Ideals.

Finally we are ready to study kernels and images of ring homomorphisms. We have seen two major examples in which congruence gave us ring homomorphisms: $\mathbb{Z} \to \mathbb{Z}_n$ and $F[x] \to F[x]/(p(x))$. We shall generalize this to congruence in arbitrary rings and then see that it brings us very close to a complete understanding of kernels and images of ring homomorphisms.

Recall the definition of a ring. For congruence, we need a special subring that will behave like $n\mathbb{Z}$ or like $p(x)F[x] = \{\, p(x)f(x) \mid f(x) \in F[x] \,\}$.

Definition, p. 135. A subring I of a ring R is an **ideal** if whenever $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$.

If R is commutative, we only need to worry about multiplication on one side. More generally, one can speak of **left ideals** and **right ideals** and **two-sided ideals**. Our main interest is in the two-sided ideals; these turn out to give us the congruences we want.

Before we look at examples, recall that to be a subring means I is closed under multiplication and subtraction. Thus we get

Theorem 6.1. *A nonempty subset I in a ring R is an ideal iff it satisfies*

(1) *if $a, b \in I$, then $a - b \in I$;*
(2) *if $r \in R, a \in I$, then $ra \in I$ and $ar \in I$.* $\square$

Note that if R has an identity, we can replace (1) by
$(1')$ *if $a, b \in I$, then $a + b \in I$*
because (2) implies that, since $-1 \in R$, $-b \in I$ whenever $b \in I$.

Examples. 1. $n\mathbb{Z} = \{\, kn \mid k \in \mathbb{Z} \,\}$ for any $n \in \mathbb{Z}$ is an ideal in $\mathbb{Z}$. If $n = 0$ we get the zero ideal, an ideal of any ring R. If $n = \pm 1$ we get $\mathbb{Z}$, the whole ring. Again, for any ring R, the whole ring is an ideal of R.
2. In $\mathbb{Z}_6$, the set $I = \{\, [2k] \in \mathbb{Z}_6 \mid k \in \mathbb{Z} \,\}$ is an ideal.
3. $p(x)R[x] = \{\, p(x)f(x) \mid f(x) \in R[x] \,\}$ is an ideal of $R[x]$ for any commutative ring R with 1.
4. In $\mathbb{Z}[x]$, the set $I = \{\, f(x) \in \mathbb{Z}[x] \mid f(0) \equiv 0 \pmod{n} \,\}$ is an ideal for any $n \geq 2$ in $\mathbb{Z}$. This generalizes an example on page 136 where $n = 2$.
5. For $R = \mathcal{C}(\mathbb{R}, \mathbb{R})$, fix any $r \in \mathbb{R}$. The set $I = \{\, f \in R \mid f(r) = 0 \,\}$ is an ideal. Note that it does not work to use a number other than 0.

6. For $R = M_2(\mathbb{R})$, the set of first rows $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\}$ is a right ideal but not a left ideal. (A similar thing is done for columns and left ideals in the book.) In particular, I is not a (two-sided) ideal. Check.

Examples 1, 2 and 3 above were all of a special type which we can generalize.

Theorem 6.2. *Let R be a commutative ring with identity. Let $c \in R$. The set $I = \{rc \mid r \in R\}$ is an ideal of R.*

Proof. Given two elements r_1c and r_2c in I, we have $r_1c - r_2c = (r_1 - r_2)c \in I$. For any $a \in R$, $a(r_1c) = (ar_1)c \in I$. Therefore I is an ideal. (We have implicitly used the fact that R is commutative so that multiplication on the right also works.) $\square$

We call the ideal in Theorem 6.2 the **principal ideal generated by c** and denote it by (c) or by Rc. The ideal in Example 4 was not principal. To see this, note that $n \geq 2$ and x both lie in I. If I were generated by some polynomial $p(x)$, then both n and x must be multiples of $p(x)$. But then $n = p(x)q(x)$ implies that $p(x)$ is a constant c. Note that $c \neq \pm 1$, for that would make I the whole ring, which it is not since $1 \notin I$. Now we also have $x = cr(x)$ for some $r(x)$, which is impossible since c does not divide x (i.e., c has no inverse in $\mathbb{Z}[x]$ since the only units are ± 1). In fact it is easy to see that I is generated by the two elements n and x in the sense of the next theorem.

