Rings of Fractions

R. C. Daileda

1 Multiplicative Sets

Let R be a commutative ring. A subset $S \subset R$ is called *multiplicative* if: (i) $1 \in S$ and (ii) for all $s, t \in S$, one has $st \in S$. We will call a multiplicative set S *proper* if S does *not* contain 0 or zero divisors; equivalently, if $s \in S$, $a \in R$ and $sa = 0$, then $a = 0$.

Remark 1. Not all authors require a multiplicative set S to satisfy $1 \in S$. However, for the purpose of constructing fractions this can be assumed WLOG.

Remark 2. The term *proper* is the author's. Although multiplicative sets that avoid 0 and avoid zero divisors occur frequently in the context of fractions, these sets inconveniently do not seem to have a dedicated adjective.

Example 1. For any $a \in R$, $S = \{1, a, a^2, a^3, \ldots\}$ is multiplicative.

Example 2. If $\mathfrak{p} \subset R$ is a prime ideal, then $S = R \setminus \mathfrak{p}$ is a multiplicative set.

Example 3. If R is a domain, then $R \setminus \{0\}$ is a proper multiplicative set. Any multiplicative $S \subset R \setminus \{0\}$ is also proper.

Theorem 1. *Let R be a commutative ring, $S \subset R$ a multiplicative set, and $\mathfrak{a} \subset R$ an ideal. If $S \cap \mathfrak{a} = \varnothing$ (S avoids $\mathfrak{a}$), then there exists a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ and avoiding S.*

Before proving Theorem 1, we remark that it can be rephrased as follows. If S is a multiplicative set contained in $R \setminus \mathfrak{a}$ for some ideal $\mathfrak{a}$, then S is contained in $R \setminus \mathfrak{p}$ for some *prime* ideal $\mathfrak{p}$. This shows that the multiplicative sets $R \setminus \mathfrak{p}$ are in some sense the "maximal" multiplicative sets.

Proof of Theorem 1 (Sketch). Apply Zorn's Lemma to the (nonempty) set of ideals avoiding S to produce an ideal $\mathfrak{p}$ which is maximal with respect to avoiding S. We claim that any such $\mathfrak{p}$ must be prime. To see this, let $ab \in \mathfrak{p}$ and suppose $a, b \notin \mathfrak{p}$. Then $\mathfrak{p}+(a)$ and $\mathfrak{p}+(b)$ must both intersect S. Since S is multiplicative, this implies that $(\mathfrak{p} + (a))(\mathfrak{p} + (b))$ intersects S. But $(\mathfrak{p} + (a))(\mathfrak{p} + (b)) = \mathfrak{p}^2 + (a)\mathfrak{p} + (b)\mathfrak{p} + (ab) \subset \mathfrak{p}$, which means $\mathfrak{p}$ intersects S, a contradiction. So either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, and $\mathfrak{p}$ is therefore prime. □

Remark 3. If $0 \notin S$, then S avoids (0). Theorem 1 then implies that S is contained in the complement of a prime ideal.

Remark 4. Although every multiplicative set avoiding 0 is *contained* in the complement of a prime, not every such set is actually *equal* to a prime complement. For example, the simple multiplicative set $\{1\}$ in $\mathbb{Z}$ is contained in the complement *every* prime ideal, but is equal to none of them.

2 Fractions

Throughout this section we fix a commutative ring R and a multiplicative set $S \subset R$. For $(a, s), (b, t) \in R \times S$ define

$$(a, s) \sim (b, t) \iff (\exists s' \in S)(s'(at - bs) = 0).$$

Remark 5. Notice that if $at - bs = 0$, then $(a, s) \sim (b, t)$, since any $s' \in S$ will satisfy $s'(at - bs) = 0$.

Remark 6. If S is proper, then $(a, s) \sim (b, t)$ if and only if $at - bs = 0$.

Lemma 1. *$\sim$ is an equivalence relation on $R \times S$.*

Proof. Reflexivity. Since $as - as = 0$, $(a, s) \sim (a, s)$.

Symmetry. If $(a, s) \sim (b, t)$, then $s'(at - bs) = 0$ for some $s' \in S$. Negating we obtain $s'(bs - at) = 0$, so that $(b, t) \sim (a, s)$ as well.

Transitivity. Suppose $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$. Then there are $s', s'' \in S$ so that $s'(at - bs) = 0$ and $s''(bu - ct) = 0$. Multiply the first equality by $s''u$ and the second by ss'. This yields $s's''(atu - bsu) = 0$ and $s's''(bsu - cst) = 0$. Adding these we find that $s's''(atu - cst) = s's''t(au - cs) = 0$. Since S is multiplicative, $s's''t \in S$. Hence $(a, s) \sim (c, u)$.

□

Remark 7. The equivalence $\sim$ is intended to mimic the relation on $\mathbb{Z} \times \mathbb{N}$ used to construct the rational numbers. The mysterious presence of s' in the "cross product" $s'(at - bs)$ has to do with the potential presence of zero divisors in S and will be explained later.

For $(a, s) \in R \times S$, let the *fraction* $\frac{a}{s}$ denote the equivalence class of (a, s) under $\sim$. That is,

$$\frac{a}{s} = \{(b, t) \in R \times S \,|\, (b, t) \sim (a, s)\}.$$

We call a the *numerator* and s the *denominator* of $\frac{a}{s}$. We will denote the quotient space $(R \times S)/\sim$ of all fractions by $S^{-1}R$.

Remark 8. If $s, t \in S$ and $a \in R$, then $\frac{at}{st} = \frac{a}{s}$, since $1 \cdot (ats - ast) = 0$. Thus, we can cancel across the fraction bar as usual.

