# Chapter 6. Dedekind Domains

**6.1 Definition:** A commutative ring $R$ is called **Noetherian** when it satisfies the ascending chain condition on ideals, that is when, for every chain of ideals $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ in $R$, there exists an index $m \in \mathbf{Z}^+$ such that $A_k = A_m$ for all $k \geq m$.

**6.2 Theorem:** *Let $R$ be a commutative ring. Then $R$ is Noetherian if and only if every ideal in $R$ is finitely generated as an $R$-module.*

Proof: Suppose that $R$ is Noetherian and let $A$ be any ideal in $R$. Suppose, for a contradiction, that $A$ is not finitely generated as an $R$-module. Note that $A \neq \{0\}$ (since the ideal $\{0\}$ is generated by the set $\{0\}$). Choose $0 \neq a_1 \in A$. Since $a_1 \in A$ we have $(a_1) \subseteq A$, but since $A$ is not finitely generated we have $A \neq (a_1)$, and so $(a_1) \subsetneqq A$. Choose $a_2 \in A$ with $a_2 \notin (a_1)$. Since $a_2 \notin (a_1)$ we have $(a_1) \subsetneqq (a_1, a_2)$, since $a_1, a_2 \in A$ we have $(a_1, a_2) \subseteq A$, and since $A$ is not finitely generated we have $(a_1, a_2) \neq A$, and so $(a_1) \subsetneqq (a_1, a_2) \subsetneqq A$. Continuing this procedure, we obtain an infinite ascending chain of ideals $\{0\} \subsetneqq (a_1) \subsetneqq (a_1, a_2) \subsetneqq (a_1, a_2, a_3) \subsetneqq \cdots$ which contradicts the fact that $R$ is Noetherian.

Suppose, conversely, that every ideal in $R$ is finitely generated as an $R$-module. Let $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ be an ascending chain of ideals in $R$. Let $A = \bigcup_{k=1}^{\infty} A_k$. Then $A$ is an ideal in $R$ so it is finitely generated as an $R$-module. Choose elements $a_1, a_2, \cdots, a_n$ so that $A = (a_1, \cdots, a_n)$. For each index $i \in \{1, 2, \cdots, n\}$, since $a_i \in A = \bigcup_{k=1}^{\infty} A_k$ we can choose an index $k_i$ such that $a_i \in A_{k_i}$. Let $m = \max\{k_1, k_2, \cdots, k_n\}$. For each index $i$ we have $a_i \in A_{k_i} \subseteq A_m$ and so $A = (a_1, \cdots, a_n) \subseteq A_m$. For all $k \geq m$ we have $A_k \subseteq \bigcup_{j=1}^{\infty} A_j = A \subseteq A_m \subseteq A_k$ and hence $A_k = A_m$. Thus $R$ is Noetherian, as required.

**6.3 Theorem:** *Let $R$ be a commutative Noetherian ring. For every nonzero ideal $A$ in $R$ there exist prime ideals $P_1, P_2, \cdots, P_\ell$ in $R$ such that $P_1 P_2 \cdots P_\ell \subseteq A$.*

Proof: Let $S$ be the set of all nonzero ideals $A$ in $R$ for which there do not exist prime ideals $P_i$ with $P_1 P_2 \cdots P_\ell \subseteq A$. Suppose, for a contradiction, that $S \neq \emptyset$. Since $R$ is Noetherian, it follows that every chain in $S$ has a maximal (indeed a maximum) element. By Zorn's Lemma, it follows that $S$ has a maximal element. Let $A$ be a maximal elements in $S$. Note that $A$ is not prime (because no prime ideal lies in $S$). Since $A$ is not prime we can choose elements $a, b \in R$ such that $ab \in A$ but $a \notin A$ and $b \notin A$. Since $a \notin A$ we have $A \subseteq A + (a)$ and so (since $A$ is maximal in $S$) $A + (a) \notin S$. Since $A + (a) \notin S$ we can choose prime ideals $P_i$ such that $P_1 P_2 \cdots P_\ell \subseteq A + (a)$. Similarly $A + (b) \notin R$ so we can choose prime ideals $Q_i$ such that $Q_1 Q_2 \cdots Q_m \subseteq A + (b)$. But then it follows that

$$P_1 P_2 \cdots P_\ell Q_1 Q_2 \cdots Q_m \subseteq \big(A + (a)\big)\big(B + (b)\big) = A\,A + A(b) + A(a) + (ab) \subseteq A$$

which implies that $A \notin S$, giving the desired contradiction.