Theorem 6.3. *Let R be a commutative ring with identity. Let $c_1, c_2, \ldots, c_n \in R$. Then the set $I = \{r_1c_1 + \cdots + r_nc_n \mid r_1, \ldots, r_n \in R\}$ is an ideal of R.*

Proof. Homework; generalize the proof of Theorem 6.2. $\square$

We call the ideal I of Theorem 6.3 the **ideal generated by $\mathbf{c_1, \ldots, c_n}$** and denote it by $(c_1, c_2, \ldots, c_n)$.

Comments. 1. If R does not have an identity, there is a complication in the definition since one wants the elements $c_i \in I$ (see exercise 31, p. 143).
2. If R is not commutative, one needs multiplication on both sides in the definition of I.
3. Ideals with finitely many generators are called **finitely generated ideals**. One has to work a bit to find ideals which are not finitely generated and we will avoid them in this course. One example is the ideal generated by all the indeterminates in the polynomial ring $\mathbb{R}[x_1, x_2, x_3, \ldots]$ with infinitely many indeterminates.

In analogy to congruence in $\mathbb{Z}$ and $F[x]$ we now will build a ring R/I for any ideal I in any ring R. For $a, b \in R$, we say **a is congruent to b modulo I** [and write $a \equiv b \pmod{I}$] if $a - b \in I$. Note that when $I = (n) \subset \mathbb{Z}$ is the principal ideal generated by n, then $a - b \in I \iff n|(a-b)$, so this is our old notion of congruence.

As before, we require congruence to be an equivalence relation if it is going to work for us, so we check this.

Theorem 6.4. *Let I be an ideal of a ring R. Congruence modulo I is an equivalence relation.*

Proof. reflexive: $a - a = 0 \in I$ since I is a subring.
symmetric: Assume $a \equiv b \pmod{I}$. Then $a - b \in I$. Since I is a subring, its additive inverse, $b - a$ is also in I, and so $b \equiv a \pmod{I}$.
transitive: Assume $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$. Then $a - b \in I$ and $b - c \in I$, hence the sum $a - c = (a-b) + (b-c) \in I$, so $a \equiv c \pmod{I}$. □

We use this to show that arithmetic works "modulo I".

Theorem 6.5. *Let I be an ideal of a ring R. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then*
(1) *$a + c \equiv b + d \pmod{I}$;*
(2) *$ac \equiv bd \pmod{I}$.*

Proof. (1) $(a+c) - (b+d) = (a-b) + (c-d)$. Since $a - b \in I$ and $c - d \in I$, so is $(a+c) - (b+d)$, hence $a + c \equiv b + d \pmod{I}$.
(2) $ac - bd = ac - bc + bc - bd = (a-b)c + b(c-d) \in I$ since I is closed under multiplication on both sides. Therefore $ac \equiv bd \pmod{I}$. □

Looking at this proof, we see that it is multiplication that fails if we have only a left or right ideal that is not 2-sided. The equivalence classes for this relation, are commonly called **cosets**. What do they look like? The congruence class of a modulo I is

$$\begin{aligned}
\{\, b \in R \mid b \equiv a \pmod{I} \,\} &= \{\, b \in R \mid b - a \in I \,\} \\
&= \{\, b \in R \mid b - a = i \text{ for some } i \in I \,\} \\
&= \{\, b \in R \mid b = a + i \text{ for some } i \in I \,\} \\
&= \{\, a + i \mid i \in I \,\}.
\end{aligned}$$

We denote this coset by $a + I$. As earlier, we have $a \equiv b \pmod{I}$ iff $a + I = b + I$. The set of all cosets of I (congruence classes of R modulo I) will be denoted by R/I.

Selected problems from pp. 141–145.

13 (generalized). Let I be an ideal in a ring R with 1. $I = R$ iff I contains a unit.

Proof. ($\Longrightarrow$) If $I = R$, then $1 \in I$ is a unit in I.
($\Longleftarrow$) Let $u \in I$ be a unit. Then there exists $v \in R$ with $vu = 1$. For any $r \in R$, we get $r = r \cdot 1 = r(vu) = (rv)u \in I$.

14/35. A commutative ring R with 1 is a field iff its only two ideals are (0) and R.