Remark 9. If $s, t \in S$, then both $\frac{s}{t}$ and $\frac{t}{s}$ are members of $S^{-1}R$.

Remark 10. If $0 \in S$, then $S^{-1}R$ has a single element (exercise).

For $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$, define

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \tag{1}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}. \tag{2}$$

We claim that these operations are well-defined and make $S^{-1}R$ into a commutative ring.

Well-defined. Suppose $\frac{a}{s} = \frac{a'}{s'}$ and $\frac{b}{t} = \frac{b'}{t'}$ in $S^{-1}R$. Then we can find $s_1, s_2 \in S$ so that $s_1(as' - a's) = s_2(bt' - b't) = 0$. Then $s_1 s_2 \in S$ and

$$\begin{aligned} s_1 s_2((at + bs)s't' - (a't' + b's')st) &= s_1 s_2((as' - a's)tt' + (bt' - b't)ss') \\ &= s_2 s_1(as' - a's)tt' + s_1 s_2(bt' - b't)ss' \\ &= s_2 \cdot 0 \cdot tt' + s_1 \cdot 0 \cdot ss' = 0. \end{aligned}$$

Hence $\frac{at+bs}{st} = \frac{a't'+b's'}{s't'}$, and addition is well-defined.

As for multiplication, we have

$$\begin{aligned} s_1 s_2(abs't' - a'b'st) &= s_1 s_2(abs't' - ab's't + ab's't - a'b'st) \\ &= s_1 s_2(as'(bt' - b't) + b't(as' - a's)) \\ &= as's_1 s_2(bt' - b't) + b'ts_2 s_1(as' - a's) \\ &= as's_1 \cdot 0 + b'ts_2 \cdot 0 = 0, \end{aligned}$$

which proves that $\frac{ab}{st} = \frac{a'b'}{s't'}$. Therefore multiplication is also well-defined.

$(S^{-1}R, +)$ is an abelian group. Let $\frac{a}{s}, \frac{b}{t}, \frac{c}{u} \in S^{-1}R$. Then

$$\frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u}\right) = \frac{a}{s} + \frac{bu + ct}{tu} = \frac{atu + (bu + ct)s}{stu} = \frac{(at + bs)u + cst}{stu} = \frac{at + bs}{st} + \frac{c}{u} = \left(\frac{a}{s} + \frac{b}{t}\right) + \frac{c}{u},$$

so that addition of fractions is associative. It is clearly commutative. The element $\frac{0}{1}$ is the additive identity, since

$$\frac{0}{1} + \frac{a}{s} = \frac{0s + 1a}{1s} = \frac{a}{s}.$$

And the inverse of $\frac{a}{s}$ is $\frac{-a}{s}$, since

$$\frac{a}{s} + \frac{-a}{s} = \frac{as - as}{s^2} = \frac{0}{s^2} = \frac{0}{1}.$$

$(S^{-1}R, \cdot)$ is a commutative monoid. Multiplication of fractions is obviously commutative, and it is easily seen to be associative:

$$\frac{a}{s}\left(\frac{b}{t} \cdot \frac{c}{u}\right) = \frac{a}{s} \cdot \frac{bc}{tu} = \frac{abc}{stu} = \frac{ab}{st} \cdot \frac{c}{u} = \left(\frac{a}{s} \cdot \frac{b}{t}\right)\frac{c}{t}.$$

The identity element is $\frac{1}{1}$ since

$$\frac{1}{1} \cdot \frac{a}{s} = \frac{1a}{1s} = \frac{a}{s}.$$

Distributivity. Because multiplication of fractions is commutative, we only need to check distributivity on one side. Indeed, we have

$$\begin{aligned}\frac{a}{s}\left(\frac{b}{t} + \frac{c}{u}\right) &= \frac{a}{s} \cdot \frac{bu + ct}{tu} = \frac{a(bu + ct)}{stu} = \frac{abu + act}{stu} \\ &= \frac{(abu)(stu) + (act)(stu)}{(stu)^2} = \frac{abu}{stu} + \frac{act}{stu} \\ &= \frac{ab}{st} + \frac{ac}{su} = \frac{a}{s} \cdot \frac{b}{t} + \frac{a}{s} \cdot \frac{c}{u}.\end{aligned}$$

Altogether, we have now proven the following result.

Theorem 2. *Let R be a commutative ring and $S \subset R$ a multiplicative set. Under addition and multiplication of fractions as given by* (1) *and* (2)*, $S^{-1}R$ is a commutative ring, called the* localization *of R at (or by) S.*

Remark 11. The ring $S^{-1}R$ is also called a *ring of fractions.*

Remark 12. Observe that for any $s \in S$, $\frac{0}{1} = \frac{0}{s}$ and $\frac{1}{1} = \frac{s}{s}$.

Remark 13. If two fractions have the same denominator, we can add them as usual:

$$\frac{a}{s} + \frac{b}{s} = \frac{as + bs}{s^2} = \frac{(a + b)s}{s^2} = \frac{a + b}{s}.$$

Example 4. The set $\mathbb{N}$ is multiplicative in $\mathbb{Z}$. The ring $\mathbb{N}^{-1}\mathbb{Z}$ is a field (see below). It is usually denoted by $\mathbb{Q}$ and is called the field of *rational numbers.*

Example 5. If $\mathfrak{p} \subset R$ is a prime ideal and $S = R \setminus \mathfrak{p}$, the localization $S^{-1}R$ is usually denoted $R_{\mathfrak{p}}$, and by abuse of notation is called the *localization of R at $\mathfrak{p}$*, despite the fact that we are localizing at S.

