13. Let A and B be two sets and let $f\colon A \to B$ be an invertible function. Show that there exists a unique $g\colon B \to A$ that satisfies

$$g \circ f = \mathrm{Id}_A \quad \text{and} \quad f \circ g = \mathrm{Id}_B \,.$$

Solution:
We prove this exercise by contradiction. Let us assume that there exist two distinct functions g_1 and g_2 satisfying

$$g_1 \circ f = \mathrm{Id}_A, \quad f \circ g_1 = \mathrm{Id}_B,$$

and

$$g_2 \circ f = \mathrm{Id}_A, \quad f \circ g_2 = \mathrm{Id}_B \,.$$

Hence, for each $a \in A$ and each $b \in B$, we have

$$g_1(f(a)) = \mathrm{Id}_A(a) = a, \quad f(g_1(b)) = \mathrm{Id}_B(b) = b,$$

and

$$g_2(f(a)) = \mathrm{Id}_A(a) = a, \quad f(g_2(b)) = \mathrm{Id}_B(b) = b.$$

From above, and the fact that f is bijective, we get $g_1 = g_2$, which is in contradiction with the assumption $g_1 \neq g_2$. Therefore, g is unique. $\square$

14. Let $h\colon \mathbb{N} \to \mathbb{R}$ be defined by

$$h(1) = 2$$
$$h(n+1) = \sqrt{3 + 3h(n)}.$$

Prove by induction that $\forall n \in \mathbb{N}\colon h(n) < 4$.

Solution:
Induction basis: For $n = 1$, we have $h(1) = 2 < 4$.

Induction step: We assume that $h(n) < 4$ is true, for some $n \in \mathbb{N}$. We want to prove $h(n+1) < 4$ is true.
We have $h(n+1) = \sqrt{3 + 3h(n)}$. Since the square root is an increasing function (A function h is called an increasing on the interval I if for all $x, y \in I$ such as $x \leq y$, one has $h(x) \leq h(y)$), and by using the induction hypothesis, we find that

$$h(n+1) = \sqrt{3 + 3h(n)} < \sqrt{3 + 3 \cdot 4} = \sqrt{15} < 4.$$

We concluded the proof as we showed both the induction basis and induction step.
$\square$

15. Prove by induction that for each $n \in \mathbb{N} \setminus \{1, 2\}$ we have $2n + 1 < 2^n$.

Solution:
Induction basis: For $n = 3$, we have $2 \cdot 3 + 1 = 7 < 2^3 = 8$.

Induction step: We assume that $2n + 1 < 2^n$ is true for some $n \in \mathbb{N} \setminus \{1, 2\}$. We want to show that $2(n + 1) + 1 < 2^{n+1}$. We observe that

$$2(n + 1) + 1 < 2(n + 1) + 2n = 4n + 2 = 2(2n + 1) < 2 \cdot (2^n) = 2^{n+1}.$$

Where we used the fact that $n \geq 3$ (for the first inequality) and the induction hypothesis $2n + 1 < 2^n$ (for the last inequality). We concluded the proof as we showed both the induction basis and induction step. $\square$

16. Let $\mathbb{F} = (F; \{+, \cdot\})$ be a field (cf. Definition 1.22). Prove that

    (a) $\forall x \in F \colon x = x + x \Rightarrow x = 0$.

    (b) $\forall x \in F \colon x \cdot 0 = 0 \cdot x = 0$.

    (c) $\forall x, y \in F \colon x \cdot y = 0 \Rightarrow x = 0$ or $y = 0$.

    Note that you are allowed to use (16a) to prove (16b), and that your are allowed to use (16a) and (16b) to prove (16c).

    Solution:
    We first prove (16a). Let $x \in F$ with $x = x + x$. We want to show that $x = 0$. Let $y \in F$ be such that $x + y = y + x = 0$. (cf. Axiom inverse (i)). Then $x = x + x$ implies that

    $$0 = y + x = y + (x + x) = (y + x) + x = 0 + x = x,$$

    and therefore, $0 = x$.

    Next, we show (16b). Let $x \in F$. Then we have that

    $$x \cdot 0 = x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0);$$

    where the last equality follows from the distributivity property. Thus, $x \cdot 0 = (x \cdot 0) + (x \cdot 0)$, and therefore, by (16a) we have that $x \cdot 0 = 0$. The missing equality follows from the commutativity axiom.

