CHAPTER 7

DEDEKIND RINGS

1. Hereditary Rings.

Definition 1.1: A ring Λ is left hereditary if every left ideal is projective.

Lemma 1.2: Let Λ be a ring and let P be a Λ-module. Then P is projective if and only if for every exact sequence $Q \to Q' \to 0$, where Q is injective, $\mathrm{Hom}(P,Q) \to \mathrm{Hom}(P,Q') \to 0$ is exact.

Proof: Necessity follows from proposition 2.10 of Chapter 3. Let $A \to A'' \to 0$ be exact; we may embed this sequence in a commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & A' & \to & A & \to & A'' & \to & 0, \\ & & & & i\downarrow & & \downarrow i' & & \\ & & & & Q & \xrightarrow{f} & Q'' & \to & 0 \end{array}$$

where Q is injective, $Q'' = Q/A'$. Let $g\colon P \to A''$ be a morphism. There exists $\tilde{g}\colon P \to Q$ such that $f\tilde{g} = i'g$. But then $\mathrm{im}\,\tilde{g} \subset \mathrm{im}\, i$, so there exists $g'\colon P \to A$ such that $fg' = g$, and P is projective by proposition 2.10 of Chapter 3.

Lemma 1.2': A module Q is injective if and only if for every exact sequence $0 \to P' \to P$ where P is projective, $\mathrm{Hom}(P,Q) \to \mathrm{Hom}(P',Q) \to 0$ is exact.

Proof: Necessity follows from proposition 3.5. Let $0 \to A' \to A$ be exact, and embed this sequence in a commutative diagram with exact rows and columns:

$$\begin{array}{ccccc} & & & & 0 \\ & & & & \downarrow \\ & & & & M \\ & & & & \downarrow \\ 0 & \to & P' & \xrightarrow{f'} & P \\ & & i'\downarrow & & \downarrow i \\ 0 & \to & A' & \xrightarrow{f} & \Lambda \\ & & \downarrow & & \downarrow \\ & & 0 & & 0 \end{array}$$

where P is projective, $P' = i^{-1}f(A')$. Let $g: A' \to Q$ be a morphism. There exists $\tilde{g}: P \to Q$ such that $\tilde{g}f' = gi'$. But then $\tilde{g}(M) = 0$, so there exists $g': A \to Q$ such that $g'f = g$, and Q is injective by proposition 3.5 of Chapter 3.

Theorem 1.3: The following are equivalent:

i) Λ is left hereditary

ii) Each quotient module of an injective left Λ-module is injective

iii) Each submodule of a projective left Λ-module is projective.

Proof: i) $\Rightarrow$ ii) follows from the proof of proposition 3.7 of Chapter 3 which depends only on the fact that (in a principal ideal domain) every ideal is projective.

ii) $\Rightarrow$ iii) Consider a diagram with exact rows

$$\begin{array}{ccccc} P & \xleftarrow{i} & P' & \leftarrow & 0 \\ & & \downarrow f & & \\ Q & \xrightarrow{j} & Q'' & \to & 0 \end{array}$$

where P is projective and Q is injective. Q'' is injective so there exists $\tilde{f}: P \to Q''$ such that $\tilde{f}i = f$. P is projective, so there exists $f': P \to Q$ such that $jf' = \tilde{f}$. $jf'i = \tilde{f}i = f$,

so, by lemma 1.2, P' is projective.

iii) $\Rightarrow$ i) Every ideal is a submodule of Λ, which is Λ-free.

Definition 1.4: A Dedekind ring is an hereditary integral domain, that is, an integral domain every ideal of which is projective.

2. Fractional ideals.

Throughout this section K will denote an integral domain, Q its field of quotients.

Definition 2.1: A sub-K-module I of Q, $I \neq (0)$, is a fractional ideal if there exists $k \in K$, $k \neq 0$, such that $kI \subset K$; a fractional ideal I is called integral if $I \subset K$. Let $\mathcal{I}$ denote the set of fractional ideals of K. It is clear that $\mathcal{I}$ is a monoid under multiplication, with K as identity. Let I^{-1} $= \{k \mid k \in Q \text{ and } kI \subset K\}$; since $I^{-1} I \subset K$, $I^{-1} \in \mathcal{I}$. In what follows, ideal will mean fractional ideal.

Proposition 2.2: If $I \in \mathcal{I}$, then I^{-1} is isomorphic to $\mathrm{Hom}(I,K)$.

Proof: If $k \in I^{-1}$, $x \in I$, then $f_k(x) = k \cdot x$ defines $f_k \in \mathrm{Hom}(I,K)$, and $\varphi(k) = f_k$ defines a morphism $\varphi: I^{-1} \to \mathrm{Hom}(I, K)$. Conversely, let $g \in \mathrm{Hom}(I, K)$. Let $x \in I \cap K$, $x \neq 0$ and $g(x) = y$. Let $k = y/x$. Let $g' \in \mathrm{Hom}(I, Q(K))$ be given by $g'(w) = kw$. Then $(g' - g)(x) = y - y = 0$, and for any $w \in I$, $0 = w(g' - g)(x)$ $= (g' - g)(wx) = x(g' - g)(w)$, and $g' - g = 0$. If $\psi(g) = k_g$ defines $\psi: \mathrm{Hom}(I, K) \to I^{-1}$, then $\psi\varphi = i_{I^{-1}}$, and $\varphi\psi = i_{\mathrm{Hom}(I,K)}$, $\mathrm{Hom}(I, K)$ is isomorphic to I^{-1}.

