Discrete Mathematics
PVW Script

Last Updated: June, 2022

Authors: Christian Mitsch, Friedrich Ginnold, Simon Yuan, Olivier Bitter, Dimitri Stanojevic, Robin Staab, Miklós Horváth, Marc Himmelberger

diskmat-pvw-skript@vis.ethz.ch

Disclaimer:
This script only serves as additional material for practice purposes and should not serve as a substitute for the lecture material. We neither guarantee that this script covers all relevant topics for the exam, nor that it is correct. If an attentive reader finds any mistakes or has any suggestions on how to improve the script, they are encouraged to contact the authors under the indicated email address or, preferably, through a gitlab issue on https://gitlab.ethz.ch/vis/luk/pvw_script_diskmath.

Contents

1 Sets, Relations and Functions

This chapter covers the fundamentals of the crucial mathematical concepts sets, relations and functions. Many exercises are solved, which not only helps understanding the theory better but also revises some basic proof techniques.

1.1 Set fundamentals

Definition 1.1. *A **set** S is a well-defined collection of distinct objects. We call these objects **elements** and denote $x \in S$ for saying that x is an element of S. A set is considered to be an object in its own right. To say that an object x is not an element of a set S, we write $x \notin S$.*

We can describe a set by either listing all its elements (if it is finite) or by giving a predicate that fits every element in the set, i.e. $\{x \in A \mid P(x)\}$. For example, $\{2, 3, 5\}$ denotes the set which contains the numbers 2, 3 and 5. We can also describe this set with $\{x \in \mathbb{N} \mid \ prime(x) \land x < 6\}$ where $prime(x) = 1 :\Leftrightarrow x$ is a prime number. Note that the set representations are not unique, e.g. $\{2, 3, 3, 5, 5\}$ and $\{x \in \mathbb{N} \mid \ prime(x) \land x < 7\}$ describe the same set as above. With the first method, only finite sets can be represented while the second one also enables the description of infinite sets.

Two crucial concepts in set theory are subsets and set equality.

Definition 1.2. *A set A is a **subset** of a set B, denoted as $A \subseteq B$, if and only if each element of A is also an element of B. Formally $A \subseteq B :\Leftrightarrow \forall a(a \in A \to a \in B)$.*

Definition 1.3. *Two sets A and B are **equal**, denoted as $A = B$, if and only if they contain the same elements. Formally $A = B :\Leftrightarrow \forall a(a \in A \leftrightarrow a \in B)$.*

Furthermore there are some important operations on a set. The power set, union, intersection, difference and cartesian product. For the following table, let A and B be two sets.

Operation	Notation	Definition	Meaning
power set	$\mathcal{P}(A)$	$\mathcal{P}(A) := \{x \mid x \subseteq A\}$	The set which contains all subsets of A.
union	$A \cup B$	$A \cup B := \{x \mid x \in A \lor x \in B\}$	The set of all objects which are elements of A or B.
intersection	$A \cap B$	$A \cap B := \{x \mid x \in A \land x \in B\}$	The set of all objects which are elements of A and B.
difference	$A \setminus B$	$A \setminus B := \{x \mid x \in A \land x \notin B\}$	The set of all objects which are elements of A and are not elements of B.
cartesian product	$A \times B$	$A \times B := \{(a, b) \mid a \in A \land b \in B\}$	The set of all ordered pairs whose first component is an element of A and its second component is an element of B.
complement	$\overline{A}$	$\overline{A} := \{x \in U \mid x \notin A\}$	The set of all elements of some universe U that are not elements of A. (Only makes sense w.r.t. a universe!)

Note that it immediately follows from these definitions that two sets are equal if and only if they are subsets of each other. This property is usually the easiest way of proving that two sets are equal. Our general strategy for proving that two sets are equal is to prove that they are both subsets of each other.

To show that $A \subseteq B$, we have to show that each element of A is also an element of B (which is simply done by applying the definition of a subset). The standard way of doing this is to choose an arbitrary element $x \in A$ and to show that also $x \in B$. Since x is arbitrary, this implies that each element of A is also an element of B.

The following exercises use these definitions and strategies in practice, and should help you to understand them better. Keep in mind that $\emptyset$ (or $\{\}$) is the empty set, the set which has no elements, and that the cardinality $|A|$ of a finite set A is the number of elements contained in A.

Hands-On 1

1.1. Describe the set of all even positive natural numbers which have one digit using both representations that were mentioned.

1.2. Describe the set of all even positive natural numbers using the predicate representation.

1.3. Let $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ and $B = \{\{\emptyset\}, \emptyset, \{\emptyset\}\}$ be two sets. Specify each of the following sets (by listing their elements) and give their cardinality.

1. $A \cup B$
2. $A \cap B$
3. $\mathcal{P}(B)$
4. $A \setminus \mathcal{P}(B)$
5. $B \times \mathcal{P}(\emptyset)$

1.4. Let A and B be two sets. Show that $\mathcal{P}(A) = \mathcal{P}(B) \Rightarrow A = B$.

1.5. Let A, B and C be three sets. For which A is $A \times B = A \times C \Rightarrow B = C$?

1.6. Show that $(A \cup B) \setminus (A \cap B) = (A \cup C) \setminus (A \cap C) \Rightarrow B = C$.

1.7. Prove that there exist infinitely many sets S such that $S \subseteq \mathcal{P}(S)$.

1.2 Relations

Definition 1.4. *A (binary)* ***relation*** ρ *from a set* A *to a set* B *is a subset of* $A \times B$*. If* $A = B$*, then* ρ *is called a relation on* A*. We write* $(a, b) \in \rho$ *or* $a \ \rho \ b$ *to say that* $(a, b) \in A \times B$ *is an element of the relation* ρ*.*

There are a few crucial properties that relations on a set can have. The following table contains the property, its concrete definition and a graph theoretic interpretation for illustration purposes.
Let ρ be a relation on a set A.

Property	Definition	Meaning (graph theory)
reflexivity	$\forall a \ (a \ \rho \ a)$	Each vertex has a loop (an edge to itself).
irreflexivity	$\forall a \ (a \not\rho \ a)$	No vertex has a loop.
symmetry	$\forall a \forall b \ (a \ \rho \ b \leftrightarrow b \ \rho \ a)$	It can be represented as an undirected graph, possibly with loops.
antisymmetry	$\forall a \forall b \ ((a \ \rho \ b \wedge b \ \rho \ a) \rightarrow a \ = \ b)$	There are no cycles of length 2 in the graph representation.
transitivity	$\forall a \forall b \forall c \ ((a \ \rho \ b \wedge b \ \rho \ c) \rightarrow a \ \rho \ c)$	If a vertex can be reached from another vertex, then it can also be directly reached from that vertex.

The inverse, composition and the transitive closure are operations on relations. Exercise 2.2 shows how these work. Additionally there are also some connections between the properties, which are (for the most part) highlighted in the exercise 2.3.

There are two relations of special interest on a single set A, namely equivalence relations and partial order relations. They are defined through a few concrete properties.

Definition 1.5. *An* ***equivalence relation*** *is a relation on a set* A *that is* ***reflexive***, ***symmetric*** *and* ***transitive****.*

The definition immediately gives us a method of proving whether some relation is an equivalence relation or not: to prove that a relation is an equivalence relation, we prove that it is reflexive, symmetric and transitive. To prove that a relation is not an equivalence relation, disprove one of these properties.

Definition 1.6. *A* ***partial order*** *is a relation on a set* A *that is* ***reflexive***, ***antisymmetric*** *and* ***transitive****. A set* A *together with a partial order* $\preceq$ *on* A *is called a* ***partially ordered set (poset)*** *and is denoted as* $(A; \preceq)$*.*

Again the definition gives us a proof strategy: To prove that a relation is a partial order, we prove that it is reflexive, antisymmetric and transitive. To prove that a relation is not a poset, disprove one of these properties.
Additionally, we can represent posets by *Hasse diagrams* and they can have special elements like least/greatest or maximal/minimal elements, which will occur in exercises 2.7 and 2.8.

Definition 1.7. *The composition of two relations is a quite natural concept using the existence of one "connecting element". While we can generalize the concept to an arbitrary amount of relations we will now only look at the composition of two relations* ρ *and* σ*. Let* $\rho \subseteq A \times B$ *and* $\sigma \subseteq B \times C$*, then their composition is* $\rho\sigma \subseteq A \times C$ *and*

$$(a, c) \in \rho\sigma \Leftrightarrow \exists b \in B : (a \ \rho \ b \ \wedge \ b \ \sigma \ c)$$

Furthermore we can compose a relation with itself (which only makes sense if we talk about a relation on a set i.e. $\rho \subseteq A \times A$) and by repeating this we get ρ^k containing all tuples $(a, a') \subseteq A \times A$ that fulfill $\exists a_1, ..., a_{k-1} \in A : (a\ \rho\ a_1 \wedge\ a_1\ \rho\ a_2 \wedge ... \wedge a_{k-2}\ \rho\ a_{k-1} \wedge a_{k-1}\ \rho\ a')$.

Definition 1.8. *We get the transitive closure ρ^* of a relation ρ using the definition*

$$\rho^* = \bigcup_{n=1}^{\infty} p^n$$

Hands-On 2

2.1. Decide whether the relation ρ on $\{a, b, c, d\}$ with $\rho = \{(a, b), (b, a), (b, c), (b, d), (c, b), (d, b)\}$ is reflexive, irreflexive, symmetric, antisymmetric, transitive.

2.2. Let ρ be the same relation as in the previous exercise. Determine the set representation of the following relations $\widehat{\rho}$, ρ^2 and ρ^*.

2.3. Let σ be a relation on a set A. Prove or disprove the following statements:

1. If σ is not reflexive, then it is irreflexive.
2. If σ is irreflexive and $A \neq \emptyset$, then σ is not reflexive.
3. If σ is symmetric, then it is not anti-symmetric.

2.4. Let $\sim$ be a relation on $\mathbb{R}^2$ with

$$(x, y) \sim (a, b) := x^2 + b = a^2 + y$$

Prove that $\sim$ is an equivalence relation.

2.5. Let $(A, \preceq)$ be a poset. Prove or disprove that $(A, \widehat{\preceq})$ is a poset.

2.6. Prove or disprove that there exists a poset on $\mathbb{N}$ which is also an equivalence relation.

2.7. Draw the Hasse Digramm of the poset $(\mathcal{P}(\{a, b, c\}) \cup \{\{d\}\}, \subseteq)$. Determine its minimal, maximal, least and greatest elements.

2.8. Let's look at the poset $(\mathcal{P}(\{a, b, c\}) \cup \{\{d\}\}, \subseteq)$ from the previous exercise. Find the lower bounds of the subset $\{\{a, b\}, \{a, c\}\}$ and find its greatest lower bound. Is this poset a lattice?

2.9. Let $\rho \subseteq A \times B$ and $\sigma \subseteq B \times C$. Prove that the inverse of $\rho\sigma$ fulfills $\widehat{\rho\sigma} = \widehat{\sigma}\widehat{\rho}$.

2.10. For each of the following relations on $\mathbb{Z}$ decide whether or not it is reflexive, symmetric and transitive.

1. $x \sim y \iff x + y$ is even
2. $x \sim y \iff xy$ is odd
3. $x \sim y \iff x + x \cdot y$ is even

2.11. Let define $\rho \subseteq \mathbb{N}^+ \times \mathbb{N}^+$ as $a \rho b \iff gcd(a, b) = a$ ($\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$). Decide whether or not ρ is reflexive, antisymmetric and transitive.

1.3 Functions

A crucial mathematical concept is the one of functions, which can be described elegantly with relations.

Definition 1.9. *A **function** $f : A \to B$ from a domain A to a codomain B is a relation from A to B with the following properties:*

1. *f is totally defined, i.e. $\forall a \in A\, \exists b \in B(a\ f\ b)$.*
2. *f is well-defined, i.e. $\forall a \in A\, \forall b, b' \in B((a\ f\ b \wedge a\ f\ b') \to b = b')$.*

The set of all functions from A to B is denoted as B^A. A partial function is a function where condition 1 does not necessarily have to hold. It is a convenient and acceptable standard to write $f(a) = b$ instead of $a\ f\ b$ when it is clear that f is a function.

The notation B^A is motivated by the fact that if A and B are both finite, then there are $|B|^{|A|}$ such functions $f : A \to B$.

Definition 1.10. *For a function $f : A \to B$ and a set $S \subseteq A$, we call the **image** of S under the function f the set $f(S) := \{f(a) \mid a \in S\}$.*

Injectivity, surjectivity and bijectivity are crucial properties of functions.

Definition 1.11. *A function $f : A \to B$ is **injective** if $x \neq y \Rightarrow f(x) \neq f(y)$ for every $x, y \in A$. It is **surjective** if for every $b \in B$, there exists an $a \in A$ such that $b = f(a)$. It is **bijective** if it is injective and surjective.*

The definition immediately gives us methods to prove injectivity, surjectivity or bijectivity. In order to prove that a function $f : A \to B$ is injective, prove that for any $x, y \in A$ with $f(x) = f(y)$ we have $x = y$. To prove that f is surjective, prove that for any $b \in B$, there exists an $a \in A$ such that $f(a) = b$. To prove bijectivity, prove injectivity and surjectivity seperately.

Two functions can also be composed if the first function's codomain matches the second function's domain.

Definition 1.12. *The **composition** of two functions $f : A \to B$ and $g : B \to C$ is defined as $g \circ f$ where $(g \circ f)(a) = g(f(a)) \in C$ for any $a \in A$.*

Hands-On 3

3.1. Let $f : X \to Y$ be an arbitrary function and A, B subsets of X. Prove or disprove that $f(A \setminus B) = f(A) \setminus f(B)$.

3.2. Let $f : X \to Y$ be an arbitrary function and assume $X \neq \emptyset \neq Y$. Prove the following statement:

$$\forall A, B \subseteq X : f(A \cap B) = f(A) \cap f(B) \quad \iff \quad f \text{ injective}$$

3.3. Let A, B be two arbitrary non-empty sets. Prove the following statement: There exists an injective function $f : A \to B$ if and only if there exists a surjective function $g : B \to A$.

3.4. (Harder) Let $F : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ be defined as $F(g) = g \circ g$. Show that F is neither injective nor surjective.

1.4 Countability

Definition 1.13 (Countability)**.** *Let A, B be two arbitrary sets (of any cardinality). We define:*

- $A \sim B$: *A and B are of equal cardinality iff there exists a* ***bijective*** *mapping $f : A \to B$.*
- $A \preceq B$: *B has at least cardinality of A iff there exists an* ***injective*** *function $f : A \to B$.*
- *A set A is called* ***countable*** *iff $A \preceq \mathbb{N}$, otherwise we call it uncountable.*

These definitions (together with our existing knowledge) imply a variety of basic conclusions which shall be listed here. As an additional exercise one can prove them.

Corollary 1.1

- For any finite set A and infinite set B we have that $A \preceq B$ and $B \not\preceq A$.
- The by $\preceq$ defined relation is reflexive and transitive.
- Countably infinite and uncountable are the only two "options" for infinite sets, there exists nothing "in between". A proof of this can be found in the script.
- For any countable set (finite and infinite) we are able to leverage its mapping to the natural numbers to apply the concept of "well-foundedness", i.e. every subset has a smallest element. The same holds in reverse i.e. if there exists a non-well-founded subset, the set has to be uncountable.

Now we want to look at a variety of ways how we can construct such injections onto $\mathbb{N}$ (and for uncountability surjections onto $\mathbb{R}$).

1.4.1 Primes

This is probably the most used and most helpful way to quickly create an injection onto $\mathbb{N}$. It relies on the fact, that any $n \in \mathbb{N}$ has **unique prime factorization**, a fact which will be proven in chapter 2.
We proceed as follows:
Given n countable sets $A_1, ..., A_n$ and their respective injections $f_1, ..., f_n$ with $f_i : A_i \mapsto \mathbb{N}$, we can choose any n different primes $p_1, .., p_n$ and construct the following injection:

$$\begin{aligned} F : A_1 \times A_2 \times ... \times A_n &\to \mathbb{N} \\ (a_1, a_2, ..., a_n) &\mapsto p_1^{f_1(a_1)} \cdot p_2^{f_2(a_2)} \cdot .... \cdot p_n^{f_n(a_n)} \end{aligned}$$

Injectivity follows from the **unique prime factorization** theorem.

Example.

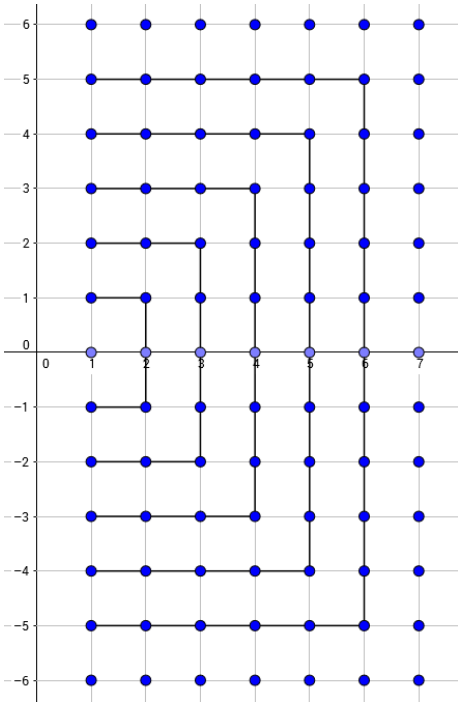
- $\mathbb{N} \times \mathbb{N}$ is countable with e.g. the following injection $(a, b) \mapsto 2^a \cdot 3^b$
- $\mathbb{Q}$ is countable with e.g. $f(\frac{p}{q}) = 2^p \cdot 3^q$ under the assumption that p and q are relative primes. This prevents us from mapping both $\frac{1}{2}$ and $\frac{2}{4}$ (**Food for thought**: What would we actually be mapping if we wouldn't make this assumption and how would it influence the correctness?).
- **Important** Let A_1, A_2 be countable sets with $A_1 \cup A_2 = A$ and their respective injections f_1, f_2 onto $\mathbb{N} - \{0\}$. For A we can define the following injective mapping $F : A \to \mathbb{N}$:

$$F(a) = \left\{ \begin{array}{ll} 2^{f_1(a)}, & \text{for } a \in A_1 \\ 3^{f_2(a)}, & \text{for } a \in A_2, a \notin A_1 \end{array} \right\}$$

1.4.2 Geometric arguments

Another useful way of constructing injections is to use a "geometric argument" i.e. convering an **entire** space (usually constructed as a product space e.g. $\mathbb{N} \times \mathbb{N}$ or $\mathbb{Z} \times \mathbb{N}$) by moving along a **single** trace.

Example.
A simple example is the following injection $f : \mathbb{N}^+ \times \mathbb{Z} \mapsto \mathbb{N}$ in which we move from inner circles to outer ones. Simply listed it would be $(0,1), (1,1), (2,1), ..., (1,2), (2,2), (3,2), (3,1), ...$



Injection $f : \mathbb{N}^+ \times \mathbb{Z} \mapsto N$

1.4.3 Important countable sets

The following table provides a quick overview over common countable sets and how we prove their countability:

$A_1 \times ... \times A_n$	Sets of finite tupels over countable sets	We create an injection from $A_i \times A_j$ to $\mathbb{N} \times \mathbb{N}$ (they are countable). From there we create an injection onto $\mathbb{N}$ (either via primes or geometrically). We generalize the argument via induction (or primes as above)
$\mathbb{Z}, \mathbb{Q}$	Integers and rationals	Simple geometric argument or primes for $\mathbb{Q}$
$\bigcup_{i=1}^{n} A_i$	Union of a finite amount of countable sets	Proof is in the exercises
$\bigcup_{i=1}^{\infty} A_i$	Union of a countably infinite amount of countable sets	Proof is in the exercises
$\{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N} f(n) \geq f(n+1)\}$	Set of all monotonically decreasing functions from $\mathbb{N}$ to $\mathbb{N}$	Proof is in the exercises

1.4.4 Proving countability and uncountability

Sometimes your task is to prove that a given set is countable or uncountable. Therefore we will recap the most common ideas used.

Using injections To prove that some set A is countable : construct an injection from A to a countable set, transitivity of the "dominated by" relation implies that A is countable too. To prove that set B is uncountable construct an injection from an uncountable set C to B. If B was countable, transitivity would imply that C is too, which is a contradiction. Hence B is uncountable.

Cantor's diagonal argument to show uncountability Assume we want to show that the set of **infinite** strings over a set A with at least 2 elements is uncountable. We can do so by assuming the contrary (i.e. it is countable) and arriving at a contradiction. Let us for exemplary reasons look at the open interval $(0, 1) \subset [0, 1] \subset \mathbb{R}$ and let us assume it's countable. We already know that real numbers can have an infinitely long decimal representation and given the countability assumption we can arrange them as follows:

$$
\begin{aligned}
z_1 &= 0, \underline{a_{11}}\ a_{12}\ a_{13}\ a_{14} \dots \\
z_2 &= 0, a_{21}\ \underline{a_{22}}\ a_{23}\ a_{24} \dots \\
z_3 &= 0, a_{31}\ a_{32}\ \underline{a_{33}}\ a_{34} \dots \\
z_4 &= 0, a_{41}\ a_{42}\ a_{43}\ \underline{a_{44}} \dots \\
z_5 &= \dots \\
&\vdots \\
x &= 0, x_1\ \ x_2\ \ x_3\ \ x_4\ \dots
\end{aligned}
$$

with $\forall j, k \in \mathbb{N} : a_{j,k} \in [0, 9] \subset \mathbb{N}$. Now we define x_i as follows: $x_i = R_{10}(a_{ii} + 1)$. The important idea is the following: By assumption we start with a well-defined <u>countable</u> sequence of numbers. Therefore all x_i are also well-defined, and thereby x is too (even if it is infinitely long). Via our construction our x differs from all z_i at least in position i. As this is true for all $i \in \mathbb{N}$ we have that x cannot be part of our initial "**ordered and complete** sequence". As x is a well-defined real number, our sequence therefore can't be complete! This is a contradiction and $(0, 1)$ has to be uncountable.

Power sets and Cantor's theorem

Theorem 1: Cantor's Theorem

For any set A we have that there exists **no** surjective mapping $f : A \mapsto \mathcal{P}(A)$ onto its power set. This directly implies that $\mathcal{P}(A)$ always has a strictly greater cardinality than A. In particular, one can show that for any infinite set A the set $\mathcal{P}(A)$ is uncountable.

A proof of this theorem used to be an exam question. In order to encourage you to try it yourself it's part of the last hands-on.

Hands-On 4

4.1. Let A_i be a countable set for any $i \in \mathbb{N}$. Is

$$A = \bigcup_{i=1}^{n} A_i$$

countable for $n \in \mathbb{N}$? Prove your claim.

4.2. Now look at

$$A = \bigcup_{i=1}^{\infty} A_i$$

Is it countable? Prove your claim.
Can you extend your proof from exercise 1? If not, explain why.

4.3. Let

$$A = \{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N}\ f(n) \geq f(n+1)\}$$

Is A countable? Prove your claim.

4.4. Let

$$A = \{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N}\ (n\ even \to f(n) > f(n+1) \wedge n\ odd \to f(n) < f(n+1))\}$$

i.e. the set of alternating functions on $\mathbb{N}$.
Is A countable? Prove your claim.

1.5 Additional Exercises

Here, some additional challenging exercises are added, where various concepts are mixed. Especially lots of exercises about functions are covered.

Hands-On 5

5.1. Let A be an arbitrary non-empty set and let $f : A \to \mathcal{P}(A)$ be a function. Prove that $Z_f \notin f(A)$ for $Z_f := \{x \in A | x \notin f(x)\}$.

5.2. Let $\rho \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ be a relation on the set of all functions from $\mathbb{N}$ to $\mathbb{N}$ with

$$f \ \rho \ g :\Leftrightarrow |\{x \in \mathbb{N} \mid f(x) \neq g(x)\}| \leq 1.$$

Prove or disprove that ρ is an equivalence relation.

5.3. Let ρ be a relation on the set A of all functions from $\mathbb{N} \setminus \{0\}$ to $\mathbb{N} \setminus \{0\}$ with $f \, \rho \, g :\Leftrightarrow \forall x \, (f(x) \mid g(x))$. Prove that (A, ρ) is a poset and determine all minimal and least elements of it.

5.4. Let $f : A \to B$ be a function. Let's look at the following conditions:

- f is injective
- f is surjective
- f is bijective

Show that one of these conditions is sufficient and necessary for the statement: for all $X \subseteq A$ we have $f^{-1}(f(X)) = X$.

1.6 Solutions

1.6.1 Solutions for Hands-On 1

1.1

Proof. $\{2, 4, 6, 8\} = \{x \in \mathbb{N} \mid \exists k\ (2k = x) \wedge x > 0 \wedge x < 10\}$. □

1.2

Proof. $\{x \in \mathbb{N} \mid \exists k\ (2k = x) \wedge x > 0\}$. □

1.3

Proof. For simplicity, notice that $B = \{\emptyset, \{\emptyset\}\}$. For 5., keep in mind that $\mathcal{P}(\emptyset) = \{\emptyset\}$.

1. $A \cup B = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \Rightarrow |A \cup B| = 3$
2. $A \cap B = \{\emptyset, \{\emptyset\}\} \Rightarrow |A \cap B| = 2$
3. $\mathcal{P}(B) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} \Rightarrow |\mathcal{P}(B)| = 4$
4. $A \setminus \mathcal{P}(B) = \emptyset \Rightarrow |A \setminus \mathcal{P}(B)| = 0$
5. $B \times \mathcal{P}(\emptyset) = \{(\emptyset, \emptyset), (\{\emptyset\}, \emptyset)\} \Rightarrow |B \times \mathcal{P}(\emptyset)| = 2$

□

1.4

Proof. Assumption: $\mathcal{P}(A) = \mathcal{P}(B)$
Conclusion (to show): $A = B$
First, we will show that $A \subseteq B$.

Let $x \in A$ be any element of A.	
$\Rightarrow \{x\} \in \mathcal{P}(A)$	definition of power set
$\Rightarrow \{x\} \in \mathcal{P}(B)$	assumption
$\Rightarrow x \in B$	definition of power set

Now, we show that $B \subseteq A$.

Let $x \in B$ be any element of B.	
$\Rightarrow \{x\} \in \mathcal{P}(B)$	definition of power set
$\Rightarrow \{x\} \in \mathcal{P}(A)$	assumption
$\Rightarrow x \in A$	definition of power set

We have shown that $A \subseteq B$ and $B \subseteq A$. Combining these two results, we get $A = B$. □

1.5

Proof. First, we need to observe that the statement is false for $A = \emptyset$ and true otherwise.

1. Case $A = \emptyset$

   In this case, we get a counterexample for $B = \{0\}$ and $C = \{1\}$ since $\emptyset \times \{0\} = \emptyset = \emptyset \times \{1\}$, but $\{0\} \neq \{1\}$. So the statement is false for $A = \emptyset$.

2. Case $A \neq \emptyset$

We want to prove that the statement is true in this case.

Assumption: $A \times B = A \times C$

Conclusion (to show): $B = C$

Let $a \in A$ be an element of A which has to exist since $A \neq \emptyset$. We continue by making a further case distinction on B (we could also take C):

(a) Case $B = \emptyset$

$$
\begin{aligned}
& B = \emptyset \\
\Rightarrow\ & A \times B = \emptyset && \text{definition of cartesian product} \\
\Rightarrow\ & A \times C = \emptyset && \text{assumption} \\
\Rightarrow\ & C = \emptyset && \text{definition of cartesian product, } A \neq \emptyset \\
\Rightarrow\ & B = C && B = \emptyset = C
\end{aligned}
$$

(b) Case $B \neq \emptyset$

$$
\begin{aligned}
& \text{Let } x \in B \text{ be an arbitrary element of } B. \\
\Rightarrow\ & (a, x) \in A \times B && \text{definition of cartesian product} \\
\Rightarrow\ & (a, x) \in A \times C && \text{assumption} \\
\Rightarrow\ & x \in C && \text{definition of cartesian product}
\end{aligned}
$$

So we have proven that $B \subseteq C$. Analogously, we get that $C \subseteq B$. By definition of set equality we conclude that $B = C$.

Since the statement is true in all cases, we get that $A \times B = A \times C \Rightarrow B = C$ for all $A \neq \emptyset$.

All in all, we get that the statement is correct, if and only if, $A \neq \emptyset$. □

1.6

Proof. We have to show that $B = C$ by individually showing that $B \subseteq C$ and $C \subseteq B$.
1. $B \subseteq C$
Let $b \in B$ be arbitrary. We can distinct two cases
1. Case: $b \in A$
We have

$$
\begin{aligned}
b \in A &\Rightarrow b \in (A \cup B) \wedge b \in (A \cap B) \\
&\Rightarrow b \notin (A \cup B) \setminus (A \cap B) \\
&\overset{As.}{\Rightarrow} b \notin (A \cup C) \setminus (A \cap C) \\
&\overset{(1)}{\Rightarrow} b \in (A \cap C) \\
0 &\Rightarrow b \in C
\end{aligned}
$$

whereas (1) is based on $b \in (A \cup C)$ via assumption.
2. Case: $b \notin A$
We have

$$
\begin{aligned}
b \notin A &\Rightarrow b \in (A \cup B) \wedge b \notin (A \cap B) \\
&\Rightarrow b \in (A \cup B) \setminus (A \cap B) \\
&\overset{As}{\Rightarrow} b \in (A \cup C) \setminus (A \cap C) \\
&\overset{(1)}{\Rightarrow} b \in (A \cup C) \\
&\overset{(2)}{\Rightarrow} b \in C
\end{aligned}
$$

whereas (1) follows from the fact that we subtract from $(A \cup C)$ and (2) follows from $b \notin A$
We therefore have $B \subseteq C$
2. $C \subseteq B$
Follows analogous as it is completely symmetric to the first case.
3. Conclusion
We have shown that

$$(A \cup B) \setminus (A \cap B) = (A \cup C) \setminus (A \cap C) \Rightarrow B \subseteq C \land C \subseteq B$$

therefore

$$(A \cup B) \setminus (A \cap B) = (A \cup C) \setminus (A \cap C) \Rightarrow B = C$$

□

1.7

Claim 1.1

$\emptyset, \mathcal{P}(\emptyset), \mathcal{P}(\mathcal{P}(\emptyset)), \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))), \dots$ is a sequence of infinitely many different sets, where $S \subseteq P(S)$ is true for all S in the sequence.

