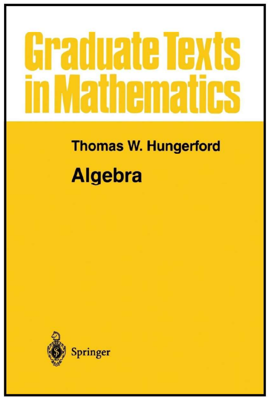
Modern Algebra

Chapter III. Rings

III.4. Rings of Quotients and Localization—Proofs of Theorems



Theorem III.4.3

Theorem III.4.3. Let S be a multiplicative subset of a commutative ring R and let $S^{-1}R$ be the set of equivalence classes of $R \times S$ under the equivalence relation of Theorem III.4.2.

(i) $S^{-1}R$ is a commutative ring with identity, where addition and multiplication are defined by

$$r/s + r'/s' = (rs' + r's)/(ss') \text{ and } (r/s)(r'/s') = (rr')/(ss').$$

(ii) If R is a nonzero ring with no zero divisors and $0 \notin S$, then $S^{-1}R$ is an integral domain.

(iii) If R is a nonzero ring with no zero divisors and S is the set of all nonzero elements of R, then $S^{-1}R$ is a field.

Proof. (i) First, if $0 \in S$ then by Note III.4.A(iii) we have $S^{-1}R$ is a zero ring, so we assume without loss of generality that $0 \notin S$. To show that addition is well defined, let $r/s = r_1/s_1$ and $r'/s' = r_1'/s_1'$. Then by Note III.4.A(i), there exist $s_2, s_3 \in S$ such that $s_2(rs_1 - r_1s) = 0$ and $s_3(r's_1' - r_1's') = 0$.

Theorem III.4.3 (continued 1)

Proof (continued). Then by Note III.4.A(i), there exist $s_2, 3_2 \in S$ such that $s_2(rs_1 - r_1s) = 0$ and $s_3(r's_1' - r_1's') = 0$. Multiplying the first equation by $s_3s's_1'$ and multiplying the second equation by s_2ss_1 we have

$$s_2s_3s's_1'(rs_1 - r_1s) = 0 \text{ and } s_2s_3ss_1(r's_1' - r_1's') = 0.$$

Adding these two equations gives

$$s_2s_3\left((rs_1 - r_1s)s's_1' + (r's_1' - r_1's')ss_1\right) = 0$$

$$\text{or } s_2s_3(rs_1s's_1' + r's_1'ss_1 - r_1ss's_1' - r_1's'ss_1) = 0$$

$$\text{or } s_2s_3\left((rs' + r's)s_1s_1' - (r_1s_1' + r_1's_1)ss'\right) = 0.$$

Therefore $(rs' + r's)/(ss') = (r_1s_1' + r_1's_1)/(s_1s_1')$ since $s_2s_3 \in S$ (because S is multiplicative), by Note II.4.A(i). Hence

$$r/s + r'/s' = (rs' + r's)/(ss') = (r_1s_1' + r_1's_1)/(s_1s_1') = r_1/s_1 + r_1'/s_1'$$

and addition on $S^{-1}R$ is well-defined.

Theorem III.4.3 (continued 2)

Proof (continued). To show multiplication is well-defined, again let $r/s = r_1/s_1$ and $r'/s' = r_1'/s_1'$. Then by Notes II.4.A(i), there exists $s_2, s_3 \in S$ such that $s_2(rs_1 - r_1s) = 0$ and $s_3(r's_1' - r_1's') = 0$. Multiplying the first equation by $r's_1's_3$ and multiplying the second equation by r_1ss_2, we get

$$s_2(rs_1 - r_1s)r's_1's_3 = s_2s_3(rr's_1s_1' - r_1r'ss_1') = 0$$

$$\text{and } s_3(r's_1' - r_1's')r_1ss_2 = s_2s_3(r_1r'ss_1' - r_1r_1'ss') = 0.$$

Adding these two equations gives

$$s_2s_3(rr's_1s_1' - r_1r'ss_1' + r_1r'ss_1' - r_1r_1'ss') = 0$$

$$\text{or } s_2s_3(rr's_1s_1' - r_1r_1'ss') = 0.$$

Therefore $(rr')/(ss') = (r_1r_1')/(s_1s_1')$ since $s_2s_3 \in S$ (because S is multiplicative), by Note III.4.A(i). Hence

$$(r/s)(r'/s') = (rr')/(ss') = (r_1r_1')/(s_1s_1') = (r_1/s_1)(r_1'/s_1')$$

and multiplication in $S^{-1}R$ is well-defined.

Theorem III.4.3 (continued 3)

Proof (continued). Next, since R is commutative then

$$(r/s)(r'/s') = (rr')/(ss') = (r'r)/(s's) = (r'/s')(r/s)$$

and so $S^{-1}R$ is commutative. For $s, s' \in S$ we have $0/s = 0/s'$ in $S^{-1}R$ and for any $r/s \in S^{-1}R$ we have

$$r/s + 0/s = (rs + 0s)/(ss) = (rs)/(ss) = r/s$$

(where the last equality holds because $(rs)s = (ss)r$) so that $0/s$ is the additive identity in $S^{-1}R$ (remember, $0/s$ represents an equivalence class). For $r/s \in S^{-1}R$ we know that $(-r)/s \in S^{-1}R$ and $r/s + (-r)/s = (rs + (-r)(s))/s = 0/s$ so that the additive inverse of $r/s \in S^{-1}R$ is $(-r)/s \in S^{-1}R$. For $s, s' \in S$, we have $s/s = s'/s'$ and for $r/s \in S^{-1}R$ we have $(r/s)(s/s) = (rs)/(ss) = r/s$ so that $s/s \in S^{-1}R$ is the multiplicative identity of $S^{-1}R$. Therefore, $S^{-1}R$ is a commutative ring with identity with addition and multiplication as given, establishing (i).