Proposition 2.3: Every integral domain K is coherent.

Proof: Let P be a projective module of finite rank. $r(P) = r_m(P)$ for some maximal ideal m (prop 5.2 of chapter 5). Since P_M is free and $(P_M)_{(0)}$ $= P_{(0)}$, $r_{(0)}(P) = r_{(0)}(P_M) = r(P_M) = r_M(P)$ for any maximal ideal M; hence P is coherent, since $r(P) = r_m(P) = r_M(P)$ for any M.

Corollary 2.4: If $I \in \mathcal{J}$ where K is an integral domain, then I is invertible if and only if I is a projective module; when this is the case, I is finitely generated.

Proof: $E(I) = (K, I, 0, \ldots)$ so I is of rank one. If I is invertible, θ: Hom $(I, K) \otimes I \to K$ is an epimorphism, $tr(I) = K$, and by proposition 5.13 of Chapter 5, I is a finitely generated projective module. If I is projective, I is coherent, and $tr(A) = K$ by proposition 5.12 of Chapter 5. Then by proposition 5.13 of Chapter 5, θ_1 Hom $(A, K) \otimes A \to K$ is an isomorphism.

Corollary 2.5: Let K be an integral domain. Then K is a Dedekind ring if and only if $\mathcal{J}$ forms an Abelian group. If K is Dedekind, then K is Noetherian.

We remark that if K is an integral domain, any projective, rank one K-module A is isomorphic to a fractional ideal of K: $A \otimes_K Q$ is free with one generator over Q, hence isomorphic to Q, so A is isomorphic to a submodule of Q, which, being finitely generated (by proposition 5.14 of Chapter 5) is in $\mathcal{J}$.

3. Some properties and characterizations of Dedekind rings.

Proposition 3.1: K is Dedekind implies that every proper integral ideal I is a product of maximal ideals.

Proof: Let A be the set of non-zero ideals in K which are not products of maximal ideals. Since K is Noetherian, A has a maximal element I, assuming A is not void. I is not a maximal ideal, hence is properly contained in a maximal ideal M. $I \subset M \subset K$, so $M^{-1} I \subset K \subset M^{-1}$, and $I \subset M^{-1} I$. Suppose $I = M^{-1} I$; then $K = II^{-1} = M^{-1}$. Hence I is properly contained

in $M^{-1} I$. Therefore $M^{-1} I \not\subset A$, and $M^{-1} I = M_1^{N_1} \cdots M_r^{N_r}$, $I = M M_1^{N_1} \cdots M_r^{N_r}$, a contradiction, and A is void.

Corollary 3.2: If K is Dedekind and $I \in \mathfrak{J}$, I is a product of maximal ideals and their inverses.

Proof: Let $k \in K$, $k \neq 0$, be such that $k I \subset K$. $k I = M_1^{N_1} \cdots M_r^{N_r}$; $k K = M_{r+1}^{N_{r+1}} \cdots M_{r+s}^{N_{r+s}}$, and $I = M_{r+1}^{-N_{r+1}} \cdots M_{r+s}^{-N_{r+s}} M_1^{N_1} \cdots M_r^{N_r}$.

Corollary 3.3: Every prime ideal in a Dedekind ring is maximal.

Proof: Each prime ideal is a product of maximal ideals, hence contains some maximal ideal.

Lemma 3.4: Let A and B be two finite sets of invertible prime ideals in an integral domain K. Suppose $\pi_A P^{r_p} = \pi_B R^{s_r}$ where the r_p and s_r are non-negative integrers. Then $A = B$ and $r_p = s_p$ for all $P \in A$.

Proof: Assume false. We may suppose $A \cap B = \phi$. Choose $P \in A$ such that P is a minimal prime of $A \cup B$. $P \supset \pi_B R^{s_r}$, hence $P \supset R$ for some $R \in B$, and $P = R$, by the minimality of P, contradicting $A \cap B = \phi$.

Proposition 3.5: If K is Dedekind, $\mathfrak{J}$ is freely generated by the maximal ideals.

Proof: If $I \in \mathfrak{J}$, $I = I_1^{-1} I_2$ for some integral I_1 and I_2. I_1 and I_2 may be assumed to be without common factors, and the representation of I as a product of maximal ideals and their inverses is unique by the lemma.

Remark 3.6: If K is a Noetherian integral domain, let $G(K)$ denote the set of projective (invertible) ideals. The proofs above give

that $G(K)$ is an Abelian group generated by the maximal elements in $G(K)$; $G(K)$ is not necessarily freely generated since its generators need not be prime ideals.

Proposition 3.7: If K is Dedekind, K is integrally closed.

