7 Tutorial 7 – November 14th, 2017

7.1 Find all invertible elements in $(\mathbb{Z}_{13}, \cdot, 1)$. For every invertible element a find its inverse a^{-1}.

Solution. Since 13 is a prime number, every non-zero element of $\mathbb{Z}_{13}$ is invertible. Hence the set of invertible elements is

$$\mathbb{Z}_{13} \setminus \{0\} = \{1, 2, \ldots, 12\}.$$

We have $1^{-1} = 1$ and $12^{-1} = (-1)^{-1} = -1 = 12$. To calculate 2^{-1} we can either guess for which $x \in \mathbb{Z}_{13} \setminus \{0\}$ we have $2\,x = 1$ (in $(\mathbb{Z}_{13}, \cdot, 1)$). Or we can rewrite $2\,x = 1$ in $(\mathbb{Z}_{13}, \cdot, 1)$ to $2\,x \equiv 1 \pmod{13}$ which leads to the following Diophantic equation:

$$2\,x + 13\,y = 1.$$

The equation has the following solution: $x = 7$ ($y = -1$). So $2^{-1} = 7$ and $7^{-1} = 2$.

Similarly, we get $3^{-1} = 9$, so $9^{-1} = 3$; $4^{-1} = 10$, so $10^{-1} = 4$; $5^{-1} = 8$, so $8^{-1} = 5$; and $6^{-1} = 11$, so $11^{-1} = 6$.

7.2 Given the monoid $(\mathbb{Z}_{15}, \cdot, 1)$. Find all its invertible elements and their corresponding inverses.

7.3 On the set of all real numbers $\mathbb{R}$ we define an operation $\circ$ by

$$x \circ y = \frac{x + y}{2}.$$

Decide whether $(\mathbb{R}, \circ)$ forms a semigroup.

Solution. $(\mathbb{R}, \circ)$ is not a semigroup; indeed, $(a \circ b) \circ c = a \circ (b \circ c)$ if and only if $a = c$, e.g. $2 \circ (6 \circ 3) \neq (2 \circ 6) \circ 3$.

7.4 Given a non empty set A. Define an operation $\circ$ on A by

$$x \circ y = x \quad \text{for every } x, y \in A.$$

Decide whether $(A, \circ)$ is a semigroup and whether it has a neutral element.

Solution. First we prove that $(A, \circ)$ is a semigroup: Take any $x, y, z \in A$, then $x \circ (y \circ z) = x$ (indeed, the result is always the first element). On the other hand, $(x \circ y) \circ z = x \circ z = x$. Hence, $x \circ (y \circ z) = (x \circ y) \circ z$ for every $x, y, z \in A$.

If $e \in A$ is its neutral element then $x \circ e = x = e \circ x$ for every $x \in A$. The first equation holds for any $e \in A$; indeed, $x \circ e = x$. Hence, if A has more than two elements then $(A, \circ)$ has at least two "right neutral elements", so it cannot have a neutral element.

Note, that you can get the same result from the following observation: $e \circ x = e$, hence $e \circ x = x$ if and only if $e = x$ for every $x \in A$. So, A must contain only one element which is e, the neutral element.

7.5 Given a non empty set U. Consider the set $\mathcal{P}(U)$ of all its subsets. On $A = \mathcal{P}(U)$ define two binary operations: intersection $\cap$ and union $\cup$. Decide whether $(A, \cap)$ and $(A, \cup)$ form semigroups, and whether they have a neutral element.

7.6 On the set $\mathbb{Z} \times \mathbb{Z}$ of all ordered pair of integers an operation $\circ$ is given by

$$(u, v) \circ (x, y) = (u + x, v \cdot y).$$

Decide whether $(\mathbb{Z} \times \mathbb{Z}, \circ)$ is a semigroup, whether it has a neutral element. If it is a monoid find all its invertible elements.

Solution. First we prove that $(\mathbb{Z}\times\mathbb{Z}, \circ)$ satisfies the associative law. Take any $(u, v), (x, y), (a, b) \in \mathbb{Z}\times\mathbb{Z}$. Then $(u, v)\circ((x, y)\circ(a, b)) = (u, v)\circ(x+a, y\cdot b) = (u+(x+a), v\cdot(y\cdot b)) = (u+x+a, vyb)$.

