ULMS055 Mathematics Crammer

Part A: Pure Mathematics

Christian W. Bach

University of Liverpool & EPICENTER Maastricht

UNIVERSITY OF LIVERPOOL

EPICENTER
Research Center for
Epistemic Game Theory

Welcome to the Maths Crammer

- Objective: deepending & extending your knowledge of Mathematics and Statistics.

- The **Maths Crammer** is divided into three parts:
  - **Part A:** Pure Mathematics (taught by: CW Bach)
  - **Part B:** Real Analysis (taught by: RR Routledge)
  - **Part C:** Statistics (taught by: G Liu-Evans)

Set-Up

- ULMS055 is asynchronous and self-study based.
- Ideally, you work through the material before the semester starts.

Organization

- The lecture podcasts for each of the three parts are available on the ULMS055 Canvas page.
- Exercises are also posted on Canvas together with solutions.
- It is crucial that you first attempt the exercises questions by yourself before reading the provided solutions.

Part A: Lecturer

- Lecturer of **Part A**: Christian Bach
- Website: `www.epicenter.name/bach`
- Email: cwbach@liv.ac.uk
- Office hours: Thursdays at ULMS-CR2, 3.30pm-5pm
- Questions or Comments always welcome!

Part A: Program

- Logic
- Proofs
- Product Sets
- Functions
- Fields

Logic

Propositions

- A proposition is a statement that can be true or false.
  - Atomic propositions are non-decomposible statements. *Examples: "It is raining in London",* $\sum_{k=1}^{n}(4k-2)=2n^2$
  - Compound propositions contain logical connectives.
  - Note that propositions in general are typically denoted by greek letters (e.g. $\varphi, \psi, \ldots$), while atomic propositions are typically denoted by roman letters (e.g. $P, Q, \ldots$).

- Logical connectives: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
  - If φ is a proposition, then $\neg\varphi$ is a proposition.
  - If φ and ψ are propositions, then $\varphi \wedge \psi$ is a proposition.
  - If φ and ψ are propositions, then $\varphi \vee \psi$ is a proposition .
  - If φ and ψ are propositions, then $\varphi \rightarrow \psi$ is a proposition .
  - If φ and ψ are propositions, then $\varphi \leftrightarrow \psi$ is a proposition .

Truth-Values

- A model assigns a unique truth-value (T or F) to every atomic proposition.
- For every model, the truth-values for compound propositions are defined in terms of the truth-values of their compounds.

Negation

- Let φ be some proposition.
- The negation of φ is denoted by $\neg\varphi$.
- The truth-values of $\neg\varphi$ are defined in terms of φ as follows.

φ	$\neg\varphi$
T	F
F	T

Conjunction

- Let φ and ψ be propositions.
- The conjunction of φ and ψ is denoted by $\varphi \wedge \psi$.
- The truth-values of $\varphi \wedge \psi$ are defined in terms of φ and ψ as follows.

φ	ψ	$\varphi \wedge \psi$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction

- Let φ and ψ be propositions.
- The disjunction of φ and ψ is denoted by $\varphi \vee \psi$.
- The truth-values of $\varphi \vee \psi$ are defined in terms of φ and ψ as follows.

φ	ψ	$\varphi \vee \psi$
T	T	T
T	F	T
F	T	T
F	F	F

Implication

- Let φ and ψ be propositions.
- The proposition that φ implies ψ is denoted by $\varphi \to \psi$, where φ is called antecedent and ψ is called consequent.
- The truth-values of $\varphi \to \psi$ are defined in terms of φ and ψ as follows.

φ	ψ	$\varphi \to \psi$
T	T	T
T	F	F
F	T	T
F	F	T

Equivalence

- Let φ and ψ be propositions.
- The equivalence of φ and ψ is denoted by $\varphi \leftrightarrow \psi$.
- The truth-values of $\varphi \leftrightarrow \psi$ are defined in terms of φ and ψ as follows.

φ	ψ	$\varphi \leftrightarrow \psi$
T	T	T
T	F	F
F	T	F
F	F	T

Logical Equivalence

Definition 1

Let φ and ψ be propositions. φ and ψ are called logically equivalent, if they have the same truth values in every model.

