Mathematics for Machine Learning

TECHNISCHE UNIVERSITÄT DARMSTADT

Solution of the Exercises

Stefan Thaut (1800351)
Department 20 - Computer Science
May 6, 2019

Solution 2 Linear Algebra

Solution 2.1

Solution 2.1.1

1. We have to show, that $\mathbb{R} \setminus \{-1\}$ is closed under $*$, the associativity, the existence of a neutral and inverse elements and the commutativity.
   For the closure of $\mathbb{R} \setminus \{-1\}$ we can use the closure of the addition and multiplication in $\mathbb{R}$. Then we have to show that there are no a and b in $\mathbb{R} \setminus \{-1\}$, so that $a * b = -1$.

   Assuming that $\exists a, b \in \mathbb{R} \setminus \{-1\}$ with $a * b = -1$. Then it is

$$\begin{aligned} & a * b = ab + a + b = -1 \\ \iff \quad & ab + a = -1 - b \\ \iff \quad & a(b+1) = -(b+1) \\ \iff \quad & a = -\frac{b+1}{b+1} = -1 \end{aligned}$$

   So we got a contradiction and that shows that there are no $a, b \in \mathbb{R} \setminus \{-1\}$ so that $a * b = -1$.
   Consider $a, b, c \in \mathbb{R} \setminus \{-1\}$. Then it is

$$\begin{aligned} (a * b) * c &= (ab + a + b) * c \\ &= (ab + a + b)c + (ab + a + b) + c \\ &= abc + ac + bc + ab + a + b + c \\ &= abc + ab + ac + a + bc + b + c \\ &= a(bc + b + c) + a + (bc + b + c) \\ &= a * (bc + b + c) = a * (b * c) \end{aligned}$$

   That shows the associativity of $*$.

The neutral element is 0, because:

$$a * 0 = a \cdot 0 + a + 0 = 0 + a + 0 = a \text{ and}$$
$$0 * a = 0 \cdot a + 0 + a = 0 + 0 + a = a$$

for any $a \in \mathbb{R} \setminus \{-1\}$.
Consider $a^{-1} = -a/(a+1)$. Then it is

$$\begin{aligned} a * a^{-1} &= a * -\frac{a}{a+1} \\ &= a(-\frac{a}{a+1}) + a + (-\frac{a}{a+1}) \\ &= \frac{-a^2}{a+1} + a - \frac{a}{a+1} \\ &= \frac{-a^2 - a}{a+1} + \frac{a(a+1)}{a+1} \\ &= \frac{-a^2 - a}{a+1} + \frac{a^2 + a}{a+1} = 0 \end{aligned}$$

The proof of $a^{-1} * a = 0$ works analogously.
The proof of the commutativity is straight forward and based on the commutativity of the addition and multiplication in $\mathbb{R}$. Consider $a, b \in \mathbb{R} \setminus \{-1\}$. Then it is

$$a * b = ab + a + b = ba + b + a = b * a$$

So we have shown all axioms of an Abelian group. □

2. It is

$$\begin{aligned} 3 * x * x &= (3x + 3 + x) * x \\ &= (4x + 3) * x \\ &= (4x + 3)x + (4x + 3) + x \\ &= 4x^2 + 3x + 4x + 3 + x = 4x^2 + 8x + 3 \end{aligned}$$

We can now solve the quadtratic formula $4x^2 + 8x + 3 = 15 \iff 4x^2 + 8x - 12 = 0$ using the completing the square method proposed by HOEHN in [1]:

$$\begin{aligned} x &= \frac{-8 \pm \sqrt{8^2 - 4 \cdot 4 \cdot (-12)}}{2 \cdot 4} \\ &= \frac{-8 \pm \sqrt{64 + 192}}{8} \\ &= \frac{-8 \pm \sqrt{256}}{8} \\ &= \frac{-8 \pm 16}{8} = -1 \pm 2 \end{aligned}$$

Thus the solution of the equation is $x_1 = -3$ and $x_2 = 1$.

Solution 2.1.2

1. At first we have to be careful, because $(\mathbb{Z}_n, \oplus)$ would not be a group with the unmodified given mapping, because $\mathbb{Z}_n$ would not be closed under $\oplus$: Let $n = 3$, then $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. So consider $\overline{1}, \overline{2} \in \mathbb{Z}_3$, then:

$$\overline{1} \oplus \overline{2} = \overline{1 + 2} = \overline{3} \notin \mathbb{Z}_3$$

Thus we have to modify the mapping by adding a modulo to the addition:

$$\overline{a} \oplus \overline{b} = \overline{a + b \mod n} \tag{1}$$

Now $\mathbb{Z}_n$ is closed under $\oplus$.