Example 6. If R is a domain and $\mathfrak{p} = (0)$ above, then every nonzero element of $R_{(0)}$ is a unit. For if $a \in R$ and $a \neq 0$, then $a \in S$. Hence for any $s \in S$, we have $\frac{a}{s}, \frac{s}{a} \in R_{(0)}$ and $\frac{a}{s}\frac{s}{a} = \frac{as}{as} = \frac{1}{1}$. It follows that $R_{(0)}$ is a field, the *quotient field* of R.

Example 7. Let $R = \mathbb{Z}/6\mathbb{Z}$ and $S = \{1, 2, 2^2, 2^3, \ldots\} = \{1, 2, 4\}$. Notice that for any $a \in R$, in $S^{-1}R$ we have

$$\frac{a}{2} = \frac{4a}{4 \cdot 2} = \frac{4a}{2} = \frac{2a}{1} \quad \Rightarrow \quad \frac{a}{2^j} = \frac{2^j a}{1},$$

so that every fraction in $S^{-1}R$ has the form $\frac{a}{1}$. Moreover,

$$\frac{3}{1} = \frac{3 \cdot 2}{1 \cdot 2} = \frac{0}{2} = \frac{0}{1},$$

which implies $\frac{4}{1} = \frac{1}{1}$ and $\frac{5}{1} = \frac{2}{1}$. This means $S^{-1}R = \left\{\frac{0}{1}, \frac{1}{1}, \frac{2}{1}\right\}$. Because $\frac{2}{1} \neq \frac{0}{1}$, this shows that $S^{-1}R$ has exactly 3 elements and must therefore be isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We'll have a less *ad hoc* explanation for this shortly.

Remark 14. We are now in a position to say a few words about the extra s' appearing in the definition of $\sim$. Suppose we localize R at S and $s \in S$ is a zero divisor. This means there is a nonzero $a \in R$ so that $sa = 0$. This translates to the equation $\frac{s}{1} \cdot \frac{a}{1} = \frac{0}{1}$ in $S^{-1}R$. But in $S^{-1}R$ the fraction $\frac{s}{1}$ is a *unit*, so we can cancel it to get $\frac{a}{1} = \frac{0}{1}$. But *a is not zero*, so the usual notion of equivalence of fractions won't allow this to happen. Because of the "correction" factor we've included, however, $\frac{a}{1} = \frac{0}{1}$ follows from $sa = 0$.

3 The Universal Property

Let R be a commutative ring and let $S \subset R$ be a multiplicative set. The localization $S^{-1}R$ comes equipped with a natural map $\varphi_S : R \to S^{-1}R$ given by $\varphi_S(a) = \frac{a}{1}$. φ_S is a homomorphism by Remark 13, and for any $s \in S$, $\varphi_S(s) = \frac{s}{1}$ is a unit in $S^{-1}R$, with inverse $\frac{1}{s}$. That is, $\varphi(S) \subset (S^{-1}R)^\times$. In other words, in the localization $S^{-1}R$ the elements of S all become units. When S is proper, the following lemma shows that we can regard $S^{-1}R$ as an extension of R, one in which every element of S becomes invertible.

Lemma 2. *Let R be a commutative ring with multiplicative subset S. The natural map φ_S is an embedding if and only if S is proper.*

Proof. Suppose S is proper and $\varphi_S(a) = \frac{a}{1} = \frac{0}{1}$. Then $a = 0$, since S contains no zero divisors. Hence φ_S is injective. Conversely, suppose φ_S is injective, and let $a \in R$, $s \in S$ satisfy $sa = 0$. Then $0 = \varphi_S(sa) = \varphi_S(s)\varphi_S(a)$. Since $\varphi_S(s)$ is a unit, we must have $\varphi_S(a) = 0$. As φ_S is injective, this implies $a = 0$. Therefore S is proper. □

The so-called universal property of localization characterizes $S^{-1}R$ in terms of φ_S. It is the main tool for constructing maps out of localizations.

Theorem 3 (Universal Property of Localization)**.** *Let R be a commutative ring and $S \subset R$ a multiplicative set. If $\psi : R \to R'$ is a ring homomorphism satisfying $\psi(R) \subset (R')^\times$, then ψ lifts to a unique homomorphism $\widehat{\psi} : S^{-1}R \to R'$ making the diagram*

$$\begin{array}{ccc} S^{-1}R & & \\ {\scriptstyle \varphi_S}\uparrow & \searrow^{\widehat{\psi}} & \\ R & \xrightarrow[\psi]{} & R' \end{array} \tag{3}$$

commute. If ψ is an embedding, so is $\widehat{\psi}$.

Proof. Assuming $\widehat{\psi}$ exists, for any $s \in S$ we must have

$$\widehat{\psi}\left(\frac{1}{s}\right) = \widehat{\psi}\left(\left(\frac{s}{1}\right)^{-1}\right) = \widehat{\psi}\left(\frac{s}{1}\right)^{-1} = \widehat{\psi} \circ \varphi_S(s)^{-1} = \psi(s)^{-1}.$$

Therefore if $a \in R$, then

$$\widehat{\psi}\left(\frac{a}{s}\right) = \widehat{\psi}\left(\frac{a}{1}\cdot\frac{1}{s}\right) = \widehat{\psi}\left(\frac{a}{1}\right)\widehat{\psi}\left(\frac{1}{s}\right) = \widehat{\psi}\circ\varphi_S(a)\psi(s)^{-1} = \psi(a)\psi(s)^{-1}. \tag{4}$$

This proves that if $\widehat{\psi}$ exists, then it is unique, since it must be given by (4). To prove existence it suffices to show that the formula (4) yields a well-defined homomorphism with domain $S^{-1}R$.