Proof. ($\Longrightarrow$) Any nonzero ideal I contains some nonzero element, which is a unit since R is a field. By #13, $I = R$.
($\Longleftarrow$) Let $0 \neq a \in R$ and let $I = (a)$. By hypothesis, $I = R$, so I contains the identity 1. Therefore $1 = ra$ for some $r \in R$, so that r is the inverse of a. Therefore R is a field.

38. Every ideal I in $\mathbb{Z}$ is principal.

Proof. Assume $I \neq (0)$ (which is principal). Let c be the smallest positive element in I (exists by the well-ordering axiom). Then $(c) \subseteq I$. Conversely, let $a \in I$. By the division algorithm, we can write $a = cq + r$ with $0 \leq r < c$. Then $r = a - cq \in I$. By our choice of c, we must have $r = 0$, as otherwise it is a smaller positive element of I. Therefore $a \in (c)$, so $I = (c)$ is principal.

39. (a) $S = \{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \text{ odd} \}$ is a subring of $\mathbb{Q}$.
(b) $I = \{ \frac{m}{n} \in S \mid m \text{ even} \}$ is an ideal in S.
(c) S/I has exactly two cosets.

Proof. (a) Check closure under subtraction and multiplication.
(b) Check closure under subtraction and multiplication by elements of S.
(c) If $\frac{m}{n} \notin I$, then, since m and n are both odd, we see that $\frac{m}{n} = 1 + \frac{m-n}{n} \in 1 + I$. So the only cosets are I and $1 + I$.

Quotient rings and homomorphisms.

Theorem 6.5 gives the fact that addition and multiplication are well-defined on congruence classes. Translating this into the language of cosets gives

Theorem 6.8. *Let I be an ideal in a ring R. If $a + I = b + I$ and $c + I = d + I$ in R/I, then $(a + c) + I = (b + d) + I$ and $ac + I = bd + I$.* $\square$

Therefore we can define addition in the set R/I by $(a + I) + (b + I) = (a + b) + I$ and multiplication by $(a + I)(b + I) = ab + I$. So just as $\mathbb{Z}_n$ and $F[x]/(p(x))$ were rings, so is R/I. It is called the **quotient ring** or **factor ring** of R by I. It is easy to see that if R is commutative, then so is R/I and if R has an identity, then so does R/I (namely, $1_R + I$). Recall that we had natural ring homomorphisms from $\mathbb{Z}$ onto $\mathbb{Z}_n$ and from $F[x]$ onto $F[x]/(p(x))$. This holds in general.

First, we define the **kernel** of a ring homomorphism $\phi\colon R \to S$ to be $\ker \phi = \{\, r \in R \mid \phi(r) = 0 \,\}$. (Same as for linear transformations.)

Theorem 6.12. *Let I be an ideal in a ring R. The mapping $\pi\colon R \to R/I$ given by $\pi(r) = r + I$ is a surjective ring homomorphism with kernel I.*

Proof. The fact that π preserves addition and multiplication follows from the definition of addition and multiplication in R/I. It is surjective since any coset $r + I$ is the image of $r \in R$. Finally, the kernel is the set of all $r \in R$ such that $\pi(r) = 0 + I$, the zero element of R/I. But $r + I = 0 + I$ iff $r \equiv 0 \pmod{I}$ iff $r \in I$. Thus the kernel is just I. $\square$

We can generalize this idea of ideals and kernels to any ring homomorphism.

Theorem 6.10. *Let $f\colon R \to S$ be any homomorphism of rings and let $K = \ker f$. Then K is an ideal in R.*

Proof. We know $0 \in K$, so $K \neq \emptyset$. Let $a, b \in K$. Then $f(a) = f(b) = 0$, so $f(a - b) = f(a) - f(b) = 0$. For any $r \in R$, $f(ra) = f(r)f(a) = f(r) \cdot 0 = 0$. Similarly, $f(ar) = f(a)f(r) = 0$. Thus $a - b$, ra and ar are also in K, hence K is an ideal. $\square$

And furthermore, the kernel tests for injectivity just as it does for linear transformations.

