This example indicates that the structure of a factor ring may seem *worse* than that of the original ring. ▲

Every nonzero ring R has at least two ideals, the **improper ideal** R and the **trivial ideal** $\{0\}$. For these ideals, the factor rings are R/R, which has only one element, and $R/\{0\}$, which is isomorphic to R. These are uninteresting cases. Just as for a subgroup of a group, a **proper nontrivial ideal** of a ring R is an ideal N of R such that $N \neq R$ and $N \neq \{0\}$.

While factor rings of rings and integral domains may be of great interest, as the above examples indicate, Corollary 31.6, which follows our next theorem, shows that a factor ring of a field is really not useful to us.

31.5 Theorem If R is a ring with unity, and N is an ideal of R containing a unit, then $N = R$.

Proof Let N be an ideal of R, and suppose that $u \in N$ for some unit u in R. Then the condition $rN \subseteq N$ for all $r \in R$ implies, if we take $r = u^{-1}$ and $u \in N$, that $1 = u^{-1}u$ is in N. But then $rN \subseteq N$ for all $r \in R$ implies that $r1 = r$ is in N for all $r \in R$, so $N = R$. ◆

31.6 Corollary A field contains no proper nontrivial ideals.

Proof Since every nonzero element of a field is a unit, it follows at once from Theorem 31.5 that an ideal of a field F is either $\{0\}$ or all of F. ◆

Maximal and Prime Ideals

We now consider the questions of when a factor ring is a field and when it is an integral domain. In our analogy between groups and rings, we noticed that ideals in rings correspond to normal subgroups. Corollary 31.6 states that a field contains no proper nontrivial ideals. In group theory, this corresponds to a group having no proper nontrivial normal subgroups, that is, a simple group. Theorem 13.20 states that a factor group G/H is simple if and only if H is a maximal normal subgroup of G. The following definition is analogous to maximal normal subgroups.

31.7 Definition A **maximal ideal of a ring** R is an ideal M different from R such that there is no proper ideal N of R properly containing M. ■

31.8 Example Let p be a prime positive integer. We know that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\mathbb{Z}_p$. Forgetting about multiplication for the moment and regarding $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}_p$ as additive groups, we know that $\mathbb{Z}_p$ is a simple group, and consequently $p\mathbb{Z}$ must be a maximal normal subgroup of $\mathbb{Z}$ by Theorem 13.20. Since $\mathbb{Z}$ is an abelian group and every subgroup is a normal subgroup, we see that $p\mathbb{Z}$ is a maximal proper subgroup of $\mathbb{Z}$. Since $p\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$, it follows that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. We know that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}_p$, and that $\mathbb{Z}_p$ is actually a field. Thus $\mathbb{Z}/p\mathbb{Z}$ is a field. This illustrates the next theorem. ▲

31.9 Theorem **(Analogue of Theorem 13.20)** Let R be a commutative ring with unity. Then M is a maximal ideal of R if and only if R/M is a field.

Proof We first assume that M is a maximal ideal in R. Since R is a commutative ring with unity, so is R/M. Furthermore, since $M \neq R$, $0 + M \neq 1 + M$ and R/M is a nonzero ring. Let $(a + M) \in R/M$, with $a \notin M$, so that $a + M$ is not the additive identity element of R/M. Suppose $a + M$ has no multiplicative inverse in R/M. Then the set $(R/M)(a + M) = \{(r + M)(a + M) \mid (r + M) \in R/M\}$ does not contain $1 + M$. We easily see that $(R/M)(a + M)$ is an ideal of R/M. It is nontrivial because $a \notin M$, and it is a

proper ideal because it does not contain $1 + M$. By Theorem 30.11, if $\gamma : R \to R/M$ is the canonical homomorphism, then $\gamma^{-1}[(R/M)(a + M)]$ is a proper ideal of R properly containing M. But this contradicts our assumption that M is a maximal ideal, so $a + M$ must have a multiplicative inverse in R/M.

Conversely, suppose that R/M is a field. By Theorem 30.11, if N is any ideal of R such that $M \subset N \subset R$ and γ is the canonical homomorphism of R onto R/M, then $\gamma[N]$ is an ideal of R/M with $\{(0 + M)\} \subset \gamma[N] \subset R/M$. But this is contrary to Corollary 31.6, which states that the field R/M contains no proper nontrivial ideals. Hence if R/M is a field, then M is maximal. ◆

31.10 Example Since $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ and $\mathbb{Z}_n$ is a field if and only if n is a prime, we see that the maximal ideals of $\mathbb{Z}$ are precisely the ideals $p\mathbb{Z}$ for prime positive integers p. ▲

31.11 Corollary A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

Proof Corollary 31.6 shows that a field has no proper nontrivial ideals.

Conversely, if a commutative ring R with unity has no proper nontrivial ideals, then $\{0\}$ is a maximal ideal and $R/\{0\}$, which is isomorphic to R, is a field by Theorem 31.9. ◆

We now turn to the question of characterizing, for a commutative ring R with unity, the ideals $N \neq R$ such that R/N is an integral domain. The answer here is rather obvious. The factor ring R/N will be an integral domain if and only if $(a + N)(b + N) = N$ implies that either

$$a + N = N \qquad \text{or} \qquad b + N = N.$$

This is exactly the statement that R/N has no divisors of 0, since the coset N plays the role of 0 in R/N. Looking at representatives, we see that this condition amounts to saying that $ab \in N$ implies that either $a \in N$ or $b \in N$.

31.12 Example All ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. For $n = 0$, we have $n\mathbb{Z} = \{0\}$, and $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$, which is an integral domain. For $n > 0$, we have $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ and $\mathbb{Z}_n$ is an integral domain if and only if n is a prime. Thus the nonzero ideals $n\mathbb{Z}$ such that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain are of the form $p\mathbb{Z}$, where p is a prime. Of course, $\mathbb{Z}/p\mathbb{Z}$ is actually a field, so that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. Note that for a product rs of integers to be in $p\mathbb{Z}$, the prime p must divide either r or s. The role of prime integers in this example makes the use of the word *prime* in the next definition more reasonable. ▲

31.13 Definition An ideal $N \neq R$ in a commutative ring R is a **prime ideal** if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$. ■

Note that $\{0\}$ is a prime ideal in $\mathbb{Z}$, and indeed, in any integral domain.

31.14 Example Note that $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$, for if $(a, b)(c, d) \in \mathbb{Z} \times \{0\}$, then we must have $bd = 0$ in $\mathbb{Z}$. This implies that either $b = 0$ so $(a, b) \in \mathbb{Z} \times \{0\}$ or $d = 0$ so $(c, d) \in \mathbb{Z} \times \{0\}$. Note that $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$ is isomorphic to $\mathbb{Z}$, which is an integral domain. ▲

Our remarks preceding Example 31.12 constitute a proof of the following theorem, which is illustrated by Example 31.14.

31.15 Theorem Let R be a commutative ring with unity, and let $N \neq R$ be an ideal in R. Then R/N is an integral domain if and only if N is a prime ideal in R.