Theorem III.4.3 (continued 4)

Theorem III.4.3. Let S be a multiplicative subset of a commutative ring R and let $S^{-1}R$ be the set of equivalence classes of $R \times S$ under the equivalence relation of Theorem III.4.2.

(ii) If R is a nonzero ring with no zero divisors and $0 \notin S$, then $S^{-1}R$ is an integral domain.

Proof (continued). (ii) If $r/s = 0/s$ then by Note III.4.A(i), $s_1(rs - 0s) = s_1 rs = 0$ for some $s_1 \in S$. Since we have hypothesized that R has no zero divisors and $0 \notin S$, then it must be that $r = 0$ (and conversely $r = 0$ implies $r/s = 0/s$). Consequently, $(r/s)(r'/s') = (rr')/(ss') = 0/s$ in $S^{-1}R$ if and only if $rr' = 0$ in R. Since R has no zero divisors, then either $r = 0$ or $r' = 0$ and so either $r/s = 0/s$ or $r'/s' = 0/s'$ so that $S^{-1}R$ has no zero divisor and since $S^{-1}R$ is commutative, then it is an integral domain, as claimed.

Theorem III.4.3 (continued 5)

Theorem III.4.3. Let S be a multiplicative subset of a commutative ring R and let $S^{-1}R$ be the set of equivalence classes of $R \times S$ under the equivalence relation of Theorem III.4.2.

(iii) If R is a nonzero ring with no zero divisors and S is the set of all nonzero elements of R, then $S^{-1}R$ is a field.

Proof (continued). (iii) By part (ii), we have that $S^{-1}R$ is an integral domain. We only need to show that every nonzero element of $S^{-1}R$ has a multiplicative inverse. If $r/s \in S^{-1}R$ and $r/s \neq 0/s$ then $r \neq 0$ (as shown in part (ii)). So $s/r \in S^{-1}R$ and we have $(r/s)(s/r) = (rs)/(rs)$ and this is the multiplicative identity, as shown in (i). Hence $S^{-1}R$ is a field, as claimed. □

Theorem III.4.4

Theorem III.4.4. Let S be a multiplicative subset of a commutative ring R.

(i) The map $\varphi_S : R \to S^{-1}R$ given by $r \mapsto rs/s$ (for any $s \in S$) is a well-defined homomorphism of rings such that $\varphi_S(s)$ is a unit in $S^{-1}R$ for every $s \in S$.

(ii) If $0 \notin S$ and S contains no zero divisors, then φ_S is a monomorphism. In particular, any integral domain may be embedded in its quotient field.

(iii) If R has an identity and S consists of units, then φ_S is an isomorphism. In particular, the complete ring of quotients of a field F is isomorphic to F.

Proof. (i) To show φ_S is well-defined, we need to show that the value, for a given input $r \in R$, is independent of the element $s \in S$ used. If $s, s' \in S$ then we need to show that $rs/s = rs'/s'$. That is, we need $s_1(rss' - rs's) = 0$ for some $s_1 \in S$.

Theorem III.4.4 (continued 1)

Proof (continued). But since R is commutative, then $rss' - rs's = rss' - rss' = 0$ so that this holds for all $s_1 \in S$ and hence $rs/s = rs'/s'$, as needed. Let $r, r' \in R$ and $s \in S$. Then

$$\begin{aligned} \varphi_S(r + r') &= (r + r')s/s \\ &= rs/s + r's/s \text{ by Theorem III.4.3(i)} \\ &= \varphi_S(r) + \varphi_S(r') \end{aligned}$$

and

$$\begin{aligned} \varphi_S(rr') &= (rr'(s^2))/(s^2) \text{ where } s^2 \in S \text{ since } S \text{ is multiplicative} \\ &= ((rsr's))/s^2 \text{ since } R \text{ is commutative} \\ &= (rs/s)(r's/s) \text{ by Theorem III.4.3(i)} \\ &= \varphi_S(r)\varphi_S(r'). \end{aligned}$$

So φ_S is a ring homomorphism, as claimed.

Theorem III.4.4 (continued 2)

Theorem III.4.4. Let S be a multiplicative subset of a commutative ring R.

(ii) If $0 \notin S$ and S contains no zero divisors, then φ_S is a monomorphism. In particular, any integral domain may be embedded in its quotient field.

Proof (continued). Next, for $s \in S$ we have $\varphi_S(s) = s^2/s$, using s itself as the element of R. We have $s/s^2 \in S^{-1}R$ since $s \in S$ so that $s^2 \in S$ (because S is multiplicative, and hence $(s, s^2) \in R \times S$). Now $\varphi_S(s)(s/s^2) = (s^2/s)(s/s^2) = s^3/s^3 = s/s$ and s/s is a multiplicative identity of $S^{-1}R$, as shown in the proof of Theorem II.4.3(i). That is, $\varphi_S(s)$ is a unit in $S^{-1}R$, as claimed.

(ii) Let $r \in \text{Ker}(\varphi_S)$. Then $\varphi_S(r) = rs/s = 0$ in $S^{-1}R$. Now the additive identity in $S^{-1}R$ is $0/s$ as shown in the proof of Theorem III.4.3(i), so we have $rs/s = 0/s$ or $s_1(rs^2 - 0s) = 0$ for some $s_1 \in S$, or $s_1rs^2 = rs_1s^2 = 0$. Now $s_1s^2 \neq 0$ since $s, s_1 \in S$, S is multiplicative, and $0 \notin S$.

Theorem III.4.4 (continued 3)

Theorem III.4.4. Let S be a multiplicative subset of a commutative ring R.

(ii) If $0 \notin S$ and S contains no zero divisors, then φ_S is a monomorphism. In particular, any integral domain may be embedded in its quotient field.