Example.
$\varphi \to \psi$ is logically equivalent to $(\neg\psi) \to (\neg\varphi)$.

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

PROOFS

Mathematical Proofs

- Generally, all mathematical propositions are "if-then-statements".
- In a proof, the consequent is derived from the antecedent and possibly further known truths by the laws of logic.
- Unfortunately, there exists no fixed procedure of how to conduct a proof.
- However, there are some techniques that can be helpful.

Principle of Induction

- The principle of induction can be helpful, whenever properties have to be shown to hold for all natural numbers.

- Let $n_0 \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ be some natural number, and $\mathcal{A}(n)$ be some proposition for all $n \geq n_0$.

- Induction basis: show that $\mathcal{A}(n_0)$ holds.

- Induction step: for all $n \geq n_0$ show that, if $\mathcal{A}(n)$ holds, then $\mathcal{A}(n+1)$ also holds.

- Principle of induction: Then, $\mathcal{A}(n)$ holds for all $n \geq n_0$.

- **Intuition**: if $\mathcal{A}(n_0)$ is true, and if for all $n \geq n_0$ the truth of $\mathcal{A}(n)$ implies the truth of $\mathcal{A}(n+1)$, then via the chain

$$\mathcal{A}(n_0) \to \mathcal{A}(n_0+1) \to \mathcal{A}(n_0+2) \to \ldots$$

the truth of $\mathcal{A}(n)$ obtains for all $n \geq n_0$.

Example

Assertion:
$\sum_{i=1}^{n}(i+1)i = \frac{1}{3}n(n+1)(n+2)$ for all $n \geq 1$.

Proof:

- Induction basis: Let $n_0 = 1$. Observe that $\sum_{i=1}^{1}(i+1)i = 2 \cdot 1 = 2$ and $\frac{1}{3} \cdot 1 \cdot 2 \cdot 3 = 2$.
- Induction step: Let $n \geq 1$ and suppose that $\sum_{i=1}^{n}(i+1)i = \frac{1}{3}n(n+1)(n+2)$ holds. It needs to be shown that $\sum_{i=1}^{n+1}(i+1)i = \frac{1}{3}(n+1)(n+2)(n+3)$ also holds.
- Observe that $\sum_{i=1}^{n+1}(i+1)i = \left(\sum_{i=1}^{n}(i+1)i\right) + (n+2)(n+1)$
$= \frac{1}{3}n(n+1)(n+2) + (n+2)(n+1) = (\frac{1}{3}n+1)(n+1)(n+2)$
$= \frac{1}{3}(n+3)(n+1)(n+2)$.

Direct Proofs

- The general structure of a proposition to be proven is $A \to B$.
- In a direct proof, the antecedent A is assumed to be true, and the consequent B is then derived.
- Note that equivalence propositions $A \leftrightarrow B$ are logically equivalent to $(A \to B) \wedge (B \to A)$.
- To establish $A \leftrightarrow B$ a proof can thus be split into first proving $A \to B$, and then proving $B \to A$.

Proof by Contraposition

- Recall that $A \to B$ is logically equivalent to $(\neg B) \to (\neg A)$.
- In order to prove $A \to B$, it is thus possible to assume that $\neg B$ holds, and to then derive $\neg A$.

Proof by Contradiction (Indirect Proof)

- Recall that the implication $A \rightarrow B$ is only false, whenever the antecedent A is true and the consequent B is false.
- **Intuition**: “With the laws of logic it is not possible to deduce a falsehood from a truth.”
- Suppose A is true and B is false: If a contradiction can be derived, one of the two assumptions must be false, and hence $A \rightarrow B$ be true.

Circular Proof

- Sometimes statements of the following form need to be proven:

  ”If *A* holds, then the statements (i), (ii), and (iii) are equivalent“

- It suffices to prove $(i) \to (ii)$, $(ii) \to (iii)$, and $(iii) \to (i)$.

- By following the proven implications in an appropriate way, every implication between the three statements is established (by transitivity).

