VIII. Dedekind Domains & Discrete Valuation Domains

Definition 1. A ring \( R \) is a Dedekind domain if \( R \) is an integrally closed Noetherian ring with Krull dimension one.

Example 2.
1. All PIDs are Dedekind domains.
2. \( \mathbb{Z}[\sqrt{-5}] \) is a Dedekind domain.
3. The ring of integers in an algebraic number field is a Dedekind Domain.

Lemma 3. Let \( I \) be a nonzero prime ideal of a Dedekind domain \( R \) with quotient field \( K \) and let \( J = \{ x \in K \mid xI \subseteq R \} \). Then:
   1. \( R \subseteq J \).
   2. \( J \) is a fractional ideal of \( R \) and \( IJ = R \).

Theorem 4. Let \( I \) be a nonzero ideal of a Dedekind domain \( R \). Then \( I \) can be factored uniquely as a product of prime ideals \( I = P_1^{n_1}P_2^{n_2} \cdots P_r^{n_r} \) for some distinct nonzero prime ideals \( P_i \) and \( n_i \in \mathbb{Z}^+ \).

Corollary 5. Let \( I \) be a nonzero fractional ideal of a Dedekind domain \( R \). Then \( I \) can be factored uniquely as a product of prime ideals \( I = P_1^{n_1}P_2^{n_2} \cdots P_r^{n_r} \) for some distinct nonzero prime ideals \( P_i \) and \( n_i \in \mathbb{Z} \).

Note: If a nonzero fractional ideal is factored (uniquely) as a product \( I = P_1^{n_1}P_2^{n_2} \cdots P_r^{n_r} \) of nonzero prime ideals of \( R \), then \( I \) is an (integral) ideal of \( R \) if and only if \( n_i \geq 0 \) for each \( i \in \{1, 2, \ldots, r\} \).

Definition 6. Let \( I_1 \) and \( I_2 \) denote nonzero ideals of a ring \( R \). We say that \( I_1 \) divides \( I_2 \) provided \( I_2 = JI_1 \) for some ideal \( J \) in \( R \).

Corollary 7. Let \( R \) be a Dedekind domain with ideals \( I_1 \) and \( I_2 \). Then \( I_1 \) divides \( I_2 \) if and only if \( I_1 \supseteq I_2 \).

Proposition 8. Let \( I \) be a nonzero fractional ideal of a Dedekind domain \( R \). Then there exists a nonzero (integral) ideal \( J \) of \( R \) such that \( IJ \) is a principal ideal of \( R \).

Lemma 9. Let \( P_1, P_2, \ldots, P_n \) denote distinct nonzero prime ideals in a Dedekind domain \( R \). Let \( J = P_1P_2 \cdots P_n \) and set \( Q_i = P_1 \cdots P_{i-1}P_{i+1} \cdots P_n \) for each \( i \), \( 1 \leq i \leq n \). (If \( n = 1 \), take \( Q_1 = R \).) Let \( L \) be a nonzero ideal of \( R \). For each \( i \), choose \( a_i \in IQ_i \) with \( a_i \notin IJ \) and set \( a = a_1 + a_2 + \cdots + a_n \). Then \( a \in L \), but \( a \notin IP_i \) for any \( i \).
Proposition 10. Let $I$ be a nonzero ideal of a Dedekind domain $R$. There is a nonzero ideal $I'$ such that $II'$ is a principal ideal. If $J$ is a nonzero ideal of $R$, $I'$ can be chosen such that $I'$ is relatively prime to $J$.

Corollary 11. Let $I$ be a nonzero ideal of a Dedekind domain $R$ and let $0 \neq a \in I$. Then $I = (a, b)$ for some $b \in I$.

Example 12. The ring $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain that is not a PID.

Definition 13. Let $G$ be a (totally ordered) group isomorphic to $\mathbb{Z}$. A discrete valuation on a field $K$ is a function $\nu : K^* \to G$ (where $K^* = K - \{0\}$) satisfying

1. $\nu$ is surjective;
2. $\nu(xy) = \nu(x) + \nu(y)$, for all $x, y \in K^*$, (i.e. $\nu$ is a homomorphism);
3. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, for all $x, y \in K^*$ with $x + y \neq 0$.

The valuation $\nu$ is often extended to all of $K$ by defining $\nu(0) = \infty$ (then (2) and (3) hold for all $x, y \in K$).

The set $R = \{x \in K^*|\nu(x) \geq 0\} \cup \{0\}$ is a subring of $K$ called the valuation ring of $\nu$. The image $\nu(K)$ is called the value group of $\nu$.

An integral domain $R$ is called a Discrete Valuation Ring (DVR) if $R$ is the valuation ring of a discrete valuation $\nu$ on the field of fractions of $R$.

