CS21201 Discrete Structures

Tutorial 10

Rings and Fields

1. Define two operations on $\mathbb{Z}$ as

$$\begin{aligned} a \oplus b &= a+b+u, \\ a \odot b &= a+b+vab, \end{aligned}$$

where u, v are constant integers. For which values of u and v, is $(\mathbb{Z}, \oplus, \odot)$ a ring?

Solution [*Additive axioms*] $\oplus$ is clearly commutative. For associativity, we note that $(a \oplus b) \oplus c = (a+b+u) \oplus c = a+b+c+2u$, whereas $a \oplus (b \oplus c) = a \oplus (b+c+u) = a+b+c+2u$, that is, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ irrespective of u. The additive identity is $-u$, because $a \oplus (-u) = a + (-u) + u = a$ and $(-u) \oplus a = (-u) + a + u = a$. Finally, $a + (-2u - a) + u = (-2u - a) + a + u = -u$, so $-2u - a$ is the additive inverse of a. In short, the additive axioms do not impose any constraints on u (and v is not involved in this addition).

[*Multiplicative axioms*] We have $(a \odot b) \odot c = (a+b+vab) \odot c = a+b+vab+c+v(a+b+vab)c = a+b+c+v(ab+ac+bc+abc)$, whereas $a \odot (b \odot c) = a \odot (b+c+vbc) = a+(b+c+vbc)+va(b+c+vbc) = a+b+c+v(ab+ac+bc+abc)$, so $\odot$ is associative for any value of v. Although not needed in a general ring, this multiplication is commutative and has the identity 0. Again, no conditions on v (and u) are imposed.

[*Distributivity*] Because of commutativity, it suffices to look only at $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$, that is, $a \odot (b+c+u) = (a+b+vab) \oplus (a+c+vac)$, that is, $a+(b+c+u)+va(b+c+u) = (a+b+vab)+(a+c+vac)+u$, that is, $a+b+c+u+vab+vac+uva = 2a+b+c+u+vab+vac$, that is, $uva = a$. Since this must hold for all integers a, we must have $uv = 1$.

The only possibilities are therefore $u = v = 1$ and $u = v = -1$.

2. Take $u = v = 1$ is Exercise 1.

(a) Find the units of $(\mathbb{Z}, \oplus, \odot)$. Find their respective inverses.

Solution The multiplicative identity is 0. So $a \odot b = 0$ (with $a \neq -1$) implies $a+b+ab = 0$, that is, $b(a+1) = -a$, that is, $b = -\left(\frac{a}{a+1}\right)$. This b is an integer if and only if $a = 0$ or $a = -2$. The inverse of 0 is 0, and of -2 is -2.

(b) Prove that the set of all odd integers is a subring of this ring. What about the set of all even integers?

Solution It suffices to verify that $a \ominus b$ and $a \odot b$ are odd if a, b are odd. The additive inverse of b is $-2u - b = -2 - b$, which is odd if a is odd. But then, $a \ominus b = a \oplus (-2-b) = a - 2 - b + 1 = a - b - 1$ is odd if a, b are odd. Also, $a \odot b = a + b + ab$ is odd if a, b are odd.

Even integers do not constitute a subring, because closure of $\oplus$ does not hold.

3. Let $\mathbb{Z}_1$ be the ring of Exercise 1 with $u = v = 1$, and $\mathbb{Z}_2$ the ring of Exercise 1 with $u = v = -1$. Define a ring isomorphism $\mathbb{Z}_1 \to \mathbb{Z}_2$.

Solution Consider the map $f : \mathbb{Z}_1 \to \mathbb{Z}_2$ as $f(a) = -a$. Then, $f(a \oplus_1 b) = f(a+b+1) = -(a+b+1)$, whereas $f(a) \oplus_2 f(b) = (-a) \oplus_2 (-b) = (-a) + (-b) - 1 = -(a+b+1)$. Moreover, $f(a \odot_1 b) = f(a+b+ab) = -(a+b+ab)$, and $f(a) \odot_2 f(b) = (-a) \odot_2 (-b) = (-a) + (-b) - (-a)(-b) = -(a+b+ab)$.

