$$\frac{\log v(n)}{\log n}$$

does not depend on n, i.e., for all integers $n > 1$ we have $v(n) = n^c$ with a certain constant c. This implies $v(x) = |x|^c$ for all rational x, and so v is equivalent to the usual absolute value.

Now let v be non-Archimedean. By Proposition 1.25 we have $v(n) \leq 1$ for all integers n. Let A be the set of all those integers n for which $v(n) < 1$. If $A = \{0\}$, then v is trivial, which case we excluded. Thus A is a non-zero, and since $1 \notin A$ we get from (1.3) that A is a proper non-zero ideal in $\mathbb{Z}$, thus $A = m\mathbb{Z}$ with a suitable positive integer m. Since obviously m is the smallest positive element of A, it must be prime, because a factorization $m = rs$ with $r, s > 1$ would imply $1 > v(m) = v(r)v(s) = 1$, which is impossible. Put $v(m) = a$ and denote by ν the exponent induced by the prime ideal $m\mathbb{Z}$. Then $v(x) = a^{\nu(x)}$, hence v is a p-adic valuation induced by the prime $p = m$. □

Corollary. *If v is a discrete valuation of a field K, then it is non-Archimedean.*

Proof : Assume that v is Archimedean. Corollary to Proposition 1.25 implies that K is of zero characteristic, and thus contains $\mathbb{Q}$. The restriction of v to $\mathbb{Q}$ must be Archimedean, and so by the theorem it must be equivalent to $|x|$, whence non-discrete. □

1.3. Finitely Generated Modules over Dedekind Domains

1. We shall now be concerned with the structure of finitely generated modules over a Dedekind domain R with the field of quotients K. This structure is described by the following result, essentially due to Steinitz [12]:

Theorem 1.32. *Let M be a finitely generated R-module, and let A be its submodule consisting of all torsion elements, i.e., of all elements $x \in M$ which, for some non-zero $r \in R$, satisfy $rx = 0$. Then M can be written as a direct sum*

$$M = R^k \oplus I \oplus A,$$

where k is a non-negative integer, and I is an ideal of R.

For the proof of this theorem we shall need various results concerning projective modules over commutative rings, not necessarily Dedekind.

If R is a commutative ring with unit element 1, then an R-module M is called *projective* if every diagram of the form

$$\begin{array}{ccccc} & & M & & \\ & & \downarrow & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

with exact row and arbitrary R-modules A, B can be embedded in a commutative diagram

$$\begin{array}{ccccc} & & M & & \\ & \swarrow & \downarrow & & \\ A & \longrightarrow & B & \longrightarrow & 0. \end{array}$$

Proposition 1.33. *The direct sum $P = \bigoplus P_a$ of R-modules is projective if and only if every summand P_a is projective.*

Proof : Denote by i_a the canonical injection of P_a into P and by p_a the canonical projection of P onto P_a. Assume now that P is projective, the sequence $A \longrightarrow B \longrightarrow 0$ is exact, and $f: \ P_a \longrightarrow B$ is a homomorphism. Then $f_1 = f \circ p_a$ is a homomorphism of P into B, hence, by our assumption, there exists a homomorphism $g: \ P \longrightarrow A$ such that the diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow_{g} & \downarrow_{f_1} & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutes. Now it suffices to observe that the mapping $h = g \circ i_a$ makes the diagram

$$\begin{array}{ccccc} & & P_a & & \\ & \swarrow_{h} & \downarrow_{f} & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutative, and so P_a is projective.

To prove the second part of the proposition assume that all modules P_a are projective, the sequence $A \longrightarrow B \longrightarrow 0$ is exact, and a homomorphism $f: \ P \longrightarrow B$ is given. Then $f_a = f \circ i_a$ maps P_a in B, hence with a suitable $g_a: \ P_a \longrightarrow A$ the diagram

$$\begin{array}{ccccc} & & P_a & & \\ & \swarrow_{g_a} & \downarrow_{f_a} & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutes. The projectivity of P follows now from the observation that the map $h = \oplus g_a$ makes the diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow_{h} & \downarrow_{f} & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commutative. $\square$

Corollary. *Every free R-module if projective.*

Proof : As every free R-module is a direct sum of R-modules R, it suffices to establish the projectivity of R. Let $f: R \longrightarrow B$ be a homomorphism, and let the sequence $A \xrightarrow{g} B \longrightarrow 0$ be exact. If $f(1) = b$ and a is any element of A with $g(a) = b$, then the map $h: R \longrightarrow A$ given by $h(x) = xa$ has the required property. $\square$