Example 14. Let $p$ be a fixed prime number, and $K = \mathbb{Q}$. Define

$$\nu_p : \mathbb{Q}^* \to \mathbb{Z} \text{ by } \nu_p\left(\frac{a}{b}\right) = \nu_p\left(p^n\frac{a_1}{b_1}\right) = n$$

where $\frac{a}{b} = p^n\frac{a_1}{b_1}$, $p \nmid a_1$, and $p \nmid b_1$. Then $\nu_p$ is a discrete valuation on $\mathbb{Q}$, and

$$\mathbb{Z}_{(p)} = \left\{ \frac{x}{y} \mid x, y \in \mathbb{Z}, y \neq 0, \gcd(y, p) = 1 \right\}$$

is a DVR with respect to $\nu_p$.

Proposition 15. Let $R$ be a DVR and let $\nu : K \to \mathbb{Z}$ be the associated discrete valuation.

1. The set $M = \{x \in R \mid \nu(x) > 0\}$ is a principal ideal of $R$.
2. $R$ is a Noetherian local ring of dimension one with unique maximal ideal $M$.
3. $R$ is integrally closed.
4. Every nonzero ideal of $R$ is a power of $M$. 
Definition 16. Let $\nu$ be a discrete valuation on a field $K$. An extension $\nu'$ of $\nu$ to an extension field $L$ of $K$ is a discrete valuation of $\nu'$ of $L$ whose restriction on $K$ is $\nu$.

Note: Given a discrete valuation $\nu$ on a field $K$ and a simple extension $K(a)$ of $K$, there exists an extension $\nu'$ of $\nu$ which is a discrete valuation on $K'$.

Example 17. Let $\nu : \mathbb{Q}^* \to \mathbb{Z}$ denote the 2-adic valuation on the rationals defined as in Example 14 and consider the quadratic field extension $\mathbb{Q}(i)$ of $\mathbb{Q}$, where $i = \sqrt{-1}$. Recall that $\mathbb{Z}[i]$ is a UFD and note that $1 + i$ is irreducible in $\mathbb{Z}[i]$. Thus, we can express each element of $\mathbb{Q}(i)$ uniquely as $(1 + i)^n \frac{\alpha}{\beta}$ where $\alpha$ and $\beta \neq 0$ are elements of $\mathbb{Z}[i]$ not having $1 + i$ as a factor. Define

$$\nu' : \mathbb{Q}(i) \to (1/2)\mathbb{Z} = \left\{ \frac{a}{2} \bigg| a \in \mathbb{Z} \right\} \approx \mathbb{Z} \text{ by } \nu' : (1 + i)^n \frac{\alpha}{\beta} \mapsto \frac{n}{2}. $$

Then $\nu'$ is a nontrivial extension of $\nu$.

Definition 18. Let $L$ be a finite extension field of a field $K$. Let $\nu$ be a discrete valuation on $K$ with value group $G$ and valuation ring $R$. Let $\nu'$ denote an extension of $\nu$ to $L$ be a discrete valuation with value group $H$ and valuation ring $S$. The ramification index of $\nu'$ over $\nu$ is the index $[H : G]$. If $M$ is the maximal ideal of $R$ and $N$ is the maximal ideal of $S$, then the residue class degree of $\nu'$ over $\nu$ is the index $[S/N : R/M]$.

Proposition 19. Let $L$ be a finite extension field of a field $K$. Let $\nu$ be a discrete valuation on $K$ with value group $G$ and valuation ring $R$. Let $\nu'$ denote an extension of $\nu$ to $L$ be a discrete valuation with value group $H$ and valuation ring $S$. Suppose that $M$ is the maximal ideal of $R$ and $N$ is the maximal ideal of $S$. Then $[H : G] \cdot [S/N : R/M] \leq [L : K]$. 
Homework VIII:

1. Prove that every PID is a Dedekind Domain.

2. ★ Let $R$ be a Dedekind Domain. Prove that $R$ is a PID if and only if $R$ is a UFD.

3. Let $I(R)$ denote the set of nonzero fractional ideals of a Dedekind domain $R$ and let $P(R)$ denote the set of nonzero principal fractional ideals of $R$.

   (a) Prove that $I(R)$ is a multiplicative abelian group.

   (b) Prove that $P(R)$ is a subgroup of $I(R)$.

   (c) The ideal class group $C(R)$ is the quotient group $I(R)/P(R)$. Prove that $C(R)$ is trivial if and only if $R$ is a PID.

   (d) Note that, in fact, the ideal class group of a Dedekind domain $R$ gives a measure of how far away $R$ is from being a UFD. Indeed, $R$ is a UFD if and only if $C(R)$ is trivial and $R$ is a HFD if and only if $|C(R)| \leq 2$. (You do NOT need to prove this result.)

4. Let $F$ be any field and $f$ be an irreducible polynomial in $F[x]$. Define $F[x]_f = \left\{ \frac{g}{h} \mid g, h \in F[x], h \neq 0, f \nmid h \right\}$. That is,

   $$F[x]_f = \{\text{all rational functions in } F(x) \text{ whose denominator is not divisible by } f\}.$$

   Check that $\nu$ is discrete valuation on $F(x)$ and that the corresponding valuation ring is $F[x]_f$.

5. Let $R$ be a DVR. Prove that $R$ is a Euclidian Domain. (Hint: Start by proving that the discrete valuation, restricted to $R; \nu: R \to \mathbb{N}_0$ is a norm.)