Proof: Let $x \in Q$ be integral over K. There exists $k \in K$, $k \neq 0$, such that $kx^N \in K$ for all $N \geq 0$. $(kx^N) = M_1^{r_{M_1}(kx^N)} \ldots M_s^{r_{M_s}(kx^N)}$. For all maximal ideals M in K, $r_M(kx^N) = r_M(k) + Nr_M(x) \geq 0$. Since this holds for all $N \geq 0$, $r_M(x) \geq 0$ for all M. Hence the ideal $K(x)$ is a product of maximal ideals, and is contained in K, $x \in K$.

Remark 3.8: We observe that if I and J are ideals (in any commutative ring Λ) such that $I + J = \Lambda$, then $IJ \subset I \cap J = (I + J)\, I \cap J = I(I \cap J) + J(I \cap J) \subset IJ + JI = IJ$. Now let K be Dedekind. K is a Noetherian integrally closed domain such that every prime ideal is maximal, hence minimal and relevant. Thus $P^{(N)} = P^N$ for all prime ideals P in K, and the unique representation of any integral ideal in $\mathfrak{I}$ as a product of maximal ideals is its unique reduced primary decomposition. $\mathfrak{I}$ is isomorphic to $\mathfrak{D}$, the group of divisors in K. Hence we can define an order function on members of $\mathfrak{I}$. Let S be the set of all prime ideals in a Dedekind ring K. Note that if $I \in \mathfrak{I}$, then $I = \{\alpha | \alpha \in Q, \operatorname{ord}_P \alpha \geq \operatorname{ord}_P I$ for all $P \in S\}$.

Lemma 3.9: Let K be a Dedekind ring, let $I \in \mathfrak{I}$ and let $T \subset S$ be a finite set. Then there exists $\alpha \in I$ such that $\operatorname{ord}_P \alpha = \operatorname{ord}_P I$ for all $P \in T$.

Proof: Assume $\text{ord}_p I = 0$ for all $P \in S - T$. By theorem 7.11 of Chapter 6, there exists $\alpha \in Q$ such that $\text{ord}_p \alpha = \text{ord}_p I$ for all $P \in T$ and $\text{ord}_p \alpha \geq 0$ for all $P \in S - T$.

Proposition 3.10: Let K be Dedekind, $I \in \mathcal{I}$. Then a minimal set of generators of I has at most two elements.

Proof: Let $\beta \in I$, $\beta \neq 0$. Let $T \subset S$ be a finite set for which $\text{ord}_p I = \text{ord}_p \beta$ for all $P \in S - T$. Choose $\alpha \in I$ such that $\text{ord}_p \alpha = \text{ord}_p I$ for all $P \in T$. Then $(\alpha, \beta) \subset I$ while $\text{ord}_p(\alpha + \beta) = \min(\text{ord}_p \alpha, \text{ord}_p \beta) \leq \text{ord}_p I$ for all $P \in S$, $I = (\alpha, \beta)$.

We will now obtain four characterizations of Dedekind rings. We need the

Lemma 3.11: Let K be a Noetherian integral domain and let $J \in \mathcal{I}$. Suppose $I \in \mathcal{I}$ is such that $I^N \subseteq J$ for all $N \geq 0$. Then I is included in the integral closure of K.

Proof: Let $a \in I$ and let $I_N = (a, \ldots, a^N)$. Then $I_1 \subset I_2 \subset \ldots$ is an ascending chain of submodules of J. For some N, $I_N = I_{N-1}$, $a^N \in (a, \ldots, a^{N-1})$ and a is integral over K.

Theorem 3.12: Let K be an integral domain. The following are equivalent:

i) K is Dedekind. ($\mathcal{I}$ is a group)

ii) K is Noetherian, integrally closed, and every prime ideal is maximal.

iii) K is Noetherian and every prime ideal is invertible.

iv) Every proper integral ideal is a product of prime ideals.

Proof: i) $\Rightarrow$ ii) has been shown.

ii) $\Rightarrow$ iii) Every prime ideal P is relevant, hence is the minimal ideal of a principal ideal, say $(\alpha) = PR$. $K = \alpha^{-1}(\alpha) = P(\alpha^{-1} R)$, $P^{-1} = \alpha^{-1} R$.

iii) $\Rightarrow$ iv) We will prove that every prime ideal is minimal, hence maximal. Thus the (unique) reduced primary decomposition of any proper integral ideal I will be a product of prime ideals. Assume $0 \subset R \subset P$, where R and P are prime ideals, $P \neq R$. Then $RP^{-1} \subset K$, $(RP^{-1})P \subset R$. $R \not\subset P$, so $R \supset RP^{-1}$, $RP = R$. Thus $RP^N = R$ for all N and $R \subset \bigcap_N P^N = (0)$ by proposition 1.9 of Chapter 6.

iv) $\Rightarrow$ i) Let P be a prime ideal. We first show that for any $a \in K - P$, $P = P(P + (a))$. $P \supset P(P + (a))$ is clear. Let $\overline{K} = K/P$, $\overline{a} = a \pmod P$. By hypothesis $P + (a) = \pi_A R^{M_R}$, $P + (a^2) = \pi_B S^{N_S}$, where A and B are finite sets of prime ideals. $(\overline{a}) = \pi_{\overline{A}} \overline{R}^{M_R}$, $(\overline{a}^2) = \pi_{\overline{B}} \overline{S}^{N_S}$, and since $(\overline{a})$ and $(\overline{a}^2)$ are invertible in $\overline{\mathfrak{J}}$, so are all $\overline{R} \in \overline{A}$ and $\overline{S} \in \overline{B}$. By Lemma 3.4 $\overline{A} = \overline{B}$ and $2M_R = N_R$ for all $R \in A$. Hence $(P + (a))^2 = P + (a^2)$, $P \subset (P + (a))^2 \subset P^2 + (a)$. If $b \in P$, $b = c + ad$, $c \in P^2$, $d \in K$, then $a d \in P$, $d \in P$, so $P \subset P^2 + a P = P(P + (a))$.

