# CS21001 Discrete Structures
## Tutorial 9

---

**1.** Let $R$ be a ring. Prove that the following conditions are equivalent.

(1) $R$ is commutative.
(2) $(a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.
(3) $(a+b)(a-b) = a^2 - b^2$ for all $a, b \in R$.

**2.** Let $R$ be a commutative ring with identity.

**(a)** Prove that the set $R[x]$ of all univariate polynomials with coefficients from $R$ is a commutative ring with identity. Can a non-constant polynomial be a unit of $R[x]$?
**(b)** Let $n \in \mathbb{N}$, $n \geqslant 2$, be a fixed constant. Prove that the set $R[x_1, x_2, \ldots, x_n]$ of $n$-variate polynomials with coefficients from $R$ is a commutative ring with identity.
**(c)** Prove that the set $R[[x]]$ of all infinite power series expansions with coefficients from $R$ is a commutative ring with identity. What are the units of $R[[x]]$?

**3.** If $R$ is an integral domain, which of the rings of the previous exercise is/are integral domain(s)?

**4.** Let $R$ be a commutative ring. An element $a \in R$ is said to be *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$.

**(a)** Given an example of a non-zero nilpotent element in a ring.
**(b)** Prove that if $a$ and $b$ are nilpotent, then so also is $a+b$.
**(c)** Let $R$ be with identity. Prove that if $a$ is nilpotent and $u$ is a unit, then $a+u$ is a unit.
**(d)** Prove that the set of all nilpotent elements of $R$ is an ideal of $R$. This ideal is called the *nilradical* of $R$.

**5.** Let $R$ be a commutative ring with identity, and let $a(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 \in R[x]$.

**(a)** Prove that $a(x)$ is nilpotent if and only if $a_0, a_1, a_2, \ldots, a_d$ are all nilpotent.
**(b)** Prove that $a(x)$ is a unit in $R[x]$ if and only if $a_0$ is a unit in $R$, and $a_1, a_2, \ldots, a_d$ are nilpotent.

**6.** The *characteristic* of a ring $R$ is defined to be the smallest $n \in \mathbb{N}$ for which $1 + 1 + \cdots + 1$ ($n$ times) $= 0$. In this case, we say $\operatorname{char} R = n$. If no such $n$ exists, we say that $\operatorname{char} R = 0$.

**(a)** What are the characteristics of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$?
**(b)** Prove that $\operatorname{char} R = \operatorname{char} R[x]$.
**(c)** Let $R$ be an integral domain of positive characteristic $n$. Prove that $n$ is a prime.

**7.** Let $R$ be an integral domain of prime characteristic $p$, and let $a, b \in R$. Prove that:

**(a)** The binomial coefficient $\binom{p}{r}$ is divisible by $p$ for $1 \leqslant r \leqslant p-1$.
**(b)** $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ for all $n \in \mathbb{N}_0$.

**8.** Let $R$ be a ring, and $S, T_1, T_2$ subrings of $R$. If $S \subseteq T_1 \cup T_2$, prove that $S \subseteq T_1$ or $S \subseteq T_2$.

**9.** Let $I, J$ be ideals of a ring $R$. Which of the following sets is/are ideal(s) of $R$?

**(a)** $I + J = \{a + b \mid a \in I \text{ and } b \in J\}$.
**(b)** $IJ = \{ab \mid a \in I \text{ and } b \in J\}$.
**(c)** $I \cup J = \{a \mid a \in I \text{ or } a \in J\}$.
**(d)** $I \cap J = \{a \mid a \in I \text{ and } a \in J\}$.

**10.** Let $R$ be a ring with identity, and $I$ an ideal of $R$. Prove that $I = R$ if and only if $I$ contains a unit.

**11.** Prove that a commutative ring $R$ with identity is a field if and only if the only ideals of $R$ are $\{0\}$ and $R$.

**12.** Let $R$ be a commutative ring with identity. An ideal $I$ of $R$ is called *prime* if $ab \in I$ implies either $a \in I$ or $b \in I$. An ideal $I$ of $R$ is called *maximal* if for any ideal $J$ of $R$ satisfying $I \subseteq J \subseteq R$, we must have $J = I$ or $J = R$ (that is, there exists no proper ideal of $R$ strictly containing $I$).

**(a)** Characterize all prime and all maximal ideals of $\mathbb{Z}$.
**(b)** Characterize all prime and all maximal ideals of $F[x]$, $F$ a field.
**(c)** Prove that every maximal ideal is prime.
**(d)** Give an example of a prime ideal that is not maximal.

**13.** **(a)** Prove that any ideal of $\mathbb{Z}$ is equal to $n\mathbb{Z}$ for some $n \in \mathbb{N}_0$.
**(b)** Let $m\mathbb{Z}$ and $n\mathbb{Z}$ be two ideals of $\mathbb{Z}$. Prove that $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, where $d = \gcd(m,n)$.

**14.** Let $f(x), g(x) \in F[x]$ for an infinite field $F$. If $f(a) = g(a)$ for infinitely many $a \in F$, prove that $f(x) = g(x)$.

**15.** Let $R$ be a commutative ring with identity. A subset $S \subseteq R$ is called *multiplicative* if (i) $1 \in S$, and (ii) whenever $s, t \in S$, we also have $st \in S$. Prove that the following sets are multiplicative.

