdots J_n$$

for any permutation $\{j_1, j_2, \ldots, j_n\}$ of $\{1, 2, \ldots, n\}$. Hence

$$dI_1I_2 \cdots I_n \subseteq J_1J_2 \cdots J_n$$

where d is the determinant of the matrix $(a_{i,j})$, since the determinant is the sum of terms $\epsilon(\sigma)a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$ where $\epsilon(\sigma)$ is the sign of the permutation σ of $\{1, 2, \ldots, n\}$. Similarly, for $j = 1, \ldots, n$, define

$$\varphi^{-1}((0, \ldots, 0, 1, 0, \ldots, 0)) = (b_{1,j}, b_{2,j}, \ldots, b_{n,j}) \in I_1 \oplus I_2 \oplus \cdots \oplus I_n$$

where $1 \in J_j$ on the left hand side occurs in position j. The product of the two matrices $(a_{i,j})$ and $(b_{i,j})$ is just the identity matrix, so $d \neq 0$ and the determinant of the matrix $(b_{i,j})$ is d^{-1}. As above we have

$$d^{-1}J_1J_2 \cdots J_n \subseteq I_1I_2 \cdots I_n,$$

which shows that $I_1 I_2 \cdots I_n = (a) J_1 J_2 \cdots J_n$, where $0 \neq a = d^{-1} \in K$, completing the proof of the proposition.

We now consider finitely generated modules over Dedekind Domains and prove a structure theorem for such modules extending the results in Chapter 12 for finitely generated modules over P.I.D.s.

Recall that the *rank* of M is the maximal number of R-linearly independent elements in M, or, equivalently, the dimension of $M \otimes_R K$ as a K-vector space, where K is the fraction field of R (cf. Exercises 1–4, 20 in Section 12.1).

Theorem 22. Suppose M is a finitely generated module over the Dedekind Domain R. Let $n \geq 0$ denote the rank of M and let $\mathrm{Tor}(M)$ be the torsion submodule of M. Then

$$M \cong \underbrace{R \oplus R \oplus \cdots \oplus R \oplus I}_{n \text{ factors}} \oplus \mathrm{Tor}(M)$$

for some ideal I of R, and

$$\mathrm{Tor}(M) \cong R/P_1^{e_1} \times R/P_2^{e_2} \times \cdots \times R/P_s^{e_s}$$

for some $s \geq 0$ and powers $P_i^{e_i}$, $e_1 \geq 1$, of (not necessarily distinct) prime ideals. The ideals $P_i^{e_i}$ for $i = 1, \ldots, s$ are unique and the ideal I is unique up to multiplication by a principal ideal.

Proof: Suppose first that M is a finitely generated torsion free module over R, i.e., $\mathrm{Tor}(M) = 0$. Then the natural R-module homomorphism from M to $M \otimes_R K$ is injective, so we may view M as an R-submodule of the vector space $M \otimes_R K$. If M has rank n over R, then $M \otimes_R K$ is a vector space over K of dimension n. Let $x_1, \ldots, x_n$ be a basis for $M \otimes_R K$ over K and let $m_1, \ldots, m_s$ be R-module generators for M. Each m_i, $i = 1, \ldots, s$ can be written as a K-linear combination of $x_1, \ldots, x_n$. Let $0 \neq d \in R$ be a common denominator for all the coefficients in K of these linear combinations, and set $y_i = x_i/d$, $i = 1, \ldots, n$. Then

$$M \subseteq Ry_1 + \cdots + Ry_n \subset Kx_1 + \cdots + Kx_n$$

which shows that M is contained in a *free* R-submodule of rank n and every element m in M can be written uniquely in the form

$$m = a_1 y_1 + \cdots + a_n y_n$$

with $a_1, \ldots, a_n \in R$. The map $\varphi : M \to R$ defined by $\varphi(a_1 y_1 + \cdots + a_n y_n) = a_n$ is an R-module homomorphism, so we have an exact sequence

$$0 \longrightarrow \ker \varphi \longrightarrow M \xrightarrow{\varphi} I_1 \longrightarrow 0$$