So suppose $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$ satisfy $\frac{a}{s} = \frac{b}{t}$. Then there is an $s' \in S$ so that $s'(at - bs) = 0$. Applying ψ we obtain $\psi(s')(\psi(a)\psi(t) - \psi(b)\psi(s)) = 0$. Since $\psi(s')$ is a unit in R', this implies $\psi(a)\psi(t) = \psi(b)\psi(s)$. However, both $\psi(s)$ and $\psi(t)$ are units in R' as well, and cancellation then yields $\psi(a)\psi(s)^{-1} = \psi(b)\psi(t)^{-1}$. This shows that the rule $\widehat{\psi}\left(\frac{a}{s}\right) = \psi(a)\psi(s)^{-1}$ is well-defined. It is a homomorphism since $\widehat{\psi}(\frac{1}{1}) = \psi(1)\psi(1)^{-1} = 1\cdot 1 = 1$ and for any $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$:

$$\begin{aligned}
\widehat{\psi}\left(\frac{a}{s}+\frac{b}{t}\right) &= \widehat{\psi}\left(\frac{at+bs}{st}\right) = \psi(at+bs)\psi(st)^{-1} \\
&= \psi(a)\psi(t)\psi(s)^{-1}\psi(t)^{-1} + \psi(b)\psi(s)\psi(s)^{-1}\psi(t)^{-1} \\
&= \psi(a)\psi(s)^{-1} + \psi(b)\psi(t)^{-1} \\
&= \widehat{\psi}\left(\frac{a}{s}\right) + \widehat{\psi}\left(\frac{b}{t}\right), \\
\widehat{\psi}\left(\frac{a}{s}\cdot\frac{b}{t}\right) &= \widehat{\psi}\left(\frac{ab}{st}\right) = \psi(ab)\psi(st)^{-1} \\
&= \psi(a)\psi(s)^{-1}\psi(b)\psi(t)^{-1} \\
&= \widehat{\psi}\left(\frac{a}{s}\right)\widehat{\psi}\left(\frac{b}{t}\right).
\end{aligned}$$

Finally, let $\frac{a}{s} \in S^{-1}R$. Since $\psi(s)\widehat{\psi}\left(\frac{a}{s}\right) = \psi(a)$ and $\psi(s) \in (R')^\times$, we find that $\frac{a}{s} \in \ker\widehat{\psi}$ is and only if $a \in \ker\psi$. That is

$$\ker\widehat{\psi} = S^{-1}\ker\psi = \left\{\frac{a}{s}\,\middle|\, a \in \ker\psi, s \in S\right\}. \tag{5}$$

Therefore $\widehat{\psi}$ will be injective whenever ψ is. This completes the proof. □

Remark 15. The explicit formula (4) for $\widehat{\psi}$ is not given in the statement of Theorem 3 because it can be deduced from the diagram (3). Nonetheless, the rule (4) derived in the course of the proof is worth remembering.

Example 8. Recall Example 7, in which $R = \mathbb{Z}/6Z$ and $S = \{1, 2, 2^2, \ldots\} = \{1, 2, 4\}$. Let $\pi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ be the natural surjection. Since $\pi(2) = 2$ and $\pi(4) = 1$ are units in $\mathbb{Z}/3\mathbb{Z}$, Theorem 3 implies there is a unique lift $\widehat{\pi} : S^{-1}R \to \mathbb{Z}/3\mathbb{Z}$. According to (5), the kernel of $\widehat{\pi}$ consists of the fractions $\frac{0}{1}$ and $\frac{3}{s}$, $s \in S$. But

$$\frac{3}{s} = \frac{6}{2s} = \frac{0}{1},$$

which means that $\ker\widehat{\pi} = \left\{\frac{0}{1}\right\}$, i.e. $\widehat{\pi}$ is an embedding. Since π is surjective, so is $\widehat{\pi}$. $\widehat{\pi}$ therefore provides an isomorphism $S^{-1}R \cong \mathbb{Z}/3\mathbb{Z}$.

Example 9. The rational numbers are traditionally defined to be $\mathbb{N}^{-1}\mathbb{Z}$. But since $\mathbb{Z}$ is a domain, another candidate is the quotient field $\mathbb{Z}_{(0)}$. Which option is the "right" way to define $\mathbb{Q}$? Both: they're isomorphic! Under the natural map $\varphi_{(0)} : \mathbb{Z} \to \mathbb{Z}_{(0)}$, a natural number n is carried to $\frac{n}{1}$, which is a unit simply because $n \neq 0$. Theorem 3 lifts $\varphi_{(0)}$ to $\widehat{\varphi_{(0)}} : \mathbb{N}^{-1}\mathbb{Z} \to \mathbb{Z}_{(0)}$, given by

$$\frac{m}{n} \mapsto \frac{m}{1}\left(\frac{n}{1}\right)^{-1} = \frac{m}{n}.$$

Because $\mathbb{Z}$ is a domain, $\mathbb{Z} \setminus (0)$ is proper, so Lemma 2 tells us $\varphi_{(0)}$ is an embedding. Therefore $\widehat{\varphi_{(0)}}$ is an embedding, too. $\widehat{\varphi_{(0)}}$ is also surjective. To see this, let $\frac{m}{n} \in \mathbb{Z}_{(0)}$. Write $n = \epsilon n'$ with $\epsilon \in \{\pm 1\}$ and $n' \in \mathbb{N}$. Then

$$\frac{m}{n} = \frac{\epsilon m}{\epsilon n} = \frac{\epsilon m}{n'} = \widehat{\varphi_{(0)}}\left(\frac{\epsilon m}{n'}\right).$$

The induced map $\widehat{\varphi_{(0)}}$ therefore yields the desired isomorphism between $\mathbb{N}^{-1}\mathbb{Z}$ and $\mathbb{Z}_{(0)}$.

