1 Localization

Definition: Let R be an integral domain, then $S \subset R$ is multiplicative if $\forall s, s' \in S$: $ss' \in S$ and $1 \in S$ but $0 \neq S$.

Definition: Let R be an integral domain and the subset $S \subset R$ be multiplicative, then the *localization* of R at S, denoted by $S^{-1}R \subset Q_R$ is the ring,

$$S^{-1}R = \left\{ \frac{r}{s} \;\middle|\; r \in R \text{ and } s \in S \right\}$$

Definition: A *discrete valuation ring (DVR)* is a Dedekind domain with a unique maximal ideal.

Lemma 1.1. The map $I \mapsto S^{-1}I$ is a surjection from ideals of R to ideals of $S^{-1}R$.

Proof. Let D be the map from ideals of R to ideals of $S^{-1}R$ given by $D : I \mapsto S^{-1}I$. Now if $J \subset S^{-1}R$ is an ideal then consider $R \cap J \subset R$. This is an ideal of R because if $x, y \in R \cap J$ then $xy \in R$ and $xy \in J$ so $xy \in R \cap J$ and for $r \in R$, $r = \frac{r}{1} \in S^{-1}R$ so $rx \in J$ so $rx \in R \cap J$.

Take $x \in D(R \cap J)$ then $x = \frac{r}{s}$ with $r \in J$ and since $\frac{1}{s} \in S^{-1}R$, by absorption, $\frac{r}{s} = x \in J$. Take $\frac{r}{s} \in J$ with $r \in R$ then $r = s\frac{r}{s} \in J$ by absorption so $r \in R \cap J$ thus $\frac{r}{s} \in D(R \cap J)$. Therefore, $D(R \cap J) = J$ so D is surjective.

$\square$

Lemma 1.2. The map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ is a bijection between the prime ideals of R which do not intersect S and prime ideals of $S^{-1}R$.

Proof. Restrict D to the set of prime ideals of R which do not intersect S. Let P be a prime ideal of R and $P \cap S = \varnothing$. Take $\frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r}{s} \in S^{-1}P$ for $r_1, r_2 \in P$. Then $r_1 r_2 s = s_1 s_2 r \in P$. P is prime so either $r_1 \in P$ or $r_2 s \in P$. If $r_2 s \in P$ then $r_2 \in P$ because $s \notin P$. Therefore, $r_1 \in P$ or $r_2 \in P$ so $\frac{r_1}{s_1} \in S^{-1}P$ or $\frac{r_2}{s_2} \in S^{-1}P$ and therefore $S^{-1}R$ is prime. Thus, $\mathrm{Im}(D)$ is contained within the set of prime ideals of $S^{-1}R$.

Let P and Q be prime ideals of R s.t. $P \cap S = Q \cap S = \varnothing$. Then suppose that $D(P) = D(Q)$ i.e. $S^{-1}P = S^{-1}Q$. Then $\frac{p}{s_1} = \frac{q}{s_2}$ for any $p \in P$ and $q \in Q$. Thus, $s_2 p = s_1 q$ so $s_2 p \in Q$ and $s_1 q \in P$ by absorption. The ideals are prime so $p \in Q$ and $q \in P$ since $s_2 \notin Q$ and $s_1 \notin P$. Therefore, $P \subset Q$ and $P \supset Q$ so $P = Q$. Therefore, D is injective.

Let $J \in S^{-1}R$ be prime then take $xy \in R \cap J$ with $x, y \in R$. Now $xy \in J$ so $x \in J$ or $y \in J$. Therefore, since both $x, y \in R$ then $x \in R \cap J$ or $y \in R \cap J$ so $R \cap J$ is a prime ideal in R. Suppose that $\exists s \in S \cap (R \cap J)$ then $s \in J$ so by absorption, $\frac{1}{s}s \in J$ since $\frac{1}{s} \in S^{-1}R$ thus $1 \in J$ so $J = S^{-1}R$ which contradicts J being a prime ideal. Thus, $(R \cap J) \cap S = \varnothing$ so D is surjective in the set of prime ideals of $S^{-1}R$.