Proof. We will use a classic proof by induction.
1. Base
Let $S = \emptyset$, then we have $\mathcal{P}(S) = \mathcal{P}(\emptyset) = \{\emptyset\}$ and by definition of $\emptyset$ trivially $\emptyset \subseteq \{\emptyset\}$
2. Hypothesis
Let S be an arbitrary set such that $S \subseteq \mathcal{P}(S)$ (i.e. such an S exists)
3. Step
Let S be an arbitrary set such that $S \subseteq \mathcal{P}(S)$, then we claim $\mathcal{P}(S) \subseteq \mathcal{P}(\mathcal{P}(S))$

$$\mathcal{P}(S) \subseteq \mathcal{P}(\mathcal{P}(S)) \Leftrightarrow \forall x \, (x \in \mathcal{P}(S) \rightarrow x \in \mathcal{P}(\mathcal{P}(S)))$$

Let $x \in \mathcal{P}(S)$ be arbitrary. We have $x \subseteq S$ by definition of the power set. Via induction hypothesis we also have that $S \subseteq \mathcal{P}(S)$ and therefore

$$x \subseteq S \subseteq \mathcal{P}(S) \Rightarrow x \subseteq \mathcal{P}(S) \Rightarrow x \in \mathcal{P}(\mathcal{P}(S))$$

using the transitivity of the subset relation. This concludes our proof.
To be completey correct we should also show that none of these sets are equal to one another. This directly follows from the fact that for all sets S we have $|S| < |\mathcal{P}(S)|$ □

1.6.2 Solutions for Hands-On 2

2.1

- reflexivity: ρ is not reflexive since for example $(a, a) \notin \rho$.
- irreflxivity: ρ is irreflexive because $(a, a), (b, b), (c, c), (d, d) \notin \rho$.
- symmetry: ρ is symmetric because $(a, b), (b, a) \in \rho$, $(b, c), (c, b) \in \rho$ and $(b, d), (d, b) \in \rho$.
- antisymmetry: ρ is not antisymmetric because, for example $(a, b), (b, a) \in \rho$, but $a \neq b$.
- transitivity: ρ is not transitive because, for example $(a, b), (b, c) \in \rho$, but $(a, c) \notin \rho$.

2.2

- $\widehat{\rho} = \rho = \{(b, a), (a, b), (c, b), (d, b), (b, c), (b, d)\}$
- $\rho^2 = \{(a, a), (a, c), (a, d), (b, b), (c, a), (c, c), (c, d), (d, a), (d, c), (d, d)\}$
- $\rho^* = \{(a, a), (a, b), (a, c), (a, d), (b, a), (b, b), (b, c), (b, d), (c, a), (c, b), (c, c), (c, d), (d, a)$
  $(d, b), (d, c), (d, d)\}$

2.3

1. This statement is false. A counter example is $\sigma = \{(1, 1), (1, 2)\}$ on the set $A = \{1, 2\}$ because σ is not reflexive as $(2, 2) \notin \sigma$ but also it is not irreflexive as $(1, 1) \in \sigma$.
2. This statement is true. Since $A \neq \emptyset$, there exists some $a \in A$. Due to the irreflexivity, we have $(a, a) \notin \sigma$. This immediately implies that σ is not reflexive.
3. This statement is false. A counter example is $\sigma = \{(1, 1)\}$ on the set $A = \{1\}$. This is symmetric because $(1, 1) \in \sigma$, but also antisymmetric as there are no two distinct elements $a, b \in A$ such that $(a, b), (b, a) \in \sigma$ (since A only has one element). This statement furthermore holds for any equivalence relation in which the individual classes have a cardinality of 1

2.4

Proof.

- reflexivity: to show that $\sim$ is reflexive, we have to show that $(x, y) \sim (x, y)$ for all $(x, y) \in \mathbb{R}^2$. Let $(x, y) \in \mathbb{R}^2$ be arbitrary. We have that $x^2 + y = x^2 + y$ so we have according to the definition of $\sim$ also $(x, y) \sim (x, y)$.
- symmetry: we have to show that if $(x, y) \sim (a, b)$ for any $(x, y), (a, b) \in \mathbb{R}^2$, then we also have $(a, b) \sim (x, y)$. Let $(x, y), (a, b) \in \mathbb{R}^2$ such that $(x, y) \sim (a, b)$. This means that $x^2 + b = a^2 + y$ which implies that $a^2 + y = x^2 + b$, so we have $(a, b) \sim (x, y)$.
- transitivity: to show that $\sim$ is transitive, we have to show that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ for any $(a, b), (c, d), (e, f) \in \mathbb{R}^2$ implies $(a, b) \sim (e, f)$. Let $(a, b), (c, d), (e, f) \in \mathbb{R}^2$ such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. This means that $a^2 + d = c^2 + b$ and $c^2 + f = e^2 + d$ which imply $a^2 + d + c^2 + f = c^2 + b + e^2 + d \Rightarrow a^2 + f = e^2 + b$ which means $(a, b) \sim (e, f)$.

We have proven that $\sim$ is reflexive, symmetric and transitive so it is an equivalence relation according to the definition. □

2.5

Proof. We will prove that $(A, \widehat{\preceq})$ is a poset.

- reflexivity: we have to show that $a \mathrel{\widehat{\preceq}} a$ for all $a \in A$. Let $a \in A$ be arbitrary. Since $(A, \preceq)$ is a poset, we have $a \preceq a$, which implies according to the definition of the inverse that $a \mathrel{\widehat{\preceq}} a$.

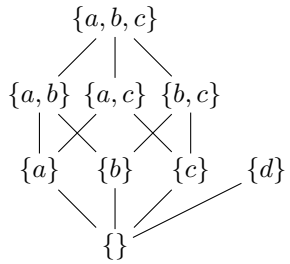
- antisymmetry: we have to show that if $a \mathrel{\widehat{\preceq}} b$ and $b \mathrel{\widehat{\preceq}} a$ for any $a, b \in A$, then we have $a = b$. Let $a, b \in A$ such that $a \mathrel{\widehat{\preceq}} b$ and $b \mathrel{\widehat{\preceq}} a$. According to the definition of the inverse, we get that $b \preceq a$ and $a \preceq b$. Since $\preceq$ is antisymmetric, we get that $a = b$.
- transitivity: we have to show that $a \mathrel{\widehat{\preceq}} b$ and $b \mathrel{\widehat{\preceq}} c$ for any $a, b, c \in A$ we have that $a \mathrel{\widehat{\preceq}} c$. Let $a, b, c \in A$ such that $a \mathrel{\widehat{\preceq}} b$ and $b \mathrel{\widehat{\preceq}} c$. According to the definition of the inverse, we have that $b \preceq a$ and $c \preceq b$. Since $\preceq$ is transitive, we get that $c \preceq a$ which implies that $a \mathrel{\widehat{\preceq}} c$

We have shown that $(A, \mathrel{\widehat{\preceq}})$ is reflexive, antisymmetric and transitive so it is a poset. □

2.6

Proof. Lets consider the relation $\rho = \{(a, a) \mid a \in \mathbb{N}\}$ on $\mathbb{N}$. ρ is obviously reflexive since $(a, a) \in \rho$ for all $a \in \mathbb{N}$. It is also symmetric because $a \ \rho \ b$ implies $b \ \rho \ a$ for all $a, b \in \mathbb{N}$ since there doesn't exist any $(a, b) \in \rho$ with $a \neq b$. For basically the same reason it is antisymmetric as well and it is also transitive because if we have $a \ \rho \ b$ and $b \ \rho \ c$ for any $a, b, c \in \mathbb{N}$, then we also have $a \ \rho \ c$ because again, there are no two different elements that are in the relation. □

2.7



The minimal element is $\{\}$, the maximal elements are $\{a, b, c\}$ and $\{d\}$. The least element is $\{\}$ while there is no greatest element.

2.8 The lower bounds of $\{\{a, b\}, \{a, c\}\}$ are $\{a\}$ and $\{\}$. Its greatest lower bound is $\{a\}$. The poset $(\mathcal{P}(\{a, b, c\}) \cup \{\{d\}\}, \subseteq)$ is not a lattice because for example $\{a\}$ and $\{d\}$ don't have a least upper bound.

2.9

Proof. We have

$$\begin{aligned}
\widehat{\rho\sigma} &= \{(c, a) \mid a \ \rho\sigma \ c\} \\
&= \{(c, a) \mid \exists b \in B : (a \ \rho \ b \ \wedge \ b \ \sigma \ c)\} \\
&= \{(c, a) \mid \exists b \in B : (b \ \sigma \ c \ \wedge \ a \ \rho \ b)\} \\
&= \{(c, a) \mid \exists b \in B : (c \ \widehat{\sigma} \ b \ \wedge \ b \ \widehat{\rho} \ a)\} \\
&= \widehat{\sigma}\widehat{\rho}
\end{aligned}$$

□

2.10

1. - Reflexivity : $\forall x \in \mathbb{Z} : x + x = 2 \cdot x$, hence $\sim$ is reflexive.
   - Symmetry : $\forall x, y \in \mathbb{Z} : x \sim y \iff x + y$ is even $\iff y + x$ is even $\iff y \sim x$, hence $\sim$ is symmetric.
   - Transitivity : $\forall x, y, z \in \mathbb{Z}$:

     $$\begin{aligned}
     x \sim y \wedge y \sim z &\Rightarrow \exists k, k' \in \mathbb{Z} : x + y = 2 \cdot k \wedge y + z = 2 \cdot k' \\
     &\Rightarrow x + z = x + 2 \cdot k' - y = x + 2 \cdot k' - (2 \cdot k - x) = 2(x + k' - k) \\
     &\Rightarrow x \sim z
     \end{aligned}$$

     Hence $\sim$ is transitive.

2.
- Reflexivity : $0 \cdot 0 = 0 \implies 0 \not\sim 0$, hence $\sim$ is not reflexive.
- Symmetry : $\forall x, y \in \mathbb{Z} : x \sim y \iff x \cdot y$ is odd $\iff y \cdot x$ is odd $\iff y \sim x$, hence $\sim$ is symmetric.
- Transitivity : $\forall x, y, z \in \mathbb{Z} : x \sim y \wedge y \sim z \implies x \cdot y$ is odd $\wedge\ y \cdot z$ is odd $\implies x, y, z$ are odd $\implies x \cdot z$ is odd $\implies x \sim z$, hence $\sim$ is transitive.

3.
- Reflexivity : $\forall x \in \mathbb{Z} : x + x \cdot x = x(1 + x) \implies x$ is even or $1 + x$ is even $\implies x \cdot (1 + x)$ is even $\implies x \sim x$, hence $\sim$ is reflexive.
- Symmetry : $0 \sim 1$ as $0 + 0 \cdot 1 = 0$ but $1 \not\sim 0$ as $1 + 1 \cdot 0 = 1$, hence $\sim$ is not symmetric.
- Transitivity : let $a, b \in \mathbb{Z}$:
  - a is even and b is even $\implies a + a \cdot b$ is even $\implies a \sim b$.
  - a is even and b is odd $\implies a + a \cdot b$ is even $\implies a \sim b$.
  - a is odd and b is even $\implies a + a \cdot b$ is odd $\implies a \not\sim b$.
  - a is odd and b is odd $\implies a + a \cdot b$ is even $\implies a \sim b$.

  It follows that $a \sim b \iff R_2(|a|) \leq R_2(|b|)$. Let $x, y, z \in \mathbb{Z} : x \sim y \wedge y \sim z \implies R_2(|x|) \leq R_2(|y|) \wedge R_2(|y|) \leq R_2(|z|) \implies R_2(|x|) \leq R_2(|z|) \implies x \sim z$, hence $\sim$ is transitive.

2.11

- Reflexivity : $\forall a \in \mathbb{N}^+ : gcd(a, a) = a$, hence ρ is reflexive.
- Antisymmetry : $\forall a, b \in \mathbb{N}^+ : a \rho b \wedge b \rho a \implies gcd(a, b) = a \wedge gcd(b, a) = b \implies a = gcd(a, b) = gcd(b, a) = b \implies a = b$, hence ρ is antisymmetric.
- Transitivity : $\forall a, b, c \in \mathbb{N}^+$:

$$\begin{aligned} a \rho b \wedge b \rho c &\Rightarrow gcd(a, b) = a \wedge gcd(b, c) = b \\ &\Rightarrow a | b \wedge b | c \\ &\Rightarrow a | c \\ &\Rightarrow gcd(a, c) = a \end{aligned}$$

  The third implication holds as the division relation is transitive, the last one holds as no integer greater than a can divide a, it follows that a is the gcd. Hence ρ is transitive.

1.6.3 Solutions for Hands-On 3

3.1

Proof. We disprove this statement with a counterexample. Let $A = \{1, 2\}$, $B = \{1\}$ and f a function from the set $\{1, 2\}$ to $\{1\}$ with $f = \{(1, 1), (2, 1)\}$. We have that $f(A \setminus B) = \{f(x) \mid x \in \{A \setminus B\}\} = \{f(x) \mid x \in \{2\}\} = \{f(2)\} = \{1\}$ but $f(A) \setminus f(B) = \{f(x) \mid x \in A\} \setminus \{f(x) \mid x \in B\} = \{1\} \setminus \{1\} = \{\}$ so $f(A \setminus B) \neq f(A) \setminus f(B)$. Since we have found a counterexample, the statement is false. □

3.2

Proof.

"$\Rightarrow$": Let $a, b \in X$ such that $a \neq b$ (if that's not possible then the function is trivially injective as there's only one element in the domain). Let $A = \{a\}$ and $B = \{b\}$. We have

$$\begin{aligned} & \{a\} \cap \{b\} && = \emptyset \\ \Rightarrow & f(\{a\} \cap \{b\}) && = \emptyset \\ \overset{Ass}{\Rightarrow} & f(\{a\}) \cap f(\{b\}) && = \emptyset \\ \Rightarrow & f(a) \neq f(b) \end{aligned}$$

using that $f(\emptyset) = \emptyset$ (because nothing will get projected onto nothing) and that $f(a) \in f(\{a\})$ as $f(\{a\})$ is a set (even if it contains only one element). Now we've exactly shown that $a \neq b \Rightarrow f(a) \neq f(b)$ i.e. injectivity.

"$\Leftarrow$": 1) $f(A \cap B) \subseteq f(A) \cap f(B)$

Let $A \cap B \neq \emptyset$, because otherwise it's trivially true. Furthermore let z be an arbitrary element in $f(A \cap B)$ with $a \in (A \cap B), f(a) = z$.

We get

$$\begin{aligned} & a \in A \land a \in B \\ \Rightarrow & f(a) \in f(A) \land f(a) \in f(B) \\ \Rightarrow & z \in f(A) \cap f(B) \\ \Rightarrow & f(A \cap B) \subseteq f(A) \cap f(B) \end{aligned}$$

2) $f(A) \cap f(B) \subseteq f(A \cap B)$

Let $z \in f(A) \cap f(B)$ be arbitrary ($\emptyset$ is again trivial). We have

$$\begin{aligned} & z \in f(A) \land z \in f(B) \\ \Rightarrow & \exists a \in A, b \in B : f(a) = z \land f(b) = z \\ \overset{Inj}{\Rightarrow} & a = b \\ \Rightarrow & \exists a \in A \cap B : f(a) = z \\ \Rightarrow & z \in f(A \cap B) \\ \Rightarrow & f(A) \cap f(B) \subseteq f(A \cap B) \end{aligned}$$

As the function is injective, there can exist at most one element a in X such that $f(a) = z$. A and B have to contain the same element.

We have shown that $f(A \cap B) = f(A) \cap f(B)$, concluding the proof.

□

3.3

Proof. Because of the iff, we have to prove two directions.

- There exists an injective function $f : A \to B \Rightarrow$ there exists a surjective function $g : B \to A$.

  Let $f : A \to B$ be an injective function. Let $a \in A$ be arbitrary (which exists because A is non-empty) and $g : B \to A$ be a function with

  $$g : \begin{cases} x \mapsto f^{-1}(x) & \text{, if the inverse } f^{-1}(x) \text{ exists} \\ x \mapsto a & \text{, else} \end{cases}$$

  . Let $a \in A$ be arbitrary and $b \in B$ such that $b = f(a)$. According to the definition of g and because f is injective (so $f^{-1}(b)$ is unique), we have that $g(b) = f^{-1}(b) = a$. Hence, g is surjective. Therefore, we have found a surjective function g in this case.

- There exists a surjective function $g : B \to A \Rightarrow$ there exists an injective function $f : A \to B$.

  Let $g : B \to A$ be a surjective function. Let $f : A \to B$ be a functions such that for any $a \in A$, we have that $f(a) := b$ for some $b \in B$ with $g(b) = a$ which exists because g is surjective. It follows $a = g(b) = g(f(a)) = (g \circ f)(a)$. Let $a, a' \in A$ with $f(a) = f(a')$. Because of the definition of f, we also get $a = (g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a') = a'$ so f is injective. Therefore, we have found an injective funtion f in this case.

□

3.4

Claim

We claim that F is not injective.

Proof. First let us take a look at the map of the constant 0 function $\forall x.\ g(x) = 0$. Trivially we have $F(g) = g \circ g = 0$ for all x. In order to show that F is not injective we will create another function g' that will also be mapped to the 0 function. Let

$$\begin{aligned} g' &: \mathbb{N} \to \mathbb{N} \\ g'(0) &\mapsto 0 \\ g'(1) &\mapsto 0 \\ g'(x) &\mapsto 1 \end{aligned}$$

Trivially $g \neq g'$. Now realize that $Im(g') = \{0, 1\}$ and therefore (as $g'(0) = 0$ and $g'(1) = 0$) $\forall x.\ (g' \circ g')(x) = g'(g'(x)) = 0$. Therefore $F(g) = F(g') \wedge g! = g'$ and by definition of injectivity F is not injective. □

Claim

We claim that F is not surjective.

Proof. We will prove this by finding a function f such that $\nexists g.\ F(g) = f$. (When this was an exam question this function was actually provided to you). Define f as

$$\begin{aligned} f &: \mathbb{N} \to \mathbb{N} \\ f(0) &\mapsto 1 \\ f(1) &\mapsto 0 \\ f(x) &\mapsto x \end{aligned}$$

Now we continue by assuming there exists a g s.t. $g \circ g = f$. We proceed by case distinction over the possible mappings of g:

Constraints

$$(g \circ g)(0) = f(0) = 1 \quad (1)$$
$$(g \circ g)(1) = f(1) = 0 \quad (2)$$
$$(g \circ g)(x) = f(x) = x \quad (3)$$

1. Case $g(0) = 0$
Then via (1)

$$\begin{aligned} (g \circ g)(0) &= f(0) \\ \Rightarrow g(g(0)) &= f(0) \\ \Rightarrow g(0) &= f(0) \\ \Rightarrow g(0) &= 1 \end{aligned}$$

A contradiction.
2. Case $g(0) = 1$
Then via (1)

$$\begin{aligned} (g \circ g)(0) &= f(0) \\ \Rightarrow g(g(0)) &= f(0) \\ \Rightarrow g(1) &= 1 \end{aligned}$$

using this we get via (2)

$$\begin{aligned} (g \circ g)(1) &= f(1) \\ \Rightarrow g(g(1)) &= f(1) \\ \Rightarrow g(1) &= 0 \end{aligned}$$

A contradiction.
3. Case $g(0) = k$ with $k > 1$
Then via (1)

$$\begin{aligned} (g \circ g)(0) &= f(0) \\ \Rightarrow g(g(0)) &= 1 \\ \Rightarrow g(k) &= 1 \end{aligned}$$

Now we get via (3)

$$\begin{aligned} (g \circ g)(k) &= f(k) \\ \Rightarrow g(g(k)) &= k \\ \Rightarrow g(1) &= k \end{aligned}$$

But then via (2)

$$\begin{aligned} (g \circ g)(1) &= f(1) \\ \Rightarrow g(g(1)) &= 0 \\ \Rightarrow g(k) &= 0 \end{aligned}$$

A contradiction.
As the case distinction was complete this concludes the proof. □

1.6.4 Solutions for Hands-On 4

4.1

Claim

We claim that $A = \bigcup_{i=1}^{n} A_i$ is countable.

Proof. We will prove it via induction but a proof via primes is also possible.
1. **Basis**
We've already shown that the union of two countable sets is countable.
2. **Assumption**
Assume that the union of n countable sets is countable.
3. **Step**: $n \to n+1$
We have to look at

$$\bigcup_{i=1}^{n+1} A_i = \bigcup_{i=1}^{n} A_i \cup A_{n+1}$$

and via our inductive assumption realize that $\bigcup_{i=1}^{n} A_i$ is countable. Furthermore A_{n+1} is countable by definition of the A_i's. We have already shown that the union of two countable sets is countable which concludes the proof. □

4.2

Claim

We claim that $A = \bigcup_{i=1}^{\infty} A_i$ is countable.

Proof. We can prove this geometrically. Since all sets A_i are countable, for each of them there exists an injection $f_i : A_i \to \mathbb{N}$. Using these injections, we can construct a new injection $F : \bigcup_{i=1}^{\infty} A_i \to \mathbb{N} \times \mathbb{N}$ in the following way. For all $i \in \mathbb{N}$, for all $a_i \in A_i$, we define

$$F(a_i) = (i, f_i(a))$$

Clearly, F is injective. We can easily see this, since for $a, a' \in \bigcup_{i=1}^{\infty} A_i$ and $a \neq a'$ we have $F(a) \neq F(a')$, since either a and a' are from different sets $A_i \neq A_j$ or they are from the same set A_i, in which case $f_i(a) \neq f_i(a')$ due to the injectivity of f_i. In both cases, $F(a) \neq F(a')$.
Since $\mathbb{N} \times \mathbb{N}$ is countable and F is injective, $\bigcup_{i=1}^{\infty} A_i$ is countable.

□

Note: In this proof we neglect the fact that the same element may occur multiple times in different sets. To get a rigorous definition of the function F, we would therefore need to explicitly exclude double-definitions for reoccurring elements. We omit this in favor of readability, as the correctness of the proof doesn't depend on it.
If we would have chosen the primes approach in (1) then we could have generalized it for (2) as we could make use of infinite number of primes. **Nevertheless** this does not hold for the induction approach (which is a very common mistake!). Showing that something holds for an arbitrarily large but finite n is not equal to showing that it holds for infinity!

4.3

Claim

We claim that $A = \{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N}\ f(n) \geq f(n+1)\}$ is countable.

We will provide two proofs as each one emphasizes a different yet equally important take on such a task

Proof. We start of by splitting $S_\infty := A = \{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N} f(n) \geq f(n+1)\}$ into subsets S_N, with each $S_N = \{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N} f(n) \geq f(n+1) \wedge f(0) = N\}$ i.e. all functions that "start at N". Given that every function in A has exactly one value $f(0) \in \mathbb{N}$ we have

$$S_\infty = \bigcup_{N=0}^{\infty} S_N$$

We already know that the union of countably many countable sets is countable, so we're left with showing that $\forall N \in \mathbb{N} S_N$ is countable. We will prove this via induction on N (though other methods also work here):

1. Basis

For $N = 0$ there exists only one function, namely $\forall n \in \mathbb{N} : f(n) = 0$. As the set containing this function is finite, it is countable.

2. Assumption

For arbitrary $N \in \mathbb{N}$ let S_N be countable.

3. Step $N \to N + 1$

We have to show that S_{N+1} is countable. There are two types of functions in S_{N+1}, exactly one that never falls, i.e. $\forall n \in \mathbb{N} : f(n) = N + 1$ always and all other functions which have a smallest $k \in \mathbb{N}$ such that $f(k) > f(k + 1)$. These functions will then fulfil (via monotonicity assumption) $\forall n > k : f(n) \leq N$. In particular we're able to describe them through a function in S_N, that behaves the same for all $k' \geq k + 1$. In conclusion we can identify every function $f \in S_{N+1}$ that drops at least once with the tuple $(k, f'_{k,f(n)}) \in N \times S_N$ where k marks the the first drop and $f'_{k,f(n)}$ is the function in S_N that shares the same behaviour after the drop. We have already shown that the product of countable sets is countable and as both $\mathbb{N}$ and S_N are countable via assumption so is $\mathbb{N} \times S_N$ and in turn all (minus 1) functions in S_{N+1}. Finally we unify this result with the single constant function, which obviously doesn't change the countability and our induction is finished.

□

Proof. This approach might be even more elegant than the last one. As all functions are monotonically decreasing, we can "encode" them in a string containing their consecutive values

$$\begin{aligned} \phi : \mathbb{N}^{\mathbb{N}} &\to \mathbb{N}^{\infty} \\ f &\to f(0)f(1)f(2)f(3)... = x_0x_1x_2x_3... \end{aligned}$$

As every function f has a last k for which $f(k-1) > f(k)$ the resulting string will repeat itself for all $k' > k$. Therefore we can maintain a unique encoding by just "cutting" $\phi(f)$ after position k. Let us call this mapping

$$\begin{aligned} \phi' : \mathbb{N}^{\mathbb{N}} &\to \mathbb{N}^{*} \\ f &\to f(0)f(1)f(2)f(3)...f(k_f) = x_0x_1x_2x_3...x_{k_f} \end{aligned}$$

Now every function corresponds to one **finite length** string. As ϕ' is injective by construction we are left with showing that $\mathbb{N}^* = \bigcup_{k=0}^{\infty} \mathbb{N}^k$ is countable. Every $\mathbb{N}^k$ is countable for $k \in \mathbb{N}$ (we've already shown that) and furthermore we've also shown that the countable union of countable sets is itself countable. Therefore $\bigcup_{k=0}^{\infty} \mathbb{N}^k$ is countable. This concludes the proof as it implies that A is countable. □

4.4

Claim

We claim that $A = \{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N}\ (n\ even \to f(n) > f(n+1) \wedge n\ odd \to f(n) < f(n+1))\}$ is uncountable.

Proof. We will prove that this set is uncountable, to do that we show an injection g from the set of semi-infinite bit-strings to A ($g : \{0,1\}^{\infty} \to A$). Let $\alpha \in \{0,1\}^{\infty}$ be an arbitrary semi-infinite bit-string. We define $g(\alpha) = f_\alpha$, where $f_\alpha \in A$ is defined as follows :

$$\forall n \in \mathbb{N} : f_\alpha(n) = \begin{cases} 2 & \text{if } n = 2k \text{ for some } k \in \mathbb{N} \\ \alpha_k & \text{if } n = 2k + 1 \text{ for some } k \in \mathbb{N} \end{cases}$$

Notice that α_k is the k-th bit of bit-string α. We now show that for any $\alpha \in \{0,1\}^{\infty}$ the constructed function $g(\alpha) = f_\alpha$ belongs to the set A. Let $\alpha \in \{0,1\}^{\infty}$ be an arbitrary semi-infinite bit-string.

Let $n \in \mathbb{N}$ be arbitrary, if n is even then there exists some $k \in \mathbb{N}$ with $n = 2k$, $f_\alpha(n) = 2$ and $f_\alpha(n+1) = \alpha_k \in \{0,1\}$, therefore $f_\alpha(n+1) > f_\alpha(n)$. Using a similar argument one can show that when n is odd then $f_\alpha(n) < f_\alpha(n+1)$, it follows that $g(\alpha) = f_\alpha \in A$ for all $\alpha \in \{0,1\}^\infty$. We now have to show that g is an injection. Let $\alpha \in \{0,1\}^\infty$ and $\beta \in \{0,1\}^\infty$ be two arbitrary semi-infinite bit-strings with $\alpha \neq \beta$, we have to show that $f_\alpha \neq f_\beta$. As the bit-strings α and β differ there must be a position where the two bit-strings differ, therefore there must exist some $k \in \mathbb{N}$ with $\alpha_k \neq \beta_k$. We now set $n = 2k+1$, and see that $f_\alpha(n) = \alpha_k \neq \beta_k = f_\beta(n)$, this implies that the functions $g(\alpha) = f_\alpha$ and $g(\beta) = f_\beta$ are different. This implies that the function g we gave is injective. From the existence of an injection from an uncountable set ($\{0,1\}^\infty$) to A one can easily show that A has to be uncountable too. $\square$

1.6.5 Solutions for Hands-On 5

5.1

Proof. This proof works by contradiction: Assume that $Z_f \in f(A)$. I.e. there exists at least one $a \in A$ for which $f(a) = Z_f$. Now we continue with a case distinction:
1. Case: $a \in Z_f$
Then we have

$$\begin{aligned} a \in Z_f &\Rightarrow a \notin f(a) \\ &\Rightarrow a \notin Z_f \end{aligned}$$

a contradiction.
2. Case: $a \notin Z_f$
Now we have

$$\begin{aligned} a \notin Z_f &\Rightarrow a \in f(a) \\ &\Rightarrow a \in Z_f \end{aligned}$$

also a contradiction.
As the case distinction was complete (as either $a \in Z_f$ or $a \notin Z_f$), we conclude that our assumption had to be wrong. There does not exist an $a \in A$ such that $f(a) = Z_f$ and thus $Z_f \notin f(A)$ This concludes the proof. □

5.2

Proof. We will show that this relation is not transitive. Let $f, g, h \in \mathbb{N}^{\mathbb{N}}$ such that $f : n \mapsto 1$ and

$$g : \begin{cases} n \mapsto 0 & \text{, if } n = 0 \\ n \mapsto 1 & \text{, else} \end{cases}$$

$$h : \begin{cases} n \mapsto 0 & \text{, if } n = 0 \vee n = 1 \\ n \mapsto 1 & \text{, else} \end{cases}$$

It's easy to see that these functions satisfy $f \ \rho \ g$, $g \ \rho \ h$, but not $f \ \rho \ h$. Therefore, we have found a counterexample for transitivity and thus ρ is not an equivalence relation. □

5.3

Proof. We will show that ρ on A is reflexive, antisymmetric and transitiv seperately.