Now if P is invertible, $K = P + (a)$ for all $a \in K - P$ and P is maximal. If P is any prime ideal and $\alpha \in P$, $\alpha \neq 0$, $P \supset (\alpha) = \pi_A R^{M_R}$ where A is a finite set of prime ideals, and $P \supset R$ for some $R \in A$, but R is invertible, hence maximal, so $P = R$, and every prime ideal is invertible. Thus every integral ideal, is invertible.

4. Valuations, valuation rings.

Definitions 4.1: A valuation of a field F is a function $|\ |$ from F to the reals such that:

i) $|\alpha| > 0$ for $\alpha \neq 0$, $|0| = 0$.

ii) $|\alpha\,\beta| = |\alpha|\ |\beta|$

iii) $|\alpha + \beta| \leq |\alpha| + |\beta|$

If $|\alpha + \beta| \leq \max(|\alpha|, |\beta|)$, then $|\ |$ is called a non-Archimedian valuation. Observe that if $|\ |$ is non-Archimedian and $|\alpha| > |\beta|$, then $|\alpha + \beta| \leq |\alpha|$ and $|\alpha| = |\alpha + \beta - \beta|$, $\max(|\alpha + \beta|, |\beta|) = |\alpha + \beta|$, so that $|\alpha + \beta| = |\alpha|$.

Definition 4.2: A valuation which is non-Archimedian and non-trivial (there is an $\alpha \in F$, $\alpha \neq 0$, with $|\alpha| \neq 1$) is called discrete if $\operatorname{im} |\ |$ is an infinite cyclic (multiplicative) group.

Definition 4.3: Let $|\ |$ be a non-Archimedian valuation on a field F. Define $\mathcal{O} = \{\alpha | \alpha \in F, |\alpha| \leq 1\}$ and $P = \{\alpha | \alpha \in F, |\alpha| < 1\}$. By the definition of a non-Archimedian valuation, $\mathcal{O}$ is a ring and P is its only maximal ideal. $\mathcal{O}$ is called the valuation ring of $|\ |$ and will be denoted $\mathcal{O}(P)$ when more than one such ring are being considered.

Proposition 4.4: Let $\mathcal{O}$ be a valuation ring. Let I and J be proper ideals in $\mathcal{O}$. Then $I \subset J$ or $J \subset I$.

Proof: Assume $I \not\subset J$. Let $a \in I$, $a \notin J$. Let $b \in J$, $b \neq 0$.

$a \notin (b)$, so $a/b \notin \mathcal{O}$, $|a/b| > 1$, $|b/a| < 1$, $b/a \in \mathcal{O}$,

$b \in (a) \subset I$.

Definition 4.5: The ordinal type of the totally ordered set of proper prime ideals of $\mathcal{O}$ is called the rank of the valuation $|\ |$.

Proposition 4.6: Let $\mathcal{O}$ be a valuation ring in a field F. Then

any proper subring R of F containing $\mathcal{O}'$ is the localization $\mathcal{O}'_P$ of $\mathcal{O}'$ at a prime ideal $P \subset \mathcal{O}'$.

Proof: Let I be the set of non-units of R. If $x, y \in I$, then x/y or y/x, say y/x, is in $\mathcal{O}'$, hence in R, and $x(1 + y/x) = x + y \in I$. Hence I is an integral ideal of R. I is a prime R-ideal contained in the maximal ideal of $\mathcal{O}'$, so $R = \mathcal{O}'_I$.

Corollary 4.7: The (non-Archimedian) valuation $|\ |$ on F is of rank one if and only if $\mathcal{O}'$ is a maximal proper subring of F.

Proposition 4.8: A valuation ring $\mathcal{O}'$ is Noetherian if and only if its value group (image $|\ |$) is discrete and when this is the case $|\ |$ is of rank one.