Proof (continued). Since S has no zero divisors and $r(s_1s^2) = 0$ then we must have $r = 0$. That is, $\text{Ker}(\varphi_S) = \{0\}$ and by Theorem I.2.3(i) (to apply Theorem I.2.3, we technically need to consider φ_S restricted to the additive group in R, since Theorem I.2.3 applies to homomorphisms of groups), φ_S is an injective homomorphism; that is, φ_S is a monomorphism, as claimed. If R is an integral domain (i.e., a commutative ring with identity and no zero divisors) and S is the set of all nonzero elements of R (including 1) then $S^{-1}R$ is the field of quotients of R and, since φ_S is injective, φ_S embeds R in $S^{-1}R$ (notice $1 \in S$ in this case), as claimed.

Theorem III.4.4 (continued 4)

Theorem III.4.4. Let S be a multiplicative subset of a commutative ring R.

(iii) If R has an identity and S consists of units, then φ_S is an isomorphism. In particular, the complete ring of quotients of a field F is isomorphic to F.

Proof (continued). **(iii)** First, since S consists of units then $0 \notin S$ and S contains no zero divisors (since s is a unit and $sr = 0$ implies $0 = s^{-1}0 = s^{-1}(sr) = (s^{-1}s)(r) = r$), so by part (ii), φ_S is a monomorphism. For any $r/s \in S^{-1}R$ we have $rs^{-1} \in R$ and $\varphi_S(rs^{-1}) = ((rs^{-1})s)/s = r/s$ so that φ_S is surjective and hence φ_S is an isomorphism, as claimed. For field F, the complete ring of quotients has $S = F \setminus \{0\}$, so that $0 \notin S$ and S consists of units, and hence $\varphi_S : F \to S^{-1}F$ is an isomorphism. That is, the complete ring of quotients (or, equivalently, "quotient field") is isomorphic to F, as claimed. □

Theorem III.4.5

Theorem III.4.5. Let S be a multiplicative subset of a commutative ring R and let T be any commutative ring with identity. If $f : R \to T$ is a homomorphism of rings such that $f(s)$ is a unit in T for all $s \in S$, then there exists a unique homomorphism of rings $\overline{f} : S^{-1}R \to T$ such that $\overline{f}\varphi_S = f$. The ring $S^{-1}R$ is completely determined (up to isomorphism) by this property.

Proof. First, let $f : R \to T$ be a homomorphism such that $f(s)$ is a unit in T for all $s \in S$. Define mapping $\overline{f} : S^{-1}R \to T$ as $\overline{f}(r/s) = f(r)(f(s))^{-1}$. We need to show $\overline{f}$ is well-defined. Let $r/s = r'/s'$. Then $s_1(rs' - r's) = 0$ for some $s_1 \in S$. Now $\overline{f}(r/s) = f(r)(f(s))^{-1}$ and $\overline{f}(r'/s') = f(r')(f(s'))^{-1}$ since f is a homomorphism. Next $f(s_1(rs' - r's)) = f(0)$ or $f(s_1)(f(r)f(s') - f(r')f(s)) = 0$. Since $f(s_1)$ is a unit in T by hypothesis, then $f(r)r(s') - f(r')f(s) = 0$ or $f(r)f(s') = f(r')f(s)$ or $f(r)(f(s))^{-1} = f(r')(f(s'))^{-1}$ (since $f(s)$ and $f(s')$ are units) or $\overline{f}(r/s) = \overline{f}(r'/s')$ as needed, and $\overline{f}$ is well defined, as claimed.

Theorem III.4.5 (continued 1)

Proof (continued). To see that $\overline{f} : S^{-1}R \to T$ is a ring homomorphism, consider

$$\begin{aligned} \overline{f}(r/s + r'/s') &= \overline{f}((rs' + r's)/(ss')) \text{ by Theorem III.4.3(i)} \\ &= f(rs' + r's)(f(ss'))^{-1} = f(rs' + r's)(f(s))^{-1}(f(s'))^{-1} \\ &= f(r)f(s')(f(s))^{-1}(f(s'))^{-1} + f(r)f(s)(f(s))^{-1}(f(s'))^{-1} \\ &= f(r)(f(s))^{-1} + f(r')(f(s'))^{-1} \\ &= \overline{f}(r/s) + \overline{f}(r'/s') \text{ since } f \text{ is a homomorphism} \\ &\quad \text{and } R \text{ is commutative,} \end{aligned}$$

and

$$\begin{aligned} \overline{f}((r/s)(r'/s')) &= \overline{f}(rr'/(ss')) \text{ by Theorem III.4.3(i)} \\ &= f(rr')(r(ss'))^{-1} = f(r)(f(s))^{-1}f(r')(f(s'))^{-1} \\ &= \overline{f}(r/s)\overline{f}(r'/s') \text{ since } f \text{ is a homomorphism,} \\ &\quad \text{and } R \text{ and } T \text{ are commutative.} \end{aligned}$$

Theorem III.4.5 (continued 2)

Proof (continued). Also, for $r \in R$ we have

$$\overline{f}\varphi_S(r) = \overline{f}(rs/s) = f(rs)(f(s))^{-1} = f(r)f(s)(f(s))^{-1} = f(r)$$

so that $\overline{f}\varphi_S = f$ on R, as claimed.

Now suppose $g : S^{-1}R \to T$ is another homomorphism such that $g\varphi_S = f$. Then for all $x \in S$ we have $g(\varphi_S(s)) = f(s)$ is a unit in T. Consequently $g((\varphi_S(s))^{-1}) = (f(\varphi_S(s)))^{-1}$ for every $s \in S$ by Exercise III.1.15(c) (since $\varphi_S(s)$ is a unit in $S^{-1}R$ by Theorem III.4.4(i), and $g(\varphi_S(s))$ is a unit, the hypotheses of Exercise III.1.15(c) are satisfied). Since $\varphi_S(s) = s^2/s$ then $(\varphi_S(s))^{-1} = s/s^2 \in S^{-1}R$. Thus for each $r/s \in S^{-1}R$:

$$g(r/s_= f((rs/s)(s/s^2) = g(\varphi_S(r)(\varphi_S(s))^{-1}) = g(\varphi_S(r))g((\varphi_S(s))^{-1})$$

$$= f(\varphi_S(r))(g(\varphi_S(s))^{-1} = f(r)(f(s))^{-1} = \overline{f}(r/s).$$

Therefore, $g = \overline{f}$, so that homomorphism $\overline{f}$ is unique.

