Hungerford: Algebra

III.4. Rings of Quotients and Localization

1. Determine the complete ring of quotients of the ring $\mathbb{Z}_n$ for each $n \geq 2$.

**Proof:** Denote $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, and the set of all non zero divisors of $\mathbb{Z}_n$ by $S(\mathbb{Z}_n)$.

(1.1) Claim: $S(\mathbb{Z}_n) = \{m : (m, n) = 1\}$.

Suppose that $0 < m < n$ and $(m, n) = d$. If $\overline{m} \notin S(\mathbb{Z}_n)$. Then there exists an $x$ with $0 < x < n$ such that $\overline{mx} = 0$. Thus $n|(mx)$. If $(m, n) = 1$, then $n|x$, contrary to the assumption that $0 < x < n$.

Conversely, assume that $d > 1$. Then for some positive integers $m'$ and $n'$ with $0 < m' < n$ and $0 < n' < n$, we have $m = m'd$ and $n = n'd$. Therefore

$$\overline{mn'} = \overline{mm'} = \overline{mn} = 0 \in \mathbb{Z}_n,$$

and so $\overline{m} \notin S(\mathbb{Z}_n)$. Thus $S(\mathbb{Z}_n) \supseteq \{m : (m, n) = 1\}$. This proves the claim.

By the claim, we can write $S^{-1}\mathbb{Z}_n = \{\overline{m}/\overline{s} : (n, s) = 1\}$.

**Example:** For $n = 4$,

$$S^{-1}\mathbb{Z}_4 = \{1/3, 2/3\} \cup \mathbb{Z}_4.$$

2. Let $R$ be a multiplication subset of a commutative ring with identity and let $T$ be a multiplication subset of the ring $S^{-1}R$. Let $S_* = \{r \in R : r/s \in T \text{ for some } s \in S\}$. Then $S_*$ is a multiplicative subset of $R$ and there is a ring isomorphism $S_*^{-1}R \cong T^{-1}(S^{-1}R)$.

**Proof:** We may assume that $0 \notin S$.

For any $r, r' \in S_*$, there exist $s, s' \in S$ such that $r/s, r'/s' \in T$. Since $T$ is multiplicative, $(rr')/ss' \in T$; and since $S$ is multiplicative, $ss' \in S$. Thus $rr' \in S_*$, and so $S_*$ is also multiplicative.

We now define a map $f : S_*^{-1}R \rightarrow T^{-1}(S^{-1}R)$. For any $r/w \in S_*^{-1}R$ with $r \in R$ and $w \in S_*$, there exists $s \in S$ such that $w/s \in T$. Thus we define

$$f(r/w) = (r/s)/(w/s) \in T^{-1}(S^{-1}R).$$

(2.1) $f$ is well-defined.

Suppose that $r/w = r'/w'$ in $S_*^{-1}R$. As $w, w' \in S_*$, there exist $s, s' \in S$ such that $w/s, w'/s' \in T$.

Since $r/w = r'/w'$ in $S_*^{-1}R$, we have, for some $r'' \in S_*$, $r''(rw' - r'w) = 0$ in $R$, and for some $s'' \in S$, 

$$s''(rw' - r'w) = 0 \in R,$$
\( r''/s'' \in T \). It follows that in \( R \), we also have

\[
r''(rw's's' - r'wss') = 0.
\]

Hence in \( S^{-1}R \), we have \((r''/s'')(w'/s') - (rw'')(ss') = 0\), and so \((r/s)(w'/s') = (rw'')(ss') = (r''w)/(ss') = (r'/s')(w/s)\). This, in turn, implies that in \( T^{-1}(S^{-1}R)\),

\[
f(r/w) = (r/s)/(w/s) = (r'/s')/(w'/s') = f(r'/w').
\]

(2.2) \( f : S^{-1}_*R \mapsto T^{-1}(S^{-1}R) \) is a ring homomorphism.

Let \( r_1/w_1, r_2/w_2 \in S^{-1}_*R \). Then \( \exists s_1, s_2 \in S \) such that \( w_1/s_1, w_2/s_2 \in T \), which implies that \( (w_1/w_2)/(s_1s_2) \in T \).

\[
f(r_1/w_1 + r_2/w_2) = f((r_1w_2 + r_2w_1)/(w_1w_2)) \quad \text{(addition in } S^{-1}_*R)\]

\[
= ((r_1w_2 + r_2w_1)/(s_1s_2))/((w_1w_2)/(s_1s_2)) \quad \text{(definition of } f)\]

\[
= ((r_1/s_1)(w_2/s_2) + (r_2/s_2)(w_1/s_1))/((w_1/s_1)(w_2/s_2)) \quad \text{(addition and multiplication in } T^{-1}(S^{-1}R)\]

\[
= (r_1/s_1)/(w_1/s_1) + (r_2/s_2)/(w_2/s_2) \quad \text{(addition in } T^{-1}(S^{-1}R)\]

\[
= f(r_1/w_1) + f(r_2/w_2) \quad \text{(definition of } f)\]

Let 1 denote the identity of \( R \). Since \( S \) is multiplicative, \( 1/1 = s/s \) in \( S^{-1}R \) for any \( s \in S \). For any \( w/s \in T \), \((w/s)(1/1)(w/s) - (w/s)(1/1)) = 0/s and so \((1/1)(1/1) = (w/s)/(w/s) \) in \( T^{-1}(S^{-1}R) \).