Theorem 6.11. *Let $f\colon R \to S$ be any homomorphism of rings with kernel K. Then f is injective iff $K = (0)$.*

Proof. ($\Longrightarrow$) We know $f(0) = 0$. If $f(r)$ also equals 0, then $r = 0$ since f is injective. Therefore $K = (0)$.
($\Longleftarrow$) Conversely, assume $f(a) = f(b)$. Then $f(a-b) = f(a)-f(b) = 0$, so $a-b \in K = (0)$. Therefore $a - b = 0$ and $a = b$, so f is injective. $\square$

When $f\colon R \to S$ is a surjective homomorphism, we say that S is a **homomorphic image** of R. Some information is lost in passing from R to S, but also some is retained (think of $\mathbb{Z} \to \mathbb{Z}_n$). We next see that every surjective homomorphism really acts just like $R \to R/I$.

Theorem 6.13. (First Isomorphism Theorem) *Let $f\colon R \to S$ be a surjective homomorphism of rings with kernel K. Then the quotient ring R/K is isomorphic to S.*

Proof. Define a function $\phi\colon R/K \to S$ by $\phi(r + K) = f(r)$. We must check that ϕ is well-defined (does not depend on the name for the coset). Assume that $r + K = t + K$; then $r - t \in K$, so $f(r) = f(r - t + t) = f(r - t) + f(t) = 0 + f(t) = f(t)$. Therefore ϕ is well-defined. We check that ϕ is a homomorphism:

$$\phi((r + K) + (t + K)) = \phi((r + t) + K) = f(r + t) = f(r) + f(t) = \phi(r + K) + \phi(t + K)$$
$$\phi((r + K)(t + K)) = \phi((rt) + K) = f(rt) = f(r)f(t) = \phi(r + K)\phi(t + K)$$

For any $s \in S$, we know there is some $r \in R$ with $f(r) = s$, and therefore $\phi(r + K) = s$ showing that ϕ is surjective. To show that ϕ is injective, we show that $\ker \phi$ is zero in R/K: if $\phi(r + K) = 0$, then $f(r) = 0$, so $r \in K$, hence $r + K = 0 + K$. Therefore $\phi\colon R/K \to S$ is an isomorphism. $\square$

The 2nd and 3rd isomorphism theorems are left to Math 413.

Examples. 1. $F[x]/(x - a)$ comes from looking at the homomorphism $F[x] \to F$ defined by $f(x) \mapsto f(a)$. The kernel is $(x - a)$ by the factor theorem ($f(a) = 0 \implies x - a$ divides $f(x)$). Since the homomorphism is surjective, it is an isomorphism of $F[x]/(x - a)$ with F. (Compare to problem 6, p. 123.)

2. We saw that the ideals in $\mathbb{Z}$ all look like (n) for some integer $n \geq 0$. Thus the homomorphic images are either isomorphic to $\mathbb{Z}$ itself (when $n = 0$) or to $\mathbb{Z}/(n) = \mathbb{Z}_n$ (when $n > 0$).

3. We showed that $I = \{\, f \in R \mid f(r) = 0 \,\}$ is an ideal in $R = \mathcal{C}(\mathbb{R}, \mathbb{R})$ for any fixed $r \in \mathbb{R}$. The homomorphism $\phi\colon R \to \mathbb{R}$ defined by $\phi(f) = f(r)$ is surjective [$\phi(s) = s$ for any constant function $s \in \mathbb{R}$] and has kernel I. Thus R/I is isomorphic to $\mathbb{R}$.

Exercise 3, p. 151. Let F be a field, R a nonzero ring and $f\colon F \to R$ a surjective homomorphism. We claim f is actually an isomorphism. We need to show that it is injective, which means (Theorem 6.11) that its kernel is zero. But its kernel must be an ideal in F and a field has only two ideals: (0) and F. The kernel can't be all of F, for then the image is just the zero ring. Therefore the kernel must be zero.

Exercise 5, p. 151. If I is an ideal in an integral domain R, then R/I need no longer be an integral domain. Indeed, a simple example of this is $R = \mathbb{Z}$ and $I = (6)$. We shall soon see exactly which ideals can be factored out to give an integral domain.

Exercise 8(a), p. 151. Let $I = \{0, 3\}$ in $\mathbb{Z}_6$. I is an ideal since it is the principal ideal (3). $\mathbb{Z}_6/I \cong \mathbb{Z}_3$ via the mapping $n + I \mapsto [n]_3$ as this is the only possible homomorphism since 1 must map to 1; there are several details to check. We define a function $\phi\colon \mathbb{Z}_6 \to \mathbb{Z}_3$ by $\phi([n]_6) = [n]_3$ and check that it is well-defined. It is clearly surjective and one can check that it is a homomorphism (see Example 1, p. 7 of Chapter 3 notes). Now check that $I = \ker\phi$ and use the First Isomorphism Theorem. This exercise is a special case of the Third Isomorphism Theorem (see Exercise 33).

