

**Exercise 1.** We have

$$\begin{aligned}
 l &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & r &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & s &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\
 e = s \circ s &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & t = l \circ s &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & u = s \circ l &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.
 \end{aligned}$$

a) Cayley table.

$\circ$	$e$	$l$	$r$	$s$	$t$	$u$
$e$	$e$	$l$	$r$	$s$	$t$	$u$
$l$	$l$	$r$	$e$	$t$	$u$	$s$
$r$	$r$	$e$	$l$	$u$	$s$	$t$
$s$	$s$	$u$	$t$	$e$	$r$	$l$
$t$	$t$	$s$	$u$	$l$	$e$	$r$
$u$	$u$	$t$	$s$	$r$	$l$	$e$

b) Not commutative, the table would have to be symmetrical alongside the main diagonal. For example  $l \circ s \neq s \circ l$ .

There is a neutral element, the identity permutation  $e$ .

Each element has an inverse since every row and every column of the table contains  $e$ . (Meaning that for each element, there exists another which „turns it“ into  $e$ .)

c) Semigroup because function composition is associative. (We have  $a \circ (b \circ c) = (a \circ b) \circ c$ , see discrete structures notes.)

Monoid because there is a neutral element.

Group because each element has an inverse.

Not an abelian group, ring, etc. because it is not commutative.

**Exercise 2.** To show that  $(\mathcal{P}(X), \Delta)$  is an abelian group we show that it

a) is associative by showing  $x \Delta (y \Delta z) = (x \Delta y) \Delta z$ .

The expression  $a \in x \Delta y$  tells us that  $a$  is either in  $x$  or  $y$ , but not in both of them. The expression  $p = u \oplus v$  tells us that  $p$  is true if either  $u$  or  $v$  is true, but not both of them. The truth value of  $a \in x \Delta y$  is thus equal to  $a \in x \oplus a \in y$ .

Assume that  $a \in x \Delta (y \Delta z)$ . We can transform this to

$$\begin{aligned} a \in x \Delta (y \Delta z) &\iff a \in x \oplus (a \in y \Delta z) \\ &\iff a \in x \oplus (a \in y \oplus a \in z) \iff a \in x \oplus a \in y \oplus a \in z. \end{aligned}$$

Assume that  $a \in (x \Delta y) \Delta z$ . We can transform this to

$$\begin{aligned} a \in (x \Delta y) \Delta z &\iff (a \in x \Delta y) \oplus a \in z \\ &\iff (a \in x \oplus a \in y) \oplus a \in z \iff a \in x \oplus a \in y \oplus a \in z. \end{aligned}$$

The above transformations depends on  $\oplus$  being associative. This is true as shown by the following table

$x$	$y$	$z$	$y \oplus z$	$x \oplus y$	$x \oplus (y \oplus z)$	$(x \oplus y) \oplus z$
0	0	0	0	0	0	0
0	0	1	1	0	1	1
0	1	0	1	1	1	1
0	1	1	0	1	0	0
1	0	0	0	1	1	1
1	0	1	1	1	0	0
1	1	0	1	0	0	0
1	1	1	0	0	1	1

We have thus shown that  $a \in x \Delta (y \Delta z) \iff a \in (x \Delta y) \Delta z$  which is equivalent to  $x \Delta (y \Delta z) = (x \Delta y) \Delta z$ .

b) contains a neutral element by showing that there exists an  $e \in \mathcal{P}(X)$  such that  $e \Delta x = x = x \Delta e$  for arbitrary  $x \in \mathcal{P}(X)$ .

Consider that  $x \Delta e = (x \setminus e) \cup (e \setminus x)$ . Choose  $e = \emptyset$ . We now have

$$\begin{aligned} x \Delta e &= (x \setminus \emptyset) \cup (\emptyset \setminus x) = x \quad \text{and} \\ e \Delta x &= (\emptyset \setminus x) \cup (x \setminus \emptyset) = x \end{aligned}$$

since  $x \setminus \emptyset = x$ ,  $\emptyset \setminus x = \emptyset$  and  $x \cup \emptyset = \emptyset \cup x = x$ .

This assertion depends on  $\cup$  being commutative. Consider two sets  $X$  and  $Y$  and an  $a \in X \cup Y$ . We know that  $a \in X$  and/or  $a \in Y$ . Thus  $a \in Y \cup X$ . If  $a \notin X \cup Y$  then  $a$  is neither in  $X$  nor  $Y$ , it is thus also not in  $Y \cup X$ .

c) contains an inverse for each element by showing that for each  $x \in \mathcal{P}(X)$  there exists an  $x^{-1} \in \mathcal{P}(X)$  such that  $x \Delta x^{-1} = x^{-1} \Delta x = \emptyset$ .

Consider again that  $x \Delta e = (x \setminus e) \cup (e \setminus x)$ . Choose  $x^{-1} = x$ . We now have

$$x^{-1} \Delta x = x \Delta x^{-1} = (x \setminus x) \cup (x \setminus x) = \emptyset$$

since  $x \setminus x = \emptyset$ .

d) is commutative by showing that  $x \Delta y = y \Delta x$  holds for arbitrary  $x, y \in \mathcal{P}(X)$ . We have

$$\begin{aligned} x \Delta y &= y \Delta x \\ (x \setminus y) \cup (y \setminus x) &= (y \setminus x) \cup (x \setminus y) \end{aligned}$$

which holds since  $\cup$  is commutative.

