CS21201 Discrete Structures

Tutorial 10

Abstract Algebraic Structures

1. 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.

2. **(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.

3. Define an operation $\circ$ on $G = \mathbb{R}^* \times \mathbb{R}$ as $(a,b) \circ (c,d) = (ac, bc+d)$. Prove that $(G,\circ)$ is a non-Abelian group.

Solution [Closure] Obvious.

[Associativity] We have $(a,b) \circ ((c,d) \circ (e,f)) = (a,b) \circ (ce, de+f) = (ace, bce+de+f)$, and $((a,b) \circ (c,d)) \circ (e,f) = (ac, bc+d) \circ (e,f) = (ace, bce+de+f)$.

[Identity] We have $(1,0) \circ (a,b) = (a,b)$ and $(a,b) \circ (1,0) = (a,b)$, so $(1,0)$ is the identity in G.

[Inverse] We have $(a,b) \circ (\frac{1}{a}, -\frac{b}{a}) = (1,0)$ and $(\frac{1}{a}, -\frac{b}{a}) \circ (a,b) = (1,0)$. Since $a \in \mathbb{R}^*$, $\frac{1}{a}$ is defined.

[Non-Abelian] We have $(1,2) \circ (2,3) = (2,7)$, whereas $(2,3) \circ (1,2) = (2,5)$.

4. Let G be a (multiplicative) group, and H, K subgroups of G. Prove that:

(a) $H \cap K$ is a subgroup of G.

Solution Let $a,b \in H \cap K$. Since $a,b \in H$ and H is a subgroup, we have $ab, a^{-1} \in H$. Likewise, $ab, a^{-1} \in K$. That is, $ab, a^{-1} \in H \cap K$.

(b) $H \cup K$ need not be a subgroup of G.

Solution Take $G = \mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,15\}$, $H = \{1,4\}$, and $K = \{1,11\}$. $H \cup K = \{1,4,11\}$ is not closed under multiplication: $4 \times 11 \equiv 14 \pmod{15}$.

(c) $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Solution [If] Obvious.

[Only if] $H \cup K$ is a subgroup of G. Suppose that H is not contained in K. Then, there exists $h \in H$ such that $h \notin K$. Take any $k \in K$. Since h, k are both in $H \cup K$, and $H \cup K$ is a subgroup, we have $hk \in H \cup K$. Suppose that $hk \in K$. Since $k \in K$, we have $k^{-1} \in K$, so $(hk)k^{-1} = h \in K$, a contradiction. Therefore $hk \in H$. But $h \in H$, so $h^{-1} \in H$, and therefore $h^{-1}(hk) = k \in H$. It follows that $K \subseteq H$.

(d) Define $HK = \{hk \mid h \in H,\ k \in K\}$. Define KH analogously. Prove that HK is a subgroup of G if and only if $HK = KH$.

Solution [If] Let $h, h_1, h_2 \in H$ and $k, k_1, k_2 \in K$. We have $(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$. Since $KH = HK$, $k_1h_2 = h_3k_3$ for some $h_3 \in H$ and $k_3 \in K$. Therefore $(h_1k_1)(h_2k_2) = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$. Next, consider $(hk)^{-1} = k^{-1}h^{-1}$. Since $KH = HK$, we have $k^{-1}h^{-1} = h_4k_4$ for some $h_4 \in H$ and $k_4 \in K$, so $(hk)^{-1} = h_4k_4 \in HK$.

[Only if] Take $hk \in HK$. Since HK is a subgroup, we have $(hk)^{-1} \in HK$, that is, there exist $h_1 \in H$ and $k_1 \in K$ such that $(hk)^{-1} = h_1k_1$. But then, $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$. That is, $HK \subseteq KH$.

Conversely, take $kh \in KH$. We have $h^{-1} \in H$ and $k^{-1} \in K$, so $h^{-1}k^{-1} \in HK$. Since HK is a subgroup, we have $(h^{-1}k^{-1})^{-1} = kh \in HK$. Therefore $KH \subseteq HK$.

Additional Exercises

5. 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.

6. 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)** $\mathbb{Q}[\sqrt{5}] = \mathbb{Q}\left[\frac{1+\sqrt{5}}{2}\right]$.

7. 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.

8. 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.

9. 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?

10. 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.

11. 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.

12. 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 $a, b \in R$.

13. 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 $R[[x]]$?

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

15. 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 $S \subseteq T_2$.

16. Let G be a group. Suppose that there exists some $n \in \mathbb{N}$ such that for all $a, b \in G$, we have $(ab)^n = a^n b^n$ and $(ab)^{n+1} = a^{n+1} b^{n+1}$. Prove that G is Abelian.

17. Let H and K be two subgroups of a (multiplicative) group G. Suppose that $HK = KH$ (so this is a subgroup), and $H \cap K = \{e\}$. Prove that for every element $a \in HK$, there exist a unique $h \in H$ and a unique $k \in K$ such that $a = hk$.

18. Let G be a (multiplicative) group, and H a subgroup of G.

(a) Prove that the following conditions are equivalent.

(1) $aH = bH$.
(2) $a^{-1}b \in H$.

(b) Define a relation ρ on G as $a \rho b$ if and only if $aH = bH$ (or equivalently, $a^{-1}b \in H$). Prove that ρ is an equivalence relation.

(c) What are the equivalence classes of ρ?

(d) Prove that the equivalence classes of ρ are equinumerous.

19. [*Lagrange's theorem*] Let G be a finite group, and H a subgroup. Then, the order of H divides the order of G. (The order of a group is the number of elements in it.)

20. Let I be a non-empty index set (not necessarily finite), and let a_i, $i \in I$, be symbols. Define G to be the set of all symbolic sums of the form $\sum_{i \in I} n_i a_i$, where all $n_i \in \mathbb{Z}$, and only finitely many n_i are non-zero. Define addition on G as $\sum_{i \in I} m_i a_i + \sum_{i \in I} n_i a_i = \sum_{i \in I} (m_i + n_i) a_i$. Prove that G is an Abelian group under this addition. G is called the *free Abelian group* generated by the symbols a_i, $i \in I$.