Proof: i) Let $\mathcal{O}'$ be Noetherian and $I \subset \mathcal{O}'$ be an ideal. Let $I = (u_1, \ldots, u_n)$ and let $|u_1| \geq |u_i|$ for $2 \leq i \leq N$. Then $|u_i/u_1| \leq 1$, $u_i \in u_1 \mathcal{O}'$, and $I = (u_1)$. Thus I is principal. Let P be the maximal ideal of $\mathcal{O}'$ and $P = (x)$. If $P = (0)$, $\mathcal{O}'$ is a field and $|\ |$ is trivial. Assuming $P = (x) \neq 0$, we have that $\mathcal{O}'$ is a regular local ring of dimension one. By proposition 6.11 of Chapter 6, if $y \in \mathcal{O}'$, $y \in M^N$, $y \notin M^{N+1}$, then $(y) = M^N$, $y = \lambda x^N$ where λ is a unit, $|y| = |x^N| = |x|^N$ and $|x|$ generates the value group.

ii) If $|\ |$ is discrete, let $|\pi|$ generate the value group. We may assume $|\pi| < 1$ (replacing π by π^{-1} if necessary). $(\pi) = \{\alpha | \alpha \in F, |\alpha| \leq |\pi|\} = \{\alpha | \alpha \in F, |\alpha| < 1\}$, so (π) is the maximal ideal of $\mathcal{O}'$. Let I be an ideal, $I \subset M^N$, $I \not\subset M^{N+1}$. Let $a \in I$, $a \notin M^{N+1}$. $a = \lambda \pi^N$, λ a unit, $M^N = (a) \subset I \subset M^N$, and I is principal.

Proposition 4.9: Let $\mathcal{O}'$ be a valuation ring in a field F. Then $\mathcal{O}'$ is integrally closed.

Proof: Let $\alpha \in F$ and $\alpha^N + a_1 \alpha^{N-1} + \ldots + a_N = 0$, $a_i \in \mathcal{O}'$. Assume $|\alpha| > 1$. Then $|\alpha^N| > |a_i \alpha^{N-i}|$, $1 \leq i \leq N$, $|\alpha^N + a_1 \alpha^{N-1} + \ldots + a_N| = |\alpha^N| > 1 > 0$, a contradiction.

Theorem 4.10: The following are equivalent

i) $\mathcal{O}'$ is a discrete rank one valuation ring.

ii) $\mathcal{O}'$ is a discrete valuation ring.

iii) $\mathcal{O}'$ is a local Dedekind ring, not a field.

iv) $\mathcal{O}'$ is a regular local ring of dimension one.

Proof: i) $\Rightarrow$ ii) is obvious.

ii) $\Rightarrow$ iii) $\mathcal{O}'$ is a Noetherian, integrally closed domain with one prime ideal by propositions 4.8 and 4.9, hence is Dedekind by ii) of theorem 3.12.

iii) $\Rightarrow$ iv) follows from corollary 7.4 of Chapter 6, which states that the localization of an integrally closed Noetherian integral domain at a relevant prime ideal is regular and of dimension one, and the fact that $\mathcal{O}'_M = \mathcal{O}'$.

iv) $\Rightarrow$ i): Let c, $0 < c < 1$ be a constant. Define $|\ |$ on $Q(\mathcal{O}')$ by $|\pi| = c$ where π generates M, $|\lambda| = 1$ if λ is a unit in $\mathcal{O}'$ and $|0| = 0$. Any other element of $\mathcal{O}'$ is a unit times a power (positive, negative or zero) of π by proposition 6.10 of Chapter 6, so $|\ |$ is well defined. $|\ |$ is clearly non-Archimedian and discrete with valuation ring $\mathcal{O}'$. It is of rank one by proposition 4.8.

Corollary 4.11: If K is a Noetherian integrally closed domain and

P is a minimal prime ideal of K, then K_p is a discrete rank one valuation ring. If the minimal prime ideals of K are indexed by I, $K = \bigcap_{i \in I} L_{p_i}$.

Proof: K_p is a regular local ring of dimension one by corollary 7.4 of Chapter 6, hence is a discrete rank one valuation ring by the theorem. We define each valuation by fixing c, $0 < c < 1$, and defining $|\alpha|_{p_i} = c^{\operatorname{ord}_{p_i} \alpha}$ for $\alpha \in Q(K)$. $\alpha \in K$ if and only if $\operatorname{ord}_{p_i} \alpha \geq 0$ for all $i \in I$, which holds if and only if $\alpha \in \hat{\theta}(P_i) = K_{p_i}$ for all $i \in I$.

5. The structure of finitely generated torsion free nodules over Dedekind rings.

In the remainder of this chapter we will completely determine the structure of finitely generated modules over Dedekind rings.

Definition 5.1: Let K be an integral domain. Let A be a K-module. An element $a \in A$ is said to be a torsion element if there exists $k \in K$, $k \neq 0$, such that $ka = 0$. The set A_T of all torsion elements of A is a submodule of A, called the torsion submodule. If $A_T = 0$, A is said to be torsion free. A/A_T is torsion free, and $0 \to A_T \to A \to A/A_T \to 0$ is an exact sequence.

Proposition 5.2: Let K be an integral domain, $\pi: K \to Q$ be its field of fractions and let A be a K-module. Then $\ker (\pi \otimes i_A)$, $\pi \otimes i_S: K \otimes A \to Q \otimes A$, is isomorphic to A_T.

Proof: If $a \in A_T$ and $k a = 0$ with $k \in K$, $k \neq 0$, then $1 \otimes a \to 1/k \otimes ka = 0$. If $1 \otimes a = 0$ in $K \otimes A$, there exists $k \in K$, $k \neq 0$, such that $k a = 0$.

Corollary 5.3: A flat module A over an integral domain is torsion free.

Proof: $0 \to K \otimes A \to Q \otimes A$ is exact, so $A_T = 0$.