Exercise 19, p. 152. Let $I,\ J$ be ideals in R and define $f\colon R \to R/I \times R/J$ by $f(a) = (a + I, a + J)$. [For an example, again see Example 1, p. 7 of Chapter 3 notes.]
(a) f is a homomorphism: $f(a+b) = (a+b+I, a+b+J) = (a+I, a+J)+(b+I, b+J) = f(a) + f(b)$ and $f(ab) = (ab + I, ab + J) = (a + I, a + J)(b + I, b + J) = f(a)f(b)$.
(b) It was surjective in the example mentioned above: $\mathbb{Z}_6 \to \mathbb{Z}_6/(3) \times \mathbb{Z}_6/(2) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. On the other hand, for $\mathbb{Z} \to \mathbb{Z}/(2) \times \mathbb{Z}/(4)$, nothing maps onto $(1, 0)$ since $n \equiv 1 \pmod 2$ implies $n \not\equiv 0 \pmod 4$.
(c) Check that $\ker f = I \cap J$.
The Chinese Remainder Theorem in Chapter 13 deals with the issue of when the mapping is surjective.

Prime ideals.

What is special about an ideal I for which R/I is an integral domain or a field? For this section we assume that R is a commutative ring with identity, since these are necessary conditions to hope to have an integral domain. We want a condition on the ideal to make sure there are no zero divisors in the quotient ring. We have seen several examples in the case of principal ideals—what we needed was that the generator was irreducible (called prime in the case of $\mathbb{Z}$). The appropriate generalization is one of the equivalent forms we had for an irreducible polynomial or integer.

Definition, p. 154. An ideal P in R is **prime** if $P \neq R$ and whenever $ab \in P$, then $a \in P$ or $b \in P$.

Note: this definition is not the best generalization to noncommutative rings.

Examples. 1. Theorem 4.11 says $(p(x))$ in $F[x]$ is a prime ideal iff $p(x)$ is irreducible. And we have seen that $F[x]/(p(x))$ is a field iff $p(x)$ is irreducible (Theorem 5.10).

2. Theorem 1.8 says (p) in $\mathbb{Z}$ is a prime ideal iff p is prime. And we have seen that $\mathbb{Z}_p$ is a field iff p is prime (Theorem 2.8).

3. The zero ideal in an integral domain R is prime.

4. For a nonprincipal ideal, consider the ideal $P = (p, x)$ in $\mathbb{Z}[x]$ where p is prime. Assume $f(x) = \sum a_i x^i$, $g(x) = \sum b_j x^j \in \mathbb{Z}[x]$ with $f(x)g(x) \in P$. This says the constant term $a_0 b_0$ is divisible by p. But then either $p | a_0$ (and so $f(x) \in P$) or $p | b_0$ (and so $g(x) \in P$). Therefore P is a prime ideal. In this case, the quotient ring is $\mathbb{Z}_p$, a field.

5. Now consider (x) in $\mathbb{Z}[x]$. The quotient ring $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, an integral domain, but not a field. Is (x) a prime ideal? Assume $f(x) = \sum a_i x^i$, $g(x) = \sum b_j x^j \in \mathbb{Z}[x]$ with $f(x)g(x) \in (x)$. This says the constant term $a_0 b_0$ is 0, so either $a_0 = 0$ (and so $f(x) \in (x)$) or $b_0 = 0$ (and so $g(x) \in (x)$).

Theorem 6.14. *Let P be an ideal in R. P is a prime ideal iff R/P is an integral domain.*

Proof. ($\implies$) Assume P is prime. Then R/P is a commutative ring with identity (Theorem 6.9). We have $R/P \neq 0$ since $P \neq R$ (or equivalently $1 \notin P$). Therefore $0 \neq 1$ in R/P. Finally we check for zero divisors: if $ab + P = (a + P)(b + P) = 0 + P$, then $ab \in P$. Since P is prime, $a \in P$ or $b \in P$; that is, $a + P = 0 + P$ or $b + P = 0 + P$. Therefore R/P is an integral domain.