- reflexivity: for any $f \in \mathbb{N} \setminus \{0\}^{\mathbb{N}\setminus\{0\}}$ be arbitrary. We have that $f(x) | f(x)$ for any $x \in \mathbb{N} \setminus \{0\}$ because $f(x) \cdot 1 = f(x)$. Hence, it is reflexive.

- antisymmetry: let $f, h \in \mathbb{N} \setminus \{0\}^{\mathbb{N}\setminus\{0\}}$ such that $f \ \rho \ h$ and $h \ \rho \ f$. According to the definition of ρ, we get that $\forall x \ (f(x) \mid g(x) \wedge g(x) \mid f(x))$. Therefore, for all $x \in \mathbb{N} \setminus \{0\}$ there exist some $c_1, c_2 \in \mathbb{N}$ such that $f(x)c_1 = g(x)$ and $g(x)c_2 = f(x)$, which implies $f(x)c_1c_2 = f(x)$, so we have $c_1 = c_2 = 1$. Therefore, we have $f(x) = g(x)$ for any $x \in \mathbb{N} \setminus \{0\}$. Hence, antisymmetry is proven.

- transitivity: let $f, g, h \in \mathbb{N} \setminus \{0\}^{\mathbb{N}\setminus\{0\}}$ such that $f \ \rho \ g$ and $g \ \rho \ h$. According to the definition of ρ we have that $f \ \rho \ g :\Leftrightarrow \forall x \ (f(x) \mid g(x))$ and $g \ \rho \ h :\Leftrightarrow \forall x \ (g(x) \mid h(x))$. For any $x \in \mathbb{N}$ we get that $f(x) | g(x)$ and $g(x) | h(x)$. According to the definition of $|$, there exists $c_1, c_2 \in \mathbb{N}$ such that $f(x)c_1 = g(x)$ and $g(x)c_2 = h(x)$. So we get $f(x)(c_1c_2) = h(x)$ which means $f(x) | h(x)$. Hence, ρ is transitive.

Hence, we have proven that ρ on A is reflexive, antisymmetric and transitiv and therefore, (A, ρ) is a poset. The least element and the only minimal element is the function f that fulfills $f(n) := 1 \ \forall n \in \mathbb{N} \setminus \{0\}$. □

5.4

Proof. Let us first revise the definitions of sufficient and necessary:

- We say that A is sufficient for B if $A \Rightarrow B$ holds
- We say that A is necessary for B if $\neg A \Rightarrow \neg B$ holds

Furthermore let $f^{-1} : B \to A$ denote the inverse function of f if it exists.

We will show that injectivity is a sufficient and a necessary condition for the statement.

Let f be injective. Let $x \in X$ be arbitrary. Trivially we have that $x \in f^{-1}(f(X))$ as $f(x) \in f(X)$ and $\forall a \in A\ f(a) = f(x) \Rightarrow a \in f^{-1}(f(X))$. This implies that $X \subseteq f^{-1}(f(X))$. Now assume there exists a $y \in f^{-1}(f(X)) \wedge y \notin X$. According to the definition of the inverse, there has to exist a $z \in f(X)$ such that $f(y) = z$. Using the same definition we conclude that there also needs to exist a $x' \in X$ with $f(x') = z$ (as $z \in f(X)$). But as $y \notin X$ and $x' \in X$ they can't be the same element and we get $x' \neq y \wedge f(x') = f(y)$ which is a contradiction given $f's$ injectivity. Therefore $f^{-1}(f(X)) \subseteq X$. Putting it together yields the result $f^{-1}(f(X)) = X$

Let the statement "for all $X \subseteq A$ we have $f^{-1}(f(X)) = X$" be true. Let $a_1, a_2 \in A$ be such that $f(a_1) = f(a_2)$ and $a_1 \neq a_2$. For $X = \{a_1, a_2\}$ we get $f^{-1}(f(\{a_1, a_2\})) = f^{-1}(f(X)) = X = \{a_1, a_2\}$, which means that $f(a_1) \neq f(a_2)$ and hence, f is injective. □

2 Number Theory

2.1 Divisibility

For all variables where it's not explicitly stated otherwise we'll assume the domain to be $\mathbb{Z}$. Nevertheless most constructs and concepts usually hold for a wider variety of arithmetic structures.

Definition 2.1. *We say $a \mid b$, if there exists an integer such that b=ac. If the divisor is unique we can write $c = \frac{b}{a}$*

Moreover we define that every non-zero integer is a divisor of 0 and that 1 and -1 are divisors of every integer.

More generally we can define for all integers a and b the *division with remainder:*

Theorem 2

$$\forall a \forall b \exists c \exists r \; b = ac + r \wedge 0 \leq r < |a|$$

In the case $a \mid b$, we will get $r = 0$

2.2 Greatest Common Divisor

For every integers a and b (not both 0) we can define a greatest common divisor which we will denote as gcd(a,b):

Definition 2.2. *The gcd d for a and b is defined as:*

$$d \mid a \;\wedge\; d \mid b \;\wedge\; \forall c \; ((c \mid a \;\wedge\; c \mid b) \;\rightarrow\; c \mid d)$$

If gcd(a,b) = 1, then we call a and b *relatively prime.*

One very useful Lemma is the following:

Lemma 2.1

$\forall q \in \mathbb{Z}$ we have

$$gcd(m, n) = gcd(n, m)$$

and

$$gcd(m, n) = gcd(m, n - qm)$$

2.3 Euclid's Extended GCD Algorithm

For $a, b \in \mathbb{Z}$ (not both 0), there exist $u, v \in \mathbb{Z}$ such that

$$\text{gcd(a,b)} = \text{ua} + \text{vb}$$

We can use Euclid's Extended GCD Algorithm to efficiently compute this u and v. In this script we will show an alternative way to execute this algorithm which is more suitable for a computation by hand. In the official script of the course you can find the original description of the algorithm (which is suitable for implementation on a computer).
The algorithm can be separated into two phases

1. Calculating the gcd of the numbers a and b

2. Recovering the corresponding numbers u and v

To explain our approach we will work with the example of calculating the gcd (and corresponding u and v) for a=553 and b=26.

Phase 1
In each step of this phase you have to perform a division with remainder, i.e. to find the respective c and r for the equation $b = ac + r$.
In our example we will find $553 = 26 \cdot 21 + 7$. Now we take the smaller of the two original numbers and the remainder r and perform another division with remainder(in this case 26 and 7). We continue executing this schema until the remainder r=0. We write down all intermediate steps of what we have done in the following way:

$$553 - 26 \cdot 21 = 7 \quad (1)$$
$$26 - 7 \cdot 3 = 5 \quad (2)$$
$$7 - 5 \cdot 1 = 2 \quad (3)$$
$$5 - 2 \cdot 2 = 1 \quad (4)$$
$$2 - 1 \cdot 2 = 0 \quad (5)$$

The gcd(a,b) is the last $r \neq 0$ which we have calculated (i.e. the number behind the equal-sign in the second to last line). In our case we get gcd(553,26) = 1.

Phase 2
In this phase we will make use of what we have written down in Phase 1 to recover the u and v such that we get $553 \cdot u + 26 * v = gcd(553, 26) = 1$.
To start we take the second to last equation of our calculations in Phase 1 (remember that this equation already has the gcd(a,b) as the right hand side of the equation). For our example this means that we start with (4)

$$5 - 2 \cdot 2 = 1$$

In each step of our equations we know that one of the numbers was the remainder (the number on the right hand side) of the equation above it. In our example the equation above is (3) $7 - 1 \cdot 5 = 2$. We can now just insert (3) into (4) to get

$$5 - 2 \cdot (7 - 1 \cdot 5) = 1$$

This can be simplified to

$$(-2) \cdot 7 + 3 \cdot 5 = 1$$

Now we can use (2) to substitute the 5 so that we get

$$(-2) \cdot 7 + 3 \cdot (26 - 7 \cdot 3) = 1$$

which simplifies to

$$3 \cdot 26 - 11 \cdot 7 = 1$$

We just always continue substituting the smaller number for one of the equations higher up. So for our last step we use (1) to substitute 7.

$$3 \cdot 26 - 11 \cdot (553 - 26 \cdot 21) = 1$$

so that we finally get

$$553 \cdot (-11) + 26 \cdot 234 = 1$$

which means u = -11 and v=234.

2.4 GCD Tableau

Quite often we just need the a quick way to do all these computations together. One way to do this is writing them in a compact table. For the given numbers $a = 553$ and $b = 26$ we get the following one:

a	b	q	u_1	u_2	v_1	v_2
553	26	21	1	0	0	1
26	7	3	0	1	1	-21
7	5	1	1	-3	-21	64
5	2	2	-3	4	64	-85
2	1	0	4	-11	-85	234
1	0	2	-11	4	234	-85

by simply applying the following set of rules (given that x_i describes a variable ($x \in \{a, b, q, u_1, u_2\}$) in the i-th row):

- The first row contains our a and b as well as the $q = \lfloor \frac{a}{b} \rfloor$. The other variables are always 1 0 0 1.
- For any row $i > 1$ we have $a_i = b_{i-1}$, $b_i = a_{i-1}\ mod\ b_{i-1}$, $q_i = \lfloor \frac{a_i}{b_i} \rfloor$, $(u_1)_i = (u_2)_{i-1}$ as well as $(v_1)_i = (v_2)_{i-1}$
- For any row $i > 1$ we have $(u_2)_i = (u_1)_{i-1} - q_{i-1} * (u_2)_{i-1}$ as well as $(v_2)_i = (v_1)_{i-1} - q_{i-1} * (v_2)_{i-1}$
- Repeat this until $b = 0$
- a contains the gcd. u_1, v_1 contain the respective factors to get it via multiplication.

While these "formulas" look like a lot in the beginning, more than half of it is just simply transferring values. After having done it several times it's a really fast way to calculate the gcd.

2.5 Ideals

Definition 2.3. *We define the Ideal generated by two integers a and b in the following way:*

$$(a, b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$$

A special case is the ideal defined by only one integer

$$(a) = \{ua \mid u \in \mathbb{Z}\}$$

Moreover we know about the following two Lemmas (4.3 and 4.4) from the course script.

Collection 2.1

- For $a, b \in \mathbb{Z}$ there exists $d \in \mathbb{Z}$ such that $(a, b) = (d)$.
- Let $a, b \in \mathbb{Z}$ (not both 0). If $(a, b) = (d)$, then d is a greatest common divisor of a and b.

As a matter of fact the *gcd* of a and b is the smallest positive element in their ideal: $(a, b) = (gcd(a, b))$.

Generally it can be noted that ideals are the topic of relatively few exam problems.

2.6 Irrationality of Roots and Logarithms

Usually when you have to prove the irrationality of a number, you do a proof by contradiction. You assume that the number is rational and show that this assumption leads to a contradiction to some fundamental knowledge about numbers that you already have (in the scope of this course the contradiction will usually be with the Unique Prime Factorization)

Definition 2.4. *Every positive integer can be written uniquely as the product of primes.*

Example. Here we show as an example that $\log_5 7$ is irrational:

1. Assume that $\log_5 7 \in \mathbb{Q}$ i.e. $log_5 7 = \frac{a}{b}$
2. Show that this leads to a contradiction

$$log_5 7 = \frac{a}{b}$$
$$7 = 5^{\frac{a}{b}}$$
$$7^b = 5^a$$

This contradicts the unique prime factorization, because it would mean that two numbers with different prime factorizations are equal. Thus $\log_5 7$ has to be irrational.

For roots the script already gives us the following theorem (4.9) which could be proved through a similar approach.

Theorem 3

$\sqrt{n}$ is irrational unless n is a square ($n = c^2$ for some $c \in \mathbb{Z}$)

2.7 Least Common Multiples

The least common multiple of two positive integers a and b is well-defined and unique. It can be denoted lcm(a,b).

Definition 2.5. *The lcm l for a and b is defined as*

$$a \mid l \ \wedge \ b \mid l \ \wedge \ \forall m((\ a \mid m \ \wedge \ b \mid m) \rightarrow l \mid m\ )$$

The least common multiple is closely related to the greatest common divisor (gcd). In fact it holds that:

$$gcd(a,b) \cdot lcm(a,b) = ab$$

This can be explained by looking at the unique prime factorization of a and b

$$a = \prod_i p_i^{e_i} \qquad b = \prod_i p_i^{f_i}$$

It follows that

$$gcd(a,b) = \prod_i p_i^{min(e_i,f_i)}$$

and

$$lcm(a,b) = \prod_i p_i^{max(e_i,f_i)}$$

Hands-On 1

1.1. Give the prime factorization of 45 and 42. Then use the factorizations to calculate:

1. gcd (45,42)
2. lcm (45,42)
3. $45 \cdot 42$

1.2. Let n be a positive integer and let D_n be the set of all positive divisors of n. Show

$$|D_n| \text{ is not even } \iff \exists r \in \mathbb{N} \text{ such that } r^2 = n$$

1.3. Prove that gcd(x-zy, y) = gcd(x,y)

1.4. Let $a, b \in \mathbb{Z}$ be any two different integers. Prove that there exists infinitely many $k \in \mathbb{Z}$ such that $a + k$ and $b + k$ are relatively prime. (You can use 1.3)

2.8 Modular Congruences and Arithmetic

Definition 2.6. *We define modular congruence in the following way*

$$a \equiv_m b :\Longleftrightarrow m \mid (a - b)$$

We say that *a is congruent to b modulo m.*

Lemma 2.2

It follows that

$$a = b \Longrightarrow a \equiv_m b$$

and

$$a \not\equiv_m b \Longrightarrow a \neq b$$

The second lemma can be very useful for proving inequalities with case distinction (e.g. for m=2 you can do a case distinction for even and odd numbers).

Note these important rules which are given in Lemma 4.14 (script):
If $a \equiv_m b$ and $c \equiv_m d$, then

$$a + c \equiv_m b + d \quad and \quad ac \equiv_m bd$$

For any $m \geq 1$, $\equiv_m$ is an equivalence relation on $\mathbb{Z}$ with m equivalence classes [0], [1], ... , [m-1]. Each of those equivalence classes is represented by one of the possible remainder modulo m.

We introduce the notation for a remainder modulo m $R_m(a)$.This remainder is just a number $R_m(a) \in \mathbb{Z}$, which represents the remainder in a *division with remainder* of a by m. The concept of a remainder modulo m and congruence modulo m are very similar. In fact the two concepts are closely connected through Lemma 4.16 (script)

1. $a \equiv_m R_m(a)$
2. $a \equiv_m b \Longleftrightarrow R_m(a) = R_m(b)$

The following arithmetic rules concerning the remainder operator, which are given by Lemma 4.18, are important and will be useful in many exam problems for number theory and are also essential to understanding the Diffie-Hellman protocol:

1. $R_m(a + b) = R_m(R_m(a) + R_m(b))$
2. $R_m(ab) = R_m(R_m(a) * R_m(b))$

2.9 Multiplicative Inverses

Lemma 2.3

The congruence equation $ax \equiv_m 1$ has a solution $x \in \mathbb{Z}_m$ if and only if gcd(a,m) = 1. The solution is unique.

We call x the *multiplicative inverse of a modulo m.* And we use the following notations $x \equiv_m a^{-1}$ or $x \equiv_m \frac{1}{a}$. If $gcd(a, m) \neq 1$ then no multiplicative inverse modulo m exists for a.
To calculate the multiplicative inverse efficiently we can use Euclid's Extended GCD Algorithm. If we set $b = m$, then the Algorithm will give us u and v such that $au + mv = 1$. It then follows that $m \mid (au - 1)$ which is the definition of $au \equiv_m 1$. This means that the u we found through the algorithm is our multiplicative inverse $x = u$.

Hands-On 2

2.1. Show that for every odd $a \in \mathbb{N}$ holds either $3 \mid a$, or $3 \mid (a + 2)$, or $3 \mid (a + 4)$

2.2. Show that $11 \mid (2^{2016} + 3^{2016} - 1)$

2.3. Let s_a be the sum of the decimal digits of $a \in \mathbb{N}$. Show that

$$R_9(a) = R_9(s_a)$$

2.4. Calculate $R_9(98877766665555544444433333332222222211111111)$.

2.10 Chinese Remainder Theorem

Definition 2.7. *For $m_1, m_2, ..., m_r$ pairwise relatively prime, the systems of congruence equations*

$$\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ &... \\ x &\equiv_{m_r} a_r \end{aligned}$$

has a unique solution satisfying $0 \leq x < M = \prod_{i=1}^{r} m_i$

The Chinese Remainder Theorem can be useful in two different ways:

1. It tells us that for a certain set of equations a unique solution exists in a certain range of numbers. This can be useful for more abstract exercises where we are not given explicit values.
2. It can show us how to construct the solution, i.e. how to find the x which satisfies all the equations. This will give us the explicit solution in exercises with explicit values in the problem.

We will now show how to construct this explicit solution:
First we define $M_i = M/m_i$ for each i. Now for each of these M_i we have to find the multiplicative inverse modulo m_i, i.e. we have to find N_i such that

$$M_i N_i \equiv_{m_i} 1$$

As explained in the previous chapter you can find these N_i by using Euclid's Algorithm, but often the numbers are small and you can save time by trying out the possibilities in your head.
Now you can already calculate the solution to the equation system by using the sub-results you just calculated:

$$x = R_M \left(\sum_{i=1}^{r} a_i M_i N_i \right)$$

2.11 Diffie-Hellman protocol

The Diffie-Hellmann protocol is used to solve the *key distribution* problem. The final goal of the protocol is that both communicating parties (usually called Alice and Bob) are in possession of a secret key, which no outside party can know. The protocol is based on the important assumption that *exponentiation can be computed efficiently, but computing logarithms (the inverse operation) can* ***not*** *be done efficiently.*
The public parameters of the protocol are a (very large) prime number p and the generator g. These parameters are known by everybody including potential adversarial parties. Moreover Alice and Bob can only communicate through a public/insecure channel. The protocol works in the following way

1. Alice selects x_A randomly from {0, ..., p-2}. This x_A will stay secret.
2. Alice efficiently calculates $y_A := R_p(g^{x_A})$. y_A will be public.
3. Bob selects x_B randomly from {0, ..., p-2}. This x_B will stay secret.
4. Bob efficiently calculates $y_B := R_p(g^{x_B})$. y_B will be public.
5. Now Alice and Bob exchange their respective public keys y_A and y_B through the public/insecure channel (due to the inefficiency of calculating logarithms it is not possible to calculate x_A even if y_A, p and g are known)
6. Alice efficiently calculates $k_{AB} := R_p(y_B^{x_A})$
7. Bob efficiently calculates $k_{BA} := R_p(y_A^{x_B})$
8. Through modular arithmetics we can see that $k_{AB} \equiv_p k_{BA}$:

$$k_{AB} \equiv_p y_B^{x_A} \equiv_p (g^{x_B})^{x_A} \equiv_p g^{x_A x_B} \equiv_p (g^{x_A})^{x_B} \equiv_p y_A^{x_B} \equiv_p k_{BA}$$

Thus we have achieved our goal: Alice and Bob are both in possession of the same secret key.

Hands-On 3

3.1. Calculate all the solutions $0 \leq x < 130$ for the following system of equations

$$x \equiv_2 1$$
$$x \equiv_5 2$$
$$x \equiv_{13} 3$$

3.2. Calculate all solutions in $\mathbb{N}$ for the following system of equations. Justify why you have all answers.

$$x \equiv_{10} 6$$
$$x \equiv_{15} 11$$

3.3. Calculate all solutions in $0 \leq x < 195$ for the following system of equations. Justify why you have all answers.

$$2 \cdot x^2 + 8 \equiv_{13} 6$$
$$x \equiv_{15} 2$$

3.4. Alice and Bob use the Diffie-Hellman key agreement protocol to communicate. The public parameters are $p = 19$ $g = 2$. The secret parameters which they choose are $x_A = 6$ and $x_B = 11$. Calculate y_A, y_B and the keys k_{AB} and k_{BA}

3.5. We give you an exercise that goes a bit beyond the material already covered, but you should be able to follow the steps below without reading ahead:
Find an isomorphism from $\mathbb{Z}_3 \times \mathbb{Z}_5$ to $\mathbb{Z}_{15}$ using the CRT. Prove your answer.

(a) Define a reasonable function $\phi : \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$

(b) Prove that ϕ is a function (i.e. well-defined and totally defined)

(c) Prove that ϕ is a homomorphism, i.e. that for all $a, c \in \mathbb{Z}_3$ and all $b, d \in \mathbb{Z}_5$:

$$\phi((a, b) \oplus (c, d)) = \phi((a, b)) \oplus_{15} \phi((c, d))$$

($\oplus$ is component-wise addition in $\mathbb{Z}_3$ and $\mathbb{Z}_5$ respectively)

(d) Prove that ϕ is surjective

(e) Prove that ϕ is bijective (this is easy!)

And now you've found a bijective homomorphism - in other words an isomorphism.

2.12 Solutions

2.12.1 Solution for Hands-On 1

Exercise 1.1
The prime factorizations are
$45 = 3^2 \cdot 5^1$
$42 = 2^1 \cdot 3^1 \cdot 7^1$

We get the gcd by taking the minimum occurring exponent of each prime factor.
$gcd(45, 42) = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 3$

We get the lcm by taking the maximum occurring exponent of each prime factor.
$lcm(45, 42) = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 18 \cdot 35 = 630$

Now we can calculate
$45 \cdot 42 = gcd(45, 42) \cdot lcm(45, 42) = 630 \cdot 3 = 1890$

Exercise 1.2
We give a proof of the form $S \Rightarrow T$ and $\neg S \Rightarrow \neg T$, which in turn proves $S \Leftrightarrow T$. We do this to obtain two very similar logical derivations, so we can reuse the same idea for both directions. (S is the right-hand side.)
($S \Rightarrow T$) Assume $\exists r \in \mathbb{N}$ s.t. $r^2 = n$. This r is therefore in D_n and unique. For every other element $a \in D_n$ exists a unique element $\in D_n$ for which $a \neq b$ s.t. $ab = n$. Let m denote the number of pairs of such two elements a and b for which $a < b$. (The $<$ means we only count each pair once.) Since elements in those pairs and r cover all elements in D_n we have $|D_n| = 2m + 1$. Cleary, $|D_n|$ is not even.
($\neg S \Rightarrow \neg T$) Assume $\neg\exists r \in \mathbb{N}$ s.t. $r^2 = n$. Thus for every other element $a \in D_n$ exists a unique element $\in D_n$ for which $a \neq b$ s.t. $ab = n$. Let m denote the number of pairs of such two elements a and b for which $a < b$. Since the elements in those pairs cover all elements in D_n we have $|D_n| = 2m$. Cleary, $|D_n|$ is even.
Exercise 1.3
Let p = gcd(x-zy,y) $\Rightarrow\ p \mid (x - zy)\ \wedge\ p \mid y$
$\Rightarrow \exists n_1 \in \mathbb{N}\ pn_1 = x - zy\ \wedge\ \exists n_2 \in \mathbb{N}\ pn_2 = y$
$\Rightarrow pn_1 = x - zpn_2$
$\Rightarrow pn_1 + zpn_2 = x$
$\Rightarrow p(n_1 + zn_2) = x \Rightarrow p \mid x\ \wedge\ p \mid y$

Let $q \in \mathbb{N}$ with $q \mid x\ \wedge\ q \mid y$
$\Rightarrow \exists m_1 qm_1 = x\ \wedge\ \exists m_2\ qm_2 = y$
$\Rightarrow x - zy = qm_1 - zqm_2$
$\Rightarrow x - zy = q(m_1 - zm_2)$
$\Rightarrow q \mid (x - zy)\ \wedge\ q \mid y$
We know that q is a common divisor of $x - zy$ and y, so by definition, it must also divide $gcd(x - zy, y) = p$.
$\Rightarrow q \mid p$
$\Rightarrow p \mid x\ \wedge\ p \mid y\ \wedge\ (\forall q(q \mid x \wedge q \mid y) \rightarrow q \mid p)$
$\Rightarrow p = gcd(x, y)$
$\Rightarrow gcd(x - zy, y) = gcd(x, y)$
Exercise 1.4
W.l.o.g. assume that $b > a$. We have by (1.3) that

$$\begin{aligned} gcd(a + k, b + k) &= gcd(a + k, b + k - (a + k)) \\ &= gcd(a + k, b - a) \end{aligned}$$

Now we can see that we just have to choose k in a way such that $gcd(a + k, b - a) = 1$. There exists an infinite amount of such k_i e.g. $k_i = p_i - a$ where p_i is a prime that is not part of the prime factorization of $b - a$ (Trivially there exists an infinite number of such p_i). Feel encouraged to come up with another general form for the k_i.

2.12.2 Solution for Hands-On 2

Exercise 2.1
We use a case distinction which covers all possible cases for a remainder modulo 3:

1. Case $R_3(a) = 0 \Rightarrow 3 \mid a$
2. Case $R_3(a) = 1 \Rightarrow \exists k\ a = 3.k + 1 \Rightarrow \exists k\ a + 2 = 3.k + 3 \Rightarrow 3 \mid (a + 2)$
3. Case $R_3(a) = 2 \Rightarrow \exists k\ a = 3.k + 2 \Rightarrow 3 \mid (a + 1) \Rightarrow 3 \mid (a + 4)$

The statement hold for all possible cases, thus it holds for every $a \in \mathbb{N}$. Thus it holds for every odd a.

Exercise 2.2
Check $R_{11}(2^{2016} + 3^{2016})$ under consideration of $R_{11}(2^{10}) = 1$ and $R_{11}(3^5) = 1$.

$R_{11}(2^{2016} + 3^{2016})$
$= R_{11}((2^{10})^{201} \cdot 2^6 + (3^5)^{403} \cdot 3)$
$= R_{11}(R_{11}(2^{10})^{201} \cdot R_{11}(2^6) + R_{11}(3^5)^{403} \cdot R_{11}(3))$
$= R_{11}(1 \cdot R_{11}(2^6) + 1 \cdot R_{11}(3))$
$= R_{11}(9 + 3) = R_{11}(1) = 1$

$\Rightarrow 11 \mid (2^{2016} + 3^{2016} - 1)$

Exercise 2.3
Let a have n digits and let a_k be the k'th digit of a.

$a = \sum_{k=0}^{n-1} a_k 10^k = \sum_{k=0}^{n-1} a_k(10^k - 1) + \sum_{k=0}^{n-1} a_k = \sum_{k=0}^{n-1} a_k(10^k - 1) + s_a$

Now we consider that $R_9(10^k - 1) = R_9(R_9(10)^k - 1)) = R_9(1 - 1) = 0$

Thus $\sum_{k=0}^{n-1} a_k(10^k - 1) + s_a \equiv_9 s_a$ and it follows that $R_9(a) = R_9(s_a)$

Exercise 2.4
We use from Exercise 1.3 hat $R_9(a) = R_9(s_a)$.