Therefore, D is a bijection from the set of prime ideals of R which are disjoint with S and the prime ideals of $S^{-1}R$. $\square$

Theorem 1.3. If R is a Dedekind domain with $S \subset R$ then $S^{-1}R$ is Dedekind.

Proof. Let R be a Dedekind domain. By Lemma **??**, the map $I \mapsto S^{-1}I$ is a surjection. If $J_1 \subset J_2 \subset \cdots$ is an increasing chain of ideals of $S^{-1}R$ then $J_i = S^{-1}I_i$. Suppose that $I_i \supset I_{i+1}$, then $S^{-1}I_i \supset S^{-1}I_{i+1}$ so if $J_i \subsetneq J_{i+1}$ then $I_i \subsetneq I_{i+1}$. Therefore, $I_1 \subset I_2 \subset \cdots$ is an increasing chain of ideals of R. Since R is Noetherian, the chain of I_i terminates i.e. after some n, $I_n = I_{n+1} = \cdots$ so $I_n \supset I_{n+1} \supset \cdots$ and therefore, $J_n \supset J_{n+1} \supset \cdots$. Thus, the chain of J_i also terminates at n so $S^{-1}R$ is Noetherian.

Suppose that α is integral over $S^{-1}R$. Then, for some monic polynomial $Q \in S^{-1}R[x]$, $Q(\alpha) = \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$. But each $c_i \in S^{-1}R$ so $c_i = \frac{r_i}{s_i}$ for $r_i \in R$ and $s_i \in S$. Multiply through by $s^n = (s_{n-1}s_{n-2}\dots s_0)^n$,

$$Q(\alpha)s^n = (s\alpha)^n + r_{n-1}(s_{n-2}\dots s_0)(s\alpha)^{n-1} + \cdots + s^{n-1}(s_{n-1}s_{n-2}\cdots s_1)r_0 = 0$$

Thus, $s\alpha$ is integral over R. However, R is Dedekind and thus integrally closed so $s\alpha \in R$. Since $s\alpha \in R$ and $s \in S$ then $\frac{s\alpha}{s} = \alpha \in S^{-1}R$ so $S^{-1}R$ is integrally closed.

Let $J \subset S^{-1}R$ be a non-zero prime ideal of $S^{-1}R$. By Lemma **??**, $J = S^{-1}I$ where I is a non-zero prime ideal which is disjoint with S. Since I is a non-zero prime ideal of R and R is Dedekind, then I is maximal. Suppose that $J \subsetneq L \subset S^{-1}R$. Then $L = S^{-1}F$ for an ideal F. Then $I \subsetneq F$ so $F = R$ and thus $L = S^{-1}F = S^{-1}R$ so J is maximal. Thus, $S^{-1}R$ is Dedekind. $\square$

Definition: Let R be a Dedekind domain and $\mathfrak{p} \subset R$ be a prime ideal then the *loclization* of R at $\mathfrak{p}$ is $R_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}R$ for $S_{\mathfrak{p}}^{-1} = R\backslash\mathfrak{p}$.

Theorem 1.4. Let R be a Dedekind domain and $\mathfrak{p} \subset R$ be a prime ideal then $S_{\mathfrak{p}}^{-1} = R\backslash\mathfrak{p}$ is multiplicative and $R_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}R$ is a DVR.

