Abstract Algebraic Structures

Q1. Define two operations on $\mathbb{Z}$ as:

$$a \oplus b = a + b + u, \quad a \odot b = a + b + vab$$

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

Solution 1: [Additive axioms] 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, $a + (-2u - a) + u = (-2u - a) + a + u = -u$, $-2u - a$ 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 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 $u = v = -1$.

Q2. Take $u = 1$ and $v = 1$ in Question 1.

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

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

Solution 2:

(a) 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, $b = -(\frac{a}{a+1})$. 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) 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, $a \oplus b = a \oplus (-2-b) = a-2-b+1 = a-b-1$ 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 $\odot$ does not hold.

Q3. Let $\mathbb{Z}_1$ be the ring from Question 1 with $u = v = 1$, and $\mathbb{Z}_2$ the ring from Question 1 with $u = v = -1$. Define a ring isomorphism $f : \mathbb{Z}_1 \to \mathbb{Z}_2$.

Solution 3: 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 $f(a) \odot_2 f(b) = (-a) \odot_2 (-b) = (-a) + (-b) - (-a)(-b) = -(a + b + ab)$.

Q4. Let R be a commutative ring with identity, and $R[x]$ be the set of univariate polynomials with coefficients from R. Define addition and multiplication of polynomials in the usual way. Prove that $R[x]$ is an integral domain if and only if R is an integral domain.

Solution 4: [$\Rightarrow$] 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 $d \geq 0$, and $B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_ex^e$ with $b_e \neq 0$ and $e \geq 0$. Since $A(x)B(x) = 0$ we have $a_db_e = 0$. This implies that R is not an integral domain.

Q5. Prove that $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

Solution 5: Closure under subtraction and multiplication is easy to check. Since 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.

Q6. Let G be a (multiplicative) group, and H, K subgroups of G. Prove that $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Solution 6: [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 $K \subseteq H$.

Q7. Let G be the set of all points on the hyperbola $xy = 1$ along with the point $(0, \infty)$ at infinity. Define the operation:

$$\left(a, \frac{1}{a}\right) + \left(b, \frac{1}{b}\right) = \left(a + b, \frac{1}{a + b}\right)$$

Prove that G is an abelian group under this operation.

Solution 7: (a) Closure: For any $a, b \in \mathbb{R}$, either $a + b \neq 0$ and $\left(a + b, \frac{1}{a+b}\right) \in G$, or $a + b = 0$ and the result is $(0, \infty) \in G$. Hence G is closed under the operation.

(b) Associativity: Using the definition of the operation and the associativity of real addition, we have

$$\left(\left(a,\frac{1}{a}\right)+\left(b,\frac{1}{b}\right)\right)+\left(c,\frac{1}{c}\right)=\left(a+b+c,\frac{1}{a+b+c}\right)=\left(a,\frac{1}{a}\right)+\left(\left(b,\frac{1}{b}\right)+\left(c,\frac{1}{c}\right)\right).$$

If $a+b+c=0$, then both sides equal $(0,\infty)$. Thus associativity holds.

(c) Identity: The element $e=(0,\infty)$ serves as the identity, since

$$\left(a,\frac{1}{a}\right)+e=\left(a+0,\frac{1}{a+0}\right)=\left(a,\frac{1}{a}\right)$$

and similarly $e+\left(a,\frac{1}{a}\right)=\left(a,\frac{1}{a}\right)$.

(d) Inverse: The inverse of $\left(a,\frac{1}{a}\right)$ is $\left(-a,-\frac{1}{a}\right)$ because

$$\left(a,\frac{1}{a}\right)+\left(-a,-\frac{1}{a}\right)=(0,\infty)=e.$$

(e) Commutativity: Since real addition is commutative,

$$\left(a,\frac{1}{a}\right)+\left(b,\frac{1}{b}\right)=\left(a+b,\frac{1}{a+b}\right)=\left(b+a,\frac{1}{b+a}\right)=\left(b,\frac{1}{b}\right)+\left(a,\frac{1}{a}\right).$$

Thus the operation is commutative.

Hence, G is an abelian group under the given operation.

Q8. Define an operation 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 8: [Closure] since for (a,b), $(c,d)\in\mathbb{R}^*\times\mathbb{R}$ we have ($(a,b)\circ(c,d)=(ac,bc+d)$ with $ac\in\mathbb{R}^*$ and $bc+d\in\mathbb{R}$.

[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 $(2,3)\circ(1,2)=(2,5)$. Hence $(G,\circ)$ is non-abelian.