Theorem III.4.5 (continued 3)

Proof (continued). Now we show that $S^{-1}R$ is completely determined (up to isomorphism) by R, S, and the stated properties. Let $\mathcal{C}$ be the category whose objects are all (f, T), where T is a commutative ring with identity and $f : R \to T$ is a homomorphism of rings such that $f(s)$ is a unit in T for every $s \in S$. Define a morphism in $\mathcal{C}$ from (f_1, T_1) to (f_2, T_2) to be a homomorphism of rings $g : T_1 \to T_2$ such that $gf_1 = f_2$. To verify that $\mathcal{C}$ is a category (by Definition I.7.1), we need to verify that $g = \hom(T_1, T_2)$ is a morphism. Let (f_1, T_1), (f_2, T_2), (f_3, T_3) be objects in $\mathcal{C}$. Suppose $gT_1 \to T_2$ and $h : T_2 \to T_3$, where $gf_1 = f_2$ and $hf_2 = f_3$, are ring homomorphisms. Then $h \circ g : T_1 \to T_3$ is a ring homomorphism and $(h \circ g)f_1 = f(g(f_1) = hf_2 = f_3$. Because function composition is associative, then we have associativity of morphisms. For the identity on (f, T), we simply take the identity homomorphism $1_T : T \to T$. If $g : T_1 \to T_2$ is an isomorphism and $gf_1 = f_2$, then $g^{-1} : T_2 \to T_1$ is an isomorphism and $g^{-1}(gf_1) = g^{-1}f_2$ or $g^{-1}f_2 = f_1$. Also, $g \circ g^{-1} = 1_{T_2}$ and $g^{-1} \circ g = 1_{T_1}$. That is, a ring isomorphism is an equivalence.

Theorem III.4.5 (continued 4)

Proof (continued). If $g : T_1 \to T_2$ is not an isomorphism (but still is a homomorphism), then g is not a bijection and no inverse mapping $T_2 \to T_1$ exists. That is, if g is not an isomorphism then it is not an equivalence. For given object $(\varphi_S, S^{-1}T)$ in category $\mathcal{C}$ there is, for every object (f_I, T_I) in $\mathcal{C}$, by Theorem III.4.5 a unique mapping $(\varphi_S, S^{-1}R) \to (f_I, T_I)$ such that $\overline{f} : S^{-1}R \to T$ is a homomorphism and $\overline{f}\varphi_S = f$; that is, there is a unique morphism mapping $(\varphi_S, S^{-1}R) \to (f_I, T_I)$ for every object (f_I, T_I) in $\mathcal{C}$. Therefore, by Definition I.7.9, $(\varphi_S, S^{-1}R)$ is a universal object in category $\mathcal{C}$. By Theorem I.710, we now have that nay two universal objects in $\mathcal{C}$ are equivalent. That is, ring S^1R is completely determined (up to isomorphism; i.e., equivalence) by the properties of this theorem (namely, for given ring R and given homomorphism $f : R \to T$, where T is any commutative ring with unity, such that $f(s)$ is a unit in T for all s in given set D, there exists unique ring homomorphism $\overline{f} : S^{-1}R \to T$ such that $\overline{f}\varphi_S = f$). □

Corollary III.4.6

Corollary III.4.6. Let R be an integral domain considered as a subring of its quotient field F (see Theorem III.4.4(ii)). If E is a field and $f : R \to E$ is a monomorphism of rings, then there is a unique monomorphism of rings, then there is a unique monomorphism of fields $\overline{f} : F \to E$, such that $\overline{f}|_R = f$. In particular, any field E_1 containing R contains an isomorphic copy F_1 of F with $R \subset F_1 \subset E_1$.

Proof. Let S be the set of all nonzero elements of R. With $f : R \to E$ as a monomorphism (and so a homomorphism) of rings, and R as an integral domain (so that S contains no zero divisors; recall be Definition III.1.5 that an integral domain has no zero divisors), then by Theorem III.4.5 (with $T = E$ and $S^{-1}R = F$) there is a unique homomorphism $\overline{f} : F \to E$ such that $\overline{f}\varphi_S = f$. Suppose for $f_1, f_2 \in F = S^{-1}R$ we have $\overline{f}(f_1) = \overline{f}(f_2)$. Notice that

$$\begin{aligned}\overline{f}(f_1) &= \overline{f}(f_1\varphi_S(s)(\varphi_S(s))^{-1}) = \overline{f}(f_1(s^2/s)(s/s^2)) = \overline{f}(f_1(s/s)(s^2/s^2)) \\ &= \overline{f}(f_1 s/s)\overline{f}(s^2/s^2) = \overline{f}\varphi_S(f_1)\overline{f}(s^2/s^2) = f(f_1)\overline{f}(s^2/s^2).\end{aligned}$$

Corollary III.4.6 (continued)

Proof (continued). Similarly $\overline{f}(f_2) = f(f_2)\overline{f}(s^2/s^2)$. So $\overline{f}(f_1) = \overline{f}(f_2)$ implies $f(f_1)\overline{f}(s^2/s^2) = f(f_2)\overline{f}(s^2/s^2)$ and, since $\overline{f}(s^2/s^2) \in E$ then $f(s^2/s^2)$ has an inverse (since $s^2/s^2 \neq 0$ in $F - S^{-1}R$ and $\overline{f}$ is a monomorphism, then $\overline{f}(s^2/s^2) \neq 0$ in E). Therefore $f(f_1) = f(f_2)$ and, since f is a monomorphism by hypothesis, then $f_1 = f_2$. Therefore, $\overline{f}$ is a monomorphism. Since R is identified with $\varphi_S(R)$ in $F = S^{-1}R$ then $\overline{f}|_R = f$, as claimed (though, strictly speaking, we have $\overline{f}\varphi_S|_R = f$).