Proof. Let R be a Dedekind domain and $\mathfrak{p}$ be a prime ideal of R. Define $S_{\mathfrak{p}} = R\backslash\mathfrak{p}$ and $R_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}R$. If $s, s' \in S_p$ then if $ss' \in \mathfrak{p}$ then either $s \in \mathfrak{p}$ or $s' \in \mathfrak{p}$ because $\mathfrak{p}$ is a prime ideal. However, $s, s' \in S_p$ so neither are in $\mathfrak{p}$. Thus, $ss' \notin \mathfrak{p}$ so $ss' \in S_{\mathfrak{p}}$. Also, $1 \notin \mathfrak{p}$ because a prime ideal cannot be the entire ring thus $1 \in S_{\mathfrak{p}}$. By Lemma **??**, there is a bijection between the prime ideals of R which do not intersect with $S_{\mathfrak{p}}$ and the prime ideals of $R_{\mathfrak{p}}$. If $\mathfrak{q} \subset R$ is a non-zero prime ideal and $\mathfrak{q} \cap S_{\mathfrak{p}} = \mathfrak{q} \cap (R\backslash\mathfrak{p}) = \varnothing$ then $\mathfrak{q} \subset \mathfrak{p}$ but R is a Dedekind domain so every non-zero prime ideal is maximal and thus $\mathfrak{q} = \mathfrak{p}$ since $\mathfrak{p} \neq R$. Thus $\mathfrak{p}$ is the unique non-zero prime ideal of R that is disjoint with $S_{\mathfrak{p}}$. Using the bijection, $S_{\mathfrak{p}}^{-1}\mathfrak{p}$ is the unique prime ideal of $R_{\mathfrak{p}}$. Furthermore, because R is Dedekind the ring $R_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}R$ is also Dedekind. Thus, $R_{\mathfrak{p}}$ has a unique maximal ideal $S_{\mathfrak{p}}^{-1}\mathfrak{p}$ since an ideal in a Dedekind domain is maximal if and only if it is prime. $\square$

Theorem 1.5. Let R be a Dedekind domain and $\mathfrak{p} \subset R$ a prime ideal and $S \subset R$ a multiplicative set such that $S \cap \mathfrak{p} = \varnothing$ then $S^{-1}R/S^{-1}\mathfrak{p}^k \cong R/\mathfrak{p}^k$.

Proof. Consider the map $\pi : S^{-1}R \to R/\mathfrak{p}^k$ given by $\pi\left(\frac{r}{s}\right) = (r + \mathfrak{p}^k)(s + \mathfrak{p}^k)^{-1}$. Iff $s \in S$ then $s \notin \mathfrak{p}$ but $(s) + \mathfrak{p}^k \subset \mathfrak{p}^k$ so by the uniqueness of Dedekind factorization, $(s) + \mathfrak{p}^k = \mathfrak{p}^r$ but $s \notin \mathfrak{p}^r$ for $r > 0$ so $(s) + \mathfrak{p}^k = R$. Therefore, there exists $r \in R$ such that $rs - 1 \in \mathfrak{p}^k$ and thus $(s + \mathfrak{p}^k)$ is invertible. Furthermore, if $\frac{r}{s} = \frac{r'}{s'}$ then $rs' = r's$ so $rs' + R = (r + \mathfrak{p}^k)(s' + \mathfrak{p}^k) = r's = (r' + \mathfrak{p}^k)(s + \mathfrak{p}^k)$ and thus $\pi\left(\frac{r}{s}\right) = \pi\left(\frac{r'}{s'}\right)$. Clearly, π is a surjective homomorphism. Now, $\frac{r}{s} \in \ker \pi$ if and only if $r + \mathfrak{p} = 0$ or equivalently $\frac{r}{s} \in S^{-1}\mathfrak{p}^k$ thus $\ker \pi = S^{-1}\mathfrak{p}^k$. Therefore, $S^{-1}R/S^{-1}\mathfrak{p}^k \cong R/\mathfrak{p}^k$. ☐

2 Properties of Discrete Valuation Rings

Theorem 2.1. Any discrete valuation ring is a principal ideal domain which admits unique factorization of the form $a = u\varpi^k$ where u is a unit and ϖ is a uniformizer i.e. $(\varpi) = \mathfrak{m}$ the unique maximal ideal.

Proof. Let R be a DVR with maximal ideal $\mathfrak{m}$. Since R is Noetherian and $\mathfrak{m}$ is an ideal of R then $\mathfrak{m}$ is an R-submodule of finite type. Let $\mathfrak{m} = c_1 R + \cdots + c_n R$. Then (c_i) is an ideal of R which is a Dedekind domain so it has a unique prime factorization. Since there is only one prime ideal, $(c_1) = \mathfrak{m}^{k_i}$. Take ϖ to be the c_i with the least k_i then $(c_i) = \mathfrak{m}^{k_i} \subset \mathfrak{m}^{k_\varpi} = (\varpi)$ so $c_i \in (\varpi)$. Therefore, $c_i = rc$ so $\mathfrak{m} = \varpi R = (\varpi)$.