Product Sets

Product Sets

Definition 2

Let M and N be non-empty sets. The set

$$M \times N := \{(m, n) : m \in M, n \in N\}$$

is called product set of M and N, where (m, n) is called ordered pair.

Two ordered pairs (m, n) and (m', n') are equal, whenever $m = m'$ and $n = n'$.

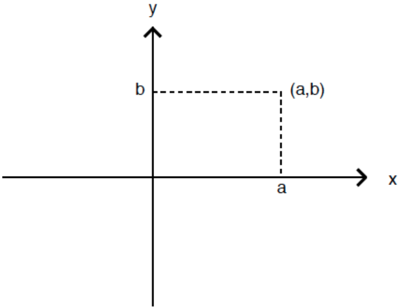
Illustration

- Consider the sets $M = \{\text{Alice}, \text{Bob}, \text{Claire}\}$ and $N = \{0, 1\}$.
- The product set of M and N is

  $$M \times N = \{(\text{Alice}, 0), (\text{Bob}, 0), (\text{Claire}, 0), (\text{Alice}, 1), (\text{Bob}, 1), (\text{Claire}, 1)\}.$$

Illustration

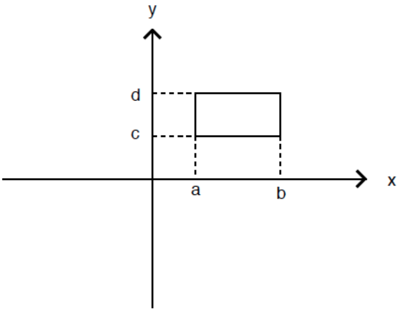
The product set $\mathbb{R} \times \mathbb{R}$ and the ordered pair $(a, b) \in \mathbb{R} \times \mathbb{R}$



Illustration

- Let $M = \{x \in \mathbb{R} : a \leq x \leq b\}$ and $N = \{x \in \mathbb{R} : c \leq x \leq d\}$, where $a, b, c, d \in \mathbb{R}$, be intervals in $\mathbb{R}$.

- The product set $M \times N$ can then be represented by the following rectangle



FUNCTIONS

Functions

Definition 3

Let M and N be sets. A subset $f \subseteq M \times N$ of the product set $M \times N$ is called function from M to N, whenever the following two properties hold.

1. For all $m \in M$ there exists $n \in N$ such that $(m, n) \in f$.
2. If $(m, n) \in f$ and $(m, n') \in f$, then $n = n'$.

Example: The product set

$$f = \{(x, x^2) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$

is a function from $\mathbb{R}$ to $\mathbb{R}$.

Notation

- If $f \subseteq M \times N$ is a function, this is denoted by $f : M \to N$.
- M is called domain of f, and N is called codomain of f.
- For every $m \in M$, the unique $n \in N$ such that $(m, n) \in f$ is also denoted by $f(m)$.
- Every $m \in M$ is also said to be mapped to $f(m)$, denoted as $m \mapsto f(m)$.

Identical Functions

Definition 4

Let $f : M \to N$ and $g : M' \to N'$ be functions. The two functions f and g are identical, whenever the following three properties hold.

1. $M = M'$
2. $N = N'$
3. $f(m) = g(m)$ for all $m \in M$

Image

Definition 5

Let $f : M \to N$ be a function, and $m \in M$ be some element in the domain M. The element $f(m) \in N$ in the codomain N is called image of m under f. The set

$$f(M) := \{n \in N : \text{ There exists } m \in M \text{ such that } f(m) = n\} \subseteq N$$

is called image of f.

- Consider the function $f(x) = x^2$ for all $x \in \mathbb{R}$.
- For instance, the image of 2 under f is 4, since $f(2) = 2^2 = 4$.
- Note that $f(\mathbb{R}) = \mathbb{R}_0^+$.

Pre-Image

Definition 6

Let $f : M \to N$ be a function, $n \in N$ be some element in the codomain of f, and $B \subseteq N$ be some subset of the codomain of f. Every $m \in M$ such that $f(m) = n$ is called a pre-image of n under f. The set

$$f^{-1}(B) = \{m \in M : f(m) \in B\} \subseteq M$$

is called pre-image of B under f.

