13.34 Prove that there is no integral domain with exactly six elements. Can your argument be adapted to show that there is no integral domain with exactly four elements? What about 15 elements? Use these observations to guess a general result about the number of elements in a finite integral domain.

Solution: Suppose, by way of contradiction, that there exists an integral domain $R$ with $|R| = 6$. Let 0 and 1 denote the additive identity and multiplicative identity of $R$, respectively. By Theorem 13.3, we know that char($R$) is the additive order of 1. The fact that $(1 + 1 + 1 + 1 + 1 + 1 =) 6 \cdot 1 = 0$ (which follows from a corollary to Lagrange’s Theorem since $|R| = 6$) implies that the additive order of 1 is either 1, 2, 3, or 6. However, Theorem 13.4 tells us that char($R$) must be prime, so char($R$) is either 2 or 3. If char($R$) = 2, then this tells us that $2 \cdot x = 0$ for all $x \in R$, which implies that every element of $R$ has additive order either 1 or 2. However, Cauchy’s Theorem for Abelian Groups (Theorem 9.5) tells us that $R$ must have an element which has additive order 3, a contradiction. Similarly, if char($R$) = 3, then every element of $R$ has additive order either 1 or 3, but Cauchy’s Theorem for Abelian Groups tells us that $R$ has an element of additive order 2, a contradiction. Hence, no such ring exists.

This argument can be adapted to show that there is no integral domain with 15 elements - the role of 2 and 3 in the above argument will be taken by 3 and 5. However, this argument cannot be adapted to show there is not integral domain with 4 elements since the argument above relies on the order of the ring being divisible by at least 2 distinct primes (in fact, there is an integral domain with 4 elements). This may lead us to guess that any finite integral domain must have order which is a power of a prime, which is indeed the case.

13.35 Let $F$ be a field of order $2^n$. Prove that char($F$) = 2.

Solution: By Theorem 13.3, we know that char($F$) is equal to the additive order of 1 (the multiplicative identity of $F$) in $F$. By a corollary to Lagrange’s Theorem, we know that $0 = |F| \cdot 1 = 2^n \cdot 1$. This implies that the additive order of 1 divides $2^n$. Now, Theorem 13.4 implies that char($F$) is prime. Since the only prime divisor of $2^n$ is 2, we must have that char($F$) = 2.

13.49 Let $x, y \in R$, where $R$ is a commutative ring with prime characteristic $p$.
   a. Show that $(x + y)^p = x^p + y^p$.
   b. Show that, for all positive integers $n$, $(x + y)^{p^n} = x^{p^n} + y^{p^n}$.
   c. Find elements $x$ and $y$ in a ring of characteristic 4 such that $(x + y)^4 = x^4 + y^4$. 

Solution: a. One can show that the binomial theorem holds in any commutative ring. Thus,
\[(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot x^i y^{p-i}.\]
Note that, for \(1 \leq i \leq p - 1\), we have that
\[\frac{p!}{(p-i)!i!} = \binom{p}{i} \in \mathbb{Z},\]
that is, \((p-i)!i!\) divides \(p!\). Since \(1 \leq i \leq p - 1\) and \(p\) is prime, it follows that \((p-i)!i!\) is coprime to \(p\). It follows that \((p-i)!i!\) divides \((p-1)!\) (using the fact that if \(a, b, c \in \mathbb{Z}\) and \(a\) divides \(bc\) and \(\gcd(a, b) = 1\) then \(a\) divides \(c\)). Hence, we can write \((p-i)!i!k_i = (p-1)!\) for some \(k_i \in \mathbb{Z}\). Thus, we have
\[
(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot x^i y^{p-i} = x^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} \cdot x^i y^{p-i}\right) + y^p
\]
\[
= x^p + \left(\sum_{i=1}^{p-1} k_i p \cdot x^i y^{p-i}\right) + y^p
\]
\[
= x^p + y^p
\]
since \(R\) has characteristic \(p\).

b. This follows from part a and induction (the details are left as an exercise).

c. In the ring \(\mathbb{Z}_4\), we have \((1 + 1)^4 = 2^4 = 0\), but \(1^4 + 1^4 = 2 \neq 0\).

13.52 Give an example of an infinite integral domain with characteristic 3.

Solution: The ring \(\mathbb{Z}_3[x]\) is infinite (since the elements \(1, x, x^2, \ldots\) are all distinct) and has characteristic 3 since any element \(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}_3[x]\) (i.e. \(a_n, a_{n-1}, \ldots, a_0 \in \mathbb{Z}_3\)) satisfies
\[3 \cdot (a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0) = (3 \cdot a_n)x^n + (3 \cdot a_{n-1})x^{n-1} + \cdots + (3 \cdot a_1)x + (3 \cdot a_0) = 0.\]
Also \(\mathbb{Z}_3[x]\) is an integral domain since \(\mathbb{Z}_3\) is (see Theorem 16.1).