If E_1 is any field containing R, then with $f : R \to E_1$ as the inclusion map (namely, $f = 1_{E_1}|R$), we have $\overline{f} : F \to E_1$ such that $\overline{f}|_R = f = 1_{E_1}|R$ (more appropriately, $\overline{f}\varphi_S|R = f = 1_{E_1}|_R$). Then the image of $\overline{f}$ is an isomorphic copy F_1 of F (since monomorphism $\overline{f}$ is a surjection onto its image). That is, $R \subset F_1 \subset E_1$ where $F_1 \cong F$, as claimed. □

Theorem III.4.13

Theorem III.4.13. If R is a commutative ring with identity then the following conditions are equivalent:

(i) R is a local ring;
(ii) all nonunits of R are contained in some ideal $M \neq R$;
(iii) the nonunits of R form an ideal.

Proof. If I is an ideal of R, then by Theorem III.2.2 I is closed under "subtraction," left multiplication by elements of R, and right multiplication by elements of R. By Theorem III.2.5(i), principal ideal (a) consists of integer multiples of a, left multiples of a by elements of by elements of R, right multiples of a by elements of R, left and right multiples of a by elements of R, and sums of these. Therefore $(a) \subset I$. By Theorem III.3.2(iv), u is a unit if and only if $(u) = R$. So $I \neq R$ if and only if I consists only of nonunits. If (ii) holds and all nonunits are in ideal $M \neq R$, then M contains all nonunites (and not unites, since $M \neq R$) so that (iii) holds.

Theorem III.4.13 (continued)

Theorem III.4.13.

(i) R is a local ring;
(ii) all nonunits of R are contained in some ideal $M \neq R$;
(iii) the nonunits of R form an ideal.

Proof (continued). If (iii) holds and the nonunits of R form an ideal M, then this ideal is maximal (or else there would be an ideal containing all the nonunits and a unit, but then this ideal would be R itself). Any ideal not equal to R similarly cannot contain any units and so can consist only of nonunits. Therefore, any ideal not equal to R is a subset of M. Hence, M is maximal. That is, R is a local ring and (i) holds. Suppose (i) holds. Then R is a local ring, so that it has a unique maximal ideal. If $a \in R$ is a nonunit, then $(a) \neq R$. But by Note III.4.E, the maximal ideal contains every ideal in R (except R itself), and so contains every principal ideal (a) where a is a nonunit. That is, all nonunits are contained in some ideal $M \neq R$ (namely, the unique maximal one in R), and (ii) holds. Hence (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii), as claimed. □

Theorem III.4.7

Theorem III.4.7. Let S be a multiplicative subset of a commutative ring R.

(i) If I is an ideal in R, then $S^{-1}I = \{a/s \mid a \in I, x \in S\}$ is an ideal in $S^{-1}R$.
(ii) If J is another ideal in R, then $S^{-1}(I+J) = S^{-1}I + S^{-1}J$, $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$, and $S^{-1}(I \cap J) = (S^{-1}I)(S^{-1}J)$.

Proof. We start with three identities in $S^{-1}R$ which can be proved by induction. We give the base case and the general case follows similarly. Since $c_1/s + c_2/s = (c_1s + c_2s)/s^2$ by Theorem II.4.3(i), then $c_1/s + c_2/s = (c_1 + c_2)/s$ by Theorem II.4.2 because $s(c_1s + c_2s) = s^2(c_1 + c_2)$. By induction we then have

$$\sum_{i=1}^{n}(c_i/s) = \left(\sum_{i=1}^{n} c_i\right)\Big/ s. \qquad (1)$$

Theorem III.4.7 (continued 1)

Proof (continued). Now $(a_1/s)(b_1s/s) = (a_1b_1s)/a^2 = a_1b_1/s$ by Note III.4.A(ii), so by substitution

$$\sum_{j=1}^{m}(a_jb_j/s) = \sum_{j=1}^{m}(a_j/s)(b_js/s). \qquad (2)$$

Since $c_1/s_1 + c_2/s_2 = (c_1s_2 + c_2s_1)/(s_1s_2)$ by Theorem III.4.3(i), then by induction

$$\sum_{k=1}^{t}(c_k/s_k) = \sum_{k=1}^{t}(c_ks_1ss_2 \cdots s_{k-1}s_{k+1} \cdots s_t)/(s_1s_2 \cdots s_t). \qquad (3)$$

(i) Let $r/s \in S^{-1}R$ and $a/s' \in S^{-1}I$. Then $(r/s)(a/s') = (ra)/(ss')$ by Theorem III.4.3(i). Since I is an ideal of R then $ra \in I$ and since S is multiplicative then $ss' \in S$. Therefore $(ra)/(ss') \in S^{-1}I$ so that $S^{-1}I$ is a left and (since R is commutative) right deal of $S^{-1}R$, as claimed.

Theorem III.4.7 (continued 2)

Proof (continued). (ii) Notice that $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal of R by Theorem III.2.6(i). Now an element of $S^{-1}(I+J)$ is of the form $(a+b)/s$ where $a \in I$, $b \in J$, and $s \in S$. By (1) with $n = 2$ we have $(a+b)/s = a/s + b/s$ where $a/s \in S^{-1}I$ and $b/s \in S^{-1}J$. Therefore $S^{-1}(I+J) \subset S^{-1}I + S^{-1}J$. An element of $S^{-1}I + S^{-1}J$ is of the form $a/s + b/s'$. By (3) with $t = 2$ we have $a/s + b/s' = (as' + bs)/(ss')$. Since I and J are ideals of R then $as' \in I$ and $bs \in J$. Since S is multiplicative then $ss' \in S$. Therefore, $(as' + bs)/(ss')$ is an element of $S^{-1}(I+J)$. That is, $S^{-1}I + S^{-1}J \in S^{-1}(I+J)$. Hence $S^{-1}(I+J) = S^{-1}I + S^{-1}J$, as claimed.