4. Let R be a commutative ring with identity, and $R[x]$ the set of univariate polynomials with coefficients from R. Define addition and multiplication of polynomials in the usual way.

(a) Prove that $R[x]$ is a ring.

Solution Straightforward verification.

(b) Prove that $R[x]$ is an integral domain if and only if R is an integral domain.

Solution [$\Rightarrow$] Take non-zero elements $a, b \in R$. Then a and b are non-zero (constant) polynomials. Since $R[x]$ is an integral domain, ab is not the zero polynomial. But ab is again a constant polynomial. It follows that $ab \neq 0$.

[$\Leftarrow$] Suppose that there exist $A(x), B(x) \in R[x]$ such that $A(x)B(x) = 0$, $A(x) \neq 0$, and $B(x) \neq 0$. Write $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with $a_d \neq 0$ and $d \geqslant 0$, and $B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_ex^e$ with $b_e \neq 0$ and $e \geqslant 0$. Since $A(x)B(x) = 0$, we have $a_db_e = 0$. This implies that R is not an integral domain.

5. Let K, L be fields, and $f : K \to L$ a non-zero ring homomorphism.

(a) Prove/disprove: $f(1_K) = 1_L$.

Solution *True*. Since f is non-zero, there exists $a \in K$ such that $f(a) \neq 0_L$. But then, $f(a) = f(a \cdot 1_K) = f(a) \cdot f(1_K)$. Since $f(a) \neq 0_L$, it is a unit, so by cancellation, we have $f(1_K) = 1_L$.

(b) Prove that f is injective.

Solution Let $f(a) = f(b)$. If $a \neq b$, then $u = a - b$ is non-zero and so a unit of K. But then, we have $1_L = f(1_K) = f(uu^{-1}) = f(u)f(u^{-1}) = f(a-b)f(u^{-1}) = (f(a) - f(b))f(u^{-1}) = 0_L \cdot f(u^{-1}) = 0_L$. By definition, a field is a non-zero ring. Therefore $0_L = 1_L$ is a contradiction.

6. (a) Prove that $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

Solution Closure under subtraction and multiplication is easy to check. Since $\mathbb{R}$ is commutative, $\mathbb{Z}[\sqrt{5}]$ is so too. Finally, take $a = 1$ and $b = 0$ in the definition to conclude that $\mathbb{Z}[\sqrt{5}]$ contains the multiplicative identity.

(b) Prove that $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ is a field.

Solution Easy verification. Particularly, take $a + b\sqrt{5} \neq 0$, and show that

$$\frac{1}{a+b\sqrt{5}} = \frac{a-b\sqrt{5}}{a^2-5b^2} = \left(\frac{a}{a^2-5b^2}\right) + \left(\frac{-b}{a^2-5b^2}\right)\sqrt{5}.$$

Since $\sqrt{5}$ is irrational, we cannot have $a^2 - 5b^2 = 0$ for rational numbers a, b. So every non-zero element of $\mathbb{Q}[\sqrt{5}]$ is a unit.

(c) Argue that $\mathbb{Z}[\sqrt{5}]$ contains infinitely many units.

Solution $(2+\sqrt{5})(-2+\sqrt{5}) = 1$, so $2+\sqrt{5}$ is a unit, and it is > 1. Therefore $(2+\sqrt{5})^n$ are units for all $n \in \mathbb{N}$, distinct from one another.

Additional Exercises

7. The set of *Gaussian integers* is defined as $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$. Prove that $\mathbb{Z}[\mathrm{i}]$ is an integral domain. What are the units in this ring? Also define the set $\mathbb{Q}[\mathrm{i}] = \{a + \mathrm{i}b \mid a, b \in \mathbb{Q}\}$. Prove that $\mathbb{Q}[\mathrm{i}]$ is a field.