The properties of an R-module equivalent to its projectivity are established in the following simple proposition:

Proposition 1.34. *The following properties of an R-module M are equivalent:*

(i) *If the sequence $0 \longrightarrow A \longrightarrow B \longrightarrow M \longrightarrow 0$ is exact, then $A \oplus M \sim B$,*

(ii) *M is a direct summand of a suitable free R-module,*

(iii) *M is projective.*

Proof : (i) $\Rightarrow$ (ii). The module M is a homomorphical image of a free module F, and so for a suitable N the sequence $0 \longrightarrow N \longrightarrow F \longrightarrow M \longrightarrow 0$ is exact. By (i) we have $F \sim M \oplus N$.

(ii) $\Rightarrow$ (iii). If $M \oplus N \sim F$ and F is free, then by the Proposition 1.33 and its Corollary we get the projectivity of M.

(iii) $\Rightarrow$ (i). Assume that the sequence

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} M \longrightarrow 0$$

is exact. Condition (iii) implies the existence of $f: M \longrightarrow B$ making the composition $M \xrightarrow{f} B \xrightarrow{p} M$ the identity map. Obviously f is an injection. If $x \in B$, then $f \circ p(x) = y$ lies in $\mathrm{Im}\ f \sim M$. Moreover $p(x-y) = 0$, thus $x-y$ lies in the image of i, and we may write $x = z + y$ with $z \in \mathrm{Im}\ i$. Finally we see that $\mathrm{Im}\ f \cap \mathrm{Im}\ i = 0$, since for $x \in \mathrm{Im}\ f \cap \mathrm{Im}\ i = 0$ one has $x = f(u)$ with some $u \in A$ and $p(x) = 0$, giving $u = p(f(u)) = 0$. Thus $x = f(0) = 0$. This implies $B \sim \mathrm{Im}\ i \oplus \mathrm{Im}\ f$, which in turn implies $B \sim A \oplus M$. $\square$

Another characterization of projective modules is provided by the next result:

Proposition 1.35. *An R-module M is projective if and only if there exists a system $(a_t)_{t \in T}$ of elements of M and a family $(f_t)_{t \in T}$ of homomorphisms of M into R such that every element $a \in M$ can be written in the form*

$$a = \sum_{t \in T} f_t(a) a_t, \tag{1.6}$$

where only for finitely many t one has $f_t(a) \neq 0$.

Proof : Assume first that M is projective, and let F be any free R-module whose image by a homomorphism, say f, is M. Proposition 1.34 (i) shows that M is a direct summand of F, and so, with a suitable homomorphism $i: M \longrightarrow F$, we have $f \circ i =$ the identity on M. If $(x_t)_{t\in T}$ is a system of free generators of F, then for every $a \in M$ we have

$$i(a) = \sum_t f_t(a)x_t$$

with some $f_t(a) \in R$. Putting $a_t = f(x_t)$ we get

$$a = \sum_t f_t(a)a_t$$

with only finitely many non-zero summands. Since, obviously, the maps $f_t : M \longrightarrow R$ are homomorphisms we arrive at our assertion.

To prove the converse assume that each $a \in M$ has the form (1.6). Let F be the free R-module with free generators x_t $(t \in T)$, and define a homomorphism $f: F \longrightarrow M$ by putting $f(x_t) = a_t$. If now $g : M \longrightarrow F$ is given by

$$g(a) = \sum_t f_t(a)x_t$$

for $a = \sum_t f_t(a)a_t$, then the composition $M \xrightarrow{g} F \xrightarrow{f} M$ equals the identity, showing that M is a direct summand of F, which allows us to conclude, by Proposition 1.34 (ii), that M is projective. □

Our next proposition connects the notion of projectivity with concepts developed in Sect. 1.

Proposition 1.36. *If R is a domain and I is a non-zero ideal in R, then I is projective as an R-module if and only if it is invertible.*

Proof : Let I be an invertible ideal in R, i.e., $II^{-1} = R$. Then, with suitable $a_1, \dots, a_n \in I$ and $x_1, \dots, x_n \in I^{-1}$ we have

$$\sum_{i=1}^{n} x_i a_i = 1.$$

If we now define, for $t = 1, 2, \dots, n$, homomorphisms f_t of I into R by $f_t(x) = xx_t$, then

$$\sum_t f_t(x)a_t = \sum_t xx_t a_t = x,$$

and so, by Proposition 1.35, I is projective.