13.54 Let \(R\) be a ring with \(m\) elements. Show that the characteristic of \(R\) divides \(m\).

Solution: Set \(n = \text{char}(R)\). Since \(|R| = m\), we know that \(m \cdot x = 0\) for any \(x \in R\) by a corollary to Lagrange's Theorem. In particular, this tells us that \(n \neq 0\). Hence, by the division algorithm, there exists \(q, r \in \mathbb{Z}\) with \(0 \leq r < n\) such that \(m = nq + r\). For any \(x \in R\), we have that
\[0 = m \cdot x = (nq + r) \cdot x = (nq) \cdot x + r \cdot x = q \cdot (n \cdot x) + r \cdot x = q \cdot 0 + r \cdot x = r \cdot x.\]
Thus, \( r \cdot x = 0 \) for all \( x \in R \). But \( n \) is the smallest positive integer with this property, and \( r < n \), so it follows that \( r = 0 \). Hence, \( m = nq = (\text{char}(R))q \), so \( \text{char}(R) \) divides \( m \).

14.12 If \( A \) and \( B \) are ideals of a ring \( R \), show that the product of \( A \) and \( B \)

\[
AB = \{a_1b_1 + \cdots + a_nb_n | n \in \mathbb{Z}_+, a_i \in A, b_i \in B \}
\]

is an ideal.

**Solution:** Note that \( 0 = (0)(0) \in AB \), so \( AB \neq \emptyset \). Now, let \( x, x' \in AB \). Then

\[
x = a_1b_1 + \cdots + a_nb_n \\
x' = a'_1b'_1 + \cdots + a'_nb'_n
\]

for some \( a_1, \ldots, a_n, a'_1, \ldots, a'_n \in A \) and \( b_1, \ldots, b_n, b'_1, \ldots, b'_n \in B \). Then

\[
x-x' = (a_1b_1 + \cdots + a_nb_n) - (a'_1b'_1 + \cdots + a'_nb'_n) = a_1b_1 + \cdots + a_nb_n + (-a'_1)b'_1 + (-a'_2)b'_2 + \cdots + (-a'_n)b'_n \in AB.
\]

It follows that \( AB \) is an additive subgroup of \( R \).

Now, let \( r \in R \) and let \( x \) be as above. Then

\[
rx = r(a_1b_1 + \cdots + a_nb_n) = (ra_1)b_1 + \cdots + (ra_n)b_n
\]

which is in \( AB \) since \((ra_1), (ra_2), \ldots, (ra_n) \in A \) since \( A \) is an ideal. Similarly

\[
xr = (a_1b_1 + \cdots + a_nb_n)r = a_1(b_1r) + \cdots + a_n(b_nr)
\]

which is in \( AB \) since \((b_1r), (b_2r), \ldots, (b_nr) \in B \) since \( B \) is an ideal. Thus, \( AB \) is an ideal.

14.16 If \( A \) and \( B \) are ideals of a commutative ring \( R \) with unity and \( A+B = R \), show that \( A \cap B = AB \).

**Solution:** First, suppose that \( x \in AB \). Then \( x = a_1b_1 + a_2b_2 + \cdots + a_nb_n \) for some \( a_1, \ldots, a_n \in A \) and \( b_1, \ldots, b_n \in B \). Note that, for any \( i \in \{1, 2, \ldots, n\} \), we have that \( a_ib_i \in A \) since \( a_i \in A \), \( b_i \in R \), and \( A \) is an ideal of \( R \). Similarly, \( a_ib_i \in B \) since \( b_i \in B \), \( a_i \in R \), and \( B \) is an ideal of \( R \). Hence, \( a_1b_1 + a_2b_2 + \cdots + a_nb_n \in A \cap B \). Thus, \( AB \subseteq A \cap B \) (note that this is always true - we did not use the assumption that \( A+B = R \) here).

Now, suppose that \( y \in A \cap B \). Since \( 1 \in R = A + B \), there exist \( a \in A \) and \( b \in B \) such that \( 1 = a + b \). Then \( y = y(1) = y(a + b) = ya + yb = ay + yb \). Since \( y \in B \), \( ay \in AB \). Since \( y \in A \), \( yb \in AB \). Hence, \( y = ay + yb \in AB \). Thus, \( A \cap B \subseteq AB \). Hence, \( A \cap B = AB \).

14.17 If an ideal \( I \) of a ring \( R \) contains a unit, show that \( I = R \).

**Solution:** Clearly \( I \subseteq R \). Conversely, suppose that \( r \in R \). By assumption, there exists a unit \( u \in I \). Then we have that \( r = (ru^{-1})u \in I \) since \( ru^{-1} \in R \) and \( u \in I \). It follows that \( R \subseteq I \), so that \( R = I \).
14.28 Let $R$ be a commutative ring with unity. Suppose that the only ideals of $R$ are \{0\} and $R$. Show that $R$ is a field.

Solution: Let $x \in R \setminus \{0\}$. Consider the ideal $(x)$ generated by $x$ (recall that since $R$ is commutative, $(x) = \{rx | r \in R\}$). Since $x \neq 0$ and $x \in (x)$, we have that \{0\} $\neq (x)$. By the assumption that the only ideals of $R$ are \{0\} and $R$, this implies that $(x) = R$. Since $1 \in R = (x)$, this implies that there is $r \in R$ such that $rx = 1$. Since $R$ is commutative, $xr = rx = 1$. Hence, $x$ has a multiplicative inverse. It follows that $R$ is a field.