Notice that IJ is an ideal of R by Theorem II.2.6(i). By definition (see Section III.2. Ideals)

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid n \in \mathbb{N}, a_i \in I, b_i \in J\}.$$

So (with the same notation) an element of $S^{-1}(IJ)$ is of the form $(a_1b_1 + a_2b_2 + \cdots + a_nb_n)/s$ for some $s \in S$.

Theorem III.4.7 (continued 3)

Proof (continued). By (1) (with $c_i = a_i b_i$) and (2) we have

$$\left(\sum_{i=1}^n a_i b_i\right) \Big/ s = \sum_{i=1}^n (a_i b_i)/s = \sum_{i=1}^n (a_i/s)(b_i s/s).$$

For each i we have $a_i/s \in S^{-1}I$, since J is an ideal then $b_i sin J$, and so $(b_i s)/s \in S^{-1}J$. Therefore, by the definition of the product of ideals $(S^{-1}I)(S^{-1}J)$, we have $(\sum_{i=1}^n a_i b_i)/s \in (S^{-1}I)(S^{-1}J)$. Therefore $S^{-1}(IJ) \subset (S^{-1}I)(S^{-1}J)$. An element of $(S^{-1}I)(S^{-1}J)$ is of the form $\sum_{k=1}^t (a'_k/s'_k)(b_k/s'') = \sum_{k=1}^t (a_k b_k)/(s'_k s''_k)$ by Theorem III.4.3(i). By (3) with $c_k = a_k b_k$ and $s_k = s'_k s''_k$ we have that this is of the form

$$\sum_{k=1}^t (c_k/s_k) = \sum_{k=1}^t (c_k s_1 s_2 \cdots s_{k-1} s_{k+1} \cdots s_t)/(s_1 s_2 \cdots s_t) = \sum_{k=1}^t (a_k b_k s'''_k)/s$$

where $s'''_k = s_1 s_2 \cdots s_{k-1} s_{k+1} \cdots s_t$ and $s = s_1 s_2 \ldots s_t$. Since J is an ideal then $b_k s'''_k \in J$, say $b_k s'''_k = b'_k \in J$, and since S is multiplicative then $s \in S$.

Theorem III.4.7 (continued 4)

Theorem III.4.7. Let S be a multiplicative subset of a commutative ring R.

(i) If I is an ideal in R, then $S^{-1}I = \{a/s \mid a \in I, x \in S\}$ is an ideal in $S^{-1}R$.

(ii) If J is another ideal in R, then $S^{-1}(I+J) = S^{-1}I + S^{-1}J$, $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$, and $S^{-1}(I \cap J) = (S^{-1}I)(S^{-1}J)$.

Proof (continued). So an element of $(S^{-1}I)(S^{-1}J)$ is of the form $\sum_{k=1}^t (a_k b'_k)/s$ where, by (1), equals $\left(\sum_{k=1}^t a_b b'_k\right)/s$. since $\sum_{k=1}^t a_k b'_k \in IJ$, then we have that an arbitrary element of $(S^{-1}I)(S^{-1}J)$ is an element of $S^{-1}(IJ)$. That is, $(S^{-1}I)(S^{-1}J) \subset S^{-1}(IJ)$. Hence $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$, as claimed.

Theorem III.4.7 (continued 5)

Proof (continued). Notice that $I \cap J$ is an ideal of R by Corollary III.2.3 An element of $S^{-1}(I \cap J)$ is of the form r/s where $r \in I \cap J$. Notice that $r \in I$ so $r/s \in S^{-1}I$, and $r \in J$ so $r/s \in S^{-1}J$. Therefore $r/s \in (S^{-1}I) \cap (S^{-1}J)$ and hence $S^{-1}(I \cap J) \subset (S^{-1}I)(S^{-1}J)$. An element of $(S^{-1}I) \cap (S^{-1}J)$ is of forms a/s and s/b' where $a \in I$, $b \in J$, and $s, s' \in S$. So $a/s = b/s'$ and $s_1(as' - bs) = 0$ for some $s_1 \in S$ by Theorem III.4.2. That is, $s_1 as' = s_1 bs$. Since I and J are ideals then $s_1 as' \in I$ and $s_1 bs \in J$. Say $c = s_1 as' = s_1 bs$ and then $c \in I \cap J$. Now $ss_1 s' \in S$ since S is multiplicative, so $c/(ss_1 s') = (s_1 s' a)/(ss_1 s') = a/s \in S^{-1}(I \cap J)$. So any element of $(S^{-1}I) \cap (S^{-1}J)$ is an element of $S^{-1}(I \cap J)$. That is, $(S^{-1}I) \cap (S^{-1}J) \subset S^{-1}(I \cap J)$. Therefore, $S^{-1}(I \cap J) = (S^{-1}I)(S^{-1}J)$, as claimed. □

Theorem III.4.8

Theorem III.4.8. Let S be a multiplicative subset of a commutative ring R with identity and let I be an ideal of R. Then $S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \varnothing$.

Proof. If $s \in S \cap I$, then $s/s \in S^{-1}I$ and s/s is the identity in $S^{-1}I$ as shown in the proof of Theorem III.4.3(i). We denote the identity in $S^{-1}R$ as $1_{S^{-1}R} = s/s$. Now $S^{-1}I$ is an ideal of $S^{-1}R$ by Theorem III.4.7(i), and by definition of an ideal $(r/s)(S^{-1}I) \sin S^{-1}I$ for all $r/s \in S^{-1}R$. With $1_{S^{-1}R} \in S^{-1}I$ we then have all elements of $S^{-1}R$ in $S^{-1}I$. Therefore, $S^{-1}I = S^{-1}R$ (of course, $S^{-1}I$ is always a subset of $S^{-1}R$), as claimed.