Proposition 5.4: If A is a finitely generated torsion free module over an integral domain K, then there exists a monomorphism of A into a finitely generated free module F; F may be chosen to have as many generators as the maximal number of linearly independent elements of A.

Proof: A may be regarded as a submodule of $Q \otimes A$. Let $(a_1,\ldots,a_N) = A$ and let the vector space $Q \otimes A$ over Q have a basis $e_1,\ldots, e_M$. $a_i = \sum_{j=1}^{M} g_{ij}\, e_j$, $g_{ij} \in Q$, Let $k \in K$, $k \neq 0$, be such that $kg_{ij} \in K$ for all g_{ij}. $a_i = \sum_{j=1}^{M} (kg_{ij})(k^{-1} e_j)$, so that A is contained in the sub-K-module F of $Q \otimes A$ generated by the $k^{-1} e_j$. F is free, and the $k^{-1} e_j$ are linearly independent over K.

Corollary 5.5: Let K be a Dedekind ring and let A be a finitely generated K-module. The following are equivalent

i) A is projective

ii) A is flat

iii) A is torsion free

Proof: i) $\Rightarrow$ ii) is clear (proposition 2.11 of Chapter 3).

ii) $\Rightarrow$ iii) was shown in corollary 5.3

iii) $\Rightarrow$ i) follows from the proposition and theorem 1.3.

Proposition 5.6: Let A be a finitely generated torsion free module over a Dedekind ring K. Then A is isomorphic to $F \oplus I$, where I is an ideal and F is free with $d(A) - 1$ generators, $d(A)$

being the maximal number of linearly independent elements of A.

Proof: We proceed by induction on $d(A)$. If $d(A) = 1$, there is a monomorphism $A \to K$ and the result is clear. Let $d(A) = N \geq 2$ and assume the result holds for $d(A) = N - 1$. We will obtain an epimorphism $f\colon A \to K$. Then if $A' = \ker f$ $d(A') = N - 1$. A will be isomorphic to $A' \oplus K$ while A' is isomorphic to $F' \oplus I$ where F is free with $d(A') - 1 = d(A) - 2$ generators, and the proof will be complete. Let $A = \{I | I \in \mathcal{L}$, $I \subset K$, and there exists $f\colon A \to I$ such that f is an epimorphism$\}$. Let I be maximal in A and let $A' = \ker f$, $f\colon A \to I$. A is isomorphic to $A' \oplus I$, so by the maximality of I, $tr(A') \subset I$. But by proposition 5.12 of Chapter 5, $\det(A') = K$, so $tr(A') = K$, and $I = K$.

Corollary 5.7: If A is a finitely generated torsion free module over a Dedekind ring, and A is isomorphic to $F \oplus I$, then I is uniquely determined up to isomorphism.

Proof: $E(A) = E(F \oplus I) = E(F) \otimes E(I)$. $E(A)_N = E(F)_{N-1} \otimes E(I)_1$ which is isomorphic to I.

Remark 5.8: We obtain a second proof that if $I \in \mathcal{I}$, then a minimal set of generators of I has at most two elements: $E(I \oplus I^{-1})_2 = E(I)_1 \otimes E(I^{-1})_1$ is isomorphic to K, so $I \oplus I^{-1}$ is free with two generators and I can be generated by two elements.

6. The structures of finitely generated torsion modules over Dedekind ring.

Now if A is a finitely generated module over a Dedekind ring, $0 \to A_T \to A \to A/A_T \to 0$ is split exact, and A is isomorphic to $A_T \oplus A/A_T$, the structure of A/A_T being shown.

We remark that we cannot represent a ring as a direct sum. This follows from our assumption that all rings are unitary and that for $f: \Lambda \to T$ to be a morphism of rings, it is necessary that $f(1_\Lambda) = i_T$: an injection of a direct factor of a ring Λ into Λ cannot be a morphism of rings. No such difficulty arises in the case of modules, for which a finite direct sum is the same as a finite direct product.

Let K be Dedekind, and let A be a finitely generated torsion module. If $A = (a_1,\ldots,a_N)$ and $k_i \in K$, $k_i \neq 0$ is such that $k_i a_i = 0$, then $k = k_1 \cdot \ldots \cdot k_N$ is such that $k A = 0$. Let $I = \text{ann } (A)$, $I \neq 0$. A is a K/I-module. Assume $I = M_1^{N_1} \ldots M_r^{N_r}$ is the representation of I as a product of maximal ideals. We will first show that K/I is isomorphic to the direct product $(K/M_1^{N_1},\ldots,K/M_r^{N_r})$ and that A is isomorphic to $(A_1,\ldots,A_r) = A_1 \oplus \ldots \oplus A_r$ where ann $(A_i) = M_i^{N_i}$.

Proposition 6.1: Let Λ be a commutative ring. Let I and J be Λ-ideals such that $I + J = \Lambda$. Then $\Lambda/I \cap J$ is isomorphic to $\Lambda/I \oplus \Lambda/J$.