(Associativity) Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$. Then it is

$$\begin{aligned}(\overline{a} \oplus \overline{b}) \oplus \overline{c} &= \overline{a + b \mod n} \oplus \overline{c} \\ &= \overline{(a+b \mod n) + c \mod n} \\ &= \overline{a+b+c \mod n} \\ &= \overline{a \mod n + (b + c \mod n)} \\ &= \overline{a} \oplus \overline{b + c \mod n} = \overline{a} \oplus (\overline{b} \oplus \overline{c})\end{aligned}$$

(Neutral Element) The neutral element is $\overline{0} \in \mathbb{Z}_n$. Let $\overline{a} \in \mathbb{Z}_n$, then it is:

$$\overline{a} \oplus \overline{0} = \overline{a + 0 \mod n} = \overline{a \mod n} = \overline{a}$$

and

$$\overline{0} \oplus \overline{a} = \overline{0 + a \mod n} = \overline{a \mod n} = \overline{a}$$

(Inverse Element) Let $\overline{a} \in \mathbb{Z}_n$. Then the inverse element of $\overline{a}$ is $\overline{a}^{-1} = \overline{n-a}$. It is

$$\begin{aligned}\overline{a} \oplus \overline{a}^{-1} &= \overline{a} \oplus \overline{n-a} \\ &= \overline{a + (n-a) \mod n} \\ &= \overline{n \mod n} = \overline{0}\end{aligned}$$

The proof of $\overline{a}^{-1} \oplus \overline{a}$ works analogously.

(Commutativity) For the proof of the commutativity in $\mathbb{Z}_n$ we use the commutativity of the addition in $\mathbb{Z}$. Let $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Then it is

$$\overline{a} \oplus \overline{b} = \overline{a + b \mod n} = \overline{b + a \mod n} = \overline{b} \oplus \overline{a}$$

We have shown, that $(\mathbb{Z}_n, \oplus)$ is an Abelian Group. □

2. Firstly we also have to modify the mapping for mathematical correctness:

$$\overline{a} \otimes \overline{b} = \overline{a \cdot b \mod n} \tag{2}$$

In table 1 we can see that for each elements $\overline{a}, \overline{b} \in \mathbb{Z}_5 \setminus \{\overline{0}\}$ the result of $\overline{a} \otimes \overline{b} \in \mathbb{Z}_5 \setminus \{\overline{0}\}$. The neutral element

Table 1: The times table of $\mathbb{Z}_5 \setminus \{\overline{0}\}$ under $\otimes$

$\otimes$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

of this mapping is $\overline{1}$, because $\overline{a} \otimes \overline{1} = \overline{a \cdot 1 \mod 5} = \overline{a}$. We can read the inverse elements of each element in $\mathbb{Z}_5 \setminus \{\overline{0}\}$ out of table 1, where the result is $\overline{1}$. And the commutativity follows directly from the commutativity of the multiplication in $\mathbb{Z}$. □

3. Consider $\overline{4} \in \mathbb{Z}_8 \setminus \{\overline{0}\}$. If we multiply $\overline{4}$ with all elements of $\mathbb{Z}_8 \setminus \{\overline{0}\}$, we get the following results:

$$\begin{array}{llll}\overline{4} \otimes \overline{1} = \overline{4} & \overline{4} \otimes \overline{2} = \overline{0} & \overline{4} \otimes \overline{3} = \overline{4} & \overline{4} \otimes \overline{4} = \overline{0} \\ \overline{4} \otimes \overline{5} = \overline{4} & \overline{4} \otimes \overline{6} = \overline{0} & \overline{4} \otimes \overline{7} = \overline{4} & \end{array}$$

Hence we see, that there is no inverse element of $\overline{4}$ in $\mathbb{Z}_8 \setminus \{\overline{0}\}$. Thus $(\mathbb{Z}_8 \setminus \{\overline{0}\})$ is not a group. □

4. The key point for showing that $(\mathbb{Z}_n \setminus \{\overline{0}\}, \otimes)$ is a group, is to show the existence of an inverse element for each element $\overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\}$.
   Assuming $n \in \mathbb{N} \setminus \{0\}$ is prime. Hence a and n are relatively prime and with that we know from Bézout theorem that there are two integers u and v such that $au + nv = 1$. That implies $\overline{au} \otimes \overline{nv} = \overline{1}$ and also $\overline{a} \otimes \overline{u} = \overline{1}$. Thus the inverse element of $\overline{a}$ is $\overline{u}$.
   Assuming $(\mathbb{Z}_n \setminus \{\overline{0}\}, \otimes)$ is a group. Also assuming n is not prime, i.e. $\exists k, l \in \mathbb{N}$ such that $1 < k, l < n$ and $n = kl$. We see that $\overline{k}, \overline{l} \in \mathbb{Z}_n \setminus \{\overline{0}\}$. But it is $\overline{k} \otimes \overline{l} = \overline{k \cdot l \mod n} = \overline{n \mod n} = \overline{0} \notin \mathbb{Z}_n \setminus \{\overline{0}\}$. Hence $\mathbb{Z}_n \setminus \{\overline{0}\}$ would not be closed under $\otimes$ and would therefore be no group. Thus n has to be prime. $\square$

References

[1] Larry Hoehn. A more elegant method of deriving the quadratic formula. *Mathematics Teacher*, 68(5):442–443, 1975.