Integral Domain.
A (nonzero) commutative ring with identity is called an integral domain if contains no zero divisors, i.e. whenever \( ab = 0 \), either \( a = 0 \) or \( b = 0 \).

Exercise.
Let \( R \) be an integral domain, and let \( a, b, c \) be three nonzero elements in \( R \). Show that if \( ab = ac \) then \( b = c \).

Solution.
\( ab - ac = a(b - c) = 0 \). Therefore either \( a = 0 \) or \( b - c = 0 \). We assumed that \( a \) is nonzero, so \( b - c = 0 \), hence \( b = c \).

Definition.
A (nonzero) commutative ring with identity is called a field if every nonzero element is a unit.

Exercise.
Prove that a field is an integral domain.

Solution.
Let \( a, b \) be two elements in a field such that \( ab = 0 \). If \( a \) is nonzero then it has an inverse. Multiply \( ab = 0 \) by \( a^{-1} \), and get \( b = 0 \). Similarly, if \( b \neq 0 \) then \( a = 0 \). Therefore, either \( a = 0 \) or \( b = 0 \).

Notation.
In any ring, if \( n \) is a positive integer then \( a^n \) stands for \( a \cdot \ldots \cdot a \) \( n \)-times. If \( R \) is a ring with identity and \( a \) is invertible, then \( a^{-n} = (a^{-1})^n \). If \( R \) is a ring with identity then \( a^0 = 1 \). The basic properties such as \( (a^m)^n = a^{mn} \) and \( a^m a^n = a^{m+n} \) hold for any ring.

Remark.
If \( R \) is an integral domain and \( a \) is a nonzero element in \( R \) then \( a^n \) is nonzero for any \( n \in \mathbb{N} \) by induction: \( a^0 = 1 \neq 0 \). Assume \( a^k \neq 0 \). If \( a^{k+1} = 0 \) then either \( a = 0 \) or \( a^n \neq 0 \) for all \( n \in \mathbb{N} \).
or \(a^k = 0\), which is impossible, which means that \(a^{k+1} \neq 0\).

**Remark.**
In a ring with identity \(R\), if \(a^n = 1\) for some \(n \in \mathbb{N} \setminus \{0\}\) then \(a\) is invertible: If \(n = 1\) then \(a\) is 1 to start with. Otherwise, \(n \geq 2\), and so \(a^n = a^{n-1} \cdot a = a \cdot a^{n-1} = 1\), so \(a\) has an inverse.

**Theorem.**
Every finite integral domain is a field.

**Proof.**
Let \(a\) be a nonzero element in a finite integral domain \(R\). Consider the set of all (nonnegative) powers of \(a\): \(\{a^n : n \in \mathbb{N}\}\). [Remember: we can consider only nonzero powers. We cannot consider negative powers because for that we need \(a\) to be invertible, which is what we need to prove] This set is contained in \(R\). Since \(R\) is finite, so is the set. Therefore, there are powers which repeats themselves, i.e. there exist \(m > n\) such that \(a^m = a^n\). Then \(0 = a^m - a^n = a^n(a^{m-n} - 1)\). \(R\) is an integral domain, and so either \(a^n = 0\) or \(a^{m-n} - 1 = 0\). The first option is impossible, because \(R\) is an integral domain. Therefore \(a^{m-n} - 1 = 0\), i.e. \(a^{m-n} = 1\). Since \(m - n \geq 1\), \(a\) is invertible.

**Notes for general knowledge.**
A ring with identity which is not necessarily commutative and has no zero divisors is called simply a domain. A ring with identity which is not necessarily commutative and all its nonzero elements are units is called a skew field. Examples of skew fields are in general difficult to construct, the easiest one is the ring of quaternions discovered by Hamilton in the 19th century: One takes the complex numbers and adds a new element \(j\) satisfying \(j^2 = -1\) and \(ij = -ji\). This new ring is a four dimensional vector space over the real numbers \(\mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij\). There are no finite noncommutative skew fields. Every finite domain is also commutative and therefore is a finite integral domain, and so a field. This fact was proven by Wedderburn in the 20th century but is beyond the scope of this course.

**Exercise.**

- Let \(R\) and \(S\) be two integral domains. Is \(R \times S\) always an integral domain, sometimes or never?
- Let \(S\) be a subring of an integral domain \(R\). Assume \(S\) contains 1. Is \(S\) necessarily an integral domain?
- Let \(S\) be a subring of a field \(R\). Assume \(S\) contains 1. Is \(S\) necessarily a field?