- Note that $f^{-1}(N) = M$ holds for every function.
- Consider the function $f(x) = x^2$ for all $x \in \mathbb{R}$.
- For instance, the pre-image of $\{0\} \subseteq N$ is $f^{-1}(\{0\}) = \{0\}$, the pre-image of $\{y\}$ with $y > 0$ is $f^{-1}(\{y\}) = \{-\sqrt{y}, \sqrt{y}\}$, and the pre-image of $\{y\}$ with $y < 0$ is $f^{-1}(\{y\}) = \emptyset$.

Observation

Let $f : M \to N$ be a function.

- Every element $m \in M$ of the domain has a unique image under f.
- It is possible that there exist elements $n \in N$ of the codomain such that $n \notin f(M)$.
- If $n \in f(M)$, then it is possible that there exist $m, m' \in M$ such that $m \neq m'$ and $m, m' \in f^{-1}(\{n\})$.

Surjection, Injection, and Bijections

Definition 7

Let $f : M \to N$ be a function.

- f is called surjective, whenever $f(M) = N$.
- f is called injective, whenever, for all $m, m' \in M$, if $m \neq m'$, then $f(m) \neq f(m')$.
- f is called bijective, whenever f is surjective as well as injective.

- A function is thus surjective, whenever every element in the codomain N also lies in the image $f(M)$ of f.
- A function is thus injective, whenever every element in the image $f(M)$ of f has a unique pre-image under f.

Surjection

Proofs

- To prove that $f : M \to N$ is surjective, consider an arbitrary element $n \in N$, and give an element $m \in M$ such that $f(m) = n$.
- To prove that $f : M \to N$ is not surjective, give an element $n \in N$ such that $n \notin f(M)$.

Examples

- Consider $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ such that $f\big((x, y)\big) = x + y$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Let $z \in \mathbb{R}$, and consider $(0, z) \in \mathbb{R} \times \mathbb{R}$. As $f\big((0, z)\big) = 0 + z = z$, the function f is surjective.
- Consider $g : \mathbb{N} \to \mathbb{Z}$ such that $g(n) = -n$ for all $n \in \mathbb{N}$. As $0 \in \mathbb{Z}$ but $0 \notin g(\mathbb{N})$, the function g is not surjective.

Injection

Proofs

- To prove that $f : M \to N$ is injective, suppose that there exist $m, m' \in M$ such that $f(m) = f(m')$. Derive from the equality $f(m) = f(m')$ that $m = m'$.
- To prove that $f : M \to N$ is not injective, give two elements $m_1, m_2 \in M$ such that $m_1 \neq m_2$ and $f(m_1) = f(m_2)$.

Examples

- Consider $g : \mathbb{N} \to \mathbb{Z}$ such that $g(n) = -n$ for all $n \in \mathbb{N}$. Suppose that there exist $m, m' \in \mathbb{N}$ such that $g(m) = g(m')$. It follows that $-m = -m'$, i.e. $m = m'$. Hence, g is injective.
- Consider $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ such that $f\big((x, y)\big) = x + y$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. As $(0, 3), (1, 2) \in \mathbb{R} \times \mathbb{R}$ and $(0, 3) \neq (1, 2)$ but $f\big((0, 3)\big) = f\big((1, 2)\big) = 3$, the function f is not injective.

Identity Function

Definition 8

Let M be a set. The function $\mathrm{id}_M : M \to M$ such that $\mathrm{id}_M(m) = m$ for all $m \in M$ is called identity function on M.

- The identity function maps each element to itself.
- Note that the identity function is bijective.

Composite Functions

Definition 9

Let M, N, O be sets, and $f : M \to N$ as well as $g : N \to O$ be functions. The function $[g \circ f] : M \to O$ such that

$$[g \circ f](m) := g\big(f(m)\big)$$

for all $m \in M$ is called composite function of f and g.