Conversely, assume I to be projective. The previous proposition implies the existence of a set of elements $(a_t)_{t\in T}$ and homomorphisms $(f_t)_{t\in T}$ of I into R such that every element x of I can be written in the form

$$x = \sum_t f_t(x)a_t$$

with only a finite number of non-zero summands, Observe that for $x, y \in I$ we have

$$yf_t(x) = f_t(yx) = f_t(xy) = xf_t(y),$$

and so the ratio $x_t = f_t(x)x^{-1}$ is, for non-zero $x \in I$, an element of the quotient field K of R, independent of the choice of x. Moreover $x_tI \subset R$, thus $x_t \in I'$, and for any fixed $x \in I$ only finitely many elements $f_t(x) = xx_t$ are non-zero, whence only a finite number of x_t's do not vanish, say $x_1, \ldots, x_n$. Thus for any $x \in I$ we obtain an equality of the form

$$x = \sum_{t=1}^{n} f_t(x)a_t = \sum_{t=1}^{n} xx_ta_t = x\sum_{t=1}^{n} x_ta_t,$$

which implies

$$1 = \sum_{t=1}^{n} x_ta_t,$$

and so $R \subset II' \subset R$, i.e., $R = II'$ and I is invertible. □

Corollary. *In a Dedekind domains all non-zero ideals are projective.*

Proof : In fact, all non-zero ideals of R are invertible, □

To prove Theorem 1.32 we need two lemmas:

Lemma 1.37. *Let R be a domain in which every ideal is projective. If M is a finitely generated R-module contained in a free R-module F, then M can be represented as a direct sum of a finite number of ideals of R.*

Proof : Observe first that M is contained in a finitely generated free R-module. Indeed, if $a_1, \ldots, a_m$ generate M, then the set of free generators of F occurring in the canonical form of those elements is finite, and consists, say, of elements $x_1, \ldots, x_n$. The R-module generated by $x_1, \ldots, x_n$ is obviously free and contains M.

Now we apply induction in n. For $n = 0$ there is nothing to prove. Assume thus the truth of our lemma for all R-modules contained in a free R-module with $n-1$ free generators. Let M be a R-module contained in a free R-module F_n with n free generators $x_1, \ldots, x_n$, and let F_{n-1} be the free R-module generated by the first $n-1$ of them. Every element x of M can be written as $r_1x_1 + \cdots + r_nx_n$ with $r_i \in R$, and the map $f : x \mapsto r_n$ is a homomorphism of M into R. Since the sequence

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

is exact, and Im f is an ideal of R, projective by assumption, we may apply Proposition 1.34 to obtain $M \sim \operatorname{Im} f \oplus \operatorname{Ker} f$. This implies that $\operatorname{Ker} f$ is finitely generated, being a homomorphic image of M, and since $\operatorname{Ker} f \subset F_{n-1}$, we may apply the inductional assumption to find that $\operatorname{Ker} f$ is a direct sum of ideals of R. Since Im f is also an ideal, the lemma follows. □

Lemma 1.38. *For every domain R any finitely generated and torsion-free R-module M is a submodule of a free R-module.*

Proof : Write $M = Rx_1 + \cdots + Rx_n$, and let K be the field of fractions of R. Then $Kx_1 + \cdots + Kx_n = M \otimes K$ is a finite-dimensional linear K-space. If $y_1, \ldots, y_m$ is its basis, then with suitable $r_{ij} \in K$ we may write

$$x_i = \sum_{j=1}^{m} r_{ij} y_j \quad (i = 1, 2, \ldots, n).$$

Now let q be a non-zero element of R satisfying $qr_{ij} \in R$ for all i and j. Then

$$M = Rx_1 + \cdots + Rx_n \subset Ry_1/q + \cdots + Ry_m/q,$$

and on the right-hand side of this inclusion we obviously have a free R-module. □

Proof of Theorem 1.32: Let M be a finitely generated module over a Dedekind domain R, and let A be its submodule consisting of all torsion elements of M. The factor-module $M_1 = M/A$ is torsion-free and finitely generated. Hence the Corollary to Proposition 1.36 and Lemmas 1.37, 1.38 imply that M_1 is a direct sum of ideals of R. The same corollary jointly with Proposition 1.33 shows that M_1 is projective, and so the exactness of the sequence

$$0 \longrightarrow A \longrightarrow M \longrightarrow M_1 \longrightarrow 0$$

gives, in view of Proposition 1.34, the decomposition

$$M \sim A \oplus M_1 \sim A \oplus I_1 \oplus \cdots \oplus I_m,$$

where $I_1, \ldots, I_m$ are ideals of R.

