Example 3.5.2 Let R be the ring of all the real-valued, continuous functions on the closed unit interval. (See Example 3.3.5.) Let

$$M = \{f(x) \in R \mid f(\tfrac{1}{2}) = 0\}.$$

M is certainly an ideal of R. Moreover, it is a maximal ideal of R, for if the ideal U contains M and $U \neq M$, then there is a function $g(x) \in U$, $g(x) \notin M$. Since $g(x) \notin M$, $g(\frac{1}{2}) = \alpha \neq 0$. Now $h(x) = g(x) - \alpha$ is such that $h(\frac{1}{2}) = g(\frac{1}{2}) - \alpha = 0$, so that $h(x) \in M \subset U$. But $g(x)$ is also in U; therefore $\alpha = g(x) - h(x) \in U$ and so $1 = \alpha\alpha^{-1} \in U$. Thus for any function $t(x) \in R$, $t(x) = 1t(x) \in U$, in consequence of which $U = R$. M is therefore a maximal ideal of R. Similarly if γ is a real number $0 \leq \gamma \leq 1$, then $M_\gamma = \{f(x) \in R \mid f(\gamma) = 0\}$ is a maximal ideal of R. It can be shown (see Problem 4 at the end of this section) that every maximal ideal is of this form. Thus here the maximal ideals correspond to the points on the unit interval.

Having seen some maximal ideals in some concrete rings we are ready to continue the general development with

THEOREM 3.5.1 *If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R if and only if R/M is a field.*

Proof. Suppose, first, that M is an ideal of R such that R/M is a field. Since R/M is a field its only ideals are (0) and R/M itself. But by Theorem 3.4.1 there is a one-to-one correspondence between the set of ideals of R/M and the set of ideals of R which contain M. The ideal M of R corresponds to the ideal (0) of R/M whereas the ideal R of R corresponds to the ideal R/M of R/M in this one-to-one mapping. Thus there is no ideal between M and R other than these two, whence M is a maximal ideal.

On the other hand, if M is a maximal ideal of R, by the correspondence mentioned above R/M has only (0) and itself as ideals. Furthermore R/M is commutative and has a unit element since R enjoys both these properties. All the conditions of Lemma 3.5.1 are fulfilled for R/M so we can conclude, by the result of that lemma, that R/M is a field.

We shall have many occasions to refer back to this result in our study of polynomial rings and in the theory of field extensions.

Problems

1. Let R be a ring with unit element, R not necessarily commutative, such that the only right-ideals of R are (0) and R. Prove that R is a division ring.

this becomes: $(ad + bc)b'd' = adb'd' + bcb'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' = bd(a'd' + b'c')$, which is the desired equality.

Clearly $[0, b]$ acts as a zero-element for this addition and $[-a, b]$ as the negative of $[a, b]$. It is a simple matter to verify that F is an abelian group under this addition.

We now turn to the multiplication in F. Again motivated by our preliminary heuristic discussion we define $[a, b][c, d] = [ac, bd]$. As in the case of addition, since $b \neq 0$, $d \neq 0$, $bd \neq 0$ and so $[ac, bd] \in F$. A computation, very much in the spirit of the one just carried out, proves that if $[a, b] = [a', b']$ and $[c, d] = [c', d']$ then $[a, b][c, d] = [a', b'][c', d']$. One can now show that the nonzero elements of F (that is, all the elements $[a, b]$ where $a \neq 0$) form an abelian group under multiplication in which $[d, d]$ acts as the unit element and where

$$[c, d]^{-1} = [d, c] \text{ (since } c \neq 0, [d, c] \text{ is in } F\text{)}.$$

It is a routine computation to see that the distributive law holds in F. F is thus a field.

All that remains is to show that D can be imbedded in F. We shall exhibit an explicit isomorphism of D into F. Before doing so we first notice that for $x \neq 0$, $y \neq 0$ in D, $[ax, x] = [ay, y]$ because $(ax)y = x(ay)$; let us denote $[ax, x]$ by $[a, 1]$. Define $\phi:D \rightarrow F$ by $\phi(a) = [a, 1]$ for every $a \in D$. We leave it to the reader to verify that ϕ is an isomorphism of D into F, and that if D has a unit element 1, then $\phi(1)$ is the unit element of F. The theorem is now proved in its entirety.

F is usually called the *field of quotients* of D. In the special case in which D is the ring of integers, the F so constructed is, of course, the field of rational numbers.

Problems

1. Prove that if $[a, b] = [a', b']$ and $[c, d] = [c', d']$ then $[a, b][c, d] = [a', b'][c', d']$.
2. Prove the distributive law in F.
3. Prove that the mapping $\phi:D \rightarrow F$ defined by $\phi(a) = [a, 1]$ is an isomorphism of D into F.
4. Prove that if K is any field which contains D then K contains a subfield isomorphic to F. (*In this sense F is the smallest field containing D.*)

*5. Let R be a commutative ring with unit element. A nonempty subset S of R is called a multiplicative system if

1. $0 \notin S$.
2. $s_1, s_2 \in S$ implies that $s_1s_2 \in S$.

Let $\mathscr{M}$ be the set of all ordered pairs (r, s) where $r \in R$, $s \in S$. In $\mathscr{M}$ define $(r, s) \sim (r', s')$ if there exists an element $s'' \in S$ such that

$$s''(rs' - sr') = 0.$$

(a) Prove that this defines an equivalence relation on $\mathscr{M}$.

Let the equivalence class of (r, s) be denoted by $[r, s]$, and let R_S be the set of all the equivalence classes. In R_S define $[r_1, s_1] + [r_2, s_2] = [r_1s_2 + r_2s_1, s_1s_2]$ and $[r_1, s_1][r_2, s_2] = [r_1r_2, s_1s_2]$.

(b) Prove that the addition and multiplication described above are well defined and that R_S forms a ring under these operations.

(c) Can R be imbedded in R_S?

(d) Prove that the mapping $\phi: R \to R_s$ defined by $\phi(a) = [as, s]$ is a homomorphism of R into R_S and find the kernel of ϕ.

(e) Prove that this kernel has no element of S in it.

(f) Prove that every element of the form $[s_1, s_2]$(where $s_1, s_2 \in S$) in R_S has an inverse in R_S.

6. Let D be an integral domain, $a, b \in D$. Suppose that $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n. Prove that $a = b$.

7. Let R be a ring, possibly noncommutative, in which $xy = 0$ implies $x = 0$ or $y = 0$. If $a, b \in R$ and $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n, prove that $a = b$.

3.7 Euclidean Rings

The class of rings we propose to study now is motivated by several existing examples—the ring of integers, the Gaussian integers (Section 3.8), and polynomial rings (Section 3.9). The definition of this class is designed to incorporate in it certain outstanding characteristics of the three concrete examples listed above.

DEFINITION An integral domain R is said to be a *Euclidean ring* if for every $a \neq 0$ in R there is defined a nonnegative integer $d(a)$ such that

1. For all $a, b \in R$, both nonzero, $d(a) \leq d(ab)$.
2. For any $a, b \in R$, both nonzero, there exist $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

We do not assign a value to $d(0)$. The integers serve as an example of a Euclidean ring, where $d(a)$ = absolute value of a acts as the required function. In the next section we shall see that the Gaussian integers also form a Euclidean ring. Out of that observation, and the results developed in this part, we shall prove a classic theorem in number theory due to