Examples:

- For every $x \in \mathbb{R}$, $|\, x \,|$ denotes x if $x \geq 0$, and $-x$ if $x < 0$.
- Consider $f : \mathbb{Z} \to \mathbb{N}_0$ such that $f(x) =|\, x \,|$ for all $x \in \mathbb{Z}$ and $g : \mathbb{N}_0 \to \mathbb{Z}$ such that $g(x) = x - 3$ for all $x \in \mathbb{N}_0$.
- Then, $[g \circ f] : \mathbb{Z} \to \mathbb{Z}$ is defined as $[g \circ f](x) := g\big(f(x)\big) = g(|\, x \,|) =|\, x \,| -3$ for all $x \in \mathbb{Z}$.
- Then, $[f \circ g] : \mathbb{N}_0 \to \mathbb{N}_0$ is defined as $[f \circ g](x) := f\big(g(x)\big) = f(x - 3) =|\, x - 3 \,|$ for all $x \in \mathbb{Z}$.

Identity Function and Composition

- Let $f : M \to N$ be a function.
- Then,
$$[\mathrm{id}_N \circ f](m) = \mathrm{id}_N\big(f(m)\big) = f(m) \text{ for all } m \in M$$
and
$$[f \circ \mathrm{id}_M](m) = f\big(\mathrm{id}_M(m)\big) = f(m) \text{ for all } m \in M.$$
- Note that $[\mathrm{id}_N \circ f] = f$ as well as $[f \circ \mathrm{id}_M] = f$.

Preservation of Surjections, Injections, and Bijections under Composition

Proposition 10

Let $f : L \to M$ and $g : M \to N$ be functions.

1. *If f and g are surjective, then $g \circ f$ is surjective.*
2. *If f and g are injective, then $g \circ f$ is injective.*
3. *If f and g are bijective, then $g \circ f$ is bijective.*

Proof

Recall that $[g \circ f] : L \to N$ such that $[g \circ f](l) = g\big(f(l)\big)$ for all $l \in L$.

1. Let $n \in N$. As g is surjective, there exists $m \in M$ such that $g(m) = n$. Since f is surjective, too, there also exists $l \in L$ such that $f(l) = m$. Then, $[g \circ f](l) = g\big(f(l)\big) = g(m) = n$. Therefore, every $n \in N$ has a pre-image under $[f \circ g]$, and consequently $[f \circ g]$ is surjective.

2. Let $l, l' \in L$ such that $[g \circ f](l) = [g \circ f](l')$. Then $g\big(f(l)\big) = g\big(f(l')\big)$. As g is injective, it follows that $f(l) = f(l')$, and as f is injective, $l = l'$ obtains. Every element in the image $[g \circ f](L)$ of $[g \circ f]$ thus has a unique pre-image under $[g \circ f]$. Consequently, $[g \circ f]$ is injective.

3. By (1) and (2) it follows immediately that $g \circ f$ is bijective.

Inverse Functions

Definition 11

Let $f : M \to N$ be a function. The function f is called invertible, if there exists a function $f^{-1} : N \to M$ such that $f^{-1} \circ f = \mathrm{id}_M$ and $f \circ f^{-1} = \mathrm{id}_N$. The function f^{-1} is called inverse of f.

It is thus the case that $[f^{-1} \circ f](m) = m$ for all $m \in M$ and $[f \circ f^{-1}](n) = n$ for all $n \in N$.

Not Every Function Is Invertible

- Let $M = \{1, 2\}$ and $N = \{1\}$.
- Let $f : M \to N$ be a function such that $f(1) = 1$ and $f(2) = 1$.
- There exist only two functions from N to M, i.e. $g : N \to M$ such that $g(1) = 1$ and $g' : N \to M$ such that $g'(1) = 2$.
- Note that $[g \circ f](2) = g\big(f(2)\big) = g(1) = 1 \neq \text{id}_M(2)$, and thus $[g \circ f] \neq \text{id}_M$.
- Also, note that $[g' \circ f](1) = g'\big(f(1)\big) = g'(1) = 2 \neq \text{id}_M(1)$, and thus $[g' \circ f] \neq \text{id}_M$.
- Neither g nor g' are thus inverse functions of f.

Characterization of Invertible Functions

Proposition 12

A function is invertible, if and only if, it is bijective.