Now we prove that with a suitable ideal $I \subset R$ we have

$$I_1 \oplus \cdots \oplus I_m \sim R^{m-1} \oplus I.$$

For this purpose it suffices to show that for any pair J_1, J_2 of ideals of R there exists an ideal J such that $J_1 \oplus J_2 \sim R \oplus J$. First we show that there is an ideal J_1' of R which is isomorphic to J_1 as an R-module, and satisfies $(J_1', J_2) = R$. Choose $A \subset R$ so that the ideal $J_1 A = aR$ is principal and $(A, J_2) = R$, which is possible according to Corollary 6 to Proposition 1.14. Write $A = \prod_{i=1}^{t} P_i^{a_i}$, and choose $b \in R$ so that for $i = 1, 2, \ldots, t$ one has

$$b \in P_i^{a_i} \setminus P_i^{a_i+1}$$

and $b \equiv 1 \pmod{J_2}$. Then bR is divisible by A, hence we may write $bR = AJ_1'$ with some ideal J_1', relatively prime to J_2. Finally we get

$$aJ_1' = J_1 AJ_1' = bJ_1,$$

which shows that $J_1 \sim bJ_1 = aJ_1' \sim J_1'$, as required.

Now consider the exact sequence

$$0 \longrightarrow J_1' \cap J_2 \longrightarrow J_1' \oplus J_2 \longrightarrow J_1' + J_2 \longrightarrow 0.$$

Since the ideals J_1' and J_2 are relatively prime, Proposition 1.13 (ii),(iii) shows that this sequence can be written as

$$0 \longrightarrow J_1' J_2 \longrightarrow J_1' \oplus J_2 \longrightarrow R \longrightarrow 0,$$

and the projectivity of R implies finally

$$J_1 \oplus J_2 \sim J_1' \oplus J_2 \sim R \oplus J_1' J_2$$

as asserted. As we have seen above, this establishes the theorem. □

Corollary. *Every non-zero finitely generated and torsion-free module over a Dedekind domain is projective.*

Proof : Follows from the theorem, Proposition 1.33 and the Corollary to Proposition 1.36.

2. Now we shall consider the question of uniqueness of the direct summands occurring in Theorem 1.32. Since the torsion submodule A is clearly unique, we may assume that our module is torsion-free.

Theorem 1.39. *If R is a Dedekind domain and M_1, M_2 are torsion-free R-modules written in the form*

$$M_1 = I_1 \oplus \cdots \oplus I_m, \quad M_2 = J_1 \oplus \cdots \oplus J_n,$$

where I_i, J_i are fractional ideals of R, then M_1 and M_2 are isomorphic if and only if $m = n$, and with a suitable element a of the field K of quotients of R one has

$$I_1 \cdots I_m = aJ_1 \cdots J_n.$$

Proof : The sufficiency of the condition given was already established in the last part of the proof of the preceding theorem. To prove its necessity assume that the modules M_1 and M_2 are isomorphic. The embedding of R in K induces an embedding of M_1 in K^m and of M_2 in K^n, and obviously M_1

spans K^m and M_2 spans K^n. The isomorphism of M_1 onto M_2 extends to a K-isomorphism of the spanned spaces, and so $m = n$.

To prove the remaining part of the theorem we assume that all ideals I_i, J_i contain the ring R. In fact, if I is one of those ideals, then with a suitable non-zero a in K we have, say, $R \subset aI = I'$. The mapping $x \mapsto ax$ shows that $I \sim I'$, whence

$$M_1 \sim I_1' \oplus \cdots \oplus I_m', \quad M_2 \sim J_1' \oplus \cdots \oplus J_m'.$$

If we prove the theorem in this case, then we shall have $I_1' \cdots I_m' = cJ_1' \cdots J_m'$ with some $c \in K$, and this obviously implies the equality $I_1 \cdots I_m = dJ_1 \cdots J_m$ with a suitable $d \in K$.