Proof: Let (π_1,π_2) : $\Lambda/I \cap J \to (\Lambda/I,\ \Lambda/J)$. (π_1, π_2) is clearly a monomorphism. Let $([x], [y]) \in (\Lambda/I, \Lambda/J)$, and $(\pi_1, \pi_2)(x) = ([x], [x])$. Taking differences, to prove (π_1, π_2) an epimorphism

it is sufficient to show that $(0, \{z\}) \in \text{im}\,(\pi_1, \pi_2)$ for all $[z] \in \Lambda/J$. Let $1 = a + b$, $a \in I$, $b \in J$. Then $z = az + bz$, $(\pi_1, \pi_2)(z) = ([bz], [az])$, $(\pi_1, \pi_2)(az) = (0, [az]) = (0, [z])$.

Corollary 6.2: If $I \subset \Lambda$ is such that $I = M_1^{N_1} \ldots M_r^{N_r}$ where the M_i are distinct maximal ideals, then Λ/I is isomorphic to $(\Lambda/M_1^{N_1}, \ldots, \Lambda/M_r^{N_r})$.

Proof: $I = M_1^{N_1} \cap \ldots \cap M_r^{N_r}$; Λ/I is isomorphic to $(\Lambda/M_1^{N_1} \ldots M_{r-1}^{N_{r-1}})_1$, and inductively Λ/I is isomorphic to $(\Lambda/M_1^{N_1}, \ldots, \Lambda/M_r^{N_r})$.

Proposition 6.3: If Λ is a commutative ring and Λ is isomorphic to $(J_1, \ldots, J_r)$, then there exists a set of orthogonal idempotents $e_1, \ldots, e_r$ with $e_i \in (0, \ldots, 0, J_i, 0, \ldots, 0)$ and $(e_1, \ldots, e_r) = 1$. If B is a Λ-module, $B = e_i B + \ldots + e_r B$. If $b \in e_i B \cap e_j B$, $b = e_i b_1 = e_j b_2 = e_i^2 b_1 = e_j e_j b_2 = 0$, and the sum is direct.

Corollary 6.4: If A is a finitely generated torsion module over a Dedekind ring and $I = \text{ann}\,(A) = M_1^{N_1} \ldots M_r^{N_r}$, then $A = A_1 \oplus \ldots \oplus A_r$, where A_i is a module over $K/M_i^{N_i}$.

Proof: A is a K/I-module and $K/I = (K/M_1^{N_1}, \ldots, K/M_r^{N_r})$.

It remains to study the structure of finitely generated modules over rings of the type K/M^N. K/M^N is a primary ring (with maximal ideal M/M^N), all of whose ideals are powers of the maximal ideal, since the only ideals of K containing M^N are lower powers of M. Let L be a primary ring all of whose ideals are powers of the maximal ideal M, and with $M^N = (0)$.

Lemma 6.5: M is a primcipal ideal, hence every proper ideal is principal. If $M = (t)$, $t^N = 0$,

Proof: Let $t \in M$, $t \notin M^2$. $M \supset (t) + M^r$, $1 \leq r \leq N$. $(t) + M^r = M^s$ for some s, but $t \notin M^2$, so $s = 1$. In particular, $M = (t) + M^N = (t)$. Hence $M^r = (t^r)$, $1 \leq r \leq N$. $(0) = M^N = (t^N)$, so $t^N = 0$.

Lemma 6.6: Let $0 \to A \xrightarrow{i} B \xrightarrow{\pi} L/M^{N-r} \to 0$ be an exact sequence of L-modules, where $N \geq r \geq 0$. Then if $f: A \to L$ is a morphism, there exists a morphism $\tilde{f}: B \to L$ such that $\tilde{f} i = f$.

Proof: If $r = N$, A is isomorphic to B, and if $r = 0$, B is isomorphic to $A \oplus L$, and the result is trivial is these cases. Assume $N > r > 0$. Let $M = (t)$. Choose $b \in B$ such that $\pi(b) = [1]$. $\pi(t^{N-r}b) = 0$ implies $t^{N-r}b = i(a_o)$ for some $a_o \in A$. $0 = t^r(t^{N-r}b) = t^r(i(a_o)) = i(t^r a_o)$, so $t^r a_o = 0$ and $t^r f(a_o) = 0$. Thus $f(a_o) \in M$, $f(a_o) = t^s v$ for some $s \geq N - r$ and $v \in L - M$. Write $f(a_o) = t^{N-r}u$, where $u = vt^{s-(N-r)}$. Note that any $x \in B$ has at least one representation $x = i(a) + kb$, $k \in L$. Define $\tilde{f}(b) = u$, $\tilde{f}(x) = f(a) + ku$. We must show that $\tilde{f}$ is well defined. Assume $i(a) + kb = i(a') + k'b$. Then $i(a - a') + (k - k')b = i(a'') + k''b = 0$. $\pi(i(a'') + k''b) = [k''] = [0]$, $k'' \in M^{N-r}$, $k'' = wt^{N-r}$ say. But $i(a'') + wt^{N-r}b = i(a'') + wi(a_o) = i(a'' + wa_o) = 0$ implies $a'' + wa_o = 0$. Now $\tilde{f}(i(a'') + wt^{N-r}b) = f(a'') + wt^{N-r}u = f(a'') + wf(a_o) = f(a'' + wa_o) = 0$, and $\tilde{f}$ is well defined. Clearly $\tilde{f}i = f$ and the lemma is proven.