Example 10. Let R be a commutative ring and $a \in R$. Suppose we want to construct from R a ring in which a is a unit. This would require inverting not only a, but also all of its positive powers. So a natural candidate for such a ring would be $R_a = S^{-1}R$, where $S = \{1, a, a^2, a^3, \ldots\}$. But we might also try to construct polynomials in a^{-1} over R. This we can achieve with the ring $R[X]/(aX - 1)$. As one might suspect, these two constructions yield isomorphic rings.

Let ψ denote the composite map $R \to R[X] \to R[X]/(aX - 1)$. Let $n \in \mathbb{N}$. Since $aX \equiv 1 \pmod{aX - 1}$, $\psi(a)$ is a unit. Therefore $\psi(a^n) = \psi(a)^n$ is a unit for all $n \in \mathbb{N}$. By Theorem 3, there is a unique lift $\widehat{\psi} : R_a \to R[X]/(aX - 1)$, given by $\widehat{\psi}\left(\frac{b}{a^n}\right) = \psi(b)\psi(a)^{-n}$. The natural map $\varphi_S : R \to R_a$ induces a homomorphism $\widehat{\varphi_S} : R[X] \to R_a[X]$, which we compose with the evaluation $E_{1/a}$ to yield a homomorphism $\varphi : R[X] \to R_a$. For any $\sum_i b_i X^i \in R[X]$ we have

$$\varphi\left(\sum_i b_i X^i\right) = \sum_i \frac{b_i}{1}\left(\frac{1}{a}\right)^i = \sum_i \frac{b_i}{a^i}.$$

In particular,

$$\varphi(aX - 1) = \frac{a}{a} - \frac{1}{1} = \frac{0}{1},$$

so that $aX - 1 \in \ker \varphi$. φ therefore induces a homomorphism $\overline{\varphi} : R[X]/(aX - 1) \to R_a$, satisfying $\overline{\varphi}(f + (aX - 1)) = \varphi(f)$. We will shows that $\widehat{\psi}$ and $\overline{\varphi}$ are inverses.

Since $\psi(a)(X + (aX - 1)) = (a + (aX - 1))(X + (aX - 1)) = aX + (aX - 1) = 1 + (aX - 1)$, $\psi(a)^{-1} = X + (aX - 1)$, so that

$$\widehat{\psi}\left(\frac{b}{a^n}\right) = \psi(b)\psi(a)^{-n} = (b + (aX - 1))(X + (aX - 1))^n = bX^n + (aX - 1).$$

So, given any $f(X) = \sum_i b_i X^i \in R[X]$, we have

$$\widehat{\psi} \circ \overline{\varphi}\,(f + (aX - 1)) = \widehat{\psi}(\varphi(f)) = \widehat{\psi}\left(\sum_i \frac{b_i}{a^i}\right) = \sum_i \widehat{\psi}\left(\frac{b_i}{a^i}\right) = \left(\sum_i b_i X^i\right) + (aX - 1) = f + (aX - 1).$$

Hence $\widehat{\psi} \circ \overline{\varphi}$ is the identity map on $R[X]/(aX - 1)$. Likewise, for any $\frac{b}{a^n} \in R_a$, we have

$$\overline{\varphi} \circ \widehat{\psi}\left(\frac{b}{a^n}\right) = \overline{\varphi}(bX^n + (aX - 1)) = \varphi(bX^n) = \frac{b}{a^n},$$

so that $\overline{\varphi} \circ \widehat{\psi}$ is also the identity, this time on R_a. We conclude that $\widehat{\psi}$ and $\overline{\varphi}$ are inverse isomorphisms, so that

$$R_a \cong R[X]/(aX - 1),$$

as claimed.

Remark 16. Although the proof in Example 10 appears somewhat lengthy, it is actually rather straightforward. We simply constructed the "obvious" maps in each direction, and then checked that they inverted one another.

Remark 17. Example 10 explains the isomorphism $\mathbb{Z}\left[\frac{1}{2}\right] \cong \mathbb{Z}[X]/(2X - 1)$ that we encountered during our discussion of algebraic integers, and provides the immediate generalization $\mathbb{Z}\left[\frac{1}{a}\right] \cong \mathbb{Z}[X]/(aX - 1)$ for nonzero $a \in \mathbb{Z}$.

4 Quotient Fields

The quotient field of a domain R plays a distinguished role among the (proper) localizations of R: it contains (a copy of) R as well as (copies of) all of its proper localizations. We begin with a lemma.

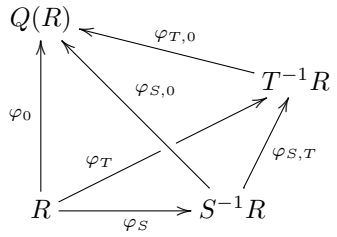
Lemma 3. *Let R be a commutative ring and let $S \subset T \subset R$ be multiplicative sets. There is a commutative diagram*

$$\begin{array}{ccc} S^{-1}R & & \\ \uparrow{\scriptstyle \varphi_S} & \searrow^{\varphi_{S,T}} & \\ R & \xrightarrow[\varphi_T]{} & T^{-1}R \end{array} \quad . \tag{6}$$

For all $\frac{a}{s} \in S^{-1}R$, $\varphi_{S,T}\left(\frac{a}{s}\right) = \frac{a}{s}$. If φ_T is an embedding, then φ_S and $\varphi_{S,T}$ are also embeddings.