where I_1 is the image of φ in R, hence is an ideal in R. The submodule $\ker \varphi$ is also a torsion free R-module whose rank is at most $n - 1$ (since it is contained in $Ry_1 + \cdots + Ry_{n-1}$), and it follows by comparing ranks that I_1 is nonzero and that $\ker \varphi$ has rank precisely $n - 1$. By (4) of Theorem 15, I_1 is a projective R-module, so this sequence splits:

$$M \cong I_1 \oplus (\ker \varphi).$$

By induction on the rank, we see that a finitely generated torsion free R-module is isomorphic to the direct sum of n nonzero ideals of R:

$$M \cong I_1 \oplus I_2 \oplus \cdots \oplus I_n.$$

Since $I_1, \ldots, I_n$ are each projective R-modules, it follows that any finitely generated torsion free R-module is projective.

If now M is any finitely generated R-module, the quotient $M/\mathrm{Tor}(M)$ is finitely generated and torsion free, hence projective by what was just proved. The exact sequence

$$0 \longrightarrow \mathrm{Tor}(M) \longrightarrow M \longrightarrow M/\mathrm{Tor}(M) \longrightarrow 0$$

therefore splits, and so

$$M \cong \mathrm{Tor}(M) \oplus (M/\mathrm{Tor}(M)).$$

By the results in the previous paragraph $M/\mathrm{Tor}(M)$ is isomorphic to a direct sum of n nonzero ideals of R, and by Proposition 21 we obtain

$$M \cong \underbrace{R \oplus R \oplus \cdots \oplus R \oplus I}_{n \text{ factors}} \oplus \mathrm{Tor}(M)$$

for some ideal I of R. The uniqueness statement regarding the ideal I is also immediate from the uniqueness statement in Proposition 21(3).

It remains to prove the statements regarding the torsion submodule $\mathrm{Tor}(M)$. Suppose then that N is a finitely generated torsion R-module. Let $I = \mathrm{Ann}(N)$ be the annihilator of N in R and suppose $I = P_1^{e_1} \cdots P_t^{e_t}$ is the prime ideal factorization of I in R, where $P_1, \ldots, P_t$ are distinct prime ideals. Then N is a module over R/I, and

$$R/I \cong R/P_1^{e_1} \times R/P_2^{e_2} \times \cdots \times R/P_t^{e_t}.$$

It follows that

$$N \cong (N/P_1^{e_1}N) \times (N/P_2^{e_2}N) \times \cdots \times (N/P_t^{e_t}N)$$

as R-modules. Each N/P^eN is a finitely generated module over $R/P^e \cong R_P/P^eR_P$ where R_P is the localization of R at the prime P, i.e., is a finitely generated module over R_P that is annihilated by P^eR_P. Since R is a Dedekind Domain, each R_P is a P.I.D. (even a D.V.R.), so we may apply the Fundamental Theorem for Finitely Generated Modules over a P.I.D. to see that each N/P^eN is isomorphic as an R_P-module to a direct sum of finitely many modules of the form R_P/P^fR_P where $f \leq e$. It follows that each N/P^eN is isomorphic as an R-module to a direct sum of finitely many modules of the form R/P^fR where $f \leq e$. This proves that N is isomorphic to the direct sum of finitely many modules of the form $R/P_i^{f_i}$ for various prime ideals P_i. Hence $\mathrm{Tor}(M)$ can be decomposed into a direct sum as in the statement in the theorem.

Finally, it remains to prove that the ideals $P_i^{e_i}$ for $i = 1, \ldots, s$ in the decomposition of $\mathrm{Tor}(M)$ are unique. This is similar to the uniqueness argument in the proof of Theorem 10 in Section 12.1 (cf. also Exercises 11–12 in Section 12.1): for any prime ideal P of R, the quotient $P^{i-1}M/P^iM$ is a vector space over the field R/P and the difference $\dim_{R/P} P^{i-1}M/P^iM - \dim_{R/P} P^iM/P^{i+1}M$ is the number of direct summands of M isomorphic to R/P^i, hence is uniquely determined by M. This concludes the proof of the theorem.