unit element $1 + U$. We might ask: In what relation is R/U to R? With the experience we now have in hand this is easy to answer. There is a homomorphism ϕ of R *onto* R/U given by $\phi(a) = a + U$ for every $a \in R$, whose kernel is exactly U. (The reader should verify that ϕ so defined is a homomorphism of R onto R/U with kernel U.)

We summarize these remarks in

LEMMA 3.4.1 *If U is an ideal of the ring R, then R/U is a ring and is a homomorphic image of R.*

With this construction of the *quotient ring* of a ring by an ideal satisfactorily accomplished, we are ready to bring over to rings the homomorphism theorems of groups. Since the proof is an exact verbatim translation of that for groups into the language of rings we merely state the theorem without proof, referring the reader to Chapter 2 for the proof.

THEOREM 3.4.1 *Let R, R' be rings and ϕ a homomorphism of R onto R' with kernel U. Then R' is isomorphic to R/U. Moreover there is a one-to-one correspondence between the set of ideals of R' and the set of ideals of R which contain U. This correspondence can be achieved by associating with an ideal W' in R' the ideal W in R defined by $W = \{x \in R \mid \phi(x) \in W'\}$. With W so defined, R/W is isomorphic to R'/W'.*

Problems

1. If U is an ideal of R and $1 \in U$, prove that $U = R$.
2. If F is a field, prove its only ideals are (0) and F itself.
3. Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.
4. If R is a commutative ring and $a \in R$,
   (a) Show that $aR = \{ar \mid r \in R\}$ is a two-sided ideal of R.
   (b) Show by an example that this may be false if R is not commutative.
5. If U, V are ideals of R, let $U + V = \{u + v \mid u \in U, v \in V\}$. Prove that $U + V$ is also an ideal.
6. If U, V are ideals of R let UV be the set of all elements that can be written as finite sums of elements of the form uv where $u \in U$ and $v \in V$. Prove that UV is an ideal of R.
7. In Problem 6 prove that $UV \subset U \cap V$.
8. If R is the ring of integers, let U be the ideal consisting of all multiples of 17. Prove that if V is an ideal of R and $R \supset V \supset U$ then either $V = R$ or $V = U$. Generalize!

9. If U is an ideal of R, let $r(U) = \{x \in R \mid xu = 0 \text{ for all } u \in U\}$. Prove that $r(U)$ is an ideal of R.

10. If U is an ideal of R let $[R:U] = \{x \in R \mid rx \in U \text{ for every } r \in R\}$. Prove that $[R:U]$ is an ideal of R and that it contains U.

11. Let R be a ring with unit element. Using its elements we define a ring $\tilde{R}$ by defining $a \oplus b = a + b + 1$, and $a \cdot b = ab + a + b$, where $a, b \in R$ and where the addition and multiplication on the right-hand side of these relations are those of R.
    (a) Prove that $\tilde{R}$ is a ring under the operations $\oplus$ and $\cdot$.
    (b) What acts as the zero-element of $\tilde{R}$?
    (c) What acts as the unit-element of $\tilde{R}$?
    (d) Prove that R is isomorphic to $\tilde{R}$.

*12. In Example 3.1.6 we discussed the ring of rational 2×2 matrices. Prove that this ring has no ideals other than (0) and the ring itself.

*13. In Example 3.1.8 we discussed the real quaternions. Using this as a model we define the quaternions over the integers mod p, p an odd prime number, in exactly the same way; however, now considering all symbols of the form $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are integers mod p.
    (a) Prove that this is a ring with p^4 elements whose only ideals are (0) and the ring itself.
    **(b) Prove that this ring is *not* a division ring.

If R is any ring a subset L of R is called a *left-ideal* of R if
1. L is a subgroup of R under addition.
2. $r \in R$, $a \in L$ implies $ra \in L$.

(One can similarly define a *right-ideal*.) An ideal is thus simultaneously a left- and right-ideal of R.

14. For $a \in R$ let $Ra = \{xa \mid x \in R\}$. Prove that Ra is a left-ideal of R.

15. Prove that the intersection of two left-ideals of R is a left-ideal of R.

16. What can you say about the intersection of a left-ideal and right-ideal of R?

17. If R is a ring and $a \in R$ let $r(a) = \{x \in R \mid ax = 0\}$. Prove that $r(a)$ is a right-ideal of R.

18. If R is a ring and L is a left-ideal of R let $\lambda(L) = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$. Prove that $\lambda(L)$ is a two-sided ideal of R.

*19. Let R be a ring in which $x^3 = x$ for every $x \in R$. Prove that R is a commutative ring.

20. If R is a ring with unit element 1 and ϕ is a homomorphism of R *onto* R' prove that $\phi(1)$ is the unit element of R'.

21. If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that $I(\phi) \neq R$, prove that $\phi(1)$ is the unit element of R'.

3.5 More Ideals and Quotient Rings

We continue the discussion of ideals and quotient rings.

Let us take the point of view, for the moment at least, that a field is the most desirable kind of ring. Why? If for no other reason, we can divide in a field, so operations and results in a field more closely approximate our experience with real and complex numbers. In addition, as was illustrated by Problem 2 in the preceding problem set, a field has no homomorphic images other than itself or the trivial ring consisting of 0. Thus we cannot simplify a field by applying a homomorphism to it. Taking these remarks into consideration it is natural that we try to link a general ring, in some fashion, with fields. What should this linkage involve? We have a machinery whose component parts are homomorphisms, ideals, and quotient rings. With these we will forge the link.

But first we must make precise the rather vague remarks of the preceding paragraph. We now ask the explicit question: Under what conditions is the homomorphic image of a ring a field? For commutative rings we give a complete answer in this section.

Essential to treating this question is the converse to the result of Problem 2 of the problem list at the end of Section 3.4.

LEMMA 3.5.1 *Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a field.*

Proof. In order to effect a proof of this lemma for any $a \neq 0 \in R$ we must produce an element $b \neq 0 \in R$ such that $ab = 1$.

So, suppose that $a \neq 0$ is in R. Consider the set $Ra = \{xa \mid x \in R\}$. We claim that Ra is an ideal of R. In order to establish this as fact we must show that it is a subgroup of R under addition and that if $u \in Ra$ and $r \in R$ then ru is also in Ra. (We only need to check that ru is in Ra for then ur also is since $ru = ur$.)

Now, if $u, v \in Ra$, then $u = r_1a$, $v = r_2a$ for some $r_1, r_2 \in R$. Thus $u + v = r_1a + r_2a = (r_1 + r_2)a \in Ra$; similarly $-u = -r_1a = (-r_1)a \in Ra$. Hence Ra is an additive subgroup of R. Moreover, if $r \in R$, $ru = r(r_1a) = (rr_1)a \in Ra$. Ra therefore satisfies all the defining conditions for an ideal of R, hence is an ideal of R. (Notice that both the distributive law and associative law of multiplication were used in the proof of this fact.)

By our assumptions on R, $Ra = (0)$ or $Ra = R$. Since $0 \neq a = 1a \in Ra$, $Ra \neq (0)$; thus we are left with the only other possibility, namely that $Ra = R$. This last equation states that every element in R is a multiple of