$R_9(9887776666555554444443333333222222221111111111) = R_9(9{+}2{\cdot}8{+}3{\cdot}7{+}4{\cdot}6{+}5{\cdot}5{+}6{\cdot}4{+}7{\cdot}3{+}8{\cdot}2{+}9) =$
$R_9(5 \cdot 5 + 2(2 \cdot 8 + 3 \cdot 7 + 4 \cdot 6 + 9)) = R_9(25 + 2 \cdot 70) = R_9(165) = R_9(1 + 6 + 5) = R_9(3) = 3$

2.12.3 Solution for Hands-On 3

Exercise 3.1
Since 2, 5 and 13 are relatively prime, the Chinese Remainder Theorem tells us that there is only one unique solution for $0 \leq x < 130 = 2 \cdot 5 \cdot 13$
First we calculate $M_i = M/m_1$
$M_1 = 130/2 = 65 \quad M_2 = 130/5 = 26 \quad M_3 = 130/13 = 10$
Now we find N_i such that $M_i \cdot N_i \equiv_{m_i} 1$
$65 \cdot N_1 \equiv_2 1 \;\Rightarrow\; N_1 = 1$
$26 \cdot N_2 \equiv_5 1 \;\Rightarrow\; N_2 = 1$
$10 \cdot N_3 \equiv_{13} 1 \;\Rightarrow\; N_3 = 4$
Now we can calculate our x:
$x = R_{130}(1 \cdot 65 \cdot 1 + 2 \cdot 26 \cdot 1 + 3 \cdot 10 \cdot 4) = R_{130}(237) = 107$

Exercise 3.2
Note that 10 and 15 are not relative prime. Therefore we cannot use the CRT directly. To remedy this we will decompose the system into the individual prime factors: Via $10 = 2 \cdot 5$ and $15 = 3 \cdot 5$ our system

$$\begin{aligned} x &\equiv_{10} 6 \\ x &\equiv_{15} 11 \end{aligned}$$

becomes

$$\begin{aligned} x &\equiv_2 0 \\ x &\equiv_3 2 \\ x &\equiv_5 1 \end{aligned}$$

as 6 *mod* 2 = 0 and 11 *mod* 3 = 2. Note that both 11 and 6 are 1 mod 5. If that would not be the case the system would not have a solution. Now we will solve this system via CRT as 2, 3 and 5 are relative primes. The CRT solution (see procedure in task 1) is $x = 26$ which is unique up to $2 * 3 * 5 = 30$. Not by coincidence 30 is also the lcm of 10 and 15. Therefore the general solution to the system is

$$x = 26 + n \cdot 30, \quad n \in \mathbb{N}$$

It is easy to see that all numbers of this form are solutions to the system. To prove it is the only set of solutions assume there exists another solution x_o. Then $x_o \pm 30$ would also be a solution (show why). We can therefore construct a solution $x_i \neq 26$ in the range $0 \leq x_i < 30$. This is a contradiction to the CRT.
Exercise 3.3
First let us bring the system into a more orderly form.

$$\begin{aligned} 2 \cdot x^2 + 8 &\equiv_{13} 6 \\ x &\equiv_{15} 2 \end{aligned}$$

is equivalent to

$$\begin{aligned} 2 \cdot x^2 &\equiv_{13} 11 \\ x &\equiv_{15} 2 \end{aligned}$$

is equivalent to (7 is the multiplicative inverse of 2 mod 13)

$$\begin{aligned} x^2 &\equiv_{13} 12 \\ x &\equiv_{15} 2 \end{aligned}$$

Now we need to decompose the equation $x^2 \equiv_{13} 12$. A simple quadratic form has at most 2 solutions. One trick to find these more easily is to add 13 to the right side until we hit a square number. In our case we get the sequence 12, $25 = 5^2$. So we know that 5 and $-5 \equiv_{13} 8$ are the two solutions to our system (another trick is using that $x^2 = k$ implies $(-x)^2 = k$). Now we have the two systems:

$$x \equiv_{13} 5$$
$$x \equiv_{15} 2$$

and

$$x \equiv_{13} 8$$
$$x \equiv_{15} 2$$

Solving each one with the CRT gives us $x_0 = 122$ and $x_1 = 47$ respectively. These are unique in $0 \leq x_i < 13 * 15 = 195$. Therefore we've computed all solutions to our initial system.

Exercise 3.4

$y_A = R_{19}(2^6) = 7$
$y_B = R_{19}(2^{11}) = 15$

Now we can calculate the keys
$k_{AB} = R_{19}(15^6) = 11$
$k_{BA} = R_{19}(7^{11}) = 11$

Note that as expected we got $k_{AB} = k_{BA}$. This means Alice and Bob both calculated the same key.

Exercise 3.5

(a) Define a reasonable function $\phi : \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$

We define ϕ as follows:

$$\phi((a, b)) = x \text{ such that } x \equiv_3 a \wedge x \equiv_5 b$$

(b) Prove that ϕ is a function (i.e. well-defined and totally defined)

We can use the fact that 3 and 5 are coprime and what we know about the CRT to conclude that such an x exists for any choice of a and b (ϕ is totally defined) and also that such a solution is unique in Z_{15} (ϕ is well-defined).

(c) Prove that ϕ is a homomorphism, i.e. that for all $a, c \in \mathbb{Z}_3$ and all $b, d \in \mathbb{Z}_5$:

$$\phi((a, b) \oplus (c, d)) = \phi((a, b)) \oplus_{15} \phi((c, d))$$

($\oplus$ is component-wise addition in $\mathbb{Z}_3$ and $\mathbb{Z}_5$ respectively)

We first calculate that $(a, b) \oplus (c, d) = (a \oplus_3 b, c \oplus_5 d)$. Thus, the left-hand side is equal to some $x \in \mathbb{Z}_{15}$ where:

$$x \equiv_3 a \oplus_3 b \equiv_3 a + b$$
$$x \equiv_5 c \oplus_5 d \equiv_3 c + d$$

From the definition of ϕ, we also get that $\phi((a, b)) = y, \phi((c, d)) = z$ for some $y, z \in \mathbb{Z}_{15}$ where:

$$y \equiv_3 a \qquad z \equiv_3 c$$
$$y \equiv_5 b \qquad z \equiv_5 d$$

Now all that's left is to combine these equations to get:

$$y + z \equiv_3 a + b$$
$$y + z \equiv_5 c + d$$

And because 15 is a multiple of both 3 and 5 also:

$$y \oplus_{15} z \equiv_3 a + b$$
$$y \oplus_{15} z \equiv_5 c + d$$

From which we see that $x \in \mathbb{Z}_{15}$ and $y \oplus_{15} z \in \mathbb{Z}_{15}$ are solutions to the same system of modular congruences with coprime moduli, and because the solution to this system is unique in $\mathbb{Z}_{15}$, we know:

$$\phi((a, b) \oplus (c, d)) = x = y \oplus_{15} z = \phi((a, b)) \oplus_{15} \phi((c, d))$$

(d) Prove that ϕ is surjective

We need to show that any $a \in \mathbb{Z}_{15}$ is the solution to some system of modular congruences.

Let $a \in \mathbb{Z}_{15}$ be arbitrary. We can trivially check that x is a solution to the system:

$$x \equiv_3 R_3(a)$$
$$x \equiv_5 R_5(a)$$

Therefore, for all $a \in \mathbb{Z}_{15}$, we can find $(b, c) \in \mathbb{Z}_3 \times \mathbb{Z}_5$ such that $\phi((b, c)) = a$ and thus, ϕ is surjective.

(e) Prove that ϕ is bijective (this is easy!)

Any surjection from a finite set to another finite set of equal cardinality is a bijection. As $\mathbb{Z}_3 \times \mathbb{Z}_5$ and $\mathbb{Z}_{15}$ are both finite and have the same number of elements (15), we know that our surjection ϕ must also be a bijection.

Now we have proved all we need in order to claim that ϕ is an isomorphism from $\mathbb{Z}_3 \times \mathbb{Z}_5$ to $\mathbb{Z}_{15}$.

3 Algebra

3.1 Algebras

This section is meant to provide a general introduction into algebras by simply recapitulating the useful definitions and introducing the concepts needed in the following subchapters.

Definition 3.1 (Algebra)**.** *An algebra is the combination of a set and several operations on that set. Strictly speaking we have a set S of elements which the operations "operate on" and a set Ω which contains all the operations that we defined. We call*

$$\langle S; \Omega \rangle$$

an algebra on S. For every operation $\omega \in \Omega$ we require ω to be of the form

$$\omega : S^n \to S \ , n \in \mathbb{N}$$

or in words: it does not "leave" the set S and it always takes the same amount of arguments.

While it is good to know this general definition, we will now mainly focus on one special case of algebras, in explicit algebras with one binary operation (i.e. on operation that takes two arguments).

Definition 3.2 (Associativity)**.** *An operation ω on a set G is called **associative** if and only if we have for any a, b, c in G*

$$a \ \omega \ (b \ \omega \ c) = (a \ \omega \ b) \ \omega \ c$$

- It is quite popular to just not use any parentheses at all when only using ω. This practise is generally (i.e. in the context of this course) **not** recommendable, as we lose formalism (in a strict sense $a \ \omega \ b \ \omega \ c$ is not properly defined) and therefore usually points in the exam.

Example. An example of associative operations would be addition and multiplication on the set $\mathbb{R}$, while exponentiation is not associative on $\mathbb{R}$ i.e. $\left(2^3\right)^2 = 8^2 = 64 \neq 2^{\left(3^2\right)} = 2^9 = 512$

Definition 3.3 (Identity)**.** *An operation ω on a set G has an **identity** if and only if*

$$\exists e \in G \ \forall a \in G \quad a \ \omega \ e = e \ \omega \ a = a$$

We call e the "neutral element" or simply identity.
We can weaken this condition to

$$\exists e' \in G \ \forall a \in G \quad a \ \omega \ e' = a$$

and then call e' a "right-neutral element". The definition of "left-neutral element" follows symmetrically.
If we have a right- and a left-neutral element then they have to be equal since

$$e_l = e_l \ \omega \ e_r = e_r$$

- Given the small proof above it follows that there exists at most one neutral element per operation ω, as e is left- and right-neutral.
- Addition and multiplication on $\mathbb{R}$ have the neutral element 0 respectively 1

Definition 3.4 (Inverse)**.** *An operation ω on a set G is **invertible** if and only if for all $a \in G$ there exists an $\widehat{a} \in G$ such that*

$$a \ \omega \ \widehat{a} = \widehat{a} \ \omega \ a = e$$

*where e denotes the identity of ω. We call $\widehat{a}$ the **inverse element** of a.*

- Given this formalism we have division and subtraction as as special case of multiplication and addition with the respective inverse elements. It should be mentioned that the function that maps an element to its inverse is unary and not binary. This usually leads to some confusion when working with "$-$" in rings as we're used to interpret "$-$" as a binary operator while in our context it simply denotes the inverse of the element.

Example. For every element $a \in \mathbb{R}\backslash\{0\}$ we have an inverse element regarding addition and multiplication, namely $-a$ and $\frac{1}{a}$.
On $\mathbb{Z}$ we still have the inverse regarding addition but no longer regarding multiplication.
On $\mathbb{N}$ for neither of the operations.
We therefore conclude that it is very important to look at the set that we are operating on in order to define the properties of an operation ω.

Definition 3.5 (Commutativity)**.** *An operation ω on a set G is called **commutative** if and only if for all $a, b \in G$*

$$a \ \omega \ b = b \ \omega \ a$$

- If an algebra has a commutative operation we usually call this algebra "abelian"

Example. Addition and multiplication are commutative on $\mathbb{R}$, while exponentiation is not, e.g. $2^3 \neq 3^2$

Given all these definitions we can now classify algebras with only one operation based on the fulfilment of the definitions. We get the following chart:

$\bullet$	Associativity	Identity	Inverse	Commutativity
Monoid	Needed	Needed	Not Needed	Not Needed
Group	Needed	Needed	Needed	Not Needed
Abelian Group	Needed	Needed	Needed	Needed

3.2 Groups

We already know from the previous chapter what conditions an algebra has to fulfil in order to be considered a group. As proofs involving groups are usually "stricter" than other kinds of proofs we abbreviate and formulate each of the three conditions as a so-called "group-axiom" in order to define groups more easily.

Definition 3.6 (Group)**.** *A **group** is an algebra*

$$\langle G; * \rangle$$

fulfilling the following conditions/axioms:

G1 *$*$ is associative in G*

G2 *There exists a (unique) neutral element e in G*

G3 *Every element $a \in G$ has an inverse element $\widehat{a}$ in G*

We write (unique) in parentheses as the fact that they there can be only one straight-up follows from the three axioms. It is often recommended to denote a group in a more verbose way, i.e. by explicitly

stating the neutral element (here e) and the operator that sends an element on its inverse:

$$\widehat{\ }: G \to G$$
$$a \mapsto \widehat{a}$$

which allows us to write

$$\langle G; *, \widehat{\ }, e \rangle$$

We have already seen that every operator has a unique neutral element, we therefore only need to proof that the same holds for inverse elements.
Furthermore this can be seen as an exemplary proof regarding statements about general groups as it uses **only** the three axioms.

Claim

Let $\langle G; *, \widehat{\ }, e \rangle$ be a group. Then for every $a \in G$ we have exactly one inverse element $\widehat{a}$.

Proof. Let a be an arbitrary element in G. By axiom **G3** we know that there exists at least one inverse element $\widehat{a}$.
Let $\widehat{a}'$ be another inverse element, then:

$$\widehat{a} \overset{G2}{=} \widehat{a} * e \overset{G3}{=} \widehat{a} * (a * \widehat{a}') \overset{G1}{=} (\widehat{a} * a) * \widehat{a}' \overset{G3}{=} e * \widehat{a}' \overset{G2}{=} \widehat{a}'$$

□

There are several lemmas in the script that you can use in your exam without having to proof them (obviously as long as it isn't your task to proof them), they are as follows

Collection 3.1

Following lemmas hold for every group, i.e. let $\langle G; *, \widehat{\ }, e \rangle$ be a group and a, b any two elements in them.

- $\widehat{(\widehat{a})} = a$
- $\widehat{a * b} = \widehat{b} * \widehat{a}$
- $a * b = a * c \Rightarrow b = c$ *(left cancellation law)*
- $b * a = c * a \Rightarrow b = c$ *(right cancellation law)*
- $a * x = b$ has a unique solution x for every a, b

While one can usually use these lemmas without proving them it is a quite useful exercise to prove them. (Therefore they are included in the Hands-On part)
One type of group is used quite often and therefore its notation should be known:

Example.

- The group $\langle \mathbb{Z}_n; \oplus, \ominus, 0 \rangle$ is the group of all natural numbers (including 0) up to $n-1$ using the binary operation $\oplus$ which denotes the addition modulo n. It is important to remember that despite the fact that we are not used to it $\ominus$ is an operation that takes only **one** element and **not** two. We sometimes simply write $\mathbb{Z}_n$.
- The group $\langle \mathbb{Z}_p - \{0\}; \odot, ^{-1}, 1 \rangle$ is the group of all natural numbers (excluding 0) up to $p-1$ using the binary operation $\odot$ which denotes the multiplication modulo p. In order for it to be a group p has to be prime. We sometimes write this as $\mathbb{Z}_p^*$ (we will define this notation later).

3.2.1 Subgroups

Definition 3.7 (Subgroup)**.** *A set of elements H is called a* ***subgroup*** *of a group $\langle G; *, \widehat{\ }, e\rangle$ if the following conditions hold*

- *$\langle H; *, \widehat{\ }, e\rangle$ is a group*
- *$H \subseteq G$*
- *For all $a, b \in H$ we have $a * b \in H$ (it is closed under its operation)*
- *$e \in H$ (it is closed regarding the identity)*
- *Every $a \in H$ has an inverse element $\widehat{a} \in H$ (it is closed under inversion)*

We conclude that there always exist two trivial subgroups of a group $\langle G; *, \widehat{\ }, e\rangle$, namely $\{e\}$ and G.
In general it is not trivial to find the number of subgroups of a group.
For a given group $\langle G; *, \widehat{\ }, e\rangle$ a usual task is to prove that some subset $H \subseteq G$ is in fact a subgroup of $\langle G; *, \widehat{\ }, e\rangle$ (or not).
The main way to find out whether a set is a subgroup is to simply check all the the individual conditions one by one. While it might not always be the fastest, it is a safe and structured way to solve the task at hand.
There are two other options, but as they are not explicitly stated in the script they require a proof when using them and are therefore part of the Hands-On.

3.2.2 Order of groups and elements - Cyclic groups and generators

One might just use the group operation over and over again on the same element. Despite the simplicity of this procedure we actually get several useful properties out of it. Most of them are captured in the following definitions:

Definition 3.8 (Order of a Group)**.** *For any given* ***finite*** *group G (G here represents the whole group, not only the set of elements) we denote the* ***order of the group*** *as*

$$|G| = \textit{number of elements in } G$$

in comparison to that we have for the order of an element

Definition 3.9 (Order of an element)**.** *Given an element a of a finite group $\langle G; *, \widehat{\ }, e\rangle$ we denote the* ***order of this element*** *with*

$$ord(a) = r$$

where r is the lowest number such that $a^r = \underbrace{a * a * \cdots * a}_{r \text{ times}} = e$

We can prove by usage of the Pigeonhole-Principle that for every finite group also the order of each of its elements has to be finite. Furthermore we have the corollary that

Corollary 3.1

Given an element a of a finite group $\langle G; *, \widehat{\ }, e\rangle$ we have

$$a^m = a^{R_{ord(a)}(m)}$$

which directly follows from the division theorem i.e. because if $m = k \cdot ord(a) + r$ with $r < ord(a)$

$$a^m = \underbrace{\underbrace{a * a * \cdots * a}_{ord(a)\ times} * \underbrace{a * a * \cdots * a}_{ord(a)\ times} * \cdots * \underbrace{a * a * \cdots * a}_{ord(a)\ times}}_{k\ times} * \underbrace{a * a * \cdots * a}_{r\ times} = e^k * a^r = a^r = a^{R_{ord(a)}(m)}$$

These definitions prove themselves to be especially useful when looking at further concepts like cyclic groups and subgroups generated by elements.
We will handle the latter first:

Theorem 4: Subgroups generated by an element

For any element a of a finite group $\langle G; *, ^{-1}, e\rangle$ we have that

$$\langle a\rangle := \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of $\langle G; *, ^{-1}, e\rangle$.

There are two remarks that have to be made regarding this theorem. The first is that we should definitely prove that we actually always generate a group by applying this procedure.

Claim

Let $\langle G; *, ^{-1}, e\rangle$ be a finite group. Then for any $a \in G$ we have that $\langle a\rangle$ is a subgroup of $\langle G; *, ^{-1}, e\rangle$.

Proof. Let $a \in G$ be arbitrary. We show that $\langle a\rangle$ is a subgroup of $\langle G; *, ^{-1}, e\rangle$ by individually showing that each required condition holds.

- For all $x, y \in \langle a\rangle$ we have that $x * y \in \langle a\rangle$
  Any element x in $\langle a\rangle$ can be written as $a^{m_x} = x$ where $m_x < ord(a)$ is the smallest natural number fulfilling $a^k = x$. We therefore have

  $$x * y = a^{m_x} * a^{m_y} = a^{m_x + m_y} \in \langle a\rangle$$

  We used already known laws of power and the definition of $\langle a\rangle$

- $e \in \langle a\rangle$
  This directly follows from the definition of the order of an element. Otherwise we also have that $a^0 = e \in \langle a\rangle$. This last part follows from the fact that $a^0 * a^k = a^k * a^0 = a^k$ (one should mention that this is not a complete proof).

- Every $x \in \langle a\rangle$ has an inverse element $x^{-1} \in \langle a\rangle$
  As $x \in \langle a\rangle$ we can write it as $x = a^{m_x}$ and as $m_x < ord(a)$ we can find the element $x^{-1} = a^{ord(a) - m_x} \in \langle a\rangle$. It follows that it is actually the inverse of x as

  $$x * x^{-1} = a^{m_x} * a^{ord(a) - m_x} = a^{ord(a)} = e$$

- The fact that $\langle a\rangle \subseteq G$ follows from the fact that $\langle G; *, ^{-1}, e\rangle$ is a group and therefore closed under its operation.

- In order to show that $\langle \langle a\rangle; *, ^{-1}, e\rangle$ is a group we additionally have to show that $*$ is associative. Luckily this follows from the fact that $*$ is also the operation in $\langle G; *, ^{-1}, e\rangle$ and therefore has to be associative as $\langle G; *, ^{-1}, e\rangle$ is a group.

As every condition hold $\langle a\rangle$ is a subgroup of $\langle G; *, ^{-1}, e\rangle$

□

The second remark is about the at first sight rather confusing use of $\mathbb{Z}$ as set of potential n. As a matter of fact it does not make a difference here whether we choose $\mathbb{N}$ or $\mathbb{Z}$, but to avoid further confusion it is helpful to remind oneself of the fact that for any **negative** n we have

$$a^n = \left(a^{-n}\right)^{-1} = \left(a^{|n|}\right)^{-1}$$

which is just the inverse element of $a^{|n|}$ and makes sense when we (informally!) think about

$$a^n * a^{-n} = a^0 = e$$

Given the earlier definition it's now very simple to define a cyclic group:

Definition 3.10 (Cyclic group)**.** *A cyclic group is a group $G = \langle g \rangle$ generated by an element $g \in G$. We call G* ***cyclic*** *and g a* ***generator*** *of G.*
From this follows that an element $g \in G$ is exactly then a generator when $ord(g) = |G|$, i.e.

$$ord(g) = |G| \Leftrightarrow g \text{ is a generator of } G$$

Most groups are not cyclic. Being cyclic is a special property that implies several interesting and important facts:

- All cyclic groups are commutative
- All cyclic groups of the same order (i.e. with the same number of elements) are isomorphic
- For $\langle \mathbb{Z}_n, \oplus, \ominus, 0 \rangle$ every element g with $gcd(g, n) = 1$ is a generator of $\langle \mathbb{Z}_n, \oplus, \ominus, 0 \rangle$
- From earlier we already know that for an element a of a group G $\langle a \rangle$ is a subgroup. By definition/construction it is a cyclic group and its order is equal to the order of a i.e.

$$ord(a) = |\langle a \rangle|$$

Finally we conclude this part by reminding ourselves of the one theorem that connects most of the given definitions and that is

Theorem 5: Lagrange

For any finite group G and any subgroup H of G we have that the order of H divides the order G i.e.

$$|H| \mid |G|$$

This theorem has several implications, most notably we have that

Claim

The order of any group element has to divide the order of the group.

Proof. For any element a of a group G we know that $\langle a \rangle$ is a subgroup of G. By Lagrange it follows that $|\langle a \rangle| \mid |G|$. Now we already know that $|\langle a \rangle| = ord(a)$. We conclude that $ord(a) \mid |G|$ □

this obviously implies for every element $a \in G$ of a group G that

$$a^{|G|} = a^{k * ord(a)} = \left(a^{ord(a)}\right)^k = e^k = e$$

It follows as a direct corollary that

Corollary 3.2: Prime orders

Every group of prime order is cyclic and therefore commutative.

A common task when it comes to cyclic groups is to find a generator. While this can obviously be done by brute-force it is usually smarter to consider (based on Lagrange) only the divisors of the group's order. We present the following example:

Example. We want to determine all generators of the group $\langle Z_{11}^*, \odot, ^{-1}, 1\rangle$. While this document only introduces this type of group in later sections one should already be familiar with the concept by either having read the lecture script or having skipped several steps ahead to look it up.
We now have that the order of our group is $|\langle Z_{11}^*, \odot, ^{-1}, 1\rangle| = 10 = 2 \cdot 5$.
As we know the order of every element has to divide the order of the group itself, for any element $x \in Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ we therefore have $ord(x) \in 1, 2, 5, 10$.
As only the neutral element, i.e. here 1, has order 1, we will only check for 2 and 5. If a number $x \in Z_{11}^*$ does not satisfy $x^2 = 1$ and $x^5 = 1$ then we know that $ord(x) = 10$ which means that x is a generator.
Checking all elements like this gives us

$$\begin{aligned}
1:&\ 1^1 = 1\\
2:&\ 2^2 = 4,\ 2^5 = 10\\
3:&\ 3^2 = 9,\ 3^5 = 1\\
4:&\ 4^2 = 5,\ 4^5 = 1\\
5:&\ 5^2 = 3,\ 5^5 = 1\\
6:&\ 6^2 = 3,\ 6^5 = 10\\
7:&\ 7^2 = 5,\ 7^5 = 10\\
8:&\ 8^2 = 7,\ 8^5 = 10\\
9:&\ 9^2 = 4,\ 9^5 = 1\\
10:&\ 10^2 = 1
\end{aligned}$$

We conclude that the set of generators of $\langle Z_{11}^*, \odot, ^{-1}, 1\rangle$ is $\{2, 6, 7, 8\}$

Hands-On 1

This Hands-On contains three major subparts. The first is the normal Hands-On part with exercises regarding the specific topics. The second contains several proofs for claims that have been made earlier and the third contains more challenging tasks. As we've taken an approach that tends to giving more tasks, you're absolutely not expected to finish all tasks within the provided time.

1.1. Working with group axioms Let $\langle G; *, \widehat{\ }, e\rangle$ be a group.

(a) Show that the function f_a defined as

$$\begin{aligned} f_a : G &\to G\\ x &\mapsto a * x \end{aligned}$$

with $a \in G$ arbitrary is bijective. Use **only** the group axioms, apply an axiom only once per step and only in one place.

(b) Show that the following statement holds for any $x, y \in G$

$$((x * y) * \widehat{x}) * \widehat{y} = e \Leftrightarrow x * y = y * x$$

Use **only** the group axioms, apply an axiom only once per step and only in one place.

(c) Show that every group of order < 6 has to be commutative.

(d) Show that every group that only contains self-inverse elements has to be commutative.

(e) Given any two subgroups H_1, H_2 of a group G: Is $H_1 \bigcup H_2 \neq \emptyset$ a subgroup of G? Are $H_1 \bigcap H_2$ or $H_1 \backslash H_2$ subgroups?

(f) Show that for any two elements $a, b \in G$ we have $ord(a * b) = ord(b * a)$

1.2. Subgroups

(a) Give the smallest non-trivial subgroup of $\langle \mathbb{Z}_{30}; \oplus \rangle$

(b) Let G have 77 elements and H be a subgroup of G with $H \neq G$. Show that H is commutative.

(c) Given any abelian group $\langle G; \odot \rangle$ with the neutral element e. Is the set $H_k,\ k \in \mathbb{N}$ containing all elements which fulfill $h^k = e$ a subgroup of $\langle G; \odot \rangle$? Assume we would now define $H'_k \subseteq G,\ k \in \mathbb{N}$ as the set of all elements that have order k. Is the statement now true or false for H'_k?

1.3. Cyclic groups and generators

(a) Find all generators of $\langle \mathbb{Z}^*_{17}; \odot \rangle$.

(b) Find all generators of $\langle \mathbb{Z}_{20}; \oplus \rangle$

(c) If we have two cyclic groups $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$, is (g_1, g_2) a generator of $G_1 \times G_2$?

(d) Given the groups G_1 and G_2 as $\mathbb{Z}_m$ and $\mathbb{Z}_n$ with addition. Give a necessary and sufficient condition which has to hold such that for any generators of G_1 and G_2 we have that (g_1, g_2) is a generator of $G_1 \times G_2$. (Fancy extra task: Try to generalize this statement for any kind of cyclic groups)

(e) Let $m > 1$ be a natural number and G a cyclic group with $|G| = m * k,\ k \in \mathbb{N} \backslash \{0\}$. Show that there always exists an element $a \in G$ such that $a \neq e$ and $a^m = e$

1.4. Proofs from the script For these tasks let $a, b \in \langle G; *, \widehat{\ }, e \rangle$.

(a) Show that $\widehat{(\widehat{a})} = a$

(b) Show that $\widehat{a * b} = \widehat{b} * \widehat{a}$

(c) Show that $a * b = a * c \Rightarrow b = c$

(d) Prove the **One-Step Subgroup Test**
Let $\langle G; \circ \rangle$ be a group and $H \subseteq G$. Then H is a subgroup of $\langle G; \circ \rangle$ if and only if

- $H \neq \emptyset$
- $a, b \in H \Rightarrow a \circ b^{-1} \in H$

1.5. Challenge This challenge will guide you through a proof of Lagrange's theorem. Assume in this context the finite group $\langle G; *, \widehat{\ }, e \rangle$ with a subgroup H

(a) Show that the follwing relation is an equivalence relation on $\langle G; *, \widehat{\ }, e \rangle$:

$$x \backsim y \Leftrightarrow x^{-1}y \in H$$

(b) Let us define for any $x \in G$ the set $xH := \{y \in G \mid \exists h \in H\ y = x * h\}$
Show that this set corresponds to the equivalence classes of the relation $\backsim$

(c) Show that for all xH we have that $|xH| = |H|$ (Hint: Use subtask 1.4 or 1.1)

(d) Put it all together and enjoy your glory!

3.3 Morphisms

Having been briefly mentioned in the earlier parts we will now look at the concept of homomorphisms and their "extension", the isomorphisms. While they are both more general concepts we will look at them specifically regarding groups.

First we have

Definition 3.11 (Group homomorphism and isomorphism)**.** *Let $\langle G; *, ^{-1}, e_G\rangle$ and $\langle H; \cdot, \widehat{\ }, e_H\rangle$ be two groups. Then we call a mapping*

$$\phi : G \to H$$

*a **homomorphism** if it fulfils:*
For any a, b in G

$$\phi(a * b) = \phi(a) \cdot \phi(b)$$

*As an extension we call ϕ an **isomorphism** when it is a **homomorphism** as well as **bijective**.*

Homomorphisms and isomorphisms have several useful properties which are often asked to be proved:

For homomorphisms we have (again given the groups G and H)

Collection 3.2: Homomorphisms

- $\phi(e_G) = e_H$
- $\phi(a^{-1}) = \widehat{\phi(a)}$
- $\phi(a^n) = \phi(a)^n$
- Based on the statements above we have that a homomorphism always projects G onto a subgroup of H.

For isomorphisms we additionally have

Collection 3.3: Isomorphisms

- The inverse of an isomorphism is again an isomorphism
- An isomorphism always maps generators in one group onto generators in the other group. I.e. two isomorphic groups always have the same number of generators (and the complete isomorphism can be described by just giving the image of just one generator of G under ϕ)
- As direct corollary we have that "All cyclic groups with same cardinality are isomorphic"
- Isomorphisms carry commutativity i.e. if a group is isomorphic to a commutative group it has to be commutative itself

We will give an exemplary proof for the first statement of each while putting the others in the Hands-On part.