Proof. Any $s \in S$ belongs to T, and therefore $\varphi_T(s)$ is a unit in $T^{-1}R$. Theorem 3 then guarantees the existence of $\varphi_{S,T} = \widehat{\varphi_T}$ making (6) commute. If φ_T is an embedding, then T, and hence S, is proper. Therefore φ_S is an embedding as well. That $\varphi_{S,T}$ is an embedding in this situation follows directly from Theorem 3. □

Theorem 4. *Let R be a domain with quotient field $Q(R)$. If $S \subset T \subset R$ are proper multiplicative sets (i.e. $0 \notin S, T$), there is a commutative diagram of embeddings*



(7)

in which $\varphi_{*,*}\left(\frac{a}{s}\right) = \frac{a}{s}$ for all $\frac{a}{s}$.

Proof. Let $U = R \setminus \{0\}$. Then $S, T \subset U$. Successively apply Lemma 3 to the pairs (S,T), (S,U) and (T,U) to obtain $\varphi_{S,T}$, $\varphi_{S,0} = \varphi_{S,U}$ and $\varphi_{T,0} = \varphi_{T,U}$. All maps are embeddings because S, T and U are proper. The only thing to check is the commutativity of the "rightmost face" of the diagram, which is an immediate consequence of the formula $\varphi_{*,*}\left(\frac{a}{s}\right) = \frac{a}{s}$. □

Corollary 1. *The quotient field of a domain R naturally contains compatibly isomorphic copies of R and all of R's localizations.*

Remark 18. One can actually be a bit more precise. Theorem 4 (almost) proves that

$$Q(R) \cong \varinjlim S^{-1}R,$$

the limit being taken over the collection of proper multiplicative subsets of R, ordered by inclusion.

The quotient field of a domain R is unique in the sense that any field K containing R as a subring contains a unique copy of $Q(R)$. We will prove this in the following form.

Theorem 5. *Let K be a field with subring R. Let $\mathcal{F}$ denote the set of subfields of K containing R and set*

$$k = \bigcap_{F \in \mathcal{F}} F.$$

Then k is the unique subfield of K that is R-isomorphic to $Q(R)$.

Proof. Let $i : R \to k$ denote the inclusion map. Since k is a field, every nonzero element of R is a unit. By Theorem 3 i therefore induces $\widehat{i} : Q(R) \to k$. Because i is injective, $\widehat{i}$ is an embedding. Let k' denote the image of $\widehat{i}$. Then k' is a subfield of K, and for any $r \in R$ we have

$$r = i(r) = \widehat{i} \circ \varphi_0(r) \in k'.$$

Hence $k' \in \mathcal{F}$ and consequently $k \subset k'$. Since $k' \subset k$, this means $k = k'$ so that $\widehat{i}$ is an isomorphism. Furthermore, for $r \in R$ and $\frac{a}{s} \in Q(R)$ we have

$$\widehat{i}\left(\frac{r}{1} \cdot \frac{a}{s}\right) = \widehat{i}\left(\frac{ra}{s}\right) = ras^{-1} = r \cdot \widehat{i}\left(\frac{a}{s}\right),$$

so that $\widehat{i}$ is an R-isomorphism.

Suppose $\psi : Q(R) \to K$ is any embedding over R. Then for any $r \in R$ we have

$$\psi\left(\frac{r}{1}\right) = r\psi\left(\frac{1}{1}\right) = r \cdot 1 = r,$$

so that R is contained in the image k'' of ψ. This again implies that $k \subset k''$. Therefore $k' \subset k''$. Now consider the map $\varphi = \psi^{-1} \circ \widehat{i} : Q(R) \to Q(R)$. Because φ is an R-homomorphism,

$$\varphi\left(\frac{a}{s}\right) = \varphi\left(\frac{a}{1}\left(\frac{s}{1}\right)^{-1}\right) = \frac{a}{1} \cdot \varphi\left(\frac{s}{1}\right)^{-1} = \frac{a}{1}\left(\frac{s}{1} \cdot \varphi\left(\frac{1}{1}\right)\right)^{-1} = \frac{a}{s}.$$

That is, φ is the identity map. So $\psi = \psi \circ \varphi = \psi \circ \psi^{-1} \circ \widehat{i} = \widehat{i}$ and $k'' = k' = k$. □

Example 11. Let $f(X) = X^2 + pX + q \in \mathbb{Z}[X]$ be irreducible (that is, $p^2 - 4q$ is not a perfect square). Let $\alpha \in \mathbb{C}$ be one of the roots of f. We have seen that

$$\mathbb{Z}[\alpha] = \{a + b\alpha \,|\, a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$. An identical proof shows that

$$\mathbb{Q}(\alpha) = \{a + b\alpha \,|\, a, b \in \mathbb{Q}\}$$

is also a subring of $\mathbb{C}$. Let $\alpha' \in \mathbb{C}$ denote the other root of f. Notice that this means $\alpha + \alpha' = -p$ and $\alpha\alpha' = q$. Given $\beta = a + b\alpha \in \mathbb{Q}(\alpha)$, in $\mathbb{C}$ we have

$$\frac{1}{\beta} = \frac{a + b\alpha'}{(a + b\alpha)(a + b\alpha')} = \frac{a - b(p + \alpha)}{a^2 - pab + b^2q} = \frac{a - pb}{a^2 - pab + b^2q} - \frac{b}{a^2 - pab + b^2q}\alpha \in \mathbb{Q}(\alpha).$$

Therefore $\mathbb{Q}(\alpha)$ is a field. It is easy to see that $\mathbb{Q}(\alpha)$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Z}[\alpha]$. By Theorem 5, $\mathbb{Q}(\alpha)$ is (isomorphic to) the quotient field of $\mathbb{Z}[\alpha]$.