Now suppose $S^{-1}I = S^{-1}R$. The homomorphism $\varphi_S : R \to S^{-1}R$ given in Theorem III.4.4(i) gives the inverse image $\varphi_S(S^{-1}R) = R$. Since $S^{-1}I = S^{-1}R$ then $\varphi_S^{-1}(S^{-1}I) = R$. Whence because $1_R \in R$ then $\varphi_S(1_R) \in S^{-1}I$, so $\varphi_S(1_R) = a/s$ for some $a \in I$ and $s \in S$.

Theorem III.4.8 (continued)

Theorem III.4.8. Let S be a multiplicative subset of a commutative ring R with identity and let I be an ideal of R. Then $S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \varnothing$.

Proof (continued). Also, $\varphi_S(1_R) = 1_R s/s$, so we must have $a/s = 1_R s/s$ or $s_1(as - 1_R s^2) = 0$ for some $s_1 \in S$ by Theorem III.4.2. That is, $ass_1 = s^2 s_1$. But since S is multiplicative then $s^2 s_1 \in S$, and since I is an ideal then $ass_1 \in I$. Therefore $ass_1 = s^2 s_1 \in S \cap I$ and $S \cap I \neq \varnothing$, as claimed. □

Lemma III.4.9

Lemma III.4.9. Let S be multiplicative subset of a commutative ring R with identity and let I be an ideal in R.

(i) $I \subset \varphi_S^{-1}(S^{-1}I)$.

(ii) If $I = \varphi_S^{-1}(J)$ for some ideal J in $S^{-1}R$, then $S^{-1}I = J$. That is, every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I in R.

(iii) If P is a prime ideal in R and $S \cap P = \varnothing$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$ and $\varphi_S^{-1}(S^{-1}P) = P$.

Proof. (i) Since I is an ideal, then for any $a \in I$ we have $as \in I$ for all $s \in S$. So $\varphi_S(a) = (as)/s \in S^{-1}I$, and hence $a \in \varphi_2^{-1}(S^{-1}I)$. That is, $I \subset \varphi_S^{-1}(S^{-1}I)$, as claimed.

(ii) Since $I = \varphi_S^{-1}(J)$ by hypothesis, then every element of $S^{-1}I$ is of the form r/s where $r \in I = \varphi_S^{-1}(J)$; that is, $\varphi_S(r) \in J$. Therefore, $r/s = (1 + Rrs)/s^2 = (1_R/s = rs/s) = (1_R/s)\varphi_S(r)$ and this is in J since $\varphi_S(r) \in J$ and J is an ideal in $S^{-1}R$.

Lemma III.4.9 (continued 1)

Lemma III.4.9. Let S be multiplicative subset of a commutative ring R with identity and let I be an ideal in R.

(iii) If P is a prime ideal in R and $S \cap P = \varnothing$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$ and $\varphi_S^{-1}(S^{-1}P) = P$.

Proof (continued). So every element of $S^{-1}I$ is an element of J and $S^{-1}I \subset J$. Conversely, if $r/s \in J$, then $\varphi_S(r) = rs/s = rs^2/s^2 = (r/s)(s^2/s)$ and this is in J since $r/s \in J$, $s^2/s \in S^{-1}R$, and J is an ideal in $S^{-1}R$. Since $\varphi_S(r) \in J$ then $r \in \varphi_S^{-1}(J) = I$. Thus $r/s \in S^{-1}I$, and hence $J \subset S^{-1}I$. Therefore, we have $S^{-1}I = J$, as claimed.

(iii) Suppose P is a prime ideal in R and $S \cap P = \varnothing$. First, $S^{-1}P$ is an ideal of $S^{-1}R$ by Theorem III.4.7. Since $S \cap P = \varnothing$ then by Theorem III.4.7 $S^{-1}P \neq S^{-1}R$ (this is one requirement for $S^{-1}P$ to be a prime ideal in $S^{-1}R$). To show $S^{-1}P$ is a prime ideal, we consider a product of two elements of $S^{-1}P$, say $(r/s)(r'/s') \in S^{-1}P$.

Lemma III.4.9 (continued 2)

Lemma III.4.9. Let S be multiplicative subset of a commutative ring R with identity and let I be an ideal in R.

(iii) If P is a prime ideal in R and $S \cap P = \varnothing$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$ and $\varphi_S^{-1}(S^{-1}P) = P$.

Proof (continued). We then have $(rr')/(ss') = a/t$ for some $a \in P$ and some $t \in S$. Then by Theorem III.4.2, $s_1(trr' - ss'a) = 0$ for some $s_1 \in S$, or $s_1trr' = s_1ss'a$. Since $a \in P$ and P is an ideal of R then $s_1trr' = s_1ss'a \in P$. Now $s_1t \in S$ (since S is multiplicative and $S \cap P = \varnothing$, so by Theorem III.2.15 (with $a = s_1t$ and $b = rr'$ with a and b as the parameters of Theorem III.2.15), we have either $s_1t \in P$ or $rr' \in P$. But $s_1t \in S$ and $s_1t \notin P$ (since $S \cap P = \varnothing$), so we must have $rr' \in P$ (Theorem III.2.15 requires the fact that P is prime). Again based on the fact that P is prime, either $r \in P$ or $r' \in P$. Thus either $r/s \in S^{-1}P$ or $r'/s' \in S^{-1}P$. Since we considered arbitrary $(r/s)(r'/s') \in S^{-1}P$, then we now have that $S^{-1}P$ is a prime ideal in $S^{-1}R$ by Theorem III.2.15 (applied to $S^{-1}P$), as claimed.