Claim

$\phi(e_G) = e_H$

Proof.

$$\begin{aligned}
\phi(e_G) &= \phi(e_G) \cdot e_H \\
&= \phi(e_G) \cdot (\phi(e_G) \cdot \widehat{\phi(e_G)}) \\
&= (\phi(e_G) \cdot \phi(e_G)) \cdot \widehat{\phi(e_G)} \\
&= \phi(e_G * e_G) \cdot \widehat{\phi(e_G)} \\
&= \phi(e_G) \cdot \widehat{\phi(e_G)} \\
&= e_H
\end{aligned}$$

□

Claim

The inverse of an isomorphism ϕ is again an isomorphism

Proof. It is given by the definition of ϕ as an bijective function, that its inverse ϕ^{-1} is also bijective, we therefore only have to show that it is also a homomorphism.
Let $a, b \in H$ be arbitrary with $x, y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$ then we have

$$\phi^{-1}(a \cdot b) = \phi^{-1}(\phi(x) \cdot \phi(y)) = \phi^{-1}(\phi(x * y)) = x * y = \phi^{-1}(a) * \phi^{-1}(b)$$

We realize that the bijectivity of ϕ and ϕ^{-1} is crucial in several steps of this proof. □

Hands-On 2

2.1. Homomorphisms Let $\langle G; *, ^{-1}, e_G\rangle$ and $\langle H; \cdot, \widehat{\ }, e_H\rangle$ be two groups.

(a) Given the homomorphism $\phi : G \to H$ and $g_0 \in \phi^{-1}(\{e_H\})$. Show that

$$\{g \in G \mid g * g_0 * g^{-1} \in \phi^{-1}(\{e_H\})\} = G$$

2.2. Proofs - Homomorphisms Let $\langle G; *, ^{-1}, e_G\rangle$ and $\langle H; \cdot, \widehat{\ }, e_H\rangle$ be two groups and $\phi : G \to H$ a homomorphism.

(a) Show that for any $a \in G$ $\phi(a^{-1}) = \widehat{\phi(a)}$

(b) Show that for any $a \in G$ $\phi(a^n) = \phi(a)^n,\ n \in \mathbb{Z}$

(c) Show that based on the statements above we have that a homomorphism always projects G onto a subgroup of H.

2.3. Isomorphisms Let $\langle G; *, ^{-1}, e_G\rangle$ and $\langle H; \cdot, \widehat{\ }, e_H\rangle$ be two groups.

(a) Show that for any m, n with $gcd(m, n) = 1$ the following map is an isomorphism between $\langle \mathbb{Z}_{mn}; \oplus_{mn}\rangle$ and $\langle \mathbb{Z}_m; \oplus_m\rangle \times \langle \mathbb{Z}_n; \oplus_n\rangle$:

$$\begin{aligned} \phi : \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ x &\mapsto (R_m(x), R_n(x)) \end{aligned}$$

(b) Show that the condition $gcd(m, n) = 1$ is necessary for ϕ to be an isomorphism.

(c) Let m be the product of two distinct prime numbers p and q. How many non-isomorphic subgroups does $\langle \mathbb{Z}_m; \oplus\rangle$ have?

(d) Prove or disprove: If $\phi : G \to H$ is an injective homomorphism, it has to be an isomorphism.

2.4. Proofs - Isomorphisms Let $\langle G; *, ^{-1}, e_G\rangle$ and $\langle H; \cdot, \widehat{\ }, e_H\rangle$ be two cyclic groups and $\phi : G \to H$ a homomorphism.

(a) Show that an isomorphism always maps generators in one group onto generators in the other group. I.e. two isomorphic groups alway have the same number of generators (and the complete isomorphism can be described by giving the image of just one generator of G under ϕ)

(b) Show that we then have that "All cyclic groups with same finite cardinality are isomorphic"

(c) Show that isomorphisms carry commutativity i.e. if a group is isomorphic to a commutative group it itself has to be commutative.

2.5. Challenge

(a) Given two cyclic groups of order $n > 0$. How many different isomorphisms do exist between them? (This "challenge" is actually sometimes an exam question!)

3.4 Z_m^* and Euler's totient function

Finally we will look at another special kind of group and the Euler's function which is closely related to it.
The group is $\langle Z_m^*, \odot, ^{-1}, 1\rangle$ and is defined as follows

Definition 3.12 (Z_m^*)**.** *The set Z_m^* is defined as the set of all natural numbers smaller than m that are pairwise prime to m (i.e. have no common divisor). Formally we write it as*

$$Z_m^* := \{a \in \mathbb{N} \mid a < m \wedge gcd(a, m) = 1\}$$

using the multiplication modulo m, denoted as $\odot$, we can define the group

$$\langle Z_m^*, \odot, ^{-1}, 1\rangle$$

The fact that $\langle Z_m^*, \odot, ^{-1}, 1\rangle$ is actually a group follows mostly from the chapter about number theory and shall not be proved here.
Z_m^* has the interesting property that it is cyclic if and only if

$$m = 2, 4, p^e, 2 \cdot p^e$$

where $e \geq 1$ and p is an uneven prime.
Closely related to it we have the concept of Euler's totient function which simply states the cardinality of Z_m^*

Definition 3.13 (Euler's totient function)**.** *Euler's totient function φ gives for an input $m \in \mathbb{N}$ the number of numbers in $\mathbb{N}$ that are smaller and pairwise prime to m. Formally this is denoted as*

$$\begin{aligned} \varphi : \mathbb{N} &\to \mathbb{N} \\ m &\mapsto |Z_m^*| \end{aligned}$$

i.e. Z_m^* has exactly $\varphi(m)$ elements (the order of Z_m^* is $\varphi(m)$).

Obviously it's quite common to actually compute $\phi(m)$ given $m \in \mathbb{N}$. This is most easily done by using the following formula(s):

Lemma 3.1

For a given $m \in \mathbb{N}$ with the prime factorization $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_n^{e_n}$ we have

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}) \\ &= \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdot \ldots \cdot \varphi(p_n^{e_n}) \\ &= \prod_{i=1}^{n} p_i^{e_i - 1} \cdot (p_i - 1) \\ &= \prod_{i=1}^{n} p_i^{e_i} \cdot (1 - \frac{1}{p_i}) \\ &= m \prod_{i=1}^{n} (1 - \frac{1}{p_i})\end{aligned}$$

We actually most commonly use the formula on line three i.e. $\varphi(m) = \prod_{i=1}^{n} p_i^{e_i - 1} \cdot (p_i - 1)$. The reader may also notice how we used the multiplicative property of φ when dealing with pairwise prime numbers. The proof will be part of the hands-on.

Example. We want to calculate $\varphi(56) = \varphi(2 * 28) = \varphi(2^2 * 14) = \varphi(2^3 * 7)$. We put the values of the factorization into the formula and obtain

$$\varphi(56) = 2^{3-1} \cdot (2-1) \cdot 7^{1-1} \cdot (7-1) = 4 \cdot 6 = 24$$

Finally we have one more corollary that is a very direct consequence of what we already know but should nevertheless be explicitly formulated to stress its significance

Corollary 3.3: Euler, Fermat

For all $m \geq 2$ and all a with $gcd(a, m) = 1$ we have

$$a^{\varphi(m)} \equiv_m 1$$

in particular, for every prime p and every a not divisible by p we have

$$a^{p-1} \equiv_p 1$$

This corollary is particularly interesting because you will usually encounter its usage in the chapter about number theory, hereby showing a connection between these two fields. One example application is to find the inverse of some a modulo m if $\varphi(m)$ is known (for example in RSA):

$$aa^{\varphi(m)-1} \equiv_m 1 \Rightarrow a^{\varphi(m)-1} = \widehat{a}$$

Hands-On 3

3.1. Z_m^* and Euler

(a) Find the inverse of 3 in $\mathbb{Z}_{13}^*$

(b) How many elements does $\mathbb{Z}_{30}^*$ have?

(c) Find an $m \in \mathbb{N}$ such that

$$3036^m \equiv_{7105} 1$$

given that $3036 = 2^2 * 3 * 11 * 23$ and $7105 = 5 * 7^2 * 29$

(d) Show that every real ($\neq \mathbb{Z}_6^*$) subgroup of $\mathbb{Z}_6^*$ is abelian.

3.2. Challenge In this challenge we will prove the multplicativity of Euler's totient function

(a) Show that for every two natural numbers m, n with $gcd(m, n) = 1$ we have that

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

3.5 Rings

Definition 3.14. *A ring $\langle R; +, -, 0, \cdot, 1\rangle$ is an algebra for which*

(i) $\langle R; +, -, 0\rangle$ *is a commutative group.*

(ii) $\langle R; \cdot, 1\rangle$ *is a monoid.*

(iii) $a(b + c) = (ab) + (ac)$ *and* $(b + c)a = (ba) + (ca)$ *for all* $a, b, c \in R$. *(Distributivity)*

A ring is called commutative if multiplication is commutative ($ab = ba$).

This algebraic structure is important because it has two operations which are connected over the distributive laws. Many well known sets like $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are rings. Since we have two operations, a ring has both an additive and a multiplicative neutral element which we denote as 0 and 1 respectively.
We can prove some very important facts about rings which we summarize as Lemma 5.17:

Collection 3.4

(i) $0a = a0 = 0$

(ii) $(-a)b = -ab$

(iii) $(-a)(-b) = ab$

(iv) If R is non-trivial ($|R| > 1$), then $1 \neq 0$.

All 4 points can be proven with only a few lines. (i) has been proven in the lecture notes, (ii) and (iii) have been proven in exercise 9 (FS 2017) and (iv) will be proven in the next hands-on of this script.

In a ring every element has an additive inverse but not necessarily a multiplicative one. Therefore it becomes interesting to talk about the divisibility property in rings.

Definition 3.15. *For $a, b \in R$ with $a \neq b$ we say that a divides b, denoted $a \mid b$, if there exists $c \in R$ such that $ac = b$. In this case, a is called a divisor of b and b is called a multiple of a.*

We can also state from this definition that every element divides 0, since a0 = 0 for every a, and that 1 divides every element, since 1a = a.
Since $\langle R; \cdot, 1\rangle$ is a monoid and not necessarily a group, it is interesting to ask whether some elements of the ring have a multiplicative inverse. These elements are called *units* or *invertible* elements and the set containing all units is the multiplicative group of R, denoted as R^*. As we have seen in the previous chapter, we can find the order of this group using Euler's totient function.

Example. $\mathbb{Z}_6$ with addition and multiplication is a ring. Which elements of the ring have a multiplicative inverse? It's exactly those elements where $gcd(a, 6) = 1$. These are $\mathbb{Z}_6^* = \{1, 5\}$.

Another algebraic structure we can now define is the integral domain:

Definition 3.16. *An integral domain is a non-trivial commutative ring without zerodivisors:* $\forall a \forall b(ab = 0 \to a = 0 \vee b = 0)$.

In an integral domain no two elements can be multiplied to obtain 0. Previously we were not allowed to use the quotient notation $c = \frac{a}{b}$ since b might have been 0. In an integral domain we are allowed to use

it and can also prove that this quotient is unique (Lemma 5.20).

Example. Is $\mathbb{Z}_6$ an integral domain? $\mathbb{Z}_6$ contains zerodivisors since for example $2 \cdot 3 = 0$ and is thus not an integral domain. In fact $\mathbb{Z}_m$ can only be an integral domain if m is prime. If m is not prime, then it is by definition divisible by some $a \neq 0$ and $b \neq 0$, making a and b zerodivisors.

Hands-On 4

4.1. Rings

(a) How many units are in the ring $\mathbb{Z}_{12}$?

(b) Let R be a commutative Ring with at least two elements. Let $r \in R$. Show that $r \in R^* \iff \forall s \in R\ \exists t \in R\ \ s = rt$

(c) How many elements can a ring $\langle R; +, -, 0, \cdot, 1\rangle$ where $0 = 1$ contain? Justify your answer.

(d) Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring such that $a \cdot a = a$. Show that $\forall a \in R.\ a + a = 0$

(e) Using you knowledge from the last task show that R is furthermore commutative.

4.2. Integral Domains

(a) Show that the order of the element 1 in the additive group is a prime number in any finite integral domain.

3.6 Fields

Definition 3.17. *A field is a non-trivial commutative ring F in which every non-zero element is a unit, i.e., $F^* = F\backslash\{0\}$*

Remember that in a ring R, $\langle R; \cdot, 1\rangle$ is a monoid. In a field F, $\langle F\backslash\{0\}; \cdot, ^{-1}, 1\rangle$ is an abelian group. Before we look at different specific fields, we might wonder about the connection between integral domains and fields. In fact, every field is an integral domain (Theorem 5.24 - script). To prove this, we have to show that a field has no zerodivisors:

Proof. Let $u, v \in F\backslash\{0\}$ and $uv = 0$. Then $v = 1v = u^{-1}uv = u^{-1}0 = 0$, which is a contradiction. □

Now the other question we might pose is: Is every integral domain a field? $\mathbb{Z}$ is an integral domain but not a field because no elements except for 1 and -1 have a multiplicative inverse.
We can however prove that finite integral domains are fields. The intuition here is that because the quotient between two numbers is unique and there is a finite number of elements, the quotient between one and any other element should exist and be unique. Here goes the proof:

Proof. Let I be an finite integral domain. By definition I has at least two elements and no zerodivisors. Let $u \in I\backslash\{0\}$. We want to show that u has an inverse in I.
Let $X = \{ua | a \in I\backslash\{0\}\}$ be the set of all multiples of u. Since I has no zerodivisors, $0 \notin X$. Furthermore if a and a' are two distinct elements in $I\backslash\{0\}$, then according to Lemma 5.20, $ua = c$ and $ua' = c'$ are distinct as well. This implies that $X = I\backslash\{0\}$ and by the definition of X, the inverse of u must be contained in I. Hence I is a field. □

Which fields do we know? $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are some examples of infinite fields. What about finite fields?
Is it possible to construct finite fields of any cardinality? In the following we will discuss and prove that only fields of certain cardinalities exist.
First of all we know that $\mathbb{Z}_p$ is a field if an only p is prime. This follows from the fact that $\mathbb{Z}_p\backslash\{0\}$ is a multiplicative group if p is prime.
Because fields with the same cardinality are all isomorphic we call a field with p elements $\mathrm{GF}(p)$, where GF stands for Galois field.

Hands-On 5

5.1. Fields

(a) Show without using the Theorem 5.23 that $\mathbb{Z}_4$ is not a field.

(b) Let F be a finite field. Find all elements $x \in F$ that fulfil the equation $x^2 = 1$.

(c) Let F be a finite field. Using the previous exercise, show that $\prod_{a \in F^*} a = -1$.

3.7 Polynomials over Rings and Fields

From calculus we are used to deal with polynomials where the coefficients and the values a polynomial can have, lie in $\mathbb{R}$. Since the concept of polynomials is the same for all rings we can simply change the underlying algebra. This means that we still use the same idea of polynomials only that the values they can have are elements of some other ring and addition and multiplication may be defined differently. More formally:

Definition 3.18. *A polynomial $a(x)$ over a ring R in the indeterminate x is a formal expression of the form*

$$a(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = \sum_{i=1}^{d} a_i x^i$$

for some non-negative integer d, where $a_i \in R$.

The degree of a polynomial $a(x)$, denoted as $deg(a(x))$ is the largest power appearing in the polynomial, for example $deg(x^4 + 3x^2 + 5) = 4$.
We write the set of all polynomials over a ring as $R_{[x]}$. The same notation is used for polynomials over integral domains or fields, $D_{[x]}$, and $F_{[x]}$. Note that there are infinitely many polynomials in $R_{[x]}$ as long as we don't restrict the degree they can have.
When performing addition or multiplication of polynomials one must respect the properties of the underlying ring:

Example. Let's consider some examples of addition and multiplication in $\mathbb{Z}_6[x]$:

- $3x^2 + 3x^2 + x + 4x + 2 = (3 + 3)x^2 + (1 + 4)x + 2 = 5x + 2$
- $x(x^2 + 5x + 1) + 5x = x^3 + 5x^2$

Now we may ask ourselves whether the set of polynomials over a ring is a ring as well. For this we simply have to check whether the properties listed in the definition for rings hold for polynomials as well. It turns out that:

Collection 3.5

(i) For any ring R, $R[x]$ is a ring as well.

(ii) For any integral domain D, $D[x]$ is an integral domain as well.

Moreover since $R[x]$ is a ring, we can also define a set of polynomials over $R[x]$. Such a structure would be denoted as $R[x][y]$. We will see an example with finite fields in the later section.

But what about polynomials over fields? According to the definition of fields, $F[x]$ is a field only if every polynomial in $F[x]$ except for 0 has an inverse. This is not the case since there are no two polynomials of degree at least one that multiplied with each other result in the neutral element 1. Also multiplying two polynomials never reduces the degree of a polynomial.

We can also define the root of a polynomial which will be of greater importance later:

Definition 3.19. *Let $a(x) \in R[x]$. An element $\alpha \in R$ for which $a(\alpha) = 0$ is called a root of $a(x)$.*

Example. For example $2x^2 + x \in \text{GF}(3)[x]$ has the root 1 because $2(1)^2 + 1 = 0$.

3.7.1 Factorization of Polynomials

Analogously to divisibility in fields we can define divisibility of polynomials. If a polynomial can be written as the product of two lower-degree polynomials it is called reducible.

Definition 3.20. *A polynomial $a(x) \in F[x]$ with degree at least 1 is called irreducible if it is divisible only by constant polynomials and by constant multiples of $a(x)$.*

Example. Let's observe the polynomials in field $\text{GF}(3)[x]$:

- x^2 is reducible since $xx = x^2$.
- $2x^2 + x$ is reducible since $x(2x + 1) = 2x^2 + x$.
- $x^2 + 1$ is irreducible. We will now see how we can justify this.

Finding out whether a polynomial is irreducible can take time because one has to try out many possible divisors. It is therefore very important to have a good strategy which allows us to limit the number of divisor candidates we have to test. We will now look at some examples of polynomials of different degrees:

- Polynomials of degree 1 are always irreducible. This follows from the definition. It is not possible to write such a polynomial as a product of two polynomials of degree 1.
- Polynomials of degree 2 and 3 are irreducible if they have no root (Corollary 5.30). This is because if they are reducible they must have a factor of degree 1 and according to Lemma 5.29 they have such a factor if and only if they have a root
- Polynomials of degree 4 are irreducible if they don't have a root and no irreducible factors of degree 2. This means that we first check the polynomial for roots, then find the irreducible polynomials of degree 2 and test whether the polynomial of degree 4 can be factorized into two of those polynomials of degree 2.
- For higher degree polynomials of degree d we have to first check the roots of the polynomial and then test for all irreducible polynomials that have a degree $\leq d/2$.

Another technique that is very important in this topic is polynomial division. We can in fact use same procedure as we use in calculus with polynomials in $\mathbb{R}$, but we have to take into account the underlying algebra as for example in $\mathbb{Z}_5$, $2 + 4 = 1$. This means that we have to take every result we obtain from addition or subtraction, modulo the order of the additive group. This is not hard but can easily lead to errors, especially when performing subtraction. It is advised to have a clear and consistent way of writing down each step of the division.

Example. We want to divide $(x^3 + x^2 + 2)$ by $(2x + 1)$ over GF(3):

$$
\begin{array}{rl}
(x^3 + x^2 \quad + 2) & : (2x + 1) \quad = 2x^2 + x + 1 \\
-(x^3 + 2x^2 \quad\;\;) & \\
\hline
2x^2 \quad + 2 & \\
-(2x^2 + x \quad\;\;) & \\
\hline
2x + 2 & \\
-(2x + 1) & \\
\hline
\textit{Rest}: \quad 1 &
\end{array}
$$

In this example the polynomials are not divisible and we get a rest of 1.

3.7.2 Polynomial Interpolation

A polynomial in $R[x]$ can also be seen as a function $R \to R$ that can be evaluated at different points. For polynomials over fields the following property is very important:

Lemma 3.2

A polynomial $a(x) \in F[x]$ of degree at most d is uniquely determined by any $d+1$ values of $a(x)$. For this we use the following formula by Lagrange:

$$a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$$

, where

$$u_i = \frac{(x-\alpha_1)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_{d+1})}{(\alpha_i-\alpha_1)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_{d+1})}$$

This means that if we have $d+1$ distinct (α_i, β_i) pairs where $a(\alpha_i) = \beta_i$, we can recover the polynomial $a(x)$ exactly. A use case for this is sharing a secret among multiple parties. To share a secret among d parties one could pick a polynomial of degree $d-1$. Each party would get the knowledge about one position of the polynomial. The polynomial would then be forgotten and could only be recovered if every party is willing to give its share of the information. The secret itself might be the value of some other position of the polynomial.

Hands-On 6

6.1. Polynomials:

(a) Find all roots of the polynomial $a(x) = x^2 + 3x + 2$ in GF(5).

(b) Find all roots of the polynomial $a(x) = 2x^2 + 3x + 1$ in GF(7).

(c) Find a common irreducible factor of the following two polynomials from GF(5)[x]:

$$a(x) = 2x^3 + 2x^2 + 2x + 2$$
$$b(x) = 3x^4 + 4x^3 + x^2 + x + 4$$

(d) Either show or disprove that $x^4 + x^2 + 1 \in$ GF(2)[x] is irreducible.

(e) Split $x^5 + x^4 + 1 \in$GF(2)[x] into irreducible factors.

(f) Let F be a finite field. Show that there exists a non-constant polynomial $a(x) \in F[x]$ that has no roots in F.

(g) Find all irreducible monic polynomials of degree 2, 3 and 4 in $\mathbb{Z}_2[x]$.

3.8 Finite Fields

So the question remains: Is it possible to construct finite fields of other sizes than prime numbers? Similarly to constructing the set $\mathbb{Z}_m$ where the maximal number is limited by m, we define the set of polynomials over fields where the maximal degree is limited:

Definition 3.21. *Let $m(x)$ be a polynomial of degree d over a field F. Then*

$$F[x]_{m(x)} = \{a(x) \in F[x] | deg(a(x)) < d\}$$

Moreover the cardinality of $F[x]_{m(x)}$ equals $|F|^d$.

Analogously to the modulo operation we perform after every calculation in $\mathbb{Z}_m$, we have to perform a modulo operation with polynomials. That is, if after some calculation the degree of the resulting poly-

nomial is larger than $deg(m(x))$, we need to divide that polynomial by $m(x)$ and take the rest.

Example. In $\mathrm{GF}(3)[x]_{x^2}$ we have $2x(x+1) = 2x$ because we divide the resulting polynomial $2x^2 + 2x$ by x^2 where $2x$ is the rest.

Such a structure is a ring but not necessarily a field because not every polynomial might have multiplicative inverse. This is in fact very similar to what we have in $\mathbb{Z}_m$ and we can now draw a nice comparison between $\mathbb{Z}_m$ and $F[x]_{m(x)}$:
$\mathbb{Z}_m$ is a field if and only if m is prime because otherwise we have some a for which $gcd(a, m) \neq 1$ and thus a zerodivisor. The same holds in $F[x]_{m(x)}$ only that for polynomials the concept of primality is analogous to irreducibility. So $F[x]_{m(x)}$ is a field if and only if $m(x)$ is irreducible (Theorem 5.37).
So to construct a field with p^d elements we need to:

- Pick a field of prime order $\mathrm{GF}(p)$.
- Find an irreducible polynomial $m(x)$ of degree d in $\mathrm{GF}(p)[x]$.

Example. We want to construct a field with 9 elements. As $9 = 3^2$, we choose $\mathrm{GF}(3)$ and the polynomial $m(x) = x^2 + 1$, $m(x)$ is irreducible over $\mathrm{GF}(3)$ as it has degree 2 and no root. Hence $\mathrm{GF}(3)[x]_{x^2+1}$ is a finite field with 9 elements.

Hands-On 7

7.1. Extension Fields:

(a) Calculate the product of $2x + 1$ and $x + 2$ in $\mathrm{GF}(3)[x]_{x^2+x+2}$.

(b) Find all zerodivisors in the ring $\mathrm{GF}(3)[x]_{(x^2+2x)}$.

(c) Choose which of the following statements is true and prove it.
Let F be field, then ...

- ... $F[x]$ must be a field as well.
- ... $F[x]$ could be, but is not necessarily a field.
- ... $F[x]$ cannot be a field.

(d) Find all roots of the polynomial $p(y) = xy^2 + y + (x + 1) \in \mathrm{GF}(2)[x]_{x^2+x+1}[y]$. Keep in mind that $p(y)$ is polynomial over $\mathrm{GF}(2)[x]_{x^2+x+1}$, so the coefficients of $p(y)$ are polynomials themselves.

(e) Factorize the polynomial $a(y) = xy^3 + xy^2 + (x+1)y + x \in \mathrm{GF}(2)[x]_{x^2+x+1}[y]$ into irreducible polynomials.

(f) In case you want more exercises for this specific type of "nested" polynomial fields, here are more exercises:

(i) Check if $y^4 + (x+1)y^2 + y + x \in \mathrm{GF}(2)[x]_{x^2+x+1}[y]$ is reducible.

(ii) Find all roots of $x^2y^2 + (x+1)y + (x^2+1) \in \mathrm{GF}(2)[x]_{x^3+x+1}[y]$.

(iii) Factorize $xy^3 + 2y + 2x \in \mathrm{GF}(3)[x]_{x^2+x+2}[y]$

3.9 Solutions

3.9.1 Solutions for Hands-On 1

1.1

(a) We have to show the following:

Claim

The function f_a defined as

$$\begin{aligned} f_a : G &\to G \\ x &\mapsto a * x \end{aligned}$$

with $a \in G$ arbitrary is bijective.

Proof. To save space, we will sometimes apply axioms in multiple places at once, but you should make sure not to do that in the exam in such an exercise.

A function bijective if it is injective and surjective.

First we will prove that the mapping is injective using an indirect proof:
Let $x, x' \in G$ be arbitrary and let's assume that $f(x) = f(x')$. Then:

$$\begin{aligned} f(x) &= f(x') && \\ \Leftrightarrow a * x &= a * x' && \textit{def. } f \\ \Leftrightarrow \widehat{a} * (a * x) &= \widehat{a} * (a * x') && \widehat{a} \textit{ from the left on both sides} \\ \Leftrightarrow (\widehat{a} * a) * x &= (\widehat{a} * a) * x' && \textit{associativity (G1)} \\ \Leftrightarrow e * x &= e * x' && \textit{inverses (G3)} \\ \Leftrightarrow x &= x' && \textit{neutral element (G2)} \end{aligned}$$

Hence the function is injective.

To show that f_a is surjective we show that for any $b \in G$ there is some $c \in G$ such that $f(c) = b$. For any b we can define c as $c = \widehat{a} * b$, $c \in G$. We can see that $f(c) = a * (\widehat{a} * b) = (a * \widehat{a}) * b = e * b = b$. Hence the function is also surjective.

The function is injective and surjective, it follows that it is bijective. □

(b) We have to show the following:

Claim

The following statement holds for any $x, y \in G$

$$((x * y) * \widehat{x}) * \widehat{y} = e \Leftrightarrow x * y = y * x$$

Proof. We can prove this directly by transforming one into the other

$$
\begin{aligned}
&((x * y) * \widehat{x}) * \widehat{y} = e && \\
\Leftrightarrow\ &(((x * y) * \widehat{x}) * \widehat{y}) * y = e * y && \textit{y from the right on both sides} \\
\Leftrightarrow\ &((x * y) * \widehat{x}) * (\widehat{y} * y) = e * y && \textit{associativity (G1)} \\
\Leftrightarrow\ &((x * y) * \widehat{x}) * e = e * y && \textit{inverses (G3)} \\
\Leftrightarrow\ &((x * y) * \widehat{x}) * e = y && \textit{neutral element (G2)} \\
\Leftrightarrow\ &(x * y) * \widehat{x} = y && \textit{neutral element (G2)} \\
\Leftrightarrow\ &((x * y) * \widehat{x}) * x = y * x && \textit{x from the right on both sides} \\
\Leftrightarrow\ &(x * y) * (\widehat{x} * x) = y * x && \textit{assciativity (G1)} \\
\Leftrightarrow\ &(x * y) * e = y * x && \textit{inverses (G3)} \\
\Leftrightarrow\ &x * y = y * x && \textit{neutral element (G2)}
\end{aligned}
$$

Which proves both directions of the claim. □

(c) We have to show the following:

Claim

Every group of order < 6 has to be commutative.

Proof. There are two major ways of proving this. One is to realize that you need at least five elements to express non-commutativity. We get this by assuming that the group is not commutative i.e. there exist $x, y \in G$ such that $x * y \neq y * x$ We can derive the following

- $x \neq e$ and $y \neq e$
- This implies $x * y \neq x$ and $y * x \neq x$ as both imply $y = e$
- This implies $x * y \neq y$ and $y * x \neq y$ as both imply $x = e$
- $x * y \neq e$ and $y * x \neq e$ as in both cases they would be the inverse of each other and therefore commute. Following from that we have that $e, x, y, x * y, y * x$ have to be pairwise different, so any group with order smaller than 5 is commutative. Every group of order 5 has obviously prime order, is therefore cyclic and also commutative.