(2.3) For any \( w \in S_* \) and for any \( s \in S \), \( sw \in S_* \).

In fact, if \( w \in S_* \), then \( \exists s' \in S \) such that \( w/s' \in T \). For any \( s \in S \), since \( 1/1 = s/s \in S^{-1}R \),

\[
(sw)/(ss') = (1/1)(w/s) \in T,
\]

and so \( ss' \in S \), \( sw \in S_* \).

(2.4) Let \( r \in R \). If for some \( w' \in S_* \), \( rw' = 0 \), then for any \( w \in S_* \), \( r/w = (rw'/w) = 0/(ww') = 0/w \). In particular, in \( S^{-1}_*R \),

\[
\{0/w\} = \{r/w : r \in R, w \in S_* \}, \text{ and for one } w \in S_* \{rw = 0 \text{ in } R\}.
\]

(2.5) \( f \) is a bijection.

For any \((r/s)(w/s) \in T^{-1}(S^{-1}R)\), we have \( r \in R \), \( s \in S \) and \( w/s \in T \). Thus \( w \in S_* \) and so \( f(r/w) = (r/s)(w/s) \). Thus \( f \) is surjective.

By (2.3) and (2.4)

\[
\text{Ker } f = \{r/w \in S^{-1}_*R : f(r/w) = 0 \in T^{-1}(S^{-1}R)\}
\]

\[
= \{r/w \in S^{-1}_*R : \text{ for some } w \in R, s \in S \text{ with } w/s \in T, (r/s)(w/s) = (0/s)/(w/s) \in T^{-1}(S^{-1}R)\}\]
(b) We claim that for a multiplicative subset $S$ of the rational numbers, first assume that $p$ is a prime, so $a/b = 1$, and every irreducible element is a prime, for some primes $a/b, p/q, m/p/q$.

Let $Q = (Z - \{0\})^{-1}Z$ denote the field of the rational numbers. Then $\forall p/q \in Q$, $p, q \in Z$ and $q \neq 0$. Without loss of generality, we may assume that $q > 0$, and so $p/q = (2p)/2q \in E^{-1}bfZ$. This proves that $Q \subseteq E^{-1}bfZ$, and so equality must hold.

(b) We claim that for a multiplicative subset $S \subseteq Z - \{0\}$, $S^{-1}Z = Q$ if and only if for any prime $p$, $S \cap pZ \neq \emptyset$.

First assume that $S^{-1}Z = Q$. For any prime $p$, as $1/p \in Q = S^{-1}Z$, $\exists a \in Z$ and $b \in S$ such that $a/b = 1/p$, or in $Z$, $ap = b \in S$. Hence $S \cap pZ = \emptyset$.

Conversely, we assume that for any prime $p$, $S \cap pZ \neq \emptyset$. Let $a/b \in Q$. Then as $Z$ is a PID (and so a UFD, and every irreducible element is a prime), for some primes $p_1, p_2, \ldots, p_m$, and positive integers $n_1, n_2, \ldots, n_m$,

$$b = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}.$$

Since $p_iZ \cap S \neq \emptyset$, for each $i$, $\exists s_i \in Z$ such that $s_ip_i \in S$. Let $s = s_1s_2 \cdots s_m$. Then $sb = (s_1p_1)(s_2p_2) \cdots (s_mp_m) \in S$, and so $a/b = (sa)/sb \in S^{-1}Z$. This proves $Q \subseteq S^{-1}bfZ$, and completes the proof.

4. If $S = \{2, 4\}$ and $R = Z_6$, then $S^{-1}R \cong Z_3$.

Proof: For the simplicity of notation, we denote $Z_6 = \{0, 1, 2, 3, 4, 5\}$. Therefore, $|S \times R| = 12$.

As $\frac{3}{2} = \frac{3}{4} = \frac{9}{8} \neq \frac{9}{7}$, and so the equivalence class in $S^{-1}R$ represented by $\frac{9}{7}$ contains 4 elements; as $\frac{1}{4} = \frac{2}{2} = \frac{4}{4}$, and so the equivalence class in $S^{-1}R$ represented by $\frac{4}{4}$ contains 4 elements; as $\frac{5}{2} = \frac{2}{2} = \frac{4}{4}$, and so the equivalence class in $S^{-1}R$ represented by $\frac{4}{4}$ contains 4 elements. Thus $S \times R$ has exactly 3 equivalence classes.