Proof (if-direction)

- Let $f : M \to N$ be a function that is bijective.
- As f is surjective, for every element $n \in N$ there exists $m \in M$ such that $n = f(m)$.
- Since f is also injective, for every element $n \in N$ the element $m \in M$ such that $n = f(m)$ is actually unique.
- For every $n \in N$ define $f^{-1}(n)$ to be the unique element $m \in M$ such that $f(m) = n$.
- Then, $f^{-1} : N \to M$ with $n \mapsto f^{-1}(n)$ is a function from N to M.
- Let $m \in M$. Then, $[f^{-1} \circ f](m) = f^{-1}\big(f(m)\big) = f^{-1}(n) = m$, and thus $[f^{-1} \circ f] = \mathrm{id}_M$.
- Let $n \in N$. Then, $[f \circ f^{-1}](n) = f\big(f^{-1}(n)\big) = f(m) = n$, and thus $[f \circ f^{-1}] = \mathrm{id}_N$.
- Therefore, f is invertible.

Proof (only-if-direction)

- Let $f : M \to N$ be a function that is invertible.
- Then, there exists a function $f^{-1} : N \to M$ such that $[f^{-1} \circ f] = \mathrm{id}_M$ and $[f \circ f^{-1}] = \mathrm{id}_N$.
- Let $m, m' \in M$ such that $f(m) = f(m')$. Applying f^{-1} to both sides, yields $f^{-1}\big(f(m)\big) = f^{-1}\big(f(m')\big)$.
- Note that $f^{-1}\big(f(m)\big) = [f^{-1} \circ f](m) = m$ and $f^{-1}\big(f(m')\big) = [f^{-1} \circ f](m') = m'$.
- Therefore, $m = m'$, and f is thus injective.
- Let $n \in N$ and consider the element $m \in M$ for which $f^{-1}(n) = m$ holds.
- Then, $f(m) = f\big(f^{-1}(n)\big) = [f \circ f^{-1}](n) = n$, and f is thus surjective.

Fields

Fields

Definition 13

A triple $(\mathbb{F}, +, \cdot)$ is called field, where $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ are functions such that the following properties hold:

- $a + b = b + a$ and $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{F}$ **(Commutativity of $+$ and $\cdot$)**
- $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{F}$ **(Associativity of $+$ and $\cdot$)**
- $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{F}$ **(Law of Distributivity)**
- There exist $\overset{+}{n}, \overset{\cdot}{n} \in \mathbb{F}$ such that $\overset{+}{n} + a = a$ and $\overset{\cdot}{n} \cdot a = a$ for all $a \in \mathbb{F}$ **(Existence of $+$-Neutral and $\cdot$-Neutral Elements)**
- For every $a \in \mathbb{F}$ there exists $a' \in \mathbb{F}$ such that $a + a' = \overset{+}{n}$, and for every $a \in \mathbb{F} \setminus \{\overset{+}{n}\}$ there exists $a^* \in \mathbb{F}$ such that $a \cdot a^* = \overset{\cdot}{n}$ **(Every Element is $+$-Invertible and $\cdot$-Invertible)**

Some Properties of Fields

Proposition 14

Let $\mathbb{F}$ be a field.

1. $a \cdot \overset{+}{n} = \overset{+}{n}$ *for all* $a \in \mathbb{F}$
2. *Let* $a, b \in \mathbb{F}$ *such that* $a \cdot b = \overset{+}{n}$. *Then,* $a = \overset{+}{n}$ *or* $b = \overset{+}{n}$.
3. *Let* $a, b, c \in \mathbb{F}$ *such that* $a + b = \overset{+}{n}$ *and* $a + c = \overset{+}{n}$. *Then,* $b = c$. ***(Uniqueness of $+$-Inverse)***
4. *Let* $a, b, c \in \mathbb{F}$ *such that* $a \neq \overset{+}{n}$, $a \cdot b = \dot{n}$, *and* $a \cdot c = \dot{n}$. *Then,* $b = c$. ***(Uniqueness of $\cdot$-Inverse)***

Proof of (1)

Statement (1):
$a \cdot \overset{+}{n} = \overset{+}{n}$ for all $a \in \mathbb{F}$.