5 Ideals

We now turn to ideal theory in localizations of rings. Let R be a commutative ring with multiplicative subset S. If $\mathfrak{a}$ is an ideal in R, let

$$S^{-1}\mathfrak{a} = \left\{\frac{a}{s} \,\middle|\, a \in \mathfrak{a}, s \in S\right\}.$$

If $x, y \in S^{-1}\mathfrak{a}$, there are $a, b \in \mathfrak{a}$ and $s, t \in S$ so that $x = \frac{a}{s}$ and $y = \frac{b}{t}$. Then

$$x - y = \frac{a}{s} + \frac{-b}{t} = \frac{at - bs}{st} \in S^{-1}\mathfrak{a}$$

since $at - bs \in \mathfrak{a}$. If $z = \frac{c}{u} \in S^{-1}R$, then

$$zx = \frac{ca}{us} \in S^{-1}\mathfrak{a}$$

since $ca \in \mathfrak{a}$. Therefore $S^{-1}\mathfrak{a}$ is an ideal in $S^{-1}R$, which we will call the *localization* of $\mathfrak{a}$. Notice that the kernel in equation (5) is the localization of an ideal.

Going the other direction, if $\mathfrak{b}$ is an ideal in $S^{-1}R$, then $\varphi_S^{-1}(\mathfrak{b})$ is an ideal in R. We have $a \in \varphi_S^{-1}(\mathfrak{b})$ if and only if $\frac{a}{1} \in \mathfrak{b}$. Notice that for any $s \in S$, if $\frac{a}{s} \in \mathfrak{b}$, then $\frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s} \in \mathfrak{b}$. Thus $\frac{a}{1} \in \mathfrak{b}$ if and only if $\frac{a}{s} \in \mathfrak{b}$ for *some* $s \in S$. That is,

$$\varphi_S^{-1}(\mathfrak{b}) = \left\{ a \in R \,\middle|\, (\exists s \in S)\left(\frac{a}{s} \in \mathfrak{b}\right) \right\}. \tag{8}$$

So $\varphi_S^{-1}(\mathfrak{b})$ consists of all numerators of fractions in $\mathfrak{b}$. We claim that $\varphi_S^{-1}(\mathfrak{b})$ is an ideal in R. Let $a, b \in \varphi_S^{-1}(\mathfrak{b})$, $r \in R$. Then

$$\varphi_S(a-b) = \frac{a-b}{1} = \frac{a}{1} - \frac{b}{1} \in \mathfrak{b},$$

since $\mathfrak{b}$ is an ideal in $S^{-1}R$. Hence $a - b \in \varphi_S^{-1}(\mathfrak{b})$. Likewise,

$$\varphi_S(ra) = \frac{ra}{1} = \frac{r}{1} \cdot \frac{a}{1} \in \mathfrak{b},$$

again because $\mathfrak{b}$ is an ideal, so that $ra \in \varphi_S^{-1}(\mathfrak{b})$. This proves our claim. We will call $\varphi_S^{-1}(\mathfrak{b})$ the *numerator ideal* of $\mathfrak{b}$.

Let $\mathcal{I}$ denote the set of ideals in R and let $\mathcal{J}$ denote the set of ideals in $S^{-1}R$. We therefore have two mappings:

$$\begin{array}{ll} \Phi : \mathcal{I} \to \mathcal{J}, & \\ \quad \mathfrak{a} \mapsto S^{-1}\mathfrak{a} & \text{and} \\ & \Psi : \mathcal{J} \to \mathcal{I}, \\ & \quad \mathfrak{b} \mapsto \varphi_S^{-1}(\mathfrak{b}). \end{array}$$

How are they related? Let $a \in \mathfrak{a}$. Then $\varphi_S(a) = \frac{a}{1} \in S^{-1}\mathfrak{a}$, so that $a \in \varphi_S^{-1}(S^{-1}\mathfrak{a})$. Thus $\mathfrak{a} \subset \varphi_S^{-1}(S^{-1}\mathfrak{a}) = \Psi \circ \Phi(\mathfrak{a})$. Similarly, if $\frac{a}{s} \in \mathfrak{b}$, then $a \in \varphi_S^{-1}(\mathfrak{b})$, by (8). This immediately implies that $\frac{a}{s} \in S^{-1}\varphi_S^{-1}(\mathfrak{b})$, and we conclude that $\mathfrak{b} \subset S^{-1}\varphi_S^{-1}(\mathfrak{b}) = \Phi \circ \Psi(\mathfrak{b})$.

Only the second of these containments can be reversed in general. Let $x \in S^{-1}\varphi_S^{-1}(\mathfrak{b})$. Then $x = \frac{a}{s}$ for some $s \in S$ and $a \in \varphi_S^{-1}(\mathfrak{b})$, i.e. $\frac{a}{1} \in \mathfrak{b}$. Thus $x = \frac{1}{s} \cdot \frac{a}{1} \in \mathfrak{b}$, and we obtain $S^{-1}\varphi_S(\mathfrak{b}) \subset \mathfrak{b}$. We have now proven our first result on ideals.

Lemma 4. *Let R be a commutative ring, $S \subset R$ a multiplicative set, $\mathfrak{a}$ and ideal in R, and $\mathfrak{b}$ an ideal in $S^{-1}R$. Then*

1. $\mathfrak{a} \subset \varphi_S^{-1}(S^{-1}\mathfrak{a})$;
2. $\mathfrak{b} = S^{-1}\varphi_S^{-1}(\mathfrak{b})$.