**(a)** The set of all units of $R$.
**(b)** The set $\{1, f, f^2, f^3, \ldots\}$ for a non-nilpotent element $f$ of $R$.
**(c)** The set of all elements of $R$, which are not zero divisors.
**(d)** The set of all non-zero elements of $R$ if $R$ is an integral domain.
**(e)** The set of all non-multiples of a prime $p$ for $R = \mathbb{Z}$.

**16.** Let $R$ be a commutative ring with identity, and $S$ a multiplicative subset of $R$. Define a relation $\rho$ on $R \times S$ as $(r_1, s_1)\ \rho\ (r_2, s_2)$ if and only if $t(r_1 s_2 - r_2 s_1) = 0$ for some $t \in S$.

**(a)** Prove that $\rho$ is an equivalence relation.
**(b)** Denote the equivalence class of $(r,s)$ by $r/s$. Define $(r_1/s_1) + (r_2/s_2) = (r_1 s_2 + r_2 s_1)/(s_1 s_2)$, and $(r_1/s_1)(r_2/s_2) = (r_1 r_2)/(s_1 s_2)$. Show that these operations are well-defined, and the set $Q = R/\rho$ of equivalence classes is a commutative ring with identity under these operations. What are the units of $Q$?
**(c)** Prove that the map $\iota : R \to Q$ taking $r \mapsto (r/1)$ is a ring homomorphism.
**(d)** If $R$ is an integral domain and $S = R \setminus \{0\}$, prove that $Q$ is a field. This field is called the *field of fractions* or the *total quotient ring* of $R$.
**(e)** What are the fields of fractions of $\mathbb{Z}$ and $F[x]$, where $F$ is a field?

**17.** Let $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers. Take $a + \mathrm{i}b, c + \mathrm{i}d \in R$ with $c + \mathrm{i}d \neq 0$. Prove that there exist $p + \mathrm{i}q, r + \mathrm{i}s \in R$ such that $a + \mathrm{i}b = (p + \mathrm{i}q)(c + \mathrm{i}d) + (r + \mathrm{i}s)$ with $0 \leqslant |r + \mathrm{i}s| \leqslant \frac{1}{\sqrt{2}}|c + \mathrm{i}d|$. (**Hint:** First express $\frac{a+\mathrm{i}b}{c+\mathrm{i}d} = x + \mathrm{i}y$, where $x, y$ are rationals.)

**18.** Prove the following statements about congruences.

**(a)** If $a \equiv b \pmod{n}$, and $f(x) \in \mathbb{Z}[x]$, then $f(a) \equiv f(b) \pmod{n}$.
**(b)** If $a \equiv b \pmod{n}$ and $m|n$, then $a \equiv b \pmod{m}$.
**(c)** If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then $a \equiv m \pmod{\operatorname{lcm}(m,n)}$.
**(d)** $ax \equiv ay \pmod{n}$ if and only if $x \equiv y \pmod{n/d}$, where $d = \gcd(a,n)$.

**19.** Let $d = \gcd(a,n)$. Prove that the congruence $ax \equiv b \pmod{n}$ is solvable for $x$ if and only if $d|b$. How can you compute all the solutions of this congruence modulo $n$?

**20.** [*Fermat's little theorem*] Let $p$ be a prime. Prove that for all $a \in \mathbb{Z}$, we have $a^p \equiv a \pmod{p}$.

**21.** **(a)** Prove that there cannot be any non-zero homomorphism $\mathbb{Z}_n \to \mathbb{Z}$ for any $n \in \mathbb{N}$.
**(b)** Prove that there exists a non-zero homomorphism $\mathbb{Z}_m \to \mathbb{Z}_n$ taking $[1]_m \mapsto [1]_n$ if and only if $n|m$.
**(c)** Prove that the only non-zero homomorphism of $\mathbb{Z} \to \mathbb{Z}$ is the identity map.
**(d)** Let $F, K$ be fields. Prove that any non-zero homomorphism $F \to K$ is injective.

**22.** Let $f : R \to S$ be a homomorphism of rings. Prove that $f(R)$ is a subring of $S$. Prove also that the *kernel* of $f$ defined as $\ker(f) = \{a \in R \mid f(a) = 0_S\} \subseteq R$ is an ideal of $R$.

**23.** Let $m, n \in \mathbb{N}$ with $n|m$. Find the kernel of the ring homomorphism $f : \mathbb{Z}_m \to \mathbb{Z}_n$ taking $[a]_m$ to $[a]_n$.

**24.** Let $f : R \to S$ be a ring homomorphism, and $J$ an ideal of $S$. Prove that $f^{-1}(J) = \{a \in R \mid f(a) \in J\}$ is an ideal of $R$. If $T$ is a subring of $S$, is $f^{-1}(T)$ always a subring of $R$?

**25.** Prove that the map $f : \mathbb{R} \times \mathbb{R} \to \mathrm{GL}_2(\mathbb{R})$ taking $(a,b)$ to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ is a homomorphism of rings.

**26.** **(a)** Prove that every integral domain of characteristic 0 contains an isomorphic copy of $\mathbb{Z}$.
**(b)** Prove that every field of characteristic 0 contains an isomorphic copy of $\mathbb{Q}$.

**27.** Find all non-zero homomorphisms of $\mathbb{Z}[\mathrm{i}] \to \mathbb{Z}[\mathrm{i}]$.

**28.** Prove that there cannot exist a non-zero homomorphism $\mathbb{Z}[\mathrm{i}] \to \mathbb{Z}[\sqrt{2}]$.