**Exercise 3**

- a) To show  $x^{-1^{-1}} = x$  consider that, by definition,  $x \circ x^{-1} = e$  and that  $x^{-1} \circ x^{-1^{-1}} = e$ . Thus we have  $x \circ x^{-1} = x^{-1} \circ x^{-1^{-1}}$  and further  $x^{-1^{-1}} = x$ .
- b) To show that  $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$  consider that  $x \circ x^{-1} = e$  and  $y \circ y^{-1} = e$ . We have that

$$\begin{aligned}e &= x \circ x^{-1} \\e &= x \circ e \circ x^{-1} \\e &= x \circ y \circ y^{-1} \circ x^{-1} \\(x \circ y)^{-1} &= y^{-1} \circ x^{-1}.\end{aligned}$$

**Exercise 4** Assuming that  $(\mathcal{P}(X), \cup, \cap)$  is a ring,  $(\mathcal{P}(X), \cup)$  has to be an abelian group and therefore each element  $x \in (\mathcal{P}(X))$  has to have an inverse  $y$  such that  $x \cup y = e$  where  $e$  is the neutral element.

The neutral element of  $(\mathcal{P}(X), \cup)$  is  $\emptyset$  since  $\emptyset \cup x = x \cup \emptyset = x$ . Consider that, for arbitrary sets  $X$  and  $Y$ ,  $|X| \leq |X \cup Y| \geq |Y|$ . Since  $|\emptyset| = 0$ , the cardinality of  $x \cup y$  has to be zero if  $x \cup y = e$ . Thus  $(\mathcal{P}(X), \cup)$  only contains an inverse for every  $x \in \mathcal{P}(X)$  if  $X = \emptyset$ . P(S) It now remains to be shown that  $(\mathcal{P}(\emptyset), \cup, \cap)$  is a ring. We have  $x, y, z \in \mathcal{P}(\emptyset)$ ,  $x = y = z = \emptyset$  and will show that,

a)  $(\mathcal{P}(\emptyset), \cup)$  is associative by showing that we have

$$\begin{aligned} x \cup (y \cup z) &= (x \cup y) \cup z \\ \emptyset \cup (\emptyset \cup \emptyset) &= (\emptyset \cup \emptyset) \cup \emptyset \end{aligned}$$

b)  $(\mathcal{P}(\emptyset), \cup)$  contains a neutral element. Already shown for arbitrary  $X$ .

c)  $(\mathcal{P}(\emptyset), \cup)$  is commutative by

$$\begin{aligned} x \cup y &= y \cup x \\ \emptyset \cup \emptyset &= \emptyset \cup \emptyset. \end{aligned}$$

d)  $(\mathcal{P}(\emptyset), \cap)$  is associative by

$$\begin{aligned} x \cap (y \cap z) &= (x \cap y) \cap z \\ \emptyset \cap (\emptyset \cap \emptyset) &= (\emptyset \cap \emptyset) \cap \emptyset. \end{aligned}$$

e) The distributive law,

$$\begin{aligned} x \cap (y \cup z) &= x \cap y \cup x \cap z \\ \emptyset \cap (\emptyset \cup \emptyset) &= \emptyset \cap \emptyset \cup \emptyset \cap \emptyset \end{aligned}$$

holds.

**Exercise 5** To show that  $(\mathcal{P}(X), \Delta, \cap)$  is a commutative ring we will show that

- a)  $(\mathcal{P}(X), \Delta)$  is an abelian group. This was done as part of exercise 2.
- b)  $(\mathcal{P}(X), \cap)$  is a monoid. We will assume associativity and thus only show that it contains a neutral element  $e$  such that  $e \cap x = x = x \cap e$ .

Assume  $e = x$ , we now have  $e \cap x = x \cap x = x \cap e = x$ .

- c)  $(\mathcal{P}(X), \cap)$  is commutative by showing that  $x \cap y = y \cap x$ .

Consider  $a \in x \cap y$ , we know  $a \in x$  and  $a \in y$  thus  $a \in y \cap x$ .

Consider  $a \notin x \cap y$ , we know  $a \notin x$  and  $a \notin y$  thus  $a \notin y \cap x$ .

- d) the distributive law,  $x \cap (y \Delta z) = x \cap y \Delta x \cap z$ , holds.

Consider  $a \in x \cap (y \Delta z)$ . We know that  $a \in x$  and  $a$  in either  $z$  or  $y$  but not both. Thus  $a \in x \cap y$  or  $a \in x \cap z$ , but not both. Thus  $a \in x \cap y \Delta x \cap z$ .

Consider  $a \in x \cap y \Delta x \cap z$ . We know that  $a$  is either in  $x$  and  $y$  or in  $x$  and  $z$ . It is thus definitely in  $x$  and in either  $y$  or  $z$  but not in both. Thus  $a \in x \cap (y \Delta z)$ .

**Exercise 6**

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

We know that  $(\mathbb{Z}_4, +, \cdot)$  is a ring. For it to be a commutative ring  $(\mathbb{Z}_4, \cdot)$  has to be commutative. This is given since the respective table is symmetrical alongside the main diagonal.

According to axiom 1.20 it is not a field since 4 is not prime. (It states that  $\mathbb{Z}_p$  is a field if and only if  $p$  is prime.) Concretely, there doesn't exist an inverse for every element  $(0, 2)$ .

**Exercise 7** We have

$$\begin{aligned} f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix} & g &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} & g^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \\ h &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} & x &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} \end{aligned}$$



**Exercise 8**

$$14x + 6^8 = 10$$

$$14x + 18 = 10$$

$$14x = 15$$

$$x = 14^{-1} \cdot 15$$