For any $a \in R$, the ideal (a) has a prime factorization because R is a Dedekind domain. Thus, $(a) = \mathfrak{m}^k = (\varpi)^k = (\varpi^k)$. Thus, $a = u\varpi^k$ where u is a unit. ☐

3 Silverman and Tate Exercises

Excercise 2.7
For a prime p, define,

$$R = \{r \in \mathbb{Q} \mid v_p(r) \geq 0\}$$

Therefore, an arbitrary element of R can be written as $R = \frac{a}{b}$ where $p \not| b$ which is equivalent to $R = S_{(p)}^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the prime ideal (p). Therefore, R is a subring of $Q_{\mathbb{Z}} = \mathbb{Q}$ and R is a DVR with uniformizer p i.e. pR is the unique maximal ideal. We have shown that any DVR is a PID and thus a UFD. Since $S_{(p)} \cap pR = \varnothing$, by Theorem **??**, the field $R/pZ = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$. By Dedekind prime factorization, every ideal can be factored into prime ideals, $I = \mathfrak{p}^k$ since there is a unique prime ideal. Lastly, let $\frac{a}{b} \in R^\times$ be a unit then there exists $\frac{x}{y} \in R$ such that $\frac{a}{b} \cdot \frac{x}{y} = \frac{ax}{by} = 1$ then $ax = by$. However, $p \not| by$ so $p \not| ax$ and thus $p \not| a$. Therefore, $p \not| ab$.

Excercise 2.8
Consider the map $\phi : R \to p^\nu R/p^\sigma R$ given by $\phi(r) = p^\nu r + p^\sigma R$ which is clearly surjective. Now, $r \in \ker \phi$ if and only if $p^\nu r \in p^\sigma R$ or equivalently $r \in p^{\sigma-\nu}R$.

Thus, $\ker\phi = p^{\sigma-\nu}R$. Therefore, $p^\nu R/p^\sigma R \cong R/p^{\sigma-\nu}R$. Since $R = S_{(p)}^{-1}\mathbb{Z}$ and $S_{(p)} \cap (p) = \varnothing$, by Theorem **??**, $R/p^{\sigma-\nu}R = S_{(p)}^{-1}\mathbb{Z}/S_{(p)}^{-1}p^{\sigma-\nu}\mathbb{Z} \cong \mathbb{Z}/p^{\sigma-\nu}\mathbb{Z}$. Therefore, $p^\nu R/p^\sigma R \cong \mathbb{Z}/p^{\sigma-\nu}\mathbb{Z}$.

Excercise 2.9
Let $S_p = \{p^k \mid k \in \mathbb{N}\}$ then take $R = S_p^{-1}\mathbb{Z} \subset Q_{\mathbb{Z}} \cong \mathbb{Q}$ which is a Dedekind domain. Any element of $S^{-1}\mathbb{Z}$ can be written as ap^ν for $p \not| a$ and $\nu \in \mathbb{Z}$. Thus, if $ap^\nu \in R$ is a unit then there must exist $bp^\sigma \in R$ such that $abp^{\nu-\sigma} = 1$. Therefore, $ab = \pm$ so $a, b = \pm 1$. Therefore, $ap^\nu = \pm p^\nu$. Finally, we know that there is a one-to-one correspondence between the prime ideals of $\mathbb{Z}$ which do not intersect S_p, i.e. (q) for $q \neq p$, and the ideals of $R = S_p^{-1}\mathbb{Z}$. For any prime $q \in \mathbb{Z}$ we have that $S_p^{-1}(q) = qR$ is a prime ideal of R and every prime ideal of R is of this form. Furthermore, since R and $\mathbb{Z}$ are Dedekind, the maximal and prime ideals are equivalent. Finally, since $(q) \cap S_p = \varnothing$, by Theorem **??**, $R/qR \cong S_p^{-1}\mathbb{Z}/S_p^{-1}(q) \cong \mathbb{Z}/(q) = \mathbb{F}_q$.