Now let f be an isomorphism of M_1 onto M_2, and let f_r be its restriction to I_r. If $1_r \in I_r$ is the unit element of R, then denote its image $f_r(1_r)$ by $[a_{r1}, \dots, a_{rm}]$, with $a_{ri} \in J_i$ $(i = 1, 2, \dots, m)$. We shall establish the equality

$$J_s = a_{1s}I_1 + \cdots + a_{ms}I_m \quad (s = 1, 2, \dots, m).$$

Note first that if a, x and ax all lie in I_r, then $f_r(xa) = xf_r(a)$. Indeed, if $x = A/B$ with $A, B \in R$, then

$$Bf_r(ax) = Bf_r(aA/B) = f_r(aA) = Af_r(a),$$

hence

$$f_r(xa) = \frac{A}{B}f_r(a) = xf_r(a).$$

If we denote by p_s the projection of M_2 onto J_s, then in view of

$$f([x_1, \dots, x_m]) = \sum_{i=1}^{m} f_i(x_i) = \sum_{i=1}^{m} x_i f_i(1_i),$$

we obtain the following chain of equalities:

$$\begin{aligned}\sum_{i=1}^{m} a_{is}I_i &= \left\{\sum_{i=1}^{m} a_{is}x_i : \ x_i \in I_i\right\} \\ &= \{p_s(f_1(1_1)x_1 + \cdots + f_m(1_m)x_m) : \ x_i \in I_i\} \\ &= \{p_s(f([x_1, \dots, x_m])) : \ x_i \in I_i\} = J_s.\end{aligned}$$

Now, if $C = \det[a_{ij}] = \sum_P \operatorname{sgn} P \cdot A_P$ is the expansion of the determinant of $[a_{ij}]$, then, multiplying all the equalities just obtained, we get

$$J_1 \cdots J_m = \prod_{s=1}^{m} \sum_{i=1}^{m} a_{is}I_i = \sum_P A_P I_1 \cdots I_m + \cdots,$$

which implies

$$\sum_P A_P I_1 \cdots I_m \subset J_1 \cdots J_m.$$

From this we shall now deduce the inclusion $CI_1 \cdots I_m \subset J_1 \cdots J_m$. Let P be any permutation of m letters, and let $x_i \in I_i$ for $i = 1, 2, \ldots, m$. If

$$y_i = \begin{cases} \operatorname{sgn} P \cdot x_1 & \text{for } i = 1, \\ x_i & \text{for } i = 2, \ldots, m, \end{cases}$$

then

$$A_P y_1 \cdots y_m = \operatorname{sgn} P \cdot A_P x_1 \cdots x_m \in A_P I_1 \cdots I_m \subset J_1 \cdots J_m,$$

and so the sum

$$\sum_P \operatorname{sgn} P \cdot A_P x_1 \cdots x_m,$$

which equals $Cx_1 \cdots x_m$, lies in $J_1 \cdots J_m$.

If we now exchange the roles of M_1 and M_2, we get $C_1 J_1 \cdots J_m \subset I_1 \cdots I_m$, where C_1 is the determinant of the matrix $[b_{ij}]$ defined by

$$g_r(e_r) = [b_{r1}, \ldots, b_{rm}],$$

where $e_r \in J_r$ is the unit element of R, and g_r is the restriction of g, the mapping inverse to f, to J_r. One sees easily that the matrices $[a_{ij}]$ and $[b_{ij}]$ are inverses of each other, and so $CC_1 = 1$, which at once implies the equality $I_1 \cdots I_m = C_1 J_1 \cdots J_m$. □

Corollary. *If A, B are ideals in a Dedekind domain R, and M is a finitely generated torsion-free R-module such that $A \oplus M$ and $B \oplus M$ are isomorphic, then A and B are isomorphic.*

Proof : Theorem 1.32 implies that $M \sim R^n \oplus I$ with a certain $n \geq 0$ and an ideal I of R, therefore

$$A \oplus R^n \oplus I \sim B \oplus R^n \oplus I,$$

and it suffices to apply Theorem 1.39. □

3. To conclude the study of finitely generated modules over Dedekind domains we shall now consider torsion modules, and start with the case of a principal ideal domain.

