Example 23.1 shows that in $\mathbb{Z}_{12}$ the elements 2, 3, 4, 6, 8, 9, and 10 are divisors of 0. Note that these are exactly the numbers in $\mathbb{Z}_{12}$ that are not relatively prime to 12, that is, whose gcd with 12 is not 1.

If R is a ring with unity and a is a unit in R, then a is not a divisor of 0. To see this, note that if $ab = 0$, then $a^{-1}ab = 0$, so $b = 0$. Similarly, if $ba = 0$, then $baa^{-1} = 0$, so $b = 0$. Theorem 23.3 shows that in the ring $\mathbb{Z}_n$ every element is either 0, a unit, or a 0 divisor.

23.3 Theorem Let $m \in \mathbb{Z}_n$. Either $m = 0$, m is relatively prime to n, in which case m is a unit in $\mathbb{Z}_n$, or m is not relatively prime to n, in which case m is a 0 divisor in $\mathbb{Z}_n$.

Proof We first suppose that $m \neq 0$ and $\gcd(m, n) = d \neq 1$. Then, using integer multiplication

$$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n$$

is a multiple of n, so in $\mathbb{Z}_n$,

$$m\left(\frac{n}{d}\right) = 0 \in \mathbb{Z}_n.$$

Neither m nor n/d is 0 in $\mathbb{Z}_n$. Thus m is a divisor of 0.

Now suppose that $\gcd(m, n) = 1$. Then there are integers a and b such that $an + bm = 1$. By the division algorithm, there are integers q and r such that $0 \leq r \leq n - 1$ and $b = nq + r$. We can write

$$rm = (b - nq)m = bm - nqm = (1 - an) - nqm = 1 - n(a + qm).$$

So in $\mathbb{Z}_n$, $rm = mr = 1$ and m is a unit. ◆

23.4 Example Classify each nonzero element of $\mathbb{Z}_{20}$ as a unit or a 0 divisor.

Solution The greatest common divisor of m and 20 is 1 if $m = 1, 3, 7, 9, 11, 13, 17, 19$, so these are all units. For $m = 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18$, $\gcd(m, 20) > 1$, so these are all 0 divisors. We see that

$$1 \cdot 1 = 3 \cdot 7 = 9 \cdot 9 = 11 \cdot 11 = 13 \cdot 17 = 19 \cdot 19 = 1 \in \mathbb{Z}_{20}$$

which verifies that each is a unit. We also see that

$$2 \cdot 10 = 4 \cdot 5 = 6 \cdot 10 = 8 \cdot 15 = 12 \cdot 5 = 14 \cdot 10 = 16 \cdot 5 = 18 \cdot 10 = 0 \in \mathbb{Z}_{20}$$

which verifies that each of these is a 0 divisor in $\mathbb{Z}_{20}$. ▲

23.5 Corollary If p is a prime number, then every nonzero element of $\mathbb{Z}_p$ is a unit, which means that $\mathbb{Z}_p$ is a field and it has no divisors of 0.

Proof For any $0 < m \leq p - 1$, $\gcd(m, p) = 1$. So m is a unit in $\mathbb{Z}_p$ by Theorem 23.3. ◆

The preceding corollary shows that when we consider the ring $M_n(\mathbb{Z}_p)$, we are talking about a ring of matrices over a *field*. In the typical undergraduate linear algebra course, only the field properties of the real or complex numbers are used in much of the work. Such notions as matrix reduction to solve linear systems, determinants, Cramer's rule, eigenvalues and eigenvectors, and similarity transformations to try to diagonalize a matrix are valid using matrices over any field; they depend only on the arithmetic properties of a field. Considerations of linear algebra involving notions of magnitude, such as least-squares approximate solutions or orthonormal bases, make sense only when using fields where we have an idea of magnitude. The relation

$$p \cdot 1 = \underset{p \text{ summands}}{1 + 1 + \cdots + 1} = 0$$

indicates that there can be no very natural notion of magnitude in the field $\mathbb{Z}_p$.

Another indication of the importance of the concept of 0 divisors is shown in the following theorem. Let R be a ring, and let $a, b, c \in R$. The **cancellation laws** hold in R if $ab = ac$ with $a \neq 0$ implies $b = c$, and $ba = ca$ with $a \neq 0$ implies $b = c$. These are multiplicative cancellation laws. Of course, the additive cancellation laws hold in R, since $\langle R, + \rangle$ is a group.

23.6 Theorem The cancellation laws hold in a ring R if and only if R has no divisors of 0.

Proof Let R be a ring in which the cancellation laws hold, and suppose $ab = 0$ for some $a, b \in R$. We must show that either a or b is 0. If $a \neq 0$, then $ab = a0$ implies that $b = 0$ by cancellation laws. Therefore, either $a = 0$ or $b = 0$.

Conversely, suppose that R has no divisors of 0, and suppose that $ab = ac$ with $a \neq 0$. Then

$$ab - ac = a(b - c) = 0.$$

Since $a \neq 0$, and since R has no divisors of 0, we must have $b - c = 0$, so $b = c$. A similar argument shows that $ba = ca$ with $a \neq 0$ implies $b = c$. ◆

Suppose that R is a ring with no divisors of 0. Then an equation $ax = b$, with $a \neq 0$, in R can have at most one solution x in R, for if $ax_1 = b$ and $ax_2 = b$, then $ax_1 = ax_2$, and by Theorem 23.6 $x_1 = x_2$, since R has no divisors of 0. If R has unity $1 \neq 0$ and a is a unit in R with multiplicative inverse a^{-1}, then the solution x of $ax = b$ is $a^{-1}b$. In the case that R is commutative, in particular if R is a field, it is customary to denote $a^{-1}b$ and ba^{-1} (they are equal by commutativity) by the formal quotient b/a. This quotient notation must not be used in the event that R is not commutative, for then we do not know whether b/a denotes $a^{-1}b$ or ba^{-1}. In particular, the multiplicative inverse a^{-1} of a nonzero element a of a field may be written $1/a$.

Integral Domains

The integers are really our most familiar number system. In terms of the algebraic properties we are discussing, $\mathbb{Z}$ is a commutative ring with unity and no divisors of 0. Surely this is responsible for the name that the next definition gives to such a structure.

23.7 Definition An **integral domain** D is a commutative ring with unity $1 \neq 0$ that contains no divisors of 0. ■

Thus, if the coefficients of a polynomial are from an integral domain, one can solve a polynomial equation in which the polynomial can be factored into linear factors in the usual fashion by setting each factor equal to 0.

In our hierarchy of algebraic structures, an integral domain belongs between a commutative ring with unity and a field, as we shall show. Theorem 23.6 shows that the cancellation laws for multiplication hold in an integral domain.

23.8 Example We have seen that $\mathbb{Z}$ and $\mathbb{Z}_p$ for any prime p are integral domains, but $\mathbb{Z}_n$ is not an integral domain if n is not prime. A moment of thought shows that the direct product $R \times S$ of two nonzero rings R and S is not an integral domain. Just observe that for $r \in R$ and $s \in S$ both nonzero, we have $(r, 0)(0, s) = (0, 0)$. ▲