ULMS055 Mathematics Crammer

Part A: Pure Mathematics (Exercises)

Christian W. Bach

University of Liverpool & EPICENTER Maastricht

Outline

- Exercises
- Solutions

EXERCISES

Exercise I

Let φ, ψ, and χ be propositions.

(I.a) Prove that $\varphi \leftrightarrow \psi$ and $(\varphi \to \psi) \wedge (\psi \to \varphi)$ are logically equivalent.

(I.b) Prove that $\varphi \to \psi$ and $(\neg\varphi) \vee \psi$ are logically equivalent.

(I.c) Prove that $\varphi \to (\psi \to \chi)$ and $(\varphi \to \psi) \to \chi$ are not logically equivalent.

Exercise II

(II.a) Prove that $n^2 \geq 2n + 3$ for all $n \geq 3$.

(II.b) Prove that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ for all $n \geq 0$.

(II.c) Prove that $a_n = 6^{n+2} + 7^{2n+1}$ is divisable by 43 for all $n \geq 0$.

Exercise III

(III.a) Let $A = \{1, 2, 3\}$, $B = \{a, b\}$, and $C = \{a, c\}$. Form the product set $A \times (B \cap C)$.

(III.b) Let A, B, C, and D be sets such that $A \subseteq B$ and $C \subseteq D$. Prove that $A \times C \subseteq B \times D$.

(III.c) Let A, B, and C be sets. Prove that
$A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Exercise IV

(IV.a) Consider the set $\mathbb{Z} = \{\ldots, -3, -2-, 1, 0, 1, 2, 3, \ldots\}$ of integers. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function such that $f(z) = z + 1$ for all $z \in \mathbb{Z}$. Investigate whether f is *injective*, *surjective*, and *bijective*.

(IV.b) Consider the set $\mathbb{Z} = \{\ldots, -3, -2-, 1, 0, 1, 2, 3, \ldots\}$ of integers. Let $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be a function such that $f(z) = (z, z + 1)$ for all $z \in \mathbb{Z}$. Investigate whether f is *injective*, *surjective*, and *bijective*.

(IV.c) Let $f : A \to A$ be a function. Prove that $[f \circ f](A) \subseteq f(A)$.

Exercise V

- Let $\mathbb{F}_2 = \{0, 1\}$ be a set with two elements 0 and 1.

- Let $+ : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$ and $\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$ be functions defined according to the following tables:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- Note that the cells in the tables corresponding to the i-th row and j-th column define $i + j$ and $i \cdot j$, respectively.

- Show that the triple $(\mathbb{F}_2, +, \cdot)$ constitutes a field.

Solutions

Solutions I

(I.a)

φ	ψ	$\varphi \leftrightarrow \psi$	$\varphi \to \psi$	$\psi \to \varphi$	$(\varphi \to \psi) \wedge (\psi \to \varphi)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

(I.b)

φ	ψ	$\varphi \to \psi$	$\neg\varphi$	$(\neg\varphi) \vee \psi$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

(I.c) Let φ be false, ψ be false, and χ be false. Then, $\varphi \to (\psi \to \chi)$ is true, however, $(\varphi \to \psi) \to \chi$ is false.

Solutions II

(II.a)

- Induction basis: Let $n_0 = 3$. Observe that $3^2 = 9 \geq 9 = 2 \cdot 3 + 3$.
- Induction step: Let $n \geq 3$ and suppose that $n^2 \geq 2n + 3$ holds. It needs to be shown that $(n+1)^2 \geq 2n + 5$ also holds.
- Indeed, observe that $(n+1)^2 = n^2 + 2n + 1 \geq 2n + 5$, since $n^2 + 1 > 5$ for all $n \geq 3$.

Solutions II

(II.b)

- Induction basis: Let $n_0 = 0$. Observe that $\sum_{i=0}^{0} 0 = 0$ and $\frac{0\cdot(0+1)}{2} = 0$.
- Induction step: Let $n \geq 0$ and suppose that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ holds. It needs to be shown that $\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$ also holds.
- Indeed, observe that $\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2}$ $= \frac{(n+1)(n+2)}{2}$.

Solutions II

(II.c)

- Induction basis: Let $n_0 = 0$. Observe that $6^{0+2} + 7^{2\cdot 0+1} = 6^2 + 7^1 = 43$ and $43 = 43 \cdot 1$.