Proposition 1.40. *If R is a principal ideal domain and M is a finitely generated non-zero torsion R-module, then for some $n \geq 1$ there exist ideals $I_1, \ldots, I_n$ of R such that*

$$M \sim \bigoplus_{j=1}^{n} R/I_j.$$

Proof : For any non-zero prime ideal P of R denote by $M(P)$ the submodule of M consisting of all elements of M which are annihilated by some power of P, i.e.

$$M(P) = \{m \in M : \ P^r m = 0 \quad \text{for a certain } r \geq 1\}.$$

Since R is a principal ideal domain we have equivalently

$$M(P) = \{m \in M : \ \pi^r m = 0 \quad \text{for a certain } r \geq 1\},$$

where π is a generator of P. First we show that $M = \bigoplus_P M(P)$, where P runs over all prime ideals of R. Let $m \in M$ be non-zero, and let

$$\mathrm{Ann}(m) = \{r \in R : \ rm = 0\}$$

be its *annihilator*. It is a non-zero ideal, hence we can find irreducible elements $\pi_1, \ldots, \pi_s$ generating distinct prime ideals, and also exponents $\alpha_i \geq 1$ $(i = 1, 2, \ldots, s)$ so that $\mathrm{Ann}(m) = \pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s} R$. Since R is a principal ideal domain, and the elements

$$\rho_j = (\pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s}) \pi_j^{-\alpha_j} \quad (j = 1, 2, \ldots, s)$$

do not have a non-unit common divisor, thus we may find $t_1, \ldots, t_s$ in R satisfying $\sum_{i=1}^s t_i \rho_i = 1$. This implies

$$m = \sum_{i=1}^s t_i \rho_i m \in \sum_{i=1}^s M(\pi_i R),$$

because $\rho_i m$ is annihilated by $\pi_i^{\alpha_i}$. This shows that $M = \sum_P M(P)$, but since only the zero element can be annihilated by two relatively prime elements, the sum $\sum_P M(P)$ is direct, and $M = \bigoplus_P M(P)$ follows. Since the Corollary to Proposition 1.2 implies that M is a Noetherian module, there can be only finitely many non-zero terms $M(P)$ in the sum in question.

It follows that it suffices to consider modules of the form $M(P)$ with a suitable prime ideal P. Note that for such modules M their annihilator

$$\mathrm{Ann}(M) = \bigcap_{m \in M} \mathrm{Ann}(m)$$

must be a power of P, because $\mathrm{Ann}(m)$ is a power of P for non-zero $m \in M$. Therefore, let $\mathrm{Ann}(M) = \pi^t R$, where π is a generator of P and $t \geq 1$. Let $m_1, \ldots, m_n$ be a set of generators of M. We use induction in the number n of generators. If $n = 1$, then M is an epimorphic image of R, and hence $M \sim R/I$ with a suitable ideal I of R. Assume now that our assertion holds for all modules having at most $n-1$ generators. Obviously at least one of the generators m_i satisfies $\mathrm{Ann}(m_i) = \pi^t R$, and we may assume that this holds for $i = n$. The factor-module $M/m_n R$ has less than n generators, whence we may write

$$M/m_n R = \bigoplus_{i=1}^s f(x_i) R,$$

where $x_1, \ldots, x_s$ are suitable elements of M, and $f : M \longrightarrow M/m_n R$ denotes the natural map. Put $\mathrm{Ann}(f(x_i)) = \pi^{r_i} R$ $(i = 1, 2, \ldots, s)$. Then $r_i \leq t$

and with suitable $k_i \geq 0$ and $a_i \in R \setminus \pi R$ we have $\pi^{r_i} x_i = \pi^{k_i} a_i m_n$ $(i = 1, 2, \ldots, s)$.

Because of

$$0 = \pi^t x_i = \pi^{t - r_i + k_i} a_i m_n$$

we infer that $k_i \geq r_i$. Putting $y_i = x_i - \pi^{k_i - r_i} a_i m_n$, we obtain $\pi^{r_i} y_i = 0$ and $f(y_i) = f(x_i)$. This gives

$$\operatorname{Ann}(f(x_i)) = \pi^{r_i} R \subset \operatorname{Ann}(y_i) \subset \operatorname{Ann}(f(y_i)) = \operatorname{Ann}(f(x_i)),$$

thus $\operatorname{Ann}(f(y_i)) = \operatorname{Ann}(y_i)$. It follows that the restriction of the map f to $y_i R$ is an isomorphism for $i = 1, 2, \ldots, s$, and because of

$$f(y_1 R + \cdots + y_s R) = M/m_n R = \bigoplus_{i=1}^{s} f(y_i) R$$

f maps $y_1 R + \cdots + y_s R$ isomorphically onto $\bigoplus_{i=1}^{s} f(y_i) R$, and so the sum $\sum_{i=1}^{s} y_i R$ is direct. This leads to

$$M = m_n R \oplus \bigoplus_{i=1}^{s} y_i R,$$

and applying the inductional assumption we arrive at our assertion. □

Using the proposition just proved, we can now describe all finitely generated torsion modules over a Dedekind domain. It turns out that their structure is not more complicated than in the case of a principal ideal domain.