- As $\overset{+}{n}$ is the $+$-neutral element and by the law of distributivity, it is the case that

$$a \cdot \overset{+}{n} = a \cdot (\overset{+}{n} + \overset{+}{n}) = a \cdot \overset{+}{n} + a \cdot \overset{+}{n}.$$

- Since every element in $\mathbb{F}$ is $+$-invertible, $a \cdot \overset{+}{n}$ is $+$-invertible.
- Let x denote the $+$-inverse to $a \cdot \overset{+}{n}$ (i.e. $x + a \cdot \overset{+}{n} = \overset{+}{n}$).
- Then,

$$x + a \cdot \overset{+}{n} = x + (a \cdot \overset{+}{n} + a \cdot \overset{+}{n}) = (x + a \cdot \overset{+}{n}) + a \cdot \overset{+}{n}.$$

- As $x + a \cdot \overset{+}{n} = \overset{+}{n}$, it follows that $\overset{+}{n} = \overset{+}{n} + a \cdot \overset{+}{n}$
- It also holds that $a \cdot \overset{+}{n} = \overset{+}{n} + a \cdot \overset{+}{n}$, and therefore $a \cdot \overset{+}{n} = \overset{+}{n}$ ensues.

Proof of (2)

Statement (2):

Let $a, b \in \mathbb{F}$ such that $a \cdot b = \overset{+}{n}$. Then, $a = \overset{+}{n}$ or $b = \overset{+}{n}$.

- Note that either $a = \overset{+}{n}$ or $a \neq \overset{+}{n}$.
- If $a = \overset{+}{n}$, then the claim holds, thus suppose that $a \neq \overset{+}{n}$.
- Note that a is $\cdot$-invertible and let a^* be its inverse.
- Then,

$$a^* \cdot (a \cdot b) = a^* \cdot \overset{+}{n}.$$

- Observe by associativity and a^* being $\cdot$-inverse to a that

$$a^* \cdot (a \cdot b) = (a^* \cdot a) \cdot b = \dot{n} \cdot b.$$

- It follows that $\dot{n} \cdot b = a^* \cdot \overset{+}{n}$.
- As $\dot{n} \cdot b = b$ and, by part (1) of the Proposition, $a^* \cdot \overset{+}{n} = \overset{+}{n}$, it is the case that $b = \overset{+}{n}$.

Proof of (3)

Statement (3):

Let $a, b, c \in \mathbb{F}$ such that $a + b = \overset{+}{n}$ and $a + c = \overset{+}{n}$. Then, $b = c$.

- It is the case that $a + b = a + c$.
- Let a' denote the $+$-inverse of a.
- Then,
$$a' + (a + b) = a' + (a + c)$$
which by associativity is equivalent to
$$(a' + a) + b = (a' + a) + c.$$
- Therefore, $\overset{+}{n} + b = \overset{+}{n} + c$, and thus, by the $+$-neutrality of $\overset{+}{n}$, it follows that $b = c$.

Proof of (4)

Statement (4):
Let $a, b, c \in \mathbb{F}$ such that $a \neq \overset{+}{n}$, $a \cdot b = \dot{n}$, and $a \cdot c = \dot{n}$. Then, $b = c$.

- It is the case that $a \cdot b = a \cdot c$.
- Let a^* denote the $\cdot$-inverse of a.
- Then,

$$a^* \cdot (a \cdot b) = a^* \cdot (a \cdot c)$$

  which by associativity is equivalent to

$$(a^* \cdot a) \cdot b = (a^* \cdot a) \cdot c.$$

- Therefore, $\dot{n} \cdot b = \dot{n} \cdot c$, and thus, by the $\cdot$-neutrality of $\dot{n}$, it follows that $b = c$.

Examples

- The sets $\mathbb{N}$ and $\mathbb{Z}$ equipped with addition $+$ and multiplication $\cdot$ are not fields.
- The sets $\mathbb{Q}$ and $\mathbb{R}$ equipped with addition $+$ and multiplication $\cdot$ are fields with neutral elements 0 and 1.