**6.4 Definition:** A **Dedekind domain** is a Noetherian, integrally closed, integral domain in which every nonzero prime ideal is maximal.

**6.5 Definition:** Let $R$ be a Dedekind domain with quotient field $K$. For a subset $A \subset R$ we write

$$A^* = \big\{u \in K \,\big|\, uA \subseteq R\big\} = \big\{u \in K \,\big|\, ua \in R \text{ for all } a \in A\big\}.$$

Note that if $A$ is an ideal in $R$ then we have $A \subseteq R \subseteq A^*$ and $AA^* \subseteq R$.

**6.6 Theorem:** *Let $R$ be a Dedekind domain and let $P$ be a nonzero prime ideal in $R$, and let $A$ be any nonzero ideal in $R$. Then*
*(1) $R \subsetneqq P^*$,*
*(2) $A \subsetneqq AP^*$, and*
*(3) $PP^* = R$.*

Proof: We know that $P \subsetneqq R \subseteq P^*$. To prove that $R \neq P^*$ we shall construct an element $u = \frac{a}{b} \in K$ with $u \in P^* \setminus R$. Choose $0 \neq b \in P$. Choose nonzero prime ideals $P_i$ such that $P_1P_2 \cdots P_\ell \subseteq (b) = bR$ with the number $\ell$ as small as possible. Since $P$ is prime and $P_1P_2 \cdots P_\ell \subseteq (b) \subseteq P$, it follows that $P_i \subseteq P$ for some index $i$, say $P_1 \subseteq P$. Since every prime ideal in $R$ is maximal, the ideal $P_1$ is maximal. Since $P_1$ is maximal and $P_1 \subseteq P \subsetneqq R$, we have $P = P_1$. In the case that $\ell = 1$, we have $P = P_1 \subseteq (b) \subseteq P$ hence $P = (b)$. In this case, we take $a = 1$ and let $u = \frac{a}{b} = \frac{1}{b}$. Since $(b) = P \subsetneqq R$ it follows that $b$ is not a unit so $u = \frac{1}{b} \notin R$. Since $\frac{1}{b}P = \frac{1}{b}\, bR = R$, it follows that $u = \frac{1}{b} \in P^*$. Suppose now that $\ell > 1$. Since $\ell$ was chosen to be as small as possible, $P_2P_3 \cdots P_\ell$ is not a subset of $(b)$. Choose $a \in P_2P_3 \cdots P_\ell$ with $a \notin (b)$ and let $u = \frac{a}{b}$. Since $a \notin (b)$ we have $a \neq br$ for any $r \in R$ and so $u = \frac{a}{b} \notin R$. Since $a \in P_2P_3 \cdots P_\ell$ it follows that $aP = aP_1 \in P_1P_2 \cdots P\ell \subseteq (b) = bR$ and so $uP = \frac{a}{b}P \in R$ hence $\frac{a}{b} \in P^*$. Thus $R \subseteq P^*$, as required.

Let us prove Part (2). Since $R \subseteq P^*$ we have $A = AR \subset AP^*$. Suppose, for a contradiction, that $A = AP^*$. Since $R$ is Noetherian, $A$ is finitely generated as an $R$-module, so we can choose $a_1, a_2, \cdots, a_n \in A$ such that $A = (a_1, a_2, \cdots, a_n) = \text{Span}_R\{a_1, a_2, \cdots, a_n\}$.

**6.7 Theorem:** *Let $A$ be a free* $\mathbf{Z}$*-module of rank $n$. Let $B$ be a submodule of $A$. Then $B$ is free of rank $r$ for some $r \leq n$. Indeed there exists a basis $\{u_1, u_2, \cdots, u_n\}$ for $A$ over* $\mathbf{Z}$*, an integer $r$ with $0- \leq r \leq n$, and positive integers $d_1, d_2, \cdots, d_r$ with $d_1 | d_2$ , $d_2 | d_3$ , $\cdots$ , $d_{r-1} | d_r$, such that $\big\{ d_1 u_1, d_2 u_2, \cdots, d_r u_r \big\}$ is a basis for $B$ over* $\mathbf{Z}$.

Proof: I may include a proof later.