Corollary 2. *Every ideal of $S^{-1}R$ has the form $S^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a}$ in R.*

Proof. Given an ideal $\mathfrak{b}$ in $S^{-1}R$, $\mathfrak{a} = \varphi_S^{-1}(\mathfrak{b})$ works. □

What happens is we attempt to show that $\varphi_S^{-1}(S^{-1}\mathfrak{a}) \subset \mathfrak{a}$? If a is a member of the left hand side, then $\frac{a}{1} \in S^{-1}\mathfrak{a}$. It's tempting to conclude that $a \in \mathfrak{a}$, but that's not what membership in $S^{-1}\mathfrak{a}$ guarantees. To say $\frac{a}{1} \in S^{-1}\mathfrak{a}$ means there exist $a' \in \mathfrak{a}$ and $s \in S$ so that $\frac{a}{1} = \frac{a'}{s}$, or $s'(as - a') = 0$ for some $s' \in S$. This implies $ss'a = s'a' \in \mathfrak{a}$. That is, the most we can say is that a *multiple* of a (by an element of S) belongs to $\mathfrak{a}$. In order to make use of this condition we need to enforce additional hypotheses. What if $\mathfrak{a} = \mathfrak{p}$ is prime and $\mathfrak{p}$ avoids S? Then $ss'a \in \mathfrak{p}$ implies $a \in \mathfrak{p}$, as we had originally hoped, since this proves that $\varphi_S^{-1}(S^{-1}\mathfrak{p}) \subset \mathfrak{p}$. The theorem below is an immediate consequence of these computations.

Theorem 6. *Let R be a commutative ring and $S \subset R$ a multiplicative set. For any prime ideal $\mathfrak{p}$ in R that avoids S,*

$$\mathfrak{p} = \varphi_S^{-1}(S^{-1}\mathfrak{p}).$$

If $\mathfrak{p}$ is a prime ideal in R avoiding a multiplicative subset S, and $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in S^{-1}\mathfrak{p}$, then there exist $p \in \mathfrak{p}$ and $u \in S$ so that $\frac{ab}{st} = \frac{p}{u}$. So there is an $s' \in S$ with $s'(abu - pst) = 0$, which implies $abs'u = pss't \in \mathfrak{p}$. Because $\mathfrak{p}$ is prime and $s', u \notin \mathfrak{p}$, we must have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Then $\frac{a}{s}$ or $\frac{b}{t}$ belongs to $S^{-1}\mathfrak{p}$. This *almost* proves that $S^{-1}\mathfrak{p}$ is a prime ideal: we haven't shown $S^{-1}\mathfrak{p}$ is actually proper. But Theorem 6 tells us this has to be the case. If $S^{-1}\mathfrak{p} = S^{-1}R$, we'd then have $\mathfrak{p} = \varphi_S^{-1}(S^{-1}\mathfrak{p}) = \varphi_S^{-1}(S^{-1}R) = R$, which is impossible. So $S^{-1}\mathfrak{p}$ is indeed proper, and is therefore prime.

If $\mathfrak{q}$ is a prime in $S^{-1}R$, then $\varphi_S^{-1}(\mathfrak{q})$ is a prime in R, simply because φ_S is a homomorphism. The ideal $\varphi_S^{-1}(\mathfrak{q})$ avoids S, for if $s \in S \cap \varphi_S^{-1}(\mathfrak{q})$, then the unit $\frac{s}{1}$ belongs to $\mathfrak{q}$, a contradiction. Lemma 4 and Theorem 6 now yield our final result.

Theorem 7. *Let R be a commutative ring, let $S \subset R$ be a multiplicative set, and let*

$$\mathrm{Spec}_S(R) = \{\mathfrak{p} \subset R \,|\, \mathfrak{p} \text{ is a prime ideal and } \mathfrak{p} \cap S = \varnothing\}.$$

The maps $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ and $\mathfrak{q} \mapsto \varphi_S^{-1}(\mathfrak{q})$ are inverse bijections between $\mathrm{Spec}_S(R)$ and $\mathrm{Spec}(S^{-1}R)$.

Example 12. With everything as above, fix a prime $\mathfrak{P}$, let $S = R \setminus \mathfrak{P}$ and set $R_{\mathfrak{P}} = S^{-1}\mathfrak{P}$. Let $\mathfrak{P}_{\mathfrak{P}} = S^{-1}\mathfrak{P}$, which is a prime ideal in $R_{\mathfrak{P}}$ by Theorem 7. If $\frac{a}{s} \notin \mathfrak{P}_{\mathfrak{P}}$, then $a \notin \mathfrak{P}$. This means that $a \in S$ and hence that $\frac{a}{s}$ is a unit in $R_{\mathfrak{P}}$. In other words, every element in the complement of $\mathfrak{P}_{\mathfrak{P}}$ is a unit. Since $\mathfrak{P}_{\mathfrak{P}}$ is proper, the units of $R_{\mathfrak{P}}$ must lie outside of $\mathfrak{P}_{\mathfrak{P}}$. Thus $\mathfrak{P}_{\mathfrak{P}} = R_{\mathfrak{P}} \setminus R_{\mathfrak{P}}^{\times}$, proving that $R_{\mathfrak{P}}$ is a local ring with unique maximal ideal $\mathfrak{P}_{\mathfrak{P}}$. Every other prime in $R_{\mathfrak{P}}$ must correspond to a prime in R avoiding $R \setminus \mathfrak{P}$, by Theorem 7. Any such prime must lie inside of $\mathfrak{P}$. So every prime in $R_{\mathfrak{P}}$ can be written uniquely the form $S^{-1}\mathfrak{p}$ for some prime $\mathfrak{p} \subset \mathfrak{P}$. These results are worth recording.

Proposition 1. *Let R be a commutative ring and let $\mathfrak{P}$ be a prime ideal in R. Then $R_{\mathfrak{P}}$ is a local ring with unique maximal ideal $\mathfrak{P}_{\mathfrak{P}}$. The primes in $R_{\mathfrak{P}}$ are in one-to-one correspondence with the primes contained in $\mathfrak{P}$.*