Define $\phi : S^{-1}R \rightarrow Z_3$ by $\phi(\frac{9}{7}) = 0, \phi(\frac{4}{4}) = 1$ and $\phi(\frac{4}{4}) = 2$. Then one can verify that this is a ring epimorphism (verification is routine and so omitted here). Since $|S^{-1}R| = Z_3| = 3$, $\phi$ is also a monomorphism and so $\phi$ is an isomorphism.

5. Let $R$ be an integral domain with quotient field $F$. It $T$ is an integral domain such that $R \subseteq T \subseteq F$, then $F$ is (isomorphic to) the quotient field of $T$.

Proof: Let $E$ be the field of quotients of $T$. Then there is an monomorphism $f : T \rightarrow E$. By Corollary III-4.6 (Let $R$ be an integral domain considered as a subring of its quotient field $F$. If
\( E \) is a field and \( f : R \mapsto E \) is a monomorphism of rings, then there is a unique monomorphism of fields \( \tilde{f} : F \mapsto E \) such that the restriction of \( \tilde{f} \) to \( R \) is \( f \). We here apply Corollary III-4.6 with \( T \) replacing \( R \), there is a field monomorphism \( \tilde{f} : E \mapsto F \) extending \( f \). View this isomorphism as an embedding, we may assume that

\[ T \subseteq E \subseteq F. \]

Now apply Corollary III-4.6 to \( R \) with \( E \) replacing \( F \) in Corollary III-4.6, then we have

\[ R \subseteq F \subseteq E. \]

8. Let \( R \) be a commutative ring with identity, \( I \) an ideal of \( R \) and \( \pi : R \mapsto R/I \) the canonical projection.

(a) If \( S \) is a multiplicative subset of \( R \), then \( \pi S = \pi(S) \) is a multiplicative subset of \( R/I \).

(b) The mapping \( \theta : S^{-1}R \mapsto (\pi S)^{-1}(R/I) \) given by \( r/s \mapsto \pi(r)/\pi(s) \) is a well defined function.

(c) \( \theta \) is a ring epimorphism with kernel \( S^{-1}I \) and hence induces a ring isomorphism \( S^{-1}R/S^{-1}I \cong (\pi S)^{-1}(R/I) \).

**Proof:**

(a) \( \forall s, s' \in S \), as \( S \) is a multiplicative subset, \( ss' \in S \). Thus \( \pi(s)\pi(s') = \pi(ss') \in \pi(S) = \pi(S) \) and so \( \pi(S) \) is a multiplicative subset.

(b) Suppose that \( r/s = r'/s' \in S^{-1}R \). Then \( rs' = r's \). Since \( \pi : R \mapsto R/I \) is a homomorphism,

\[ \pi(r)\pi(s') = \pi(r's) = \pi(r's) = \pi(r)\pi(s'). \]

It follows that \( \theta(r/s) = \pi(r)/\pi(s) = \pi(r'/s') = \theta(r'/s') \) in \( (\pi S)^{-1}(R/I) \).

(c) For any \( r/s, r'/s' \in S^{-1}R \),

\[ \theta(r/s + r'/s') = \theta((r/s + r'/s')/ss') = \pi((rs' + r's)/ss') = \pi(r')/\pi(s') = \theta(r'/s'). \]

\[ \theta((r/s)(r'/s')) = \theta((rr')/(ss')) = \pi(rr')/\pi(ss') = \pi(r')/\pi(s') \]

\[ = (\pi(r)/\pi(s))(\pi(r')/\pi(s')) = \theta(r/s)\theta(r'/s'). \]

For any \( a/b \in (\pi S)^{-1}(R/I) \) with \( a \in R/I \) and \( b \in \pi S \), since \( \pi \) is an epimorphism, \( \exists r \in R, s \in S \) such that \( a = \pi(r) \) and \( b = \pi(s) \). Therefore, \( \theta(r/s) = a/b \) and so \( \theta \) is also an epimorphism.

\[ \text{Ker} \theta = \{ r/s \in S^{-1}R : \theta(r/s) = 0 \in (\pi S)^{-1}(R/I) \} \]

\[ = \{ r/s \in S^{-1}R : \pi(r)/\pi(s) = 0/\pi(s) \in (\pi S)^{-1}(R/I) \} \]

\[ = \{ r/s \in S^{-1}R : \pi(r) = 0 \in R/I \text{ and } \pi(s) \in \pi(S) \} \]

\[ = \{ r/s \in S^{-1}R : r \in I \text{ and } s \in S \} = S^{-1}I. \]
9. Let $S$ be a multiplicative subset of a commutative ring with identity. If $I$ is an ideal in $R$, then $S^{-1}(\text{Rad } I) = \text{Rad } (S^{-1}(I))$.