    Finally, we want to prove (16c). Let $x, y \in F$ and let us assume that $x \cdot y = 0$ and $x \neq 0$. We will show that $y = 0$. By Axiom inverse (ii) there exists $z \in F$ such that $z \cdot x = 1$. Thus,

    $$0 = z \cdot 0 = z \cdot (x \cdot y) = (z \cdot x) \cdot y = 1 \cdot y = y.$$

    Note that the first identity follows from (16b), the second identity from the assumption $x \cdot y = 0$, the third identity follows from the associativity axiom, the last one follows from the axiom of the neutral element. $\square$

17. Let $A := \mathbb{R}\times\mathbb{R}$ and let $\star\colon A^2 \to A$ be defined as follows: For all $((x,y),(z,w)) \in A^2$

$$\star((x,y),(z,w)) = (xz - yw, xw + yz).$$

(a) Prove that $\star$ is associative and commutative;

(b) prove that for each $(x,y) \in A$ we have $\star((x,y),(1,0)) = (x,y)$;

(c) prove that for each $(a,b) \in A \setminus \{(0,0)\}$ there exists $(x,y) \in A$ such that

$$\star((a,b),(x,y)) = (1,0).$$

Solution:
For simplicity, We write that $\star((x,y),(z,w)) = (x,y) \star (z,w)$.

(a) **Commutativity:** Let $x,y,z,w \in \mathbb{R}$, then

$$(x,y) \star (z,w) = (xz - yw, xw + yz) = (zx - wy, zy + wx) = (z,w) \star (x,y).$$

Where we used the fact that the multiplication is commutative.

Associativity: Let $x,y,z,w,a,b \in \mathbb{R}$, then

$$\begin{aligned}
&((x,y) \star (z,w)) \star (a,b) = \\
&((xz - yw, xw + yz) \star (a,b) = \\
&(xza - ywa - xwb - yzb, xzb - ywb + xwa - yza) = \\
&(xza - xwb - yzb - ywa, xzb + xwa + yza - ywb) = \\
&(x(za - wb) - y(zb - wa), x(zb + wa) + y(za - wb)) = \\
&(x,y) \star (za - wb, zb + wa) = \\
&(x,y) \star ((z,w) \star (a,b)).
\end{aligned}$$

Above, we used the properties of multiplication, addition, and subtraction.

(b) **Identity:** Let $x,y \in \mathbb{R}$, it is easy to find that $(x,y) \star (1,0) = (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) = (x,y)$. Again, we used the properties of the multiplication.

(c) **Inverse:** Let $(a,b) \in A \setminus \{(0,0)\}$. We let $x := \frac{a}{a^2+b^2}$ and $y := \frac{-b}{a^2+b^2}$. Then, we have:

$$(a,b) \star (x,y) = \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{-ab}{a^2+b^2} + \frac{ab}{a^2+b^2}\right) = (1,0).$$

That means: for every $(a,b) \in A \setminus \{(0,0)\}$, there exists $(x,y) \in A$ such that $(a,b) \star (x,y) = (1,0)$.

$\square$

18. Let $A \subset \mathbb{R}$ with $A \neq \emptyset$, let $k \in \mathbb{R}$, let $B := \{-a \mid a \in A\}$, and let us assume that $\sup A = k$. Prove that $\inf B = -k$.

Solution:
For the exercise, we need to check

- B is non-empty and a subset of real numbers:
This is directly deduced from the fact that $A \subset \mathbb{R}$ and $A \neq \emptyset$ and from the definition of B.

- B is bounded from below:

$$\sup A = k \overset{Def1.36}{\Rightarrow} \forall a \in A : k \geq a \Rightarrow \forall a \in A : -k \leq -a,$$

which means that $\forall (b = -a) \in B$ we have $-k \leq b$. Thus $-k \in \mathbb{R}$ is a lower bound of B and therefore $\inf B$ exists.

- $\inf B = -k$

$$\begin{aligned}\sup A = k &\overset{Def1.36}{\Rightarrow} (\forall x \in \mathbb{R} : x \geq A \Rightarrow x \geq k) \Rightarrow (\forall a \in A, \forall x \in \mathbb{R} : x \geq a \Rightarrow x \geq k)\\ &\Rightarrow (\forall a \in A, \forall x \in \mathbb{R} : -x \leq -a \Rightarrow -x \leq -k)\\ &\Rightarrow (\forall b \in B, \forall y \in \mathbb{R} : y \leq b \Rightarrow y \leq -k)\\ &\overset{Def1.36}{\Rightarrow} -k = \inf B = \inf(-A).\end{aligned}$$

All implications hold true in the other direction as well, they are equivalences.
Another way: Since $\sup A = k$. Then, by the definition of the supremum for A, we have: for all $\epsilon > 0$ there exists $a \in A$ such that $a > k - \epsilon$. Then, we write $b = -a < -k + \epsilon$. We conclude that for all $\epsilon > 0$ there exists $b \in B$ such that $b < -k + \epsilon$.

□