- Induction step: Let $n \geq 0$ and suppose that $6^{n+2} + 7^{2n+1}$ is divisible by 43. It needs to be shown that $6^{n+3} + 7^{2n+3}$ is also divisible by 43.

- Indeed, observe that $6^{n+3} + 7^{2n+3} = 6 \cdot 6^{n+2} + 7^2 \cdot 7^{2n+1}$ $= 6 \cdot 6^{n+2} + 49 \cdot 7^{2n+1} = 6 \cdot 6^{n+2} + (43 \cdot 7^{2n+1} + 6 \cdot 7^{2n+1})$ $= (6 \cdot 6^{n+2} + 6 \cdot 7^{2n+1}) + 43 \cdot 7^{2n+1} = 6 \cdot (6^{n+2} + 7^{2n+1}) + 43 \cdot 7^{2n+1}$. As 43 divides $43 \cdot 7^{2n+1}$ and, by the inductive assumption, 43 divides $6^{n+2} + 7^{2n+1}$ and thus $6 \cdot (6^{n+2} + 7^{2n+1})$, it is also the case that 43 divides $6 \cdot (6^{n+2} + 7^{2n+1}) + 43 \cdot 7^{2n+1}$.

Solutions III

(III.a)

- $B \cap C = \{a\}$
- $A \times (B \cap C) = A \times \{a\} = \{(1,a),(2,a),(3,a)\}$

Solutions III

(III.b)

- Let $z \in A \times C$.
- Then, there exists $x \in A$ and $y \in C$ such that $z = (x, y)$.
- As $A \subseteq B$, it is the case that $x \in B$ too.
- As $C \subseteq D$, it is the case that $y \in D$ too.
- Consequently, $z = (x, y) \in B \times D$.

Solutions III

(III.c)

- **First**, it is shown that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.
- Let $u \in A \times (B \cup C)$. Then, there exist $x \in A$ and $y \in B \cup C$ such that $u = (x, y)$.
- Since $y \in B \cup C$, it is the case that $y \in B$ or $y \in C$.
- *Case 1:* if $y \in B$, then $u = (x, y) \in A \times B$ and thus $u \in (A \times B) \cup (A \times C)$.
- *Case 2:* if $y \in C$, then $u = (x, y) \in A \times C$ and thus $u \in (A \times B) \cup (A \times C)$.
- Consequently, $u \in (A \times B) \cup (A \times C)$.
- **Secondly**, it is shown that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.
- Let $v \in (A \times B) \cup (A \times C)$. Then, $v \in A \times B$ or $v \in A \times C$.
- *Case 1:* if $v \in A \times B$, then there exist $s \in A$ and $t \in B$ such that $v = (s, t)$. As $t \in B$ it also holds that $t \in B \cup C$. Hence, $v = (s, t) \in A \times (B \cup C)$.
- *Case 2:* if $v \in A \times C$, then there exist $s' \in A$ and $t' \in C$ such that $v = (s', t')$. As $t' \in C$ it also holds that $t' \in B \cup C$. Hence, $v = (s', t') \in A \times (B \cup C)$.
- Consequently, $v \in A \times (B \cup C)$.

Solutions IV

(IV.a)

- Let $z \in \mathbb{Z}$, and consider $z - 1 \in \mathbb{Z}$. As $f(z-1) = (z-1) + 1 = z$, and z was chosen arbitrarily, the function f is surjective.
- Let $z, z' \in \mathbb{Z}$ such that $f(z) = f(z')$. Then, $z + 1 = z' + 1$, thus $z = z'$, and as z, z' were chosen arbitrarily, the function f is injective.
- As the function f is surjective and injective, it is also bijective.

Solutions IV

(IV.b)

- Note that $(1,1) \in \mathbb{Z} \times \mathbb{Z}$, but there exists no $z \in \mathbb{Z}$ such that $f(z) = (z, z+1) = (1,1)$. Thus, $(1,1) \notin f(\mathbb{Z})$, and the function f is consequently not surjective.

- Let $z, z' \in \mathbb{Z}$ such that $f(z) = f(z')$. Then, $(z, z+1) = (z', z'+1)$, i.e. $z = z'$ and $z + 1 = z' + 1$. As z, z' were chosen arbitrarily, the function f is injective.

- As the function f is not both surjective and injective, it is also not bijective.