**Proof:** It is routine to show that $S^{-1}(\text{Rad } I) \subseteq \text{Rad } (S^{-1}I)$. In fact, if $\frac{a}{b} \in S^{-1}(\text{Rad } I)$, then $a \in \text{Rad } (I)$ and $b \in S$. Thus for some integer $n > 0$, $a^n \in I$. As $S$ is multiplicative, $b^n \in S$. It follows that $(\frac{a}{b})^n = \frac{a^n}{b^n} \in S^{-1}I$, and so $S^{-1}(\text{Rad } I) \subseteq \text{Rad } (S^{-1}I)$.

Conversely, let $\frac{a}{b} \in \text{Rad}(S^{-1}I)$. Then for some integer $m > 0$, $\frac{a^m}{b^m} = (\frac{a}{b})^m \in S^{-1}I$. Therefore, for some $c \in I$ and $d \in S$, $\frac{a^m}{b^m} = \frac{c}{d}$. Thus $\exists s \in S$, such that

$$s(a^m d - b^m c) = 0,$$

or equivalently, $a^m sd = b^m sc$.

Since $c \in I$ and since $I$ is an ideal, $a^m sd = b^m sc \in I$. Since $S$ is a multiplicative set, and since $b, s, d \in S$, we have $bsd \in S$ and so

$$(asd)^m = a^m sd (sd)^{m-1} \in I, (bsd)^m \in S$$

and so $\left(\frac{asd}{bsd}\right)^m \in S^{-1}I$.

Thus $\frac{asd}{bsd} \in \text{Rad}(S^{-1}I)$. But then for any $s' \in S$, $s'(asd - absd) = 0$, and so

$$\frac{a}{b} = \frac{asd}{bsd} \in \text{Rad}(S^{-1}I).$$

This proves that $\text{Rad } (S^{-1}(I)) \subseteq S^{-1}(\text{Rad } I))$.

12. A commutative ring with identity is local if and only if for all $r, s \in R$, $r + s = 1_R$ implies $r$ or $s$ is a unit.

**Proof:** Let $R$ be a commutative ring with identity $1_R$.

Suppose first that $R$ is local, and so $R$ has exactly one maximal ideal $M$. Suppose that $r, s \in R$ with $r + s = 1$. If neither $r$ nor $s$ are units, then $(r)$ and $(s)$ are principal ideals. Let $M_1$ and $M_2$ be maximal ideals of $R$ containing $(r)$ and $(s)$, respectively. Then since $M$ is the only maximal ideal of $R$, we have $M_1 = M_2 = M$, and so $r, s \in M$. Since $r + s = 1_R$, we must have $1_R \in M$, and so $M = R$, contrary to the assumption that $M \neq R$.

Conversely, assume that $\forall r, s \in R$, that $r + s = 1_R$ implies that $r$ or $s$ is a unit. By contradiction, we assume that $R$ has at least two distinct maximal ideals $M_1$ and $M_2$. Since $M_1$ and $M_2$ are distinct maximal ideals, the ideal $M_1 + M_2$ must be $R$ itself. Therefore, since $1_R \in R$, $\exists r \in M_1$ and $s \in M_2$ such that $r + s = 1_R$. Therefore, either $r$ or $s$ is a unit, and so either $M_1$ or $M_2$ equals $R$, contrary to the fact that a maximal ideal is not equal to $R$.

13. The ring $R$ consisting of all rational numbers with denominators not divisible by some (fixed) prime $p$ is a local ring.

**Proof:** Consider the ring $\mathbb{Z}$ of the integers. For a fixed prime $p$, $(p)$ is a prime ideal of $\mathbb{Z}$ and so $S = \mathbb{Z} - (p)$ is a multiplicative subset. By Theorem III-4.11(ii) (Let $P$ be a prime idea in a commutative ring $R$ with identity, the ideal $P_P = S^{-1}P$ is the unique maximal ideal of the ring
$R_P = S^{-1}R$, the localization of $R$ at $P$, $Z_{(p)}$, having $S^{-1}(p)$ as its only maximal ideal, is a local ring.

**Fact:** The structure of $Z_{(p)}$. As $(p) = pZ$, $S = Z - (p) = \{ n \in Z - \{0\} : p \nmid n \}$. Thus

$$Z_{(p)} = \{ n/m \in \mathbb{Q} : p \nmid m \}.$$  

In particular.

$$Z_{(2)} = \{ n/m \in \mathbb{Q} : m \text{ is odd} \}.$$

6