The second way is to look at each order individually

- order = 1 - trivially commutative
- order = $2, 3, 5$ - of prime order, therefore cyclic therefore commutative
- order = 4 We have 2 options: either there exists an element of order 4 or not. If yes then we again have a cyclic group. If no then all elements (except e) have order 2 i.e. all elements are self-inverse and the group has to be commutative.

□

(d) We have to show the following:

Claim

Every group that only contains self-inverse elements has to be commutative.

Proof. Let a, b be any elements within the group, then we have

$$a * b = \widehat{a * b} = \widehat{b} * \widehat{a} = b * a$$

by only using the assumption that for all a in our group $a = \widehat{a}$. □

(e) We have to show the following:

Claim

Given any two subgroups H_1, H_2 of a group G:

- $H_1 \bigcup H_2$ is **not** a subgroup of G
- $H_1 \bigcap H_2$ is a subgroup of G
- $H_1 \backslash H_2$ is **not** a subgroup of G

Proof.
- Take $\langle \mathbb{Z}_6; \oplus \rangle$ with the subgroups $\{0, 2, 4\}$ and $\{0, 3\}$. Their union is obviously no subgroup as it is not closed under $\oplus$ as $2 + 3 \notin \{0, 2, 3, 4\}$
- We will show that all conditions for a subgroup hold
  - $e \in H_1 \bigcap H_2$as it is in H_1 and H_2
  - If $a, b \in H_1 \bigcap H_2$ then also $a * b \in H_1 \bigcap H_2$ because if $a, b \in H_1 \bigcap H_2$ then $a, b \in H_1 \Rightarrow a * b \in H_1$ and $a, b \in H_2 \Rightarrow a * b \in H_2$
  - If $a \in H_1 \bigcap H_2$ then also $\widehat{a} \in H_1 \bigcap H_2$ with the same argument as above
  - The associativity follows from the associativity of G

  As all conditions hold it is a subgroup.
- This would allow $H_1 \backslash H_2 = \emptyset$ which is no subgroup. Furthermore even if we would require that $H_1 \backslash H_2 \neq \emptyset$, we could just take any of the real/proper subgroups of $\langle \mathbb{Z}_6; \oplus \rangle$ as H_2 and realize that $\mathbb{Z}_6 \backslash H_2$ is no subgroup of $\langle \mathbb{Z}_6; \oplus \rangle$.

□

(f) We have to show the following:

Claim

For any two elements $a, b \in G$ we have $ord(a * b) = ord(b * a)$

Proof. First realize that this is equivalent to showing

$$ord(a * b) = n \Rightarrow ord(b * a) \leq n$$

as we could you the argument in reverse on $ord(b * a) = n \Rightarrow ord(a * b) \leq n$ and $ord(a * b) \leq ord(b * a) \wedge ord(a * b) \geq ord(b * a) \Rightarrow ord(a * b) = ord(b * a)$
So let us assume that $ord(a * b) = n > 0$ and we need to show that $ord(b * a) \leq n$ which we will by showing that $(b * a)^n = e$

$$\begin{aligned}
& & (a * b)^n &= e \\
\Leftrightarrow & & \underbrace{(a * b) * (a * b) * ... * (a * b)}_{n \text{ times}} &= e \\
\Rightarrow & & b * \underbrace{(a * b) * (a * b) * ... * (a * b)}_{n \text{ times}} * a &= b * a \\
\Rightarrow & & b * a * \underbrace{(b * a) * (b * a) * ... * (b * a)}_{n \text{ times}} &= b * a \\
\Rightarrow & \widehat{a} * \widehat{b} * b * a * \underbrace{(b * a) * (b * a) * ... * (b * a)}_{n \text{ times}} &= \widehat{a} * \widehat{b} * b * a \\
\Rightarrow & & \underbrace{(b * a) * (b * a) * ... * (b * a)}_{n \text{ times}} &= e \\
\Leftrightarrow & & (b * a)^n &= e
\end{aligned}$$

This concludes our proof. We would like to note that we've dropped some formalism to make the proof more concise. It is advisable to mention this and also what you've dropped (i.e. paranthesization) and why it's still correct (because we're associative in groups) in the exam. □

1.2

(a) We have to give:

Claim

The smallest non-trivial subgroup of $\langle \mathbb{Z}_{30}; \oplus \rangle$

Proof. As trivial subgroup we have the subgroup of order 1. The second smallest therefore must have at least order 2 (there can only be one subgroup of order 1). We find $\langle 15 \rangle = \{0, 15\}$ fulfils this. As we've already shown that $\langle a \rangle$ is always a subgroup, we don't have to explicitly show it again. □

(b) We have to show the following:

Claim

Every real subgroup of G is commutative.

Proof. The order of the subgroup has to divide 77. We get as potential candidates for the group order: $\{1, 7, 11\}$. The case with order 1 is trivially commutative while the other orders are prime and therefore cyclic and therefore commutative. □

(c) We have to show the following:

Claim

H_k is a subgroup of G and H'_k not.

Proof. We will show this by showing that all conditions for a subgroup hold:

- $e \in H_k$ as $e^k = e$ for all $k \in \mathbb{N}$
- If $a, b \in H_k$ then $a * b \in H_k$ as

$$(a * b)^k = \underbrace{(a * b) * (a * b) * \cdots * (a * b) * (a * b)}_{k \ times} = a^k * b^k = e * e = e$$

  Where we had to use that the group is abelian.
- If $a \in H_k$ then $\widehat{a} \in H_k$ as

$$\widehat{a}^k = \widehat{a}^k * e = \widehat{a}^k * a^k = (\widehat{a} * a)^k = e^k = e$$

  Where again used that the group is abelian.
- The fact that it is associative follows from the fact that G is a group.

As all conditions hold H_k is a subgroup of G.

The same does not hold for all elements of the order k. We can e.g. choose k such that no element is in the set or realize that for every $k \neq 1$ we don't have $e \in H'_k$. □

1.3

(a) We have to find the following:

Claim

All generators of $\langle \mathbb{Z}^*_{17}; \odot \rangle$

Proof. We know that the order of $\langle \mathbb{Z}_{17}^*; \odot \rangle$ is 16 as 17 is prime. For the order of every element we therefore get that it has to be in the set $\{1, 2, 4, 8, 16\}$. We realize that when the order of an element a is ≤ 8 then $a^8 = 1$. Therefore we only have to check for every element if $a^8 \neq 1$ to find out that it is a generator. We get the following results

$$
\begin{aligned}
1: &\ 1^8 = 1 \\
2: &\ 2^8 = 1 \\
3: &\ 3^8 = 16 \\
4: &\ 4^8 = 1 \\
5: &\ 5^8 = 16 \\
6: &\ 6^8 = 16 \\
7: &\ 7^8 = 16 \\
8: &\ 8^8 = 1 \\
9: &\ 9^8 = 1 \\
10: &\ 10^8 = 16 \\
11: &\ 11^8 = 16 \\
12: &\ 12^8 = 16 \\
13: &\ 13^8 = 1 \\
14: &\ 14^8 = 16 \\
15: &\ 15^8 = 1 \\
16: &\ 16^8 = 1
\end{aligned}
$$

We therefore have the generatorset $\{3, 5, 6, 7, 10, 11, 12, 14\}$ with $|\{3, 5, 6, 7, 10, 11, 12, 14\}| = 8 = \phi(16)$. This cardinality check is great to be relatively sure that you didn't make any mistakes. □

(b) We have to find the following:

Claim

All generators of $\langle \mathbb{Z}_{20}; \oplus \rangle$

Proof. We just have to find all elements a smaller than 20 that fulfill $gcd(a, 20) = 1$. We get $\{1, 3, 7, 9, 11, 13, 17, 19\}$ with $|\{1, 3, 7, 9, 11, 13, 17, 19\}| = 8 = \phi(20)$ □

(c) We have to show the following:

Claim

For two cyclic groups $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$ (g_1, g_2) is generally not a generator of $G_1 \times G_2$

Proof. Take the cyclic groups $\langle \mathbb{Z}_2; \oplus \rangle$ and $\langle \mathbb{Z}_4; \oplus \rangle$ with $g_1 = 1 = g_2$. For $(1, 1)$ we generate now the group $\{(1, 1), (0, 2), (1, 3)(0, 0)\}$ which is not equal to $\mathbb{Z}_2 \times \mathbb{Z}_4$. □

(d) We will show the following:

Claim

m and n have to be relatively prime for this statement to hold. The same goes for the orders of general cyclic groups. We will therefore look at the general cyclic groups G_1 and G_2 with

the respective orders m and n.

Proof. First we show that this condition is necessary, then we will show that it is sufficient.

Assume that $gcd(m,n) = d$ with $d > 1$ Which let's us define $lcm(m,n) = l = \frac{m \cdot n}{d} < m \cdot n$. We already know that $g_1^r = g_1^{r+k \cdot m}$ and $g_2^r = g_2^{r+v \cdot n}$ for $m, n \in \mathbb{N}$. Further we know that we can write l as $l = q \cdot m$ or $l = p \cdot n$ with $p, q \in \mathbb{N}$. We conclude that

$$(g_1, g_2)^{1+l} = (g_1^{1+q \cdot m}, g_2^{1+p \cdot n}) = (g_1^1, g_2^1) = (g_1, g_2)$$

Therefore we can at most (exactly) generate l different elements with (g_1, g_2) and as $l < m \cdot n = |G_1 \times G_2|$ we know that it is no generator.

To show that it is sufficient we only have to realize that we will always generate exactly l elements as l is by definition the lowest number for which we can find a factorization l as $l = q \cdot m$ or $l = p \cdot n$ with $p, q \in \mathbb{N}$. Furthermore if $gcd(m,n) = 1$ so is $l = m \cdot n$ and by generating $m \cdot n$ different elements we will generate $G_1 \times G_2$. (One might develop this proof further by showing that we can't get into a "loop" earlier but this should in theory be clear from the chapter about number theory and the fact that $G_1 \times G_2$ is a group) □

(e) We will show the following:

Claim

For any cyclic group G of order $m \cdot k$ we have an element $a \in G$ such that $a^m = e$

Proof. This proof makes use of the isomorphic relationship between G and $\langle \mathbb{Z}_{m \cdot k}; \oplus \rangle$. It is obvious (or after the chapter about isomorphisms it should be obvious) that if there exists such an element in $\langle \mathbb{Z}_{m \cdot k}; \oplus \rangle$, it also has to exist in G. The element in $\langle \mathbb{Z}_{m \cdot k}; \oplus \rangle$ is just $a_{\mathbb{Z}} = k$ where k is the number in $\mathbb{Z}_{m \cdot k}$. Obviously we have $k^m = m \cdot k = 0$.

As we already know G and $\langle \mathbb{Z}_{m \cdot k}; \oplus \rangle$ are isomorph. Let ϕ such an isomorphism defined as

$$\begin{aligned} \phi : \mathbb{Z}_{m \cdot k} &\to G \\ x &\mapsto \phi(x) \end{aligned}$$

then we have $a^m = \phi(a_{\mathbb{Z}})^m = \phi(a_{\mathbb{Z}}^m) = \phi(0) = e$ using our knowledge about isomorphisms. □

1.4

(a) We have to show the following:

Claim

$\widehat{(\widehat{a})} = a$

Proof. We have

$$\widehat{(\widehat{a})} \overset{G2}{=} \widehat{(\widehat{a})} * e \overset{G3}{=} \widehat{(\widehat{a})} * (\widehat{a} * a) \overset{G1}{=} (\widehat{(\widehat{a})} * \widehat{a}) * a \overset{G3}{=} e * a \overset{G2}{=} a$$

□

otherwise we could argue the same using the uniqueness of the inverse element.

(b) We have to show the following:

Claim

$\widehat{a * b} = \widehat{b} * \widehat{a}$

Proof. We have

$$\widehat{a * b} \overset{G2}{=} \widehat{a * b} * e \overset{G3}{=} \widehat{a * b} * (a * \widehat{a}) \overset{G2}{=} \widehat{a * b} * (a * e * \widehat{a}) \overset{G3}{=} \widehat{a * b} * (a * (b * \widehat{b}) * \widehat{a}) \overset{G1}{=} (\widehat{a * b} * (a * b)) * \widehat{b} * \widehat{a} \overset{G3}{=} e * \widehat{b} * \widehat{a} \overset{G2}{=} \widehat{b} * \widehat{a}$$

again we could otherwise use that $(a * b) * \widehat{b} * \widehat{a} = e$ and rely on the uniqueness of the inverse element. □

(c) We have to show the following:

Claim

$a * b = a * c \Rightarrow b = c$

Proof. We have

$$b \overset{G2}{=} e * b \overset{G3}{=} (\widehat{a} * a) * b \overset{G1}{=} \widehat{a} * (a * b) \overset{As.}{=} \widehat{a} * (a * c) \overset{G1}{=} (\widehat{a} * a) * c \overset{G3}{=} e * c \overset{G2}{=} c$$

□

(d) We have to prove the following:

Claim

One-Step Subgroup Test

Proof. We show that $H \subseteq G$ is a subgroup of the group $\langle G; \circ \rangle$ if and only if it fulfils the "One-Step Subgroup Test".

First and foremost we realize that all parts of the "One-Step Subgroup Test" are direct corollaries of the characteristics of a subgroup. So it is trivial that

$$H \text{ is subgroup of } G \Rightarrow H \text{ fulfills the One-Step Subgroup Test}$$

We will therefore only focus on the part

$$H \text{ fulfills the One-Step Subgroup Test} \Rightarrow H \text{ is subgroup of } G$$

We will show each required condition individually

- $H \neq \emptyset$, therefore let a be an element in H. By the "second rule" we now have $a \circ a^{-1} = e \in H$
- Knowing that we have $e \in H$ we have for every a in H again by the "second rule" that $e \circ a^{-1} = a^{-1} \in H$
- As we know that all inverse elements are also in H we use the "second rule" one more time to show that for any $a, b \in H$ we have $a \circ b = a \circ (b^{-1})^{-1} \in H$
- That $H \subset G$ is already given and the fact that $\circ$ is associative follows from the fact that it is associative in $\langle G; \circ \rangle$.

We have shown the second part and therefore

$$H \text{ fulfills the One-Step Subgroup Test} \Leftrightarrow H \text{ is subgroup of } G$$

□

1.5 (Challenge)

(a) We will show that it is an equivalence relation by showing that it fulfills each requirement:

- reflexivity:

$$\forall x \in G \; x^{-1}x = e \in H$$

- symmetry:

$$\forall x, y \in G \; x^{-1}y \in H \Rightarrow \left(x^{-1}y\right)^{-1} \in H \Rightarrow y^{-1}(x^{-1})^{-1} \in H \Rightarrow y^{-1}x \in H$$

- transitivity:

$$\forall x, y, z \in G \; x^{-1}y \in H \wedge y^{-1}z \in H \Rightarrow x^{-1}yy^{-1}z \in H \Rightarrow x^{-1}z \in H$$

(b) We have for every element y in xH that

$$\exists h \in H \; x = yh \Leftrightarrow \exists \mathbf{h} \in \mathbf{H} \; \mathbf{y} = \mathbf{xh} \Leftrightarrow \exists h \in H \; x^{-1}y = h \Leftrightarrow x^{-1}y \in H \Leftrightarrow x \backsim y$$

Where the bold part comes from the fact that H is a subgroup and therefore contains the inverse element to the h of the first equation. (We could also argue with the symmetry of $\backsim$) We can follow from this equation that in fact all elements xH form an equivalence class of $\backsim$.

(c) We take a look at the map

$$\begin{aligned} \phi : H &\to xH \\ h &\mapsto xh \end{aligned}$$

which we happen to know is injective. It is also surjective as we defined xH to be the image of ϕ. As the map is therefore bijective we can conclude that $|xH| = |H|$

(d) We have an equivalence relation on G, which by definition forms a partition of G. Furthermore we know that equivalence classes have the same size and that H is one of these equivalence classes (for $x = e$). Therefore the cardinality of H has to divide the cardinality of G.

3.9.2 Solutions for Hands-On 2

2.1

(a) We have to show the following:

Claim

$$\{g \in G \mid g * g_0 * g^{-1} \in \phi^{-1}(\{e_H\}\} = G$$

Proof. First we realize that this is equivalent to stating that for all $g \in G$ we have

$$\phi(g * g_0 * g^{-1}) = e_H$$

So let $g \in G$ be arbitrary. We have

$$\phi(g * g_0 * g^{-1}) = \phi(g) \cdot \phi(g_0) \cdot \phi(g^{-1}) = \phi(g) \cdot e_H \cdot \phi(g^{-1}) = \phi(g) \cdot \widehat{\phi(g)} = e_H$$

where we used that $\phi(g^{-1}) = \widehat{\phi(g)}$ and $\phi(g_0) = e_H$ □

2.2

(a) We have to show the following:

Claim

For any $a \in G$ $\phi(a^{-1}) = \widehat{\phi(a)}$

Proof. We have

$$\begin{aligned}
\phi(a^{-1}) &= \phi(a^{-1}) \cdot e_H \\
&= \phi(a^{-1}) \cdot (\phi(a) \cdot \widehat{\phi(a)}) \\
&= (\phi(a^{-1}) \cdot \phi(a)) \cdot \widehat{\phi(a)} \\
&= \phi(a^{-1} * a) \cdot \widehat{\phi(a)} \\
&= \phi(e_G) \cdot \widehat{\phi(a)} \\
&= e_H \cdot \widehat{\phi(a)} \\
&= \widehat{\phi(a)}
\end{aligned}$$

□

(b) We have to show the following:

Claim

For any $a \in G$ $\phi(a^n) = \phi(a)^n,\ n \in \mathbb{Z}$

Proof. We will prove this by induction. Before that we remind ourselves of the fact that for $n < 0$ we have that $a^n = \left(a^{-1}\right)^{|n|}$ and we can prove it analogous. Thus it is enough to focus on the case where $n \in \mathbb{N}$.

Let $a \in G$ be arbitrary
1.**Induction basis** For $n = 0, 1$ we have $\phi(a^0) = \phi(e_G) = e_H = \phi(a)^0$ and $\phi(a^1) = \phi(a) = \phi(a)^1$
2.**Assumption** For arbitrary n we have $\phi(a^n) = \phi(a)^n$
3.**Induction step** We have $\phi(a^{n+1}) = \phi(a^n * a) = \phi(a^n) \cdot \phi(a) \overset{IA}{=} \phi(a)^n \cdot \phi(a) = \phi(a)^{n+1}$

The induction shows that the statement holds for all $n \in \mathbb{N}$, which together with our earlier thoughts shows that it holds for all $n \in \mathbb{Z}$. □

(c) We have to show the following:

Claim

A homorphisms projects a group always onto a subgroup of the codomain. I.e. $Im(\phi)$ is a subgroup of H

Proof. We will show that it fulfills the usual conditions

- We have $e_H \in Im(\phi)$ as $\phi(e_G) = e_H$
- For any $a, b \in Im(\phi)$ we have $a \cdot b \in Im(\phi)$ as

$$a \cdot b = \phi(x) \cdot \phi(y) = \phi(x * y) \in Im(\phi)$$

  where $x, y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$
- For all $a \in Im(\phi)$ we have $\widehat{a} \in Im(\phi)$. Let $a' \in G$ with $\phi(a') = a$, then

$$\phi(a'^{-1}) = \widehat{\phi(a')} = \widehat{a} \in Im(\phi)$$

The rest follows as usual. □

2.3

(a) We have to show the following:

Claim

For any m, n with $gcd(m, n) = 1$ the following map is an isomorphism:

$$\begin{aligned} \phi : \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ x &\mapsto (R_m(x), R_n(x)) \end{aligned}$$

Proof. First we will show that it is a homomorphism as we have for any $x, y \in \mathbb{Z}_{mn}$

$$\begin{aligned} \phi(x \oplus_{mn} y) &= (R_m(x \oplus_{mn} y), R_n(x \oplus_{mn} y)) \\ &= (R_m(x + y), R_n(x + y)) \\ &= (R_m(R_m(x) + R_m(y)), R_n(R_n(x) + R_n(y))) \\ &= (R_m(x), R_n(x)) \oplus_{m \times n} (R_m(y), R_n(y)) \\ &= \phi(x) \oplus_{m \times n} \phi(n) \end{aligned}$$

Now we will show its bijectivity:
By the CRT we know that there is a one-to-one relationship between $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$.

We will show that ϕ is injective and therefore constitutes such a relationship. Assume there exist $x, y \in \mathbb{Z}_{mn}$ with $x \neq y$ but with $\phi(x) = \phi(y)$. This follows from the fact that both x and y are a solution to the following system of equations

$$\begin{aligned} a &\equiv_m \phi(x) \\ a &\equiv_n \phi(x) \end{aligned}$$

Given that $x, y < m \cdot n$ and $\phi(x) < m$ and $\phi(x) < n$ we have by the CRT that this solution has to be unique i.e. $x = y$ which contradicts the assumption. It follows that ϕ has to be injective.

Knowing that $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$ we conclude that it also has to be surjective.

We have a bijective homomorphism, an isomorphism. □

(b) We have to show the following:

Claim

The condition $gcd(m, n) = 1$ is necessary for ϕ to be an isomorphism.

Proof. Assume that $gcd(m, n) = d > 1$, then $lcm(m, n) = l = \frac{m \cdot n}{d} < m \cdot n$. With $l \in \mathbb{Z}_{mn}$ we observe that $\phi(0) = (0, 0) = \phi(l)$ leading to the fact the the mapping is neither injective nor surjective. □

(c) We have to show the following:

Claim

There exist exactly 4 non-isomorphic subgroups of $\langle Z_m; \oplus \rangle$.

Proof. By Lagrange we know that the order of every subgroup has to divide the order of the group.

We get next to $\langle Z_m; \oplus \rangle$ and $\{1\}$ just subgroups with either order q or p. As both q and p are prime we know that groups of this order have to be cyclic and therefore isomorphic to $\langle \mathbb{Z}_q; \oplus \rangle$ and $\langle \mathbb{Z}_p; \oplus \rangle$ respectively.

Therefore all subgroups of $\langle Z_m; \oplus \rangle$ with order p or q are (respectively) isomorphic.

In order to show that there exist subgroups of order p and q we can simply write them down: $\langle p \rangle$ has order q and $\langle q \rangle$ has order p. □

(d) We have to show the following:

Claim

If $\phi : G \to H$ is an injective homomorphism, it has **not** to be an isomorphism.

Proof. Take any group H with a "real" subgroup G. Now take the identity-map as ϕ defined as

$$\begin{aligned} \phi : G &\to H \\ x &\mapsto x \end{aligned}$$

Obviously this map is injective but it is not surjective onto H i.e. no isomorphism. The same goes for any injective map onto a real *subgroup* of a group. □

2.4

(a) We have to show the following:

Claim

An isomorphism between cyclic groups always maps a generator to a generator

Proof. Let G and H be two isomorph finite cyclic groups with the isomorphism $\phi : G \mapsto H$ and let g be a generator of $\langle g \rangle = G$. We want to show that $H = \langle \phi(g) \rangle$ i.e. $\phi(g)$ generates H.
We have:
1. H is closed under its operation, explicitly we have $\langle \phi(g) \rangle \subseteq H$

2. ϕ is bijective and therefore for all $h \in H$ there exists exactly one $b \in G$ $\phi(b) = h$

3. $\langle g \rangle = G$ which implies that there exists a $m \in \mathbb{N}$ $g^m = b$

4. Combining 2. and 3. we get that for all $h \in H$ there exists an $m \in \mathbb{N}$ such that $\phi(g^m) = [\phi(g)^m] = h \quad \Leftrightarrow \quad H \subseteq \langle \phi(g) \rangle$

5. Based on 1. and 4. and our knowledge about sets we get $H = \langle \phi(g) \rangle$ which proves our initial statement. □

(b) We have to show the following:

Claim

Based on the above we can follow that all finite cyclic groups of the same order are isomorphic.

Proof. Let $\langle G; *, ^{-1}, 1 \rangle$ with the generator g and $\langle H; \cdot, \widehat{,}, e \rangle$ with the generator h. We just give the isomorphism

$$\begin{aligned} \phi : G &\to H \\ g^r &\mapsto h^r \end{aligned}$$

Now we show that this map has all the wished properties.

1. Homomorphism:

$$\phi(a * b) = \phi(g^r * g^j) = \phi(g^{r+j}) = h^{r+j} = h^r \cdot h^j = \phi(g^r) \cdot \phi(g^j) = \phi(a) \cdot \phi(b)$$

2. Surjectivity: Let $h' \in H$ be arbitrary, via assumption there exists a (smallest) r such that $h^r = h'$. We then have (based on equal cardinality), that $\phi(g^r) = \phi(g)^r = h^r = h'$ which proves the surjektivity.
3. Injectivity: Suppose ϕ is not injective, i.e. there exist $r, r' < |H|$ with $h^r \in H$ and $h^{r'} \in H$ with $r \neq r' \wedge h^r = h^{r'}$, which is a direct contradiction to the assumption that h is a generator of H.

□

(c) We have to show the following:

Claim

Isomorphisms carry commutativity.

Proof. We want to show that if one group is commutative then also all isomorphic groups. Let $\langle G; *, ^{-1}, 1 \rangle$ be an commutative group isomorph to $\langle H; \cdot, \widehat{,}, e \rangle$ with an isomorphism ϕ.

We will show the commutativity of H directly: Let $h_1, h_2 \in H$ with their respective preimage $g_1, g_2 \in G$ be arbitrary.

We have

$$h_1 \cdot h_2 = \phi(g_1) \cdot \phi(g_2) = \phi(g_1 * g_2) = \phi(g_2 * g_1) = \phi(g_2) \cdot \phi(g_1) = h_2 \cdot h_1$$

□

Which proves the statement.

2.5 (Challenge)

(a) We (this is normally a hint that you get with the task) know that a cyclic group of order n has $\varphi(n)$ generators.

We've already seen in the previous task that every isomorphism maps a generator in one group to a generator in the other group. Furthermore it is actually enough to give just the map of one of the generators to fully identify the isomorphism, as we can easily infer all other mappings out of this (with $\phi(g^n) = \phi(g)^n$).

One might now think that there are $\varphi(n)^2$ possible isomorphisms between these two groups, based on all possible combinations. This thought is wrong as it doesn't assume that when we map one generator onto another and by that create an isomorphism we at the same time also determine the mapping of all other generators onto generators of the other group.

As a matter of fact we can by applying this method create exactly $\varphi(n)$ different isomorphisms, i.e. by taking one generator and mapping it to each of the generators of the other group individually. If we want to repeat this procedure with the second generator of the first group we would obviously create the same $\varphi(n)$ isomorphisms.

As every isomorphism has to map every generator onto a generator we conclude that there exist exactly $\varphi(n)$ different isomorphisms between two cyclic groups of order n.

3.9.3 Solutions for Hands-On 3

3.1

(a) We have to show the following:

Claim

The inverse of 3 in $\mathbb{Z}_{13}^*$ is 9.

Proof. Obviously we have $9 \in \mathbb{Z}_{13}^*$. Furthermore we have $9 \cdot 3 = 27 \equiv_{13} 1$ □

(b) We have to show the following:

Claim

$|\mathbb{Z}_{30}^*| = 8$

Proof. We have $30 = 2 \cdot 3 \cdot 5$ therefore $\varphi(30) = 1 \cdot 2 \cdot 4$, the elements are $1, 7, 11, 13, 17, 19, 23, 29$. □

(c) We have to show the following:

Claim

The number $4 \cdot 7 \cdot 6 \cdot 28 = 4704$ solves this equation.

Proof. First we realize that $gcd(3036, 7105) = 1$ i.e. they are relativ prime. Based on that we can use our corollary of Fermat/Euler. We calculate $\varphi(7105) = 4 \cdot 7 \cdot 6 \cdot 28 = 4704$ and get that

$$3036^{4704} \equiv_{7105} 1$$

□

(d) We have to show the following:

Claim

Every real subgroup of $\mathbb{Z}_6^*$ is commutative.

Proof. Every real subgroup of $\mathbb{Z}_6^*$ must have an order < 6 and is therefore commutative by the task solved on the first Hands-On. □

3.2 (Challenge)

(a) Let $n, m \in \mathbb{N}$ be relatively prime, i.e. $gcd(n, m) = 1$. From this follows directly, that the sets of primes of each respective prime factorization are disjunctive. (Otherwise, $gcd(n, m) \neq 1$) Let $p_1^{a_1} p_2^{a_2} \cdot ... \cdot p_i^{a_i} = n$ and $q_1^{b_1} q_2^{b_2} \cdot ... \cdot q_j^{b_j} = m$ denote these factorizations with $\{p_1, p_2, ..., p_i\} \cap \{q_1, q_2, ..., q_j\} = \emptyset$. Lemma 5.12 says

$$\varphi(n) = \prod_{k=1}^{i} (p_k - 1) p_k^{a_k - 1}$$

$$\varphi(m) = \prod_{k=1}^{j} (p_k - 1) p_k^{b_k - 1}$$

Therefore, since $mn = p_1^{a_1} p_2^{a_2} \cdot ... \cdot p_i^{a_i} \cdot q_1^{b_1} q_2^{b_2} \cdot ... \cdot q_j^{b_j}$ and $\forall s, t\colon\ p_s \neq p_t$

$$\varphi(nm) \overset{Lem.5.12}{=} (\prod_{k=1}^{i} (p_k - 1) p_k^{a_k - 1}) \cdot (\prod_{k=1}^{j} (p_k - 1) p_k^{b_k - 1}) = \varphi(n) \cdot \varphi(m)$$

3.9.4 Solutions for Hands-On 4

4.1

(a) This ring has 4 units.
Units in $\mathbb{Z}_{12}$ are elements that have a multiplicative inverse. According to Definition 5.16 these are all elements a where $\gcd(a, 12) = 1$.
These are exactly $1, 5, 7$ and 11.