Solutions IV

(IV.c)

- Let $a \in [f \circ f](A)$, i.e. there exists $a^* \in A$ such that $[f \circ f](a^*) = a$, i.e. $f\big(f(a^*)\big) = a$.
- Note that $f(a^*) \in A$ and define $a' := f(a^*)$.
- As $a' \in A$ and $f(a') = a$, it is the the case that $a \in f(A)$.

Solutions V

- The tables are both symmetric with regards to the diagonal, thus $i + j = j + i$ as well as $i \cdot j = j \cdot i$ hold for all $i, j \in \mathbb{F}_2$. Consequently, $+$ and $\cdot$ are commutative.

- Since

$$\begin{array}{lll}
0+(0+0)=0=(0+0)+0 & \text{und} & 0\cdot(0\cdot 0)=0=(0\cdot 0)\cdot 0 \\
0+(0+1)=1=(0+0)+1 & \text{und} & 0\cdot(0\cdot 1)=0=(0\cdot 0)\cdot 1 \\
0+(1+0)=1=(0+1)+0 & \text{und} & 0\cdot(1\cdot 0)=0=(0\cdot 1)\cdot 0 \\
0+(1+1)=0=(0+1)+1 & \text{und} & 0\cdot(1\cdot 1)=0=(0\cdot 1)\cdot 1 \\
1+(0+0)=1=(1+0)+0 & \text{und} & 1\cdot(0\cdot 0)=0=(1\cdot 0)\cdot 0 \\
1+(0+1)=0=(1+0)+1 & \text{und} & 1\cdot(0\cdot 1)=0=(1\cdot 0)\cdot 1 \\
1+(1+0)=0=(1+1)+0 & \text{und} & 1\cdot(1\cdot 0)=0=(1\cdot 1)\cdot 0 \\
1+(1+1)=1=(1+1)+1 & \text{und} & 1\cdot(1\cdot 1)=1=(1\cdot 1)\cdot 1.
\end{array}$$

  it follows that $+$ and $\cdot$ are associative.

Solutions V

- Since

$$\begin{array}{lcl} 0\cdot(0+0)=0=0\cdot 0+0\cdot 0 & \text{und} & (0+0)\cdot 0=0=0\cdot 0+0\cdot 0\\ 0\cdot(0+1)=0=0\cdot 0+0\cdot 1 & \text{und} & (0+0)\cdot 1=0=0\cdot 1+0\cdot 1\\ 0\cdot(1+0)=0=0\cdot 1+0\cdot 0 & \text{und} & (0+1)\cdot 0=0=0\cdot 0+1\cdot 0\\ 0\cdot(1+1)=0=0\cdot 1+0\cdot 1 & \text{und} & (0+1)\cdot 1=1=0\cdot 1+1\cdot 1\\ 1\cdot(0+0)=0=1\cdot 0+1\cdot 0 & \text{und} & (1+0)\cdot 0=0=1\cdot 0+0\cdot 0\\ 1\cdot(0+1)=1=1\cdot 0+1\cdot 1 & \text{und} & (1+0)\cdot 1=1=1\cdot 1+0\cdot 1\\ 1\cdot(1+0)=1=1\cdot 1+1\cdot 0 & \text{und} & (1+1)\cdot 0=0=1\cdot 0+1\cdot 0\\ 1\cdot(1+1)=0=1\cdot 1+1\cdot 1 & \text{und} & (1+1)\cdot 1=0=1\cdot 1+1\cdot 1. \end{array}$$

  it follows that the laws of distributivity hold.

- Note that $0+0=0$ and $0+1=1$. Thus, there exists a $+$-netural element which is 0.

- Note that $1\cdot 0=0$ and $1\cdot 1=1$. Thus, there exists a $\cdot$-netural element which is 1.

Solutions V

- It is the case that $0 + 0 = 0$ as well as $1 + 1 = 0$, i.e. 0 is inverse to 0 and 1 is inverse to 1.
- Consequently, every element is $+$-invertible.
- The only element distinct from the $+$-netural element (i.e. 0) is 1 and as $1 \cdot 1 = 1$ holds it follows that 1 is inverse to 1.
- Consequently, every element distinct from the $+$-netural element is $\cdot$-invertible.
- It can now be concluded that the triple $(\mathbb{F}_2, +, \cdot)$ indeed constitutes a **field**.