Lemma 6.7: L is an injective L-module.

Proof: Let $0 \to A \xrightarrow{i} B$ be an exact sequence of L-modules. If $f: A \to L$ is a morphism, we must find a morphism $\tilde{f}: B \to L$ such that $\tilde{f}i = f$.

Let $A = \{(B', f') | B'$ is a submodule of B, $f': B' \to L$ is a morphism, and there is a commutative diagram with exact row

$$\begin{array}{ccccc} 0 & \to & A & \xrightarrow{i'} & B' \} . \\ & & f \downarrow & \swarrow & f' \\ & & L & & \end{array}$$

$(A, f) \in A$, so A is not empty. Partial order A by defining $(B', f') < (B'', f'')$ if $B' \subset B''$ and $f''|_{B'} = f'$. Let $\{(B_i', f_i')\}_{i \in I}$ be a totally ordered subset and $\overline{B} = \bigcup_{i \in I} B_i'$. If $b \in \overline{B}$, $b \in B_i'$ for some $i \in I$. Define $\overline{f}(b) = f_i'(b)$. Then $(\overline{B}, \overline{f}) \in A$, A is inductive, and by Zorn's lemma has maximal elements. Let $(\hat{B}, \hat{f}) \in A$ be maximal. Assume $x_o \in B - \hat{B}$. Let $B_1 = \hat{B} + L x_o$. If $I = \text{ann}(L x_o)$, $L x_o = (L/I) x_o$ is isomorphic to L/I. $B_1/\hat{B}$ is isomorphic to L/M^{N-r} for some r, $0 \leq r < N$, and by the preceding lemma, there exists $f_1 : B_1 \to L$ such that

$$\begin{array}{ccccccccc} 0 & \to & \hat{B} & \to & B_1 & \to & L/M^{N-r} & \to & 0 \\ & & \hat{f}\downarrow & \swarrow & f_1 & & & & \\ & & L & & & & & & \end{array}$$

is a commutative diagram with exact row. Now $(B_1, f_1) \in A$ and $(\hat{B}, \hat{f}) < (B_1, f_1)$, a contradiction, so $B = \hat{B}$ and the proof is complete.

Proposition 6.8: Let A be a finitely generated L-module. Then:

i) A is isomorphic to a direct sum $L/M^{k_1} \oplus \ldots \oplus L/M^{k_s}$, $0 < k_i \leq N$.

ii) The number of modules of type L/M^j, $0 < j \leq N$, occurring in such a decomposition is unique.

Proof: i) Let $I = \text{ann}(A)$, $I = M^k$, $0 < k \leq N$, and A is an L/M^k-module. Let $a_o \in A$ be such that $t^{k-1} a_o \neq 0$, and let $i : L/M^k \to A$ be defined by $i(\overline{k}) = \overline{k}\, a_o$. $0 \to L/M^k \xrightarrow{i} A$ is an exact sequence. Let $A' = \text{coker}(i)$. L/M^k satisfies the conditions on L in the previous lemma, hence is injective. Thus L/M^k is a direct summand of A, A is isomorphic to $L/M^k \oplus A'$.

Repeating the argument on A', since A is finitely generated, A is isomorphic to $L/M^{k_1} \oplus \ldots \oplus L/M^{k_s}$.

ii) M annihilates $M_jA/M^{j+1}A$, $j = 0,\ldots,N-1$ and $M_jA/M^{j+1}A$ is a vector space over L/M of dimension d_j say. $d_{N-1} = \dim_{L/M}(M^{N-1}A)$ is the number of summands of type L/M^N, since all other summands are annihilated by M^{N-1}. Similarly, $d_{N-2} - d_{N-1}$ is the number of summands of type L/M^{N-1}. Inductively, the number of summands of each type and the total number of summands are unique.

We summarize the results of the last two sections in the

Theorem 6.9: Let A be a finitely generated module over a Dedekind ring K. Let A' be the torsion submodule and $A'' = A/A'$. Then

i) $A \cong A' \oplus A''$

ii) $A'' \cong F \oplus I$ where F is free with $d(A'') - 1$ generators and I is an ideal isomorphic to $E(A'')_{d(A'')}$.

iii) If $A' \neq 0$ and $\operatorname{ann}(A') = M_1^{N_1} \ldots M_r^{N_r}$, then $A' \cong A'_1 \oplus \ldots \oplus A'_r$, where A'_i is uniquely determined by the condition $\operatorname{ann}(A'_i) = M_i^{N_i}$.

iv) Each A'_i is isomorphic to a finite direct sum of cyclic submodules of type $(K/M_i^{N_i})/(M_i/M_i^{N_i})^j = K/M_i^j$, $0 < j \leq N_i$, where the number of summands of each type is uniquely determined by A'_i.

As a final result we observe that for $K = Z$ we obtain the

Corollary 6.10: Let G be a finitely generated Abelian group. Then G is a direct sum of a uniquely determined number of infinite cyclic subgroups and of its Sylow subgroups; each Sylow subgroup is the direct sum of cyclic subgroups, the orders of which are uniquely determined.