(b) We know that R is a ring with at least 2 elements and R^* is its multiplicative group. We have to show the following equivalence:

Claim

$$r \in R^* \iff \forall s \in R\ \exists t \in R\ \ s = rt$$

Proof. We show both sides of the equivalence separately:
($\Longrightarrow$) : Let $r \in R^*$ and $s \in R$ be arbitrary. We have to somehow construct a t such that $s = rt$. If we don't know how to approach this, we should think about what we are given: r is element of the multiplicative group which means, that r has an inverse element, r^{-1}, such that $rr^{-1} = 1$. We can thus say that $s = 1s = rr^{-1}s$. This shows that for every $s \in R$ there exists $t = r^{-1}s$ such that $s = rt$.
($\Longleftarrow$) : We again do a direct proof of the implication. We know that $r \in R$ and we have to prove that r has a multiplicative inverse, meaning that r^{-1} exists in R. We are given that for any s we can find t such that $s = rt$. Since $1 \in R$, this implies that there is a t such that $1 = rt$. This is exactly the definition of a multiplicative inverse. $r^{-1} = t \in R$ and thus $r \in R^*$.

□

(c) We show that:

Claim

A ring where $0 = 1$ contains exactly one element.

Proof. Let R be a ring where $0 = 1$. Since the neutral element must be in the ring, R contains at least one element. Let's assume that $|R| > 1$ is the case and some $a \neq 0 \in R$. It follows that $a = 1a = 0a = 0$ using the definition of the neutral element and Lemma 5.17.
Therefore $\forall a \in R\ \ a = 0$ and thus $|R| = 1$.
(One could also use Lemma 5.17(iv) to prove this.)

□

(d) We show that:

Claim

Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring such that $a \cdot a = a$. We claim that $\forall a \in R.\ a + a = 0$

Proof. Let $a \in R$ be arbitrary. Then we have

$$\begin{aligned} a + a &\overset{As.}{=} (a + a) \cdot (a + a) \\ &\overset{Dis.}{=} (a \cdot a) + (a \cdot a) + (a \cdot a) + (a \cdot a) \\ &\overset{As.}{=} a + a + a + a \end{aligned}$$

using our assumption twice and grouping multiple distributivity (and associativity) uses. But then

$$\begin{aligned} & a+a && = a+a+a+a \\ \Rightarrow & a+a+(-a)+(-a) && = a+a+a+a+(-a)+(-a) \\ \Rightarrow & 0 && = a+a \end{aligned}$$

Using the existence of the additive inverse. This concludes the proof. (It should be mentioned that most steps can be split into more individual sub-steps. We omitted them for conciseness) □

(e) We show that

Claim

Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring such that $a \cdot a = a$. We claim that R is commutative using the result above.

Proof. First note that the result above can be rewritten as

$$a + a = 0 \Leftrightarrow a = -a$$

We need to show that $\forall a, b \in R.\ a \cdot b = b \cdot a$. Let us take $a, b \in \mathbb{R}$ arbitrary. Then $(a+b) \overset{as.}{=} (a+b) * (a+b) \overset{dist.}{=} aa + ab + ba + bb \overset{as.}{=} a + ab + ba + b \Rightarrow 0 = ab + ba$. (Due to right and left cancellation laws.) $\overset{def.-}{\Rightarrow} ba = -(ab) \overset{as.}{\Rightarrow} ab = -(ab) = ba$ Therefore, R is commutative. □

4.2

(a) Let D be an arbitrary integral domain where 1 has an additive order of c. We have to show that if D is finite, c is prime:

Proof. Suppose $c \in \mathbb{N}$ is not a prime. Then there are $m, n \in \mathbb{N}$ such that $m \cdot n = c$ (both not 1). We want to show a contradiction to the definition of integral domains. The special thing about integral domains is that they don't have zerodivisors. So to prove our claim, we have to show that if c is not prime, we have zerodivisors:
Since c is the order of the additive group, we have:

$$0 = \sum_{i=1}^{c} 1 = \sum_{i=1}^{mn} 1 =^{(1)} (\sum_{i=1}^{m} 1) \cdot (\sum_{i=1}^{n} 1)$$

Since $m < c$ and $n < c$, both factors are not 0 and thus they are zerodivisors and D cannot be an integral domain.
The last equivalence (1) is not trivial and should be proven separately. For this we can use induction over n:
Basis step: For $n = 0$ it's easy to see that both sides of the equation are 0. An empty sum evaluates to 0 and $0a = a$ for all a.
Let n be arbitrary. Under the assumption that the equation holds for n, we prove that it also holds for $n + 1$:
Induction step:

$$\sum_{i=1}^{(n+1)m} 1 = \sum_{i=1}^{nm} 1 + \sum_{i=1}^{m} 1 =^{I.H.} (\sum_{i=1}^{n} 1) \cdot (\sum_{i=1}^{m} 1) + \sum_{i=1}^{m} 1 =$$

$$(\sum_{i=1}^{n} 1) \cdot (\sum_{i=1}^{m} 1) + 1 \cdot \sum_{i=1}^{m} 1 = (\sum_{i=1}^{n} 1 + 1) \cdot (\sum_{i=1}^{m} 1) = (\sum_{i=1}^{n+1} 1) \cdot (\sum_{i=1}^{m} 1)$$

In the last steps we applied the distributivity law.

□

3.9.5 Solutions for Hands-On 5

5.1

(a) We show that:

Claim

$\mathbb{Z}_4$ is not a field.

Proof. (We give 2 possible proofs)
(1)
Let $\mathbb{Z}_4$ be a field.
According to the definition of fields, $\mathbb{Z}_4^* = \mathbb{Z}_4 \backslash \{0\}$ is a multiplicative group.
According to Definition 5.16 for all elements a in $\mathbb{Z}_4^*$ $gcd(a, 4) = 1$. However $gcd(2, 4) \neq 1$. This is a contradiction.

(2)
A field is an integral domain (Theorem 5.24). An integral domain has no zerodivisors. However 2 is a zerodivisor in $\mathbb{Z}_4$ since $2 \cdot 2 = 0$. Thus $\mathbb{Z}_4$ is not an integral domain and also not a field. □

(b) Let F be an arbitrary finite field. Note that in the following we are not dealing with numbers, but for the sake of simplicity we denote the elements we're dealing with the same way. We can derive the following:
$x^2 = 1 \iff x^2 - 1 = 0 \iff (x + 1)(x - 1) = 0$
This implies that x is either -1 or 1.
This solution holds for all fields since every field contains the elements -1 and 1.
For example in GF(3), $-1 = 2$ and $2 \cdot 2 = 1$ Such elements are inverses of themselves.

(c) Let F be an arbitrary finite field.

Claim

$$\prod_{a \in F*} a = -1$$

.

Proof. We are allowed to use the results of the previous exercise, which is that in any field only 1 and -1 are self-inverse elements.
Every other element $a \in F^*$ has a unique multiplicative inverse $a^{-1} \in F^*$ where $a \neq a^{-1}$. Let $a_1, ...a_k$ be those elements, then (after reordering them, so they appear in the appropriate pairs):

$$\prod_{a \in F*} a = a_1 \cdot a_1^{-1} \cdot .... \cdot a_{\frac{k}{2}} \cdot a_{\frac{k}{2}}^{-1} \cdot 1 \cdot (-1) = \prod_{i=1}^{\frac{k}{2}} \cdot 1 \cdot (-1) = -1.$$

For finite fields with characteristic 2 (i.e. $1 = -1$) we would have to slightly adjust the argument (since $x^2 = 1$ now only has one solution) and we'd get $\prod_{a \in F*} a = 1$ but because $1 = -1$ the claim is true here as well. □

3.9.6 Solutions for Hands-On 6

6.1

(a) We simply evaluate the polynomial for all elements in GF(5):

- $a(0) = 0 + 0 + 2 = 2$
- $a(1) = 1 + 3 + 2 = 1$
- $a(2) = 4 + 1 + 2 = 2$
- $a(3) = 4 + 4 + 2 = 0$
- $a(4) = 1 + 2 + 2 = 0$

The roots are 3 and 4. Also $(x-3)(x-4) = x^2 + 3x + 2$.

(b) We evaluate the polynomial for all elements in GF(7):

- $a(0) = 0 + 0 + 1 = 1$
- $a(1) = 2 + 3 + 1 = 6$
- $a(2) = 1 + 6 + 1 = 1$
- $a(3) = 4 + 2 + 1 = 0$
- $a(4) = 4 + 5 + 1 = 3$
- $a(5) = 1 + 1 + 1 = 3$
- $a(6) = 2 + 4 + 1 = 0$

The roots are 3 and 6. Also $2 \cdot (x-3)(x-6) = 2x^2 + 3x + 1$.

(c) We need to find a common irreducible factor of both polynomials. Such a polynomial could be either of degree 1 or degree 2.
Since it's easier, let's first check for factors of degree 1. Remember that a polynomial has a factor of degree 1 if and only if it has a root. So we can check for common roots:
After first testing 0 and 1 we find out that 2 is a root of both $a(x)$ and $b(x)$ since $a(2) = 1+3+4+2 = 0$ and $b(2) = 3 + 2 + 4 + 2 + 4 = 0$.
According to Lemma 5.29, $(x-2)$ is a common factor of both polynomials.

(d) Let's use our strategy to find out whether $x^4 + x^2 + 1$ is irreducible:

- First we check for roots of the polynomial: Neither 0, nor 1 are roots. If the polynomial is reducible, the factors have to be of degree 2.
- We look for irreducible polynomials of degree 2: For this we check $x^2, (x^2+1), (x^2+x)$ and (x^2+x+1) for roots. It turns out that (x^2+x+1) is the only irreducible polynomial of degree 2. If our polynomial is reducible, then (x^2+x+1) must be the factor.
- We check that in fact $(x^2+x+1)(x^2+x+1) = (x^4+x^2+1)$.

Therefore $(x^4 + x^2 + 1)$ is not irreducible.

(e) This exercise is tricky because it again involves higher degree polynomials. We can use the same strategy we use to test for irreducible polynomials:

- First we check for roots: Neither 0, nor 1 are roots. Therefore one of the factors must be an irreducible polynomial of degree 2.
- We find all irreducible polynomials of degree 2. We do this by checking $x^2, (x^2+1), (x^2+x)$ and (x^2+x+1) for roots. The only polynomial with no roots, and thus irreducible, is (x^2+x+1).
- We divide $(x^5 + x^4 + 1)$ by $(x^2 + x + 1)$ using polynomial division. The resulting polynomial is $(x^3 + x + 1)$. Since we know that there are no factors of degree 1, we can conclude that $(x^3 + x + 1)$ is irreducible as well and therefore we are done.

(f) This is a more difficult one. We need to show that over any finite field F there exists at least one polynomial with no roots. To prove the statement we need to construct such a polynomial given an arbitrary field F.
According to Lemma 5.29 we know that a polynomial has a root if and only if it is divisible by some polynomial of degree 1. This means that irreducible polynomials of degree ≥ 2 have no roots. In other words we can prove the statement by constructing an irreducible polynomial of degree ≥ 2.

(g) To find all irreducible monic polynomials of degree 2, 3 and 4 in $\mathbb{Z}_2[x]$, we can employ some tricks:

- Notice that for any polynomial in $\mathbb{Z}_2[x]$, we have $a(1) = 0$ if and only if there is an even number of non-zero coefficients. That means, any irreducible polynomial *must* have an odd number of terms.
- For any polynomial in $\mathbb{Z}_2[x]$, we have $a(0) = 0$ if the constant term is 0. Thus, any irreducible polynomial *must* have a constant term of 1.

Now we can see that out of all the monic polynomials of degree 2 ($x^2, x^2+1, x^2+x, x^2+x+1$), only x^2+x+1 satisfies all these conditions and indeed, we can check that it has no roots and is therefore irreducible.

Similarly we can eliminate some degree 3 polynomials: out of $x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1$, we are left with only x^3+x+1, x^3+x^2+1 which both have no roots and are thus irreducible.

For degree 4 polynomials we repeat the process to get the candidates $x^4+x^3+x^2+x+1, x^4+x^3+1, x^4+x^2+1, x^4+x+1$ which all have no roots. *But* we also need to check if any irreducible degree 2 polynomial divides one of these candidates, so we carry out long division with x^2+x+1. After this, we're left with the irreducible polynomials $x^4+x^3+x^2+x+1, x^4+x^3+1, x^4+x+1$.

Proof. Let F be an arbitrary finite field with m elements.
Let $a_1(x), a_2(x), ...a_m(x)$ be all irreducible polynomials of degree 1 in $F[x]$.
Then $p(x) = a_1(x) \cdot a_2(x) \cdot ... \cdot a_m(x) + 1$ is a polynomial which is not divisible by any polynomial of degree 1. $p(x)$ is either irreducible or it is divisible by some irreducible polynomial of degree ≥ 2. In both cases this proves the existence of an irreducible polynomial of degreee ≥ 2 and such a polynomial does not have a root.

□

3.9.7 Solutions for Hands-On 7

7.1

(a) In $\mathrm{GF}(3)[x]_{x^2+x+2}$ we need to perform a modulo operation every time the degree of a polynomial is larger than 1. We then have:

$$(2x+1)(x+2) = 2x^2 + x + x + 2 = 1$$

(b) Let's first list all elements of $\mathrm{GF}(3)[x]_{(x^2+2x)}$:
They are $\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$. As sanity check we count that the number of elements equals 3^2.
Now the question is which of those elements are zerodivisers, that is, which of them divide x^2+2x? We only have to check the polynomials of degree 1 since polynomials of degree 0 cannot divide x^2+2x. By trying out combinations of the degree 1 polynomials we find out that:

$$x(x+2) = x^2 + 2x \equiv_{x^2+2x} 0$$

and

$$2x(2x+1) = x^2 + 2x \equiv_{x^2+2x} 0.$$

Therefore the four polynomials $\{x, x+2, 2x, 2x+1\}$ are zerodivisors.

(c) $F[x]$ cannot be a field.
This follows from the fact that multiplying two polynomials of degree at least 1 results in a polynomial with higher degree. To prove this more formally we can show that at least one element in $F[x]$ has no inverse. We pick x, which is contained in $F[x]$ because $1 \in F$.
Let $a(x) = a_d x^d + \cdots + a_1 x + a_0 \neq 0$ be an arbitrary polynomial in $F[x]$, then:

$$a(x) \cdot x = a_d x^{d+1} + \cdots + a_1 x^2 + a_0 x.$$

Since there are no zerodivisors in F and $a(x) \neq 0$, this polynomial cannot be 1.

(d) This exercise seems complicated because we have a polynomial where the coefficients are polynomials as well. However once we understand what's going on, the exercise gets a lot easier.
$p(y)$ is polynomial with the coefficients x, 1 and $(x+1)$ (and 0). y itself can be any polynomial from the underlying ring $\mathrm{GF}(2)[x]_{x^2+x+1}$. First we observe $\mathrm{GF}(2)[x]_{x^2+x+1}$:
Since the modulo polynomial has degree 2, this set has only 2^2 elements, namely $\{0, 1, x, x+1\}$.
Now we only have to test which of these elements are roots of $p(y)$. For this we simply evaluate $p(y)$ for each possible candidate:

- $p(0) = x \cdot 0^2 + 0 + (x+1) = x + 1 \neq 0$
- $p(1) = x \cdot 1^2 + 1 + (x+1) = x + 1 + x + 1 = 0$
- $p(x) = x \cdot x^2 + x + (x+1) = x^3 + 1 = x^2 + x + 1 = 0$
- $p(x+1) = x \cdot (x+1)^2 + (x+1) + (x+1) = x(x^2+1) = x^2 = x + 1 \neq 0$

Therefore 1 and x are the roots of $p(y)$.

(e) Like in the previous exercise the coefficients of this polynomial are polynomials as well and $y \in \{0, 1, x, x+1\}$.
We start by looking at the roots of $a(y)$. This is done the same way as in the previous exercise:

- $a(0) = x \cdot 0^3 + x \cdot 0^2 + (x+1) \cdot 0 + x = x$
- $a(1) = x \cdot 1^3 + x \cdot 1^2 + (x+1) \cdot 1 + x = 1$
- $a(x) = x \cdot x^3 + x \cdot x^2 + (x+1) \cdot x + x = x^4 + x^3 + x^2 = 0$

- $a(x+1)$
  $= x \cdot (x+1)^3 + x \cdot (x+1)^2 + (x+1) \cdot (x+1) + x$
  $= (x^4 + x^3 + x^2 + x) + (x^3 + x) + (x^2 + 1) + x$
  $= x + (x^3 + x) + (x^2 + 1) + x$
  $= x + x + 1 = 1$

If you are confused about any of those derivations, remember that whenever a polynomial has degree ≥ 2, we have to perform a modulo operation with $x^2 + x + 1$. For example we use the fact that $x^4 + x^3 + x^2 = x^2 \cdot (x^2 + x + 1)$.

Now since x is a root of $a(y)$, we know that $(y+x)$ divides $a(y)$. ($x = -x$ because we are in GF(2)). We divide $a(y)$ by $(y + x)$ using polynomial division and find another factor, $xy^2 + y + 1$.
The question remains whether $xy^2 + y + 1$ is further reducible. To find out whether it is, we test it for roots:

- $a(0) = x \cdot 0^2 + 0 + 1 = 1$
- $a(1) = x \cdot 1^2 + 1 + 1 = x$
- $a(x) = x \cdot x^2 + x + 1 = x^3 + x + 1 = x$
- $a(x+1) = x \cdot (x+1)^2 + (x+1) + 1 = x^3 + x + x + 1 + 1 = x^3 = 1$

This shows us that $xy^2 + y + 1$ has no roots and is therefore an irreducible polynomial.
We can conclude that $(y + x)$ and $(xy^2 + y + 1)$ are the only factors of $a(y)$.

(f) These exercises are more annoying than they would appear in the exam, but nonetheless, we can practice working with fields:

(i) Check if $y^4 + (x+1)y^2 + y + x \in \mathrm{GF}(2)[x]_{x^2+x+1}[y]$ is reducible.
Here it suffices to substitute every element of $\mathrm{GF}(2)[x]_{x^2+x+1}$ for y and check for roots:

$y = 0$	$0^4 + (x+1)0^2 + 0 + x = x$
$y = 1$	$1^4 + (x+1)1^2 + 1 + x = 1 + (x+1) + 1 + x = 1$
$y = x$	$x^4 + (x+1)x^2 + x + x = x^4 + x^3 + x^2 = 0$
$y = x + 1$	$(x+1)^4 + (x+1)(x+1)^2 + (x+1) + x = (x+1) + 1 + (x+1) + x = x + 1$

So we have found a root $y = x$, and thus, the polynomial is reducible.

(ii) Find all roots of $x^2y^2 + (x+1)y + (x^2+1) \in \mathrm{GF}(2)[x]_{x^3+x+1}[y]$.
Again, the process is similar to above: Substitute every polynomial in $\mathrm{GF}(2)[x]_{x^3+x+1}$ for y and check if we find a root:

$y = 0$	$x^20^2 + (x+1)0 + (x^2+1) = x^2 + 1$
$y = 1$	$x^21^2 + (x+1)1 + (x^2+1) = x$
$y = x$	$x^2x^2 + (x+1)x + (x^2+1) = x^4 + x + 1 = x^2 + 1$
$y = x + 1$	$x^2(x+1)^2 + (x+1)(x+1) + (x^2+1) = x$
$y = x^2$	$x^2x^4 + (x+1)x^2 + (x^2+1) = x^2 + x + 1$
$y = x^2 + 1$	$x^2(x^2+1)^2 + (x+1)(x^2+1) + (x^2+1) = 0$
$y = x^2 + x$	$x^2(x^2+x)^2 + (x+1)(x^2+x) + (x^2+1) = x^2 + x + 1$
$y = x^2 + x + 1$	$x^2(x^2+x+1)^2 + (x+1)(x^2+x+1) + (x^2+1) = 0$

This gives us the two roots $y = x^2 + 1$ and $y = x^2 + x + 1$.

(iii) Factorize $xy^3 + 2y + 2x \in \mathrm{GF}(3)[x]_{x^2+x+2}[y]$ into a product of irreducible monic polynomials and one constant factor.

We first employ the same process again to find a root $y = x + 2$ i.e. a factor of $y - (x + 2) = y + (2x + 1)$.

From here, we carry out long division to get

$$xy^3 + 2y + 2x = (y + (2x + 1))(xy^2 + (x + 1)y + (2x + 2))$$

The quotient is not monic but we can take out the x (multiply by $x^{-1} = x + 1$) to get:

$$xy^3 + 2y + 2x = x(y + (2x + 1))(y^2 + (x + 2)y + (2x + 1))$$

You can verify that $(2x + 1)^2 + (x + 2)(2x + 1) + (2x + 1)$ indeed has no roots, and thus is irreducible.

We reiterate: this is much more work than an exam question would be. Even when creating the solution, I relied heavily on an online tool [1] to carry out the calculations in $\mathrm{GF}(3)[x]_{x^2+x+2}$.

[1] `https://wims.univ-cotedazur.fr/wims/en_tool~algebra~calcff.en.html`

4 Logic

4.1 Proof Systems

Definition 4.1. *Let Σ be an alphabet (i.e., a set of allowed symbols). A **proof system** is a quadruple $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$, where:*

- $\mathcal{S} \subseteq \Sigma^*$ *is the set of (syntactic representations of) mathematical statements.*
- $\mathcal{P} \subseteq \Sigma^*$ *is the set of (syntactic representations of) proof strings.*
- $\tau \colon \mathcal{S} \to \{0,1\}$ *is a **truth function**.*
- $\phi \colon \mathcal{S} \times \mathcal{P} \to \{0,1\}$ *is a **verification function**.*

A given statement $s \in \mathcal{S}$ is true if $\tau(s) = 1$. For a given statement $s \in \mathcal{S}$ and a proof $p \in \mathcal{P}$, we say that p is a *valid* proof for s if $\phi(s,p) = 1$.
So far, these were only definitions. In general, we are free to define the truth- and verification functions as we like, which can lead to not very useful proof systems:

Example. Let $\Sigma = \{0,1\}$ and $\mathcal{S} = \{0,1\}^*$. We interpret every $s \in \mathcal{S}$ as a binary encoding of a natural number $n(s) \in \mathbb{N}$. Next we define:

- $\tau(s) = 1 :\Leftrightarrow n(s)$ is an even prime.
- $\phi(s,p) = 1 :\Leftrightarrow n(s) = 2 \cdot n(p)$.

In this example, $p = 10$ is a valid proof proof for the statement $s = 100$ because $n(s) = 4 = 2 \cdot 2 = 2 \cdot n(p)$. But does that mean that 4 is an even prime? Obviously, the answer is no. We all know that the only even prime is 2. The problem is, that we have just proved a false statement![2]

Intuitively it should be clear, that proof systems which provide proofs to wrong statements, are not what we desire. If we can prove a statement, we want this statement to be true. This property of a proof system is called *soundness*. Another condition that is desirable is *completeness*. Completeness means, that every true statement can be proven by the proof system:

Definition 4.2. *Let $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ be a proof system.*

$$\begin{array}{lrcl} \textit{(i)} & \Pi \textit{ is } \textbf{\textit{sound}} & \Leftrightarrow & \forall s \in \mathcal{S}\ [\overbrace{(\exists p \in \mathcal{P}\ \phi(s,p) = 1)}^{(1)} \to \overbrace{\tau(s) = 1}^{(2)}] \\ \textit{(ii)} & \Pi \textit{ is } \textbf{\textit{complete}} & \Leftrightarrow & \forall s \in \mathcal{S}\ [\underbrace{\tau(s) = 1}_{(2)} \to \underbrace{(\exists p \in \mathcal{P}\ \phi(s,p) = 1)}_{(1)}] \end{array}$$

Note, that the only difference is the order of (1) and (2) in the implication.

Example. Consider statements of the form:

"F is satisfiable."

where F is a formula in propositional logic that uses only the variables A, B and C.
Let $\mathcal{S} = \mathcal{P} = \{0,1\}^*$. We now propose functions τ and ϕ such that $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is a sound and complete proof system for statements described above. To do so, we first note that every such formula consists of 8 symbols:

$$\Sigma_{\text{3PL}} = \{A, B, C, \wedge, \vee, \neg, (,)\}$$

We can therefore encode every symbol in Σ_{3PL} by a bitstring in $\{0,1\}^3$ and therefore, every propositional formula containing only the variables A, B and C can be encoded by replacing every symbol with the corresponding bitstring of length 3. The truth function is defined as follows: $\tau(s) = 1$ if and only if

[2] Note that $\tau(100) = 0$ because 4 is not an even prime.

$|s| = 3k$ (for some $k \in \mathbb{N}$)[3] and s encodes a syntactically correct propositional formula that is satisfiable. Next, we define the verification function: $\phi(s, p) = 1$ if and only if all of the following holds:

- s encodes a syntactically correct propositional formula that only uses the variables A, B and C (as described in the definition of τ).
- $|p| = 3$.
- The three bits of p describe a truth assignments $\mathcal{A}$ for the variables A, B and C respectively. The formula encoded by s is true under $\mathcal{A}$.

We now head on to prove soundness and completeness of our proof system:

Claim

$$\Pi \text{ is sound.}$$

Proof. Let $s \in \mathcal{S}$ and $p \in \mathcal{P}$ be arbitrary, such that $\phi(s, p) = 1$. Therefore, by the definition of ϕ, we know that s encodes a syntactically correct formula F, and that p encodes a truth assignment $\mathcal{A}$ which is a model for F. Thus, F must be satisfiable. □

Claim

$$\Pi \text{ is complete.}$$

Proof. We have to show that for an arbitrary $s \in \mathcal{S}$ with $\tau(s) = 1$ there exists a $p \in \mathcal{P}$ with $\phi(s, p) = 1$. Thus, let $s \in \mathcal{S}$ be arbitrary, such that $\tau(s) = 1$. By Definition of τ, s encodes a satisfiable formula F of propositional logic that uses only A, B and C as variables. Hence, there exists a truth assignment $\mathcal{A}$ such that $\mathcal{A} \vDash F$. We set p as the bitstring of length 3 that encodes $\mathcal{A}$. Then obviously $\phi(s, p) = 1$. □

Another important condition that we want our proof systems to fulfil, is that the verification function ϕ should be "efficiently computable". Where it is not always clear what is meant by "efficient", one generally agrees that an algorithm that has an exponential runtime is considered inefficient.
One can come up with an algorithm that parses a formula of propositional logic into a syntax tree, by linearly scanning the bitstring and dividing the string into substrings if an $\wedge$ or an $\vee$ is encountered. Then one recursively applies the method on the substrings. Such an algorithm would have a the same time complexity as *quicksort*, which is $\mathcal{O}(n^2)$ in the worst case, which is efficient enough for us. Such an algorithm - if cleverly designed - will also detect syntax errors while parsing, and therefore satisfy the first bullet point in the definition of τ. Having the formula in a syntax tree, it is easy to verify if the formula is satisfied under the truth function encoded in p, by simply traversing the tree recursively according to Definition 6.16.

4.2 Logical calculi

A logical calculus gives us a way of deriving new formulas from an existing set of formulas. This is done by applying *rules*.

Definition 4.3. *Let $M = \{F_1, \ldots, F_k\}$ be a set of formulas. A **derivation rule** is a rule for deriving a formula G from a set of formulas M. We write:*

$$M \vdash_R G$$

if G can be derived from the set M by rule R. M is called the precondition.

A logical calculus is then easily defined in terms of derivation rules:

[3] $|s|$ denotes the number of bits in the string s.

Definition 4.4. *A (logical)* ***calculus*** *K is a finite set of derivation rules: $K = \{R_1, \dots R_m\}$.*

If we have derived a new formula F_{k+1} from an initial set of formulas $M = \{F_1, \dots F_k\}$ by applying a certain rule $R_i \in K$, we can include this newly derived formula in M:

$$M_1 = M \cup \{F_{k+1}\} = \{F_1, \dots, F_k, F_{k+1}\}.$$

The next time we want to derive a new formula, we can start from M_1 instead of M and thus we may be able to derive formulas that were not possible to derive by only using M. We can repeat this procedure an arbitrary but finite amount of times. If we eventually decide to stop, and we derived a formula G in the last step, then we say that we made a *derivation* of G from M in the calculus K. Formally:

Definition 4.5. *A* ***derivation*** *of a formula G from a set M of formulas in a calculus K is a finite sequence (of some length n) of applications of rules in K, leading to G. More precisely, we have $M_0 := M$, $M_i := M_{i-1} \cup \{G_i\}$ for $1 \leq i \leq n$, where $N \vdash_{R_j} G_i$ for some $N \subseteq M_{i-1}$ and for some $R_j \in K$, and where $G_n = G$. We write*

$$M \vdash_K G$$

if there is a derivation of G from M in the calculus K.