($\impliedby$) Now assume that R/P is an integral domain. Since $1 \neq 0$ in R/P, we have $P \neq R$. Assume $ab \in P$. Then $(a + P)(b + P) = ab + P = 0 + P$. Since there are no zero divisors, we know that either $a + P = 0 + P$ or $b + P = 0 + P$. And so, either $a \in P$ or $b \in P$. $\square$

How much more do we need to assume to have R/P be a field? Our main example was (4) and (5) above: $\mathbb{Z}[x]$ modulo (x) was an integral domain, but modulo the larger ideal (p, x) it was a field. So it helps to have big ideals.

Definition, p. 156. An ideal M in R is **maximal** if $M \neq R$ and whenever I is an ideal such that $M \subseteq I \subseteq R$, then $M = I$ or $M = R$.

The same definition is used in noncommutative rings with 1. The examples (1), (2), and (4) above were maximal. And we saw that in each case, the quotient ring was a field.

Theorem 6.15. *Let M be an ideal in R. M is a maximal ideal iff R/M is a field.*

Proof. ($\Longrightarrow$) Assume M is maximal. Then R/M is a commutative ring with identity (Theorem 6.9). We have $R/M \neq 0$ since $M \neq R$. Therefore $0 \neq 1$ in R/M. Finally we check for inverses. Let $a + M$ be a nonzero element of R/M. Then $a \notin M$ and we build a bigger ideal

$$I = \{\, ra + m \mid r \in R,\ m \in M \,\}.$$

(Check that this is an ideal.) Since $a \in I$ and M is maximal, we must have $I = R$. But then $1 \in I$, so $1 = ra+m$ for some $r \in R$ and $m \in M$. This means $1+M = (r+M)(a+M)$. Since R/M is commutative, this gives an inverse for $a + M$ and so R/M is a field.

($\Longleftarrow$) Now assume that R/M is a field. Since $1 \neq 0$ in R/M, we have $M \neq R$. Assume there is an ideal I such that $M \subseteq I \subseteq R$. If $I \neq M$, let $a \in I$, $a \notin M$. Then $a + M$ has an inverse $u + M$ in R/M, so $au + M = 1 + M$. In particular, $au = 1 + m$ for some $m \in M$. Since $m \in M \subseteq I$, we have $1 = au - m \in I$ and so $I = R$. Therefore M is maximal. $\square$

Since every field is an integral domain, we obtain

Corollary 6.16. *Every maximal ideal is prime.*

Exercises, pages 157–159.

5. In $\mathbb{Z}_6$, the maximal ideals are (2) and (3).

17. *The inverse image of a prime ideal is prime.* Let $f\colon R \to S$ be a homomorphism of rings and let Q be a prime ideal in S. Then $P = f^{-1}(Q) = \{\, r \in R \mid f(r) \in Q \,\}$ is a prime ideal in R.

Proof. Since $1_S \notin Q$, $1_R \notin P$, so $P \neq R$. Let $ab \in P$. Then $f(a)f(b) = f(ab) \in Q$, so $f(a) \in Q$ or $f(b) \in Q$. By definition of P, this means $a \in P$ or $b \in P$.

19. The proof that every ideal $I \neq R$ is contained in a maximal ideal uses Zorn's lemma (a fact equivalent to the axiom of choice in set theory).
Assume R has a unique maximal ideal. Let I be the set of nonunits in R. For $r \in R$, $a \in I$, the products ar and ra are also nonunits, so they lie in I. Assume $a, b \in I$ and that $a + b$ is not in I. Then $a + b$ is a unit, hence there exists $u \in R$ with $(a + b)u = 1$. But

(a) and (b) are ideals smaller than R, hence are contained in maximal ideals. Since there is only one maximal ideal, say M, we have $a \in M$, $b \in M$ and therefore $1 = u(a+b) \in M$, a contradiction. Therefore $a+b$ is in I and I is an ideal. Conversely, assume the set I of all nonunits is an ideal. Then it is clearly the unique maximal ideal of R since no other element can be in a maximal ideal other than a nonunit.
Example: $\{\, \frac{m}{n} \in \mathbb{Q} \mid n \text{ is odd} \,\}$. (2) is the unique maximal ideal.