Theorem 1.41. *If R is a Dedekind domain and M a non-zero finitely generated and torsion R-module, then there exist ideals $I_1, \ldots, I_n$ of R such that*

$$M \sim \bigoplus_{j=1}^{n} R/I_j.$$

Proof : The set $I = \{r \in R : \ rm = 0 \quad \text{for all } m \in M\}$ is a non-zero ideal in R, and we can regard M as an R/I module via

$$r \,(\mathrm{mod}\ I) \cdot m = rm \quad (r \in R, m \in M).$$

Write

$$I = \prod_{j=1}^{t} P_j^{\alpha_j}$$

with distinct prime ideals $P_1, \ldots, P_t$ and $\alpha_j \geq 1$. Theorem 1.15 implies

$$R/I \sim \bigoplus_{j=1}^{t} R/P_j^{\alpha_j},$$

and to utilize this decomposition we need the following auxiliary result:

Lemma 1.42. *If a commutative ring S with unit e is a direct sum of its subrings S_j (with units e_j)*

$$S = \bigoplus_{j=1}^{t} S_j,$$

then every S-module M can be written in the form

$$M = \bigoplus_{j=1}^{t} M_j,$$

where $M_1, \dots, M_t$ are S-modules, and for $i \neq j$ and $s_i \in S_i$ we have $s_i M_j = 0$.

Proof : Clearly we have $e = e_1 + \cdots + e_t$. Put $M_j = e_j M$ for $j = 1, 2, \dots, t$. Then for $i \neq j$ and $s \in S_j$ we have $sM_i = 0$. Since for a in M

$$a = e_1 a + \cdots + e_t a \tag{1.7}$$

and $e_j a \in M$, the sum of the modules M_j equals M, and it remains to show that this sum is direct, i.e., the decomposition (1.7) is unique. This can be seen in the following way: if $a = m_1 + \cdots + m_t$ with $m_i \in M_i$ $(i = 1, 2, \dots, t)$, then $m_i = e_i x_i$ for suitable $x_i \in M_i$, thus

$$e_j a = \sum_{i=1}^{t} e_j m_i = \sum_{i=1}^{t} e_j e_i x_i = e_j^2 x_j = e_j x_j = m_j,$$

hence our decomposition coincides with (1.7). $\square$

We apply the lemma for $S = R/I$, $S_j = R/P_j^{\alpha_j}$, and obtain the equality

$$M = \bigoplus_{j=1}^{t} M_j,$$

where each M_j can be regarded as an $R/P_j^{\alpha_j}$-module, and for $i \neq j$ one has $(R/P_j^{\alpha_j})M_i = 0$.

To conclude the proof it is sufficient to show that every finitely generated R/P^α-module N (where P is a prime ideal of R and $\alpha \geq 1$) is isomorphic to the direct sum $\bigoplus_{j=1}^{t} R/P^{\beta_j}$ with a certain $t \geq 0$ and $1 \leq \beta_j \leq a$. If R_P denotes the valuation ring induced by the P-adic valuation, then by Proposition 1.27 (iv) the rings R/P^α and $R_P/(PR_P)^\alpha$ are isomorphic. Thus N becomes an R_P-module with the property $(PR_P)^\alpha N = 0$. Since by Theorem 1.26 R_P is a principal ideal domain, Proposition 1.40 is applicable, and we see that

$$N \sim \bigoplus_{j=1}^{t} R_P/I_j$$

with suitable ideals I_j of R_P. Theorem 1.26 implies that each I_j is a power or PR_P, and owing to $(PR_P)^\alpha N = 0$ we must have $I_j = (PR_P)^{\beta_j}$ with $1 \leq \beta_j \leq \alpha$. Since $R \subset R_P$, we can regard R_P/I_j as an R-module, and since the ring-isomorphism of R/P^{β_j} and $R_P/(PR_P)^{\beta_j}$ is also an R-module isomorphism, we obtain finally

$$N \sim \bigoplus_{j=1}^{t} R/P^{\beta_j},$$

as asserted. □

4. We conclude this chapter with the introduction of the notion of the *class-group of a Dedekind domain*, which will play an important role in the sequel. Its definition is based on the following simple result:

Proposition 1.43. *If R is a Dedekind domain and $I_1 \sim I_2$, $J_1 \sim J_2$ are two pairs of its fractional ideals, which are isomorphic as R-modules, then the products I_1J_1 and I_2J_2 are also isomorphic.*

Proof : Since obviously $I_1 \oplus J_1 \sim I_2 \oplus J_2$, Theorem 1.39 implies the existence of a non-zero $a \in K$, the field of fractions of R, such that $I_1J_1 = aI_2J_2$, and this shows that the map $x \mapsto ax$ of I_2J_2 onto I_1J_1 is an isomorphism. □

This proposition implies the compatibility of the multiplication of ideals with the partition of all fractional ideals into classes of isomorphic ideals, and so permits us to define a multiplication in the set of these classes in the following way: if $c(I), c(J)$ are classes containing I and J, respectively, then their product is defined by $c(I)c(J) = c(IJ)$. This induces a semigroup structure in the set of classes, but one sees easily that it is in fact a group structure, because the existence of inverses is implied by the invertibility of fractional ideals.

The resulting group is called the *group of ideal classes of R*, or simply the *class-group of R*, and is usually denoted by $H(R)$. If it is finite, then the number of elements of $H(R)$ is called the *class-number of R* and denoted by $h(R)$.

For further reference we point out a simple result:

Proposition 1.44. *Every class of ideals contains an ideal of R.*

Proof : If I is a fractional ideal and $c \in R$ is non-zero and satisfies $cI \subset R$, then I and cI lie in the same class. □

The importance of the class group is explained by the following result:

Theorem 1.45. *If R is a Dedekind domain, then the following statements are equivalent:*

(i) $H(R)$ is the trivial group, i.e., $h(R) = 1$,

(ii) R is a principal ideal domain (PID),

(iii) R is a unique factorization domain (UFD).

Proof : If $H(R)$ is trivial, then every non-zero ideal of R is isomorphic to R as an R-module, hence has the form aR with a certain non-zero $a \in R$, This establishes the implication (i)$\rightarrow$ (ii). The implication (ii)$\rightarrow$(iii) being clear, assume that R is a unique factorization domain. We show first that every irreducible element of R (i.e., a non-zero and non-invertible element which does not have proper divisors) generates a prime ideal. If a is irreducible and $aR = P_1 \cdots P_s$ with $s \geq 2$, then by Corollary 5 to Proposition 1.14 we get

$$P_i = a_iR + b_iR = (a_iR, b_iR) \quad (i = 1, 2, \ldots, s)$$

with suitable $a_i, b_i \in R$. For every i we have either $a \nmid a_i$ or $a \nmid b_i$, and we may assume that $a \nmid a_i$ holds for $i = 1, 2, \ldots, s$. However, $a_1 \cdots a_s \in P_1 \cdots P_s = aR$, thus a divides the product $a_1 \cdots a_s$ without dividing any of its factors, which is impossible for an irreducible element in a UFD.

This shows that irreducible elements generate prime ideals. If $H(R)$ were non-trivial, there would exist at least one non-principal prime ideal, say P, because otherwise all ideals would be principal. Write $P = (aR, bR)$ with suitable $a, b \in R$, and factorize a into irreducibles, say $a = a_1 \cdots a_r$. Since the ideals a_iR are prime, it follows that for a certain i we have $a_iR = P$, thus P is principal, contrary to our assumption. This establishes the implication (iii)$\rightarrow$(i). □

1.4. Notes to Chapter 1

1. The theory of Dedekind domains was created as a generalization of results concerning rings of integers in finite extensions of the rationals, obtained mainly by Dedekind [71]. It was observed already by Dedekind and H.Weber [82] that many of these results apply also to the rings of integral elements in function fields. However, the general theory had to wait for the introduction of abstract methods and concepts into algebra. In fact, the definition of an abstract ring, in the form used today, appears for the first time in Fraenkel [16], and the definition of an abstract field is not much older (Steinitz [10]).

The role of the ascending chain condition for ideals (the Noether condition) for the theory of commutative rings was emphasized by Noether [21]. She obtained the fundamental results for Noetherian rings, generalizing many