Example. Consider the calculus $K = \{R_1, R_2, R_3\}$ where:

$$\{F \wedge G\} \vdash_{R_1} F, \qquad \{F \wedge G\} \vdash_{R_2} G, \qquad \{F, G\} \vdash_{R_3} F \wedge G$$

We want to derive the formula $G = B \wedge A$, from the set $M = \{A \wedge B\}$:

$$\begin{aligned} &\{A \wedge B\} \vdash_{R_1} A, && \Rightarrow M_1 = \{A \wedge B, A\} \\ &\{A \wedge B\} \vdash_{R_2} B, && \Rightarrow M_2 = \{A \wedge B, A, B\} \\ &\{B, A\} \vdash_{R_3} B \wedge A, && \Rightarrow M_3 = \{A \wedge B, A, B, B \wedge A\} \end{aligned}$$

We have just showed that there is a derivation (of length 3) that started from the set $M = \{A \wedge B\}$ and lead to $G = B \wedge A$ and hence: $\{A \wedge B\} \vdash_K B \wedge A$.

Again, the above definitions introduced only a purely syntactic concept. We have never mentioned anything about whether the derivation rules actually make sense. Intuitively, we want to guarantee, that if we can derive a formula G from a set of formulas M, then we want G to be a logical consequence of M. This property is called *soundness* or *correctness* of a calculus. Another - in some sense less important - property of a calculus is *completeness*. In a complete calculus we always can derive a formula G from a set of formulas M if G is a logical consequence of M.

Definition 4.6. *Let K be a calculus, F be a formula and M be a set of formulas. We say:*

$$K \text{ is } \textbf{sound} \text{ if } \quad M \vdash_K F \;\Rightarrow\; M \vDash F$$
$$K \text{ is } \textbf{complete} \text{ if } \quad M \vDash F \;\Rightarrow\; M \vdash_K F$$

An easy way to show that a given calculus K is sound, is to show that every rule $R \in K$ is *correct*:

Definition 4.7. *A derivation rule is* ***correct*** *if for every set M of formulas and every formula F:*

$$M \vdash_R F \quad \Rightarrow \quad M \vDash F.$$

Hands-On 1

1.1. Soundness And Completeness Of Proof Systems
Let $\Sigma = \{0,1\}$, $\mathcal{S} = \mathcal{P} = \{0,1\}^3$. For the following definitions of τ and ϕ, decide whether the proof systems fulfil the soundness and completeness property. Justify your answers.

(a)
- $\tau(s) = 1$ if s contains at most one 0.
- $\phi(s,p) = 1$ if s contains at most two 0 and $s = p$.

(b)
- $\tau(s) = 1$ if s contains at least one 1.
- $\phi(s,p) = 1$ if the Hamming distance between s and p is exactly 3 and p contains exactly one 0.

1.2. Finding The Verification Function
Let $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ with $\mathcal{S} = \mathcal{P} = \mathbb{N}$. Let $\tau\colon \mathcal{S} \mapsto \{0,1\}$ with $\tau(n) = 1$ only if n has at least 4 (not necessarily different) prime factors. Define a function $\phi\colon \mathcal{S} \times \mathcal{P} \mapsto \{0,1\}$ such that Π is sound and complete. Justify your answers.
Hint: You may assume that it can be tested efficiently, whether a given natural number is prime.
Hint: If you are stuck, try solving the exercise with $\mathcal{P} = \mathbb{N}^4$.

1.3. Finding The Truth Function
Let $\mathcal{S} = \mathcal{P} = \{0,1\}^5$ and $\phi\colon \mathcal{S} \times \mathcal{P} \mapsto \{0,1\}$ such that $\phi(s,p) = 1$ only if p and s differ at exactly 4 positions and p contains at most one 0. Find a function $\tau\colon \mathcal{S} \mapsto \{0,1\}$, such that $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is a proof system that is sound and complete. Proof both soundness and completeness.

1.4. Correct Rules (Challenge)
Let K be a calculus. In this exercise we are going to show that K is sound if and only if every rule in K is correct.

1. Show that if K is sound then every rule $R \in K$ is correct.
2. Show that if every rule in K is correct then K is sound.
   Hint: For this task you may use a slight abuse of notation, namely statements of the form:

   $$M \vDash N$$

   where M and N are sets of formulas (normally only one formula is allowed on the right-hand side). We say $M \vDash N$ if for every structure $\mathcal{A}$ that is suitable for both M and N it holds that:

   $$\mathcal{A} \vDash M \quad \Rightarrow \quad \mathcal{A} \vDash N.$$

   Especially, you can use the two lemmas without a proof (but you are encouraged to try it as an exercise):

   Lemma 1 Let L, M and N be sets of formulas. Then:

   $$M \vDash N \quad \Rightarrow \quad L \cup M \vDash N.$$

   Lemma 2 Let M and N be sets of formulas. Then:

   $$M \vDash N \quad \Rightarrow \quad M \vDash M \cup N.$$

1.5. Soundness And Completeness Of Logical Calculi

(a) Give a logical calculus that is sound but not complete.

(b) Give a logical calculus that is complete but not sound.

4.3 Propositional Logic

4.3.1 Concepts: Syntax, Semantics, Interpretation, Model

Definition 4.8. *A **logic** is defined by the **syntax** and the **semantics**. The basic concept in any logic is that of a formula.*

Definition 4.9. *The **syntax** of a logic defines an alphabet Λ (of allowed symbols) and specifies which strings in Λ^* are formulas (i.e, are syntactically correct).*

Definition 4.10. *The syntax in propositional logic is defined as follows:*
*An **atomic formula** is of the form A_i with $i \in \mathbb{N}$. A **formula** is defined inductively:*

- *An atomic formula is a formula*
- *If F and G are formulas, then also $\neg F$, $(F \wedge G)$, and $(F \vee G)$ are formulas.*

The alphabet of propositional logic could be made explicit.[4]
Note that the symbols in $F \to G$ and $F \leftrightarrow G$ are not part of the syntax, but are abbreviations for $\neg F \vee G$ and $(F \wedge G) \vee (\neg F \wedge \neg G)$ respectively.

Example. Which of these are syntactically correct formulas?

a) $A_3 A_2 \vee$

b) $((A_{13} \vee A_6) \wedge (A_3 \wedge \neg A_7))$

c) $A \wedge B \wedge C$

d) $A_2 \vee A_4 \wedge A_3$

Solution

a) incorrect

b) correct

c) technically incorrect, but under standard convention it is correct. One may use A, B or C (and other letters) for atomic formulas and omit parentheses between atomic formulas with the same operator.

d) incorrect, missing necessary parentheses

Definition 4.11. *The **semantics** of a logic defines two properties:*

- *The semantics of a logic decides for each symbol in a formula F if it occurs **free** in F.*
- *The semantics of a logic also defines a function assigning to each formula F and each suitable interpretation for F a truth value in $\{0, 1\}$.*

Note that a **free symbol** is not the same as a **free variable** (which will we see later in predicate logic). The exact formal definition of syntax and semantics of a logic are not the most important concepts to know, but the syntax and semantics of the specific logic, namely propositional and predicate logic, are of high importance.

[4] The alphabet of propositional logic is $\Lambda = \{A_i, \wedge, \vee, \neg, (,) | i \in \mathbb{N}\}$

Definition 4.12. *An **interpretation** consists of a function that assigns to a certain set of symbols of Λ concrete values, where each symbol has a certain domain (of possible values).*

Typically, the domains are specified in terms of an **universe** U. For example, in predicate logic the domain for variables is U, for k-ary functions it is $U^k \to U$ and for k-ary predicates it is $U^k \to \{0,1\}$

Definition 4.13. *An interpretation is **suitable** for a formula F if it assigns a value to all symbols $\beta \in \Lambda$ occurring free in F.*

The second property of the semantics of a logic induces a function σ assigning to each Formula F, and each interpretation $\mathcal{A}$ suitable for F, a truth value $\sigma(F, \mathcal{A})$ in $\{0,1\}$. In treatments of logic one often writes $\mathcal{A}(F)$ instead of $\sigma(F, \mathcal{A})$ and calls $\mathcal{A}(F)$ **the truth value of F under interpretation $\mathcal{A}$**.

Definition 4.14. *The semantics in propositional logic is defined as follows:*
*In propositional logic, the free symbols of a formula are all symbols A_i, i.e, all the atomic formulas. For a set M of atomic formulas, an interpretation, called **truth assignment**, is a function $\alpha : M \to \{0,1\}$. A truth assignment α is suitable for a formula F if M contains all atomic formulas appearing in F. For all atomic formulas $A_i : \mathcal{A}(A_i) = \alpha(A_i)$ and*

$$\begin{array}{ll} \mathcal{A}((F \wedge G)) = 1 & \text{if and only if } \mathcal{A}(F) = 1 \text{ and } \mathcal{A}(G) = 1. \\ \mathcal{A}((F \vee G)) = 1 & \text{if and only if } \mathcal{A}(F) = 1 \text{ or } \mathcal{A}(G) = 1. \\ \mathcal{A}(\neg F) = 1 & \text{if and only if } \mathcal{A}(F) = 0. \end{array}$$

Definition 4.15. *A suitable interpretation $\mathcal{A}$ for which a formula F is true, (i.e., $\mathcal{A}(F) = 1$) is called a **model** for F, and one also writes*

$$\mathcal{A} \vDash F.$$

More generally, for a set M of formulas, a suitable interpretation for which all formulas in M are true is called a model for M, denoted as

$$\mathcal{A} \vDash M.$$

If $\mathcal{A}$ is not a model for M one writes $\mathcal{A} \nvDash M$.

4.3.2 Concepts: Satisfiability, Tautology, Consequence, Equivalence

Definition 4.16. *A formula F (or set M of formulas) is called **satisfiable** if there exists a model for F (or M), and **unsatisfiable** otherwise. The symbol $\bot$ is used for an **unsatisfiable** formula.*

Claim

Let M be a set of formulas, then the following two statements are not equivalent:

- M is satisfiable.
- Every formula in M is satisfiable.

In fact, the first statement implies the second.

Proof. We determine a set M of formulas, for which every formula in M is satisfiable, but M itself is not satisfiable.

$$M = \{A, \neg A\}$$

A and $\neg A$ are both satisfiable, but M is not satisfiable. □

Definition 4.17. *A formula F is called a **tautology** or **valid** if it is true for every suitable interpretation. The symbol $\top$ is used for a tautology.*

Note that the symbols $\bot$ and $\top$ are not formulas itself, i.e., are not part of the syntax of the logic, but they are used in expressions like $F \equiv \bot$, which is to be understood as standing for an arbitrary unsatisfiable formula. $F \equiv \bot$ just means, that F is unsatisfiable.

Lemma 4.1

A formula F is a tautology if and only if $\neg F$ is unsatisfiable.

Definition 4.18. *A formula G is a **logical consequence** of a formula F (or a set M of formulas), denoted*

$$F \vDash G \text{ (or } M \vDash G \text{),}$$

if every interpretation suitable for both F (or M) and G, which is a model for F (for M), is also a model for G.

Example. We show for any formulas F and G: $F \wedge G \vDash F$.
Let $\mathcal{A}$ be any model for $F \wedge G$, i.e, $\mathcal{A}(F \wedge G) = 1$.
Then we have, by the semantics of propositional logic, that $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$.
That means, that any model for $F \wedge G$ is also a model for F, thus $F \wedge G \vDash F$.

Definition 4.19. *Two formulas F and G are equivalent, denoted $F \equiv G$, if every interpretation suitable for both F and G yields the same truth value for F and G, i.e., if each one is a logical consequence of the other:*

$$F \equiv G :\Longleftrightarrow F \vDash G \text{ and } G \vDash F.$$

Definition 4.20. *If F is a tautology, one also writes $\vDash F$*

4.3.3 Normal Forms

Definition 4.21. *A **literal** is an atomic formula or the negation of an atomic formula.*

Definition 4.22. *A formula F is in **conjunctive normal form (CNF)** if it is a conjunction of disjunctions of literals, i.e., if it is of the form*

$$F = (L_{11} \vee ... \vee L_{1m_1}) \wedge ... \wedge (L_{n1} \vee ... \vee L_{nm_n})$$

for some literals L_{ij}.

Definition 4.23. *A formula F is in **disjunctive normal form (DNF)** if it is a disjunction of conjunctions of literals, i.e., if it is of the form*

$$F = (L_{11} \wedge ... \wedge L_{1m_1}) \vee ... \vee (L_{n1} \wedge ... \wedge L_{nm_n})$$

for some literals L_{ij}.

Theorem 6

Every formula is equivalent to a formula in CNF and also to a formula in DNF.

Example. Consider the formula $F = B \wedge (\neg B \rightarrow A)$. We can construct an equivalent formula to F in DNF and CNF with its function table.

A	B	$B \wedge (\neg B \rightarrow A)$
0	0	0
0	1	1
1	0	0
1	1	1

Each row in the function table represents one assignment or one clause.

For DNF we "or" all the rows, which evaluate to 1.
For each row we "and" all the literals as follows: If an atomic formula $A_i = 0$ in that row, then we take the literal $\neg A_i$, otherwise we take the literal A_i.
DNF:

$$\underbrace{(\neg A \wedge B)}_{\text{row 2}} \vee \underbrace{(A \wedge B)}_{\text{row 4}}$$

For CNF we "and" all the rows, which evaluate to 0.
For each row we "or" all the literals as follows: If an atomic formula $A_i = 0$ in that row, then we take the literal A_i, otherwise we take the literal $\neg A_i$.
CNF:

$$\underbrace{(A \vee B)}_{\text{row 1}} \wedge \underbrace{(\neg A \vee B)}_{\text{row 3}}$$

Note that in this example it is only by chance, that the CNF is equal to the DNF when exchanging all $\wedge$ with an $\vee$ and vice versa. It is also not always true that CNF and DNF have the same amount of clauses.

4.4 Resolution Calculus

The resolution calculus serves as a concrete example of a logical calculus. The calculus consists of only one derivation rule and a derivation serves the purpose of showing that a given formula F is unsatisfiable. An important detail about the resolution calculus is, that the precondition[5] consists of clauses:

[5] The set of formulas on the left side of the derivation rule.

Definition 4.24. *A **clause** is a set of literals.*

We can easily associate any propositional formula with a set of claues, if we transform the formula into CNF:

Definition 4.25. *The set of clauses associated to a formula*

$$F = (L_{11} \vee \cdots \vee L_{1m_1}) \wedge \cdots \wedge (L_{n1} \vee \cdots \vee L_{nm_n})$$

in CNF, denoted as the set $\mathcal{K}(F)$ is the set:

$$\mathcal{K}(F) = \{\{L_{11}, \ldots, L_{1m_1}\}, \ldots, \{L_{n1}, \ldots, L_{nm_n}\}\}$$

The set of clauses associated with a set $M = \{F_1, \ldots F_k\}$ of formulas is the union of their clause sets:

$$\mathcal{K}(M) = \bigcup_{i=1}^{k} \mathcal{K}(F_i)$$

Now we can define how the derivation rule works:

Definition 4.26. *A clause K is a **resolvent** of clauses K_1 and K_2 if there is a literal L such that $L \in K_1, \neg L \in K_2$, and*

$$K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\}).$$

If two clauses K_1, K_2 have a resolvent K, then K is derived by the rule res:

$$\{K_1, K_2\} \vdash_{res} K.$$

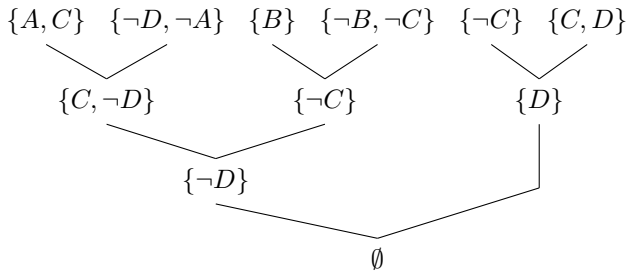
As mentioned earlier, the resolution calculus is defined as:

$$\text{Res} = \{res\}.$$

Example. Let

$$F := (A \vee C) \wedge (\neg D \vee \neg A) \wedge B \wedge (\neg B \vee \neg C) \wedge \neg C \wedge (C \vee D)$$

We want to show that F is unsatisfiable. Because F is already in CNF we can derive $\emptyset$ from $\mathcal{K}(F)$ as follows:



Hands-On 2

2.1. Propositional Logic

(a) We would like to extend propositional logic by the symbol $\downarrow$, denoting the NOR operation ($(A \downarrow B)$ is true if and only if both A and B are false). How would one extend the definitions of syntax and semantics of propositional logic, in order to incorporate NOR?

(b) For each entry, determine if the interpretation is suitable for the formula and if so, also determine if it is a model.

	$A \wedge (B \vee \neg A) \wedge \neg C$	$A \vee \neg A \vee B$	$A \vee \neg D$
$\mathcal{A} = \{A = 0, B = 0, C = 1, D = 1\}$			
$\mathcal{A} = \{A = 0, D = 0\}$			
$\mathcal{A} = \{A = 1, B = 1, C = 0\}$			

(c) For each of the following sets of formulas, either find a model or show that it is unsatisfiable:

(1) $M = \{A \vee B, C \vee D, B \wedge C, \neg D \wedge B\}$

(2) $N = \{A \to B, C \wedge D, C \to A, B \to \neg D\}$

(d) Show that $F \vDash G$ if and only if $\vDash F \to G$.

(e) Consider this statement:

$$B \vee C \vDash (B \wedge C) \vee (A \wedge \neg A)$$

Does the following text correctly prove that the statement is false? If not, prove or disprove the statement correctly.

> *"This statement is false. One can find an interpretation $\mathcal{A} = \{B = 1, C = 0\}$, which is a model for the left side, but not a model for the right side, since $\mathcal{A}(B \wedge C) = 0$ and $A \wedge \neg A$ is unsatisfiable. Therefore is $\mathcal{A}$ a counterexample and the statement is false."*

(f) Determine which of those formulas are in DNF, CNF or not in a normal form:

(1) $(B \vee \neg A) \wedge (C \vee D) \wedge (A \vee C)$

(2) $(A \vee B) \wedge C$

(3) $A \vee (B \wedge C)$

(4) $A \vee B \vee C$

(5) $(A \wedge B) \vee (\neg A \wedge C) \wedge (\neg D \wedge B)$

(g) Let $F \equiv (A \to (B \wedge C)) \wedge B$. Using the method of function tables, construct a formula equivalent to F in conjunctive normal form and a formula equivalent to F in disjunctive normal form.

2.2. The Resolution Calculus

(a) Prove or disprove the following statement about the resolution calculus:

> *"The resolution calculus is not complete."*

(b) Show that for a set of formulas M and a formula F it holds that:

$$M \vDash F \quad \text{if and only if} \quad M \cup \{\neg F\} \text{ is unsatisfiable.}$$

(c) Show that $A \vDash A \vee B$ using the resolution calculus.

4.5 Predicate logic

4.5.1 Syntax, Free Variables

Definition 4.27. *The syntax in predicate logic is defined as follows:*

- *A **variable symbol** is of the form x_i with $i \in \mathbb{N}$*
- *A **function symbol** is of the form $f_i^{(k)}$ with $i, k \in \mathbb{N}$, where k denotes the number of arguments of the function. Function symbols for $k = 0$ are called **constants**.*
- *A **predicate symbol** is of the form $P_i^{(k)}$ with $i, k \in \mathbb{N}$, where k denotes the number of arguments of the predicate. Predicate symbols for $k = 0$ are either **Verum or Falsum** i.e. always true or always false.*
- *A **term** is defined inductively: A variable is a term, and if $t_1, ..., t_k$ are terms, then $f_i^{(k)}(t_1, ..., t_k)$ is a term. For $k = 0$ one writes no parentheses.*
- *A **formula** is defined inductively:*
  - *For any i and k, if $t_1, ..., t_k$ are terms, then $P_i^{(k)}(t_1, ..., t_k)$ is a formula, called an atomic formula.*
  - *If F and G are formulas, then $\neg F$, $(F \wedge G)$, and $(F \vee G)$ are formulas.*
  - *If F is a formula, then, for any i, $\forall x_i\ F$ and $\exists x_i\ F$ are formulas.*

Definition 4.28. *Every occurrence of a variable in a formula is either **bound** or **free**. If a variable x occurs in a (sub-)formula of the form $\forall x\ G$ or $\exists x\ G$, then it is bound, otherwise it is free. The occurrence of a variable x immediately following a quantifier is also bound. Any variable x - if it is bound - can only be bound to exactly one quantifier. A formula is **closed** if it contains no free variables.*

Example. Consider the formula

$$\underset{1}{\forall}x\underset{2}{\exists}x\ P(\underset{3}{x}) \wedge \underset{4}{\forall}x(\underset{5}{\exists}x\ Q(\underset{6}{x}) \wedge R(\underset{7}{x})) \wedge S(\underset{8}{x}).$$

In this formula there are in total 4 quantifiers and 8 occurrences of the variable x.

- Occurrence 1: x directly follows the first $\forall$ quantifier and is hence bound to it.
- Occurrence 2: x directly follows the first $\exists$ quantifier and is hence bound to it.
- Occurrence 3: x is bound to the first $\exists$ quantifier (and it is not bound to the first $\forall$ quantifier).
- Occurrence 4: x directly follows the second $\forall$ quantifier and is hence bound to it.
- Occurrence 5: x directly follows the second $\exists$ quantifier and is hence bound to it.
- Occurrence 6: x is bound to the second $\exists$ quantifier.
- Occurrence 7: x is bound to the second $\forall$ quantifier.
- Occurrence 8: x is free.

4.5.2 Semantics

In predicate logic, the free symbols of a formula are all free variables, all function symbols, and all predicate symbols. An interpretation in the context of predicate logic is called a **structure** and must define a universe and the meaning of all these free symbols.

Definition 4.29. *An **interpretation** or **structure** is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ where*

- *U is a non-empty set, the so-called universe,*
- *ϕ is a function assigning to each function symbol (in a certain subset of all function symbols) a function, where for a k-ary function symbol f, $\phi(f)$ is a function $U^k \to U$.*
- *ψ is a function assigning to each predicate symbol (in a certain subset of all predicate symbols) a function, where for a k-ary predicate symbol P, $\psi(P)$ is a function $U^k \to \{0, 1\}$, and where*
- *ξ is a function assigning to each variable symbol (in a certain subset of all variable symbols) a value in U.*

For notational convenience, for a structure $\mathcal{A} = (U, \phi, \psi, \xi)$ and a function symbol f one usually writes $f^{\mathcal{A}}$ instead of $\phi(f)$. Similarly, one writes $P^{\mathcal{A}}$ instead of $\psi(P)$ and $x^{\mathcal{A}}$ instead of $\xi(x)$. One also writes $U^{\mathcal{A}}$ rather than U to make $\mathcal{A}$ explicit.

Definition 4.30. *A structure $\mathcal{A}$ is **suitable** for a formula F if it defines all function symbols, predicate symbols, and free variables of F.*

Example. Consider the formula $F = \forall x \exists y\ (P(y) \wedge Q(f(x), y)) \wedge P(z)$.
A suitable structure for F must define the universe, predicates P, Q, function f and free variable z.
An example of a suitable structure for F is $\mathcal{A}$, where
$U^{\mathcal{A}} = \mathbb{N} \setminus \{0\}$
$P^{\mathcal{A}}(x) = 1$ if and only if x is odd
$Q^{\mathcal{A}}(x, y) = 1$ if and only if $x < y$
$f^{\mathcal{A}}(x) = x$
$z^{\mathcal{A}} = 5$
This structure defines all free symbols and is hence suitable. $\mathcal{A}$ is also a model.
It is important that the predicates and functions are defined correctly.
One might think that if the structure is defined slightly different, in particular, if f is defined as $f^{\mathcal{A}}(x) = y - x$, it is also a model. But this structure is incorrect, because a function or predicate can only depend on its arguments and no other variables.
Another incorrect structure would be, if f was defined as $f^{\mathcal{A}}(x) = x - x$, which is equal to $f^{\mathcal{A}}(x) = 0$. In this case, f is not a function $U^2 \to U$, because 0 is not in U.

Definition 4.31. *For a structure $\mathcal{A} = (U, \phi, \psi, \xi)$, we define the value (in U) of terms and the truth value of formulas under that structure.*

- *The value $\mathcal{A}(t)$ of a term t is defined recursively as follows:*
  - *If t is a variable, then $\mathcal{A}(t) = \xi(t)$.*
  - *If t is of the form $f(t_1, ..., t_k)$ for terms $t_1, ..., t_k$ and a k-ary function symbol f, then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), ..., \mathcal{A}(t_k))$.*
- *The truth value of a formula F is defined recursively as follows:*
  - $\mathcal{A}((F \wedge G)) = 1$ *if and only if* $\mathcal{A}(F) = 1$ *and* $\mathcal{A}(G) = 1$;
  - $\mathcal{A}((F \vee G)) = 1$ *if and only if* $\mathcal{A}(F) = 1$ *or* $\mathcal{A}(G) = 1$;
  - $\mathcal{A}(\neg F) = 1$ *if and only if* $\mathcal{A}(F) = 0$

- *If F is of the form $F = P(t_1, ..., t_k)$ for terms $t_1, ..., t_k$ and a k-ary predicate symbol P, then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), ..., \mathcal{A}(t_k))$.*
- *If F is of the form $\forall x\ G$ or $\exists x\ G$, then let $\mathcal{A}_{[x \to u]}$ for $u \in U$ be the same structure as $\mathcal{A}$ except that $\xi(x)$ is overwritten by u (i.e., $\xi(x) = u$):*

$$\begin{aligned} \mathcal{A}(\forall x\ G) &= \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(G) = 1 \text{ for all } u \in U \\ 0 & \text{else.} \end{cases} \\ \mathcal{A}(\exists x\ G) &= \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(G) = 1 \text{ for some } u \in U \\ 0 & \text{else.} \end{cases} \end{aligned}$$

4.5.3 Summary of the General Concepts in Logic

Concept	Interpretation
Propositional Logic	Also called **truth assignment** [The function α] assigns to each atomic formula A_i (in a certain subset of all atomic formulas) a value in $\{0, 1\}$.
Predicate Logic	Also called **structure** 4-tuple (U, ϕ, ψ, ξ) Defines a non-empty universe U. [The function ϕ] assigns to each k-ary function symbol f (in a certain subset of all function symbols) a function, where $\phi(f)$ is a function $U^k \to U$. [The function ψ] assigns to each k-ary predicate symbol P (in a certain subset of all predicate symbols) a function, where $\psi(P)$ is a function $U^k \to \{0, 1\}$. [The function ξ] assigns to each variable symbol (in a certain subset of all variable symbols) a value in U.

Concept	Suitable Interpretation
Propositional Logic	A truth assignment is suitable for a formula F if it defines all free symbols: all atomic formulas in F
Predicate Logic	A structure is suitable for a formula F if it defines all free symbols: all function symbols in F all predicate symbols in F all free variables in F

Concepts	Model, Satisfiability, Tautology, Logical Consequence, Equivalence
Propositional Logic and Predicate Logic	**Model**: An interpretation $\mathcal{A}$ suitable for formula F is a model, if the formula is true under this interpretation, i.e, if $\mathcal{A}(F) = 1$. **Satisfiability**: A formula F is satisfiable if there exists a model for F. Otherwise, F is unsatisfiable ($F \equiv \bot$). **Tautology**: A formula F is a tautology ($F \equiv \top$), if the formula is true under every suitable interpretation, i.e., if $\mathcal{A}(F) = 1$ for every suitable interpretation $\mathcal{A}$. **Logical Consequence**: A formula G is a logical consequence of formula F ($F \vDash G$), if every interpretation suitable for both F and G, which is a model for F, is also a model for G. **Equivalence**: Two formulas F and G are equivalent if and only if $F \vDash G$ and $G \vDash F$.

Concept	Function Table
Propositional Logic	The function table of a formula F lists all "non-redundant"[6] suitable interpretations. and the truth value of F under those interpretations. If F has n different atomic formulas, then the function table will have 2^n rows. Each row represents exactly one "non-redundant" suitable interpretation. One can easily check if a formula F is a tautology given its function table.
Predicate Logic	For a formula in predicate logic one cannot construct a function table, because every formula in predicate logic has infinitely many "non-redundant" suitable interpretations. For example, the structure $\mathcal{A}$ is a model for the formula $G \equiv \forall x\ P(x)$, where $U^{\mathcal{A}} = \mathbb{N}$ and $P^{\mathcal{A}}(x) = 1$ if and only if $x \geq 0$. But note that this does not mean, that G is a tautology, because, just like in propositional logic, a single structure only represents a single row in the function table.

4.5.4 Some basic Equivalences

Lemma 4.2

For any formulas F, G and H we have

1) $F \wedge F \equiv F$ and $F \vee F \equiv F$ (idempotence);
2) $F \wedge G \equiv G \wedge F$ and $F \vee G \equiv G \vee F$ (commutativity);
3) $(F \wedge G) \wedge H \equiv G \wedge (F \wedge H)$ and $(F \vee G) \vee H \equiv G \vee (F \vee H)$ (associativity);
4) $F \wedge (F \vee G) \equiv F$ and $F \vee (F \wedge G) \equiv F$ (absorption);
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ (distributive law);

[6] a "non-redundant" suitable interpretation only assigns to free symbols (and no other symbols).

6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ (distributive law);

7) $\neg\neg F \equiv F$ (double negation);

8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$ and $\neg(F \vee G) \equiv \neg F \wedge \neg G$ (de Morgan's rules);

9) $F \vee \top \equiv \top$ and $F \wedge \top \equiv F$ (tautology rules);

10) $F