Lemma III.4.9 (continued 3)

Lemma III.4.9. Let S be multiplicative subset of a commutative ring R with identity and let I be an ideal in R.

(iii) If P is a prime ideal in R and $S \cap P = \varnothing$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$ and $\varphi_S^{-1}(S^{-1}P) = P$.

Proof (continued). By part (i), $P \subset \varphi_S^{-1}(S^{-1}P)$. If $r \in \varphi_S^{-1}(S^{-1}P)$ then $\varphi_S(r) \in S^{-1}P$ so that $\varphi_S(r) = rs/s = at$ with $a \in P$ and $s, t \in S$. Again by Theorem III.4.2, $s_1(str - sa) = 0$ or $s_1str = s_1sa$. Since P is an ideal then $s_1sa \in P$ and so $(s_1st)r \in P$. By Theorem III.2.15 (because P is prime), either $s_1st \in P$ or $r \in P$. But $s_1st \in S$ and $S \cap P = \varnothing$ so we have $s_1st \notin P$ and hence we must have $r \in P$. Since r is an arbitrary element of $\varphi_S^{-1}(S^{-1}P)$, then we now have $\varphi_S^{-1}(S^{-1}P) \subset P$. That is, $\varphi_S^{-1}(S^{-1}P) = P$, as claimed. □

Theorem III.4.10

Theorem III.4.10. Let S be a multiplicative subset of a commutative ring R with identity. Then there is a one-to-one correspondence between the set $\mathcal{U}$ of prime ideals of R which are disjoint from S and the set $\mathcal{V}$ of prime ideals of $S^{-1}R$, given by $P \mapsto S^{-1}P$.

Proof. Let S be a given multiplicative set. Symbolically, $\mathcal{U} = \{P \mid$ is a prime ideal of R and $S \cap P = \varnothing\}$. By Lemma III.4.9(iii), the assignment of P to $S^{-1}P$ is one to one since for $S^{-1}P_1 \neq S^{-1}P_2$ we have $\varphi_S^{-1}(S^{-1}P_1) = P_1 \neq P_2 = \varphi_S^{-1}(S^{-1}P_2)$.

To show the mapping is surjective, let J be an element of $\mathcal{V}$ (i.e., J is a prime ideal of $S^{-1}R$), and let $P = \varphi_S^{-1}(J)$. By Lemma III.4.9(ii), if we show P is prime then we have $P \mapsto S^{-1}P = J$, so that the mapping is surjective ("onto"). Suppose $ab \in P$. Then, since φ_S is a homomorphism by Theorem III.4.4(i), $\varphi_S(ab) = \varphi_S(a)\varphi_S(b) \in J$ since $P = \varphi_S^{-1}(J)$.

Theorem III.4.10 (continued)

Theorem III.4.10. Let S be a multiplicative subset of a commutative ring R with identity. Then there is a one-to-one correspondence between the set $\mathcal{U}$ of prime ideals of R which are disjoint from S and the set $\mathcal{V}$ of prime ideals of $S^{-1}R$, given by $P \mapsto S^{-1}P$.

Proof (continued). Since J is prime in $S^{-1}R$, then by Theorem III.2.15 (notice that P is a prime ideal of $S^{-1}R$, so $J \neq S^{-1}R$) either $\varphi_S(a) \in J$ or $\varphi_S(b) \in J$. That is, either $a \in \varphi_S^{-1}(J) = P$ or $b \in \varphi_S^{-1}(J) = P$ and hence P is prime (again, by Theorem III.2.25). Therefore the mapping $P \mapsto S^{-1}P$ is also surjective and, hence, is a bijection. We now have that this mapping is a one-to-one correspondence from $\mathcal{U}$ to $\mathcal{V}$, as claimed. □

Theorem III.4.11

Theorem III.4.11. Let P be a prime ideal in a commutative ring R with identity, and let $S = R - P$.

(i) There is a one-to-one correspondence between the set of prime ideals of R which are contained in P and the set of prime ideals of $R_p = S^{-1}R$, given by $Q \mapsto Q_P = S^{-1}Q$;

(ii) the ideal $P_P = S^{-1}P$ in R_P is the unique maximal ideal of R_P.

Proof. (i) The prime ideals of R contained in P are precisely the prime ideals which are disjoint from the complement of P, $S = R - P$. The one-to-one correspondence is then given by Theorem III.4.10 since $S^{-1}R = R_p$

(ii) If M is a maximal ideal of R_p, then M is prime by Theorem III.2.19 (since R_P has an identity, namely s/s as shown in the proof of Theorem III.4.3(i)). That is, $M \in \mathcal{V}$ where $\mathcal{V}$ is the set of prime ideals in $R_P = S^{-1}R$.

Theorem III.4.11 (continued)

Theorem III.4.11. Let P be a prime ideal in a commutative ring R with identity, and let $S = R - P$.

(i) There is a one-to-one correspondence between the set of prime ideals of R which are contained in P and the set of prime ideals of $R_p = S^{-1}R$, given by $Q \mapsto Q_P = S^{-1}Q$;

(ii) the ideal $P_P = S^{-1}P$ in R_P is the unique maximal ideal of R_P.

Proof (continued). By Theorem III.4.10, there is a prime ideal Q of R which is disjoint from $S = R - P$ (and so is contained in P) such that $M = S^{-1}Q = Q + P$. But $Q \subset P$ implies $Q_P \subset P_P$. Since $P_P \neq R_p$ by Theorem III.4.8 (because P is a prime ideal of R so that $P \neq R$ and $S \cap P = (S - P) \cap P = \varnothing$), and $M = Q_P$ is maximal (by hypothesis) then $M = Q_P = P_P$. Therefore, P_p is a maximal ideal in R_P and (since M has chosen to be an arbitrary maximal ideal of R_P) is the unique such maximal ideal, as claimed. □