On the other hand, $((u, v) \circ (x, y)) \circ (a, b) = (u + x, v \cdot y) \circ (a, b) = ((u + x) + a, (v \cdot y) \cdot b) = (u + x + a, vyb)$. So the associativity law holds.

If $(\mathbb{Z} \times \mathbb{Z}, \circ)$ has its neutral element (e, f) then for every $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ it must hold

$$(u, v) \circ (e, f) = (u, v) = (e, f) \circ (u, v).$$

The left hand side is $(u+e, v\cdot f)$, the right hand side equals $(e+u, f\cdot v)$. So the only conditions (e, f) must satisfy are: $u + e = u$, $v \cdot f = v$ for every $u, v \in \mathbb{Z}$. Therefore, e must be 0, and f must be 1. We have shown that $(0, 1)$ is the neutral element of $(\mathbb{Z} \times \mathbb{Z}, \circ)$.

An element $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ is invertible if and only if there exists $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$(u, v) \circ (x, y) = (0, 1) = (x, y) \circ (u, v).$$

Hence, $u+x = 0$, and $v\cdot y = 1$ The first identity gives $x = -u$, the second identity immediately implies that $v \neq 0$. But since $\frac{1}{v}$ must be an integer, v is either 1 or -1. Let us summarize: invertible elements are $(u, 1), (u, -1)$ for an arbitrary integer u. Moreover, $(u, 1)^{-1} = (-u, 1)$, and $(u, -1)^{-1} = (-u, -1)$.

7.7 On the set $A = \mathbb{Q} \setminus \{0\}$ an operation $\star$ is given by

$$x \star y = \frac{1}{3}xy.$$

Show that $(A, \star)$ is a group.

7.8 For the group $(A, \star)$ from the exercise 7.5, decide whether the subset B forms a subsemigroup, a submonid, and a subgroup of the group $(A, \star)$ where

1. $B = \{3k\,;\, k \in \mathbb{Z}\}$,
2. $B = \{x\,;\, x \in \mathbb{Q}, x > 0\}$.

Solution. 1) To verify that $\star$ is a binary operation on B it suffices to show that $3k\star 3l$ belongs to B for any $3k, 3l \in B$. We have $3k \star 3l = \frac{1}{3}3k\,3l = 3\,kl$ and therefore belongs to B. Hence B forms a subsemigroup of $(A, \star)$.

Since $3 \in B$ (indeed, $3 = 3 \cdot 1$), B forms a submonoid of $(A, \star)$.

The set B forms a subgroup of $(A, \star)$ if and only if the inverse $(3k)^{-1}$ belongs to B for any element $3k \in B$. From the exercise 7.5 we know that $(3k)^{-1} = \frac{9}{3k}$. It is clear that not for every $k \in Z$ we have $\frac{9}{3k} \in B$. Indeed, for 6 we have $\frac{9}{6}$ is not an integer divisible by 3, hence 6^{-1} does not belong to B. We have shown that B does not form a subgroup of $(A, \star)$.

2) For two positive rational numbers x, y it holds that $\frac{1}{3}\,xy$ is again a positive rational number. Hence, B forms a subsemigroup of $(A, \star)$. Moreover, 3 is a positive rational number, hence B forms a submonoid of $(A, \star)$.

For every rational number $x > 0$ the number $x^{-1} = \frac{9}{x}$ is again a positive rational number. Hence B forms a subgroup of $(A, \star)$.

Answers

7.2 There are $\phi(15)$ invertible elements in $(\mathbb{Z}_{15}, \cdot, 1)$. Moreover, $\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$. These are

$$\{1, 2, 4, 7, 8, 11, 13, 14\}.$$

We have $1^{-1} = 1$, $2^{-1} = 8$, $4^{-1} = 4$, $7^{-1} = 13$, $8^{-1} = 2$, $11^{-1} = 11$, $13^{-1} = 7$, and $14^{-1} = 14$.

7.5 $(\mathcal{P}(U), \cap)$ and $(\mathcal{P}(U), \cup)$ are semigroups. The neutral element of $(\mathcal{P}(U), \cap)$ is U, the neutral element of $(\mathcal{P}(U), \cup)$ is $\emptyset$.

7.7 It is a semigroup with its neutral element $e = 3$. Moreover, every $x \in \mathbb{Q} \setminus \{0\}$ is invertible and $x^{-1} = \frac{9}{x}$ for every x.