8. Prove that $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \left\{a + \left(\frac{1+\sqrt{5}}{2}\right)b \mid a, b \in \mathbb{Z}\right\}$ is an integral domain. Argue that $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ contains infinitely many units. Prove that $\mathbb{Q}\left[\frac{1+\sqrt{5}}{2}\right] = \left\{a + \left(\frac{1+\sqrt{5}}{2}\right)b \mid a, b \in \mathbb{Q}\right\}$ is a field. Prove/Disprove the following equalities as sets: **(a)** $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, **(b)** $\mathbb{Q}[\sqrt{5}] = \mathbb{Q}\left[\frac{1+\sqrt{5}}{2}\right]$.

9. Prove that $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is an integral domain. Find all the units in this ring. Prove that $\mathbb{Q}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\}$ is a field.

10. Let $n \geqslant 2$, and let $(R_i, +_i, \times_i)$ be rings for $i = 1, 2, 3, \ldots, n$. Define two operations on the Cartesian product $R = R_1 \times R_2 \times \cdots \times R_n$ as $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 +_1 b_1, a_2 +_2 b_2, \ldots, a_n +_n b_n)$ and $(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \times_1 b_1, a_2 \times_2 b_2, \ldots, a_n \times_n b_n)$ (component-wise operations).

(a) Prove that $(R, +, \cdot)$ is a ring.
(b) If each R_i is commutative, prove that R is commutative too.
(c) If each R_i is with identity, prove that R is with identity too. What are the units of R in this case?
(d) Prove/Disprove: If each R_i is an integral domain, then R is also an integral domain.
(e) Prove/Disprove: If each R_i is a field, then R is also a field.

11. Let R be the set of all functions $\mathbb{Z} \to \mathbb{Z}$. For $f, g \in R$, define $(f+g)(n) = f(n) + g(n)$ and $(fg)(n) = f(n)g(n)$ for all $n \in \mathbb{Z}$.

(a) Prove that R is a commutative ring with identity under these two operations.
(b) What are the units of R?
(c) Is R an integral domain?

12. Let R be the set of all functions $\mathbb{Z} \to \mathbb{Z}$. For $f, g \in R$, define $(f+g)(n) = f(n) + g(n)$ and $(fg)(n) = f(g(n))$ for all $n \in \mathbb{Z}$. Prove/Disprove: R is a ring under these two operations.

13. Let R be the set of all n-bit words for some $n \in \mathbb{N}$. Which of the following is/are ring(s)?

(a) R under bitwise OR and AND operations.
(b) R under bitwise XOR and AND operations.

14. Let R be an integral domain. A non-zero non-unit $p \in R$ is called *prime* in R if $p|(ab)$ implies $p|a$ or $p|b$ (for all $a, b \in R$). A non-zero non-unit $p \in R$ is called *irreducible* if $p = ab$ implies that either a or b is a unit.

(a) What are the primes of $\mathbb{Z}$? What are the irreducible elements of $\mathbb{Z}$?
(b) Prove that every prime is also irreducible.
(c) Demonstrate by an example that all irreducible elements need not be prime.

15. 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 $a, b \in R$.

16. Let R be a commutative ring with identity.

(a) 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.

(b) 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 $R[[x]]$?

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

18. 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.

19. 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.

20. 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.

21. 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 $n \in \mathbb{N}_0$.

22. 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 $S \subseteq T_2$.

23. 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 $f(x) = g(x)$.

24. 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 $R = \mathbb{Z}$.

25. Let R be a commutative ring with identity, and S a multiplicative subset of R. Define a relation ρ 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 ρ 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?

26. 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.)

27. **(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 $\mathbb{Z}_m \to \mathbb{Z}_n$ if and only if $n|m$.
(c) Prove that the only non-zero homomorphism of $\mathbb{Z} \to \mathbb{Z}$ is the identity map.

28. 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.

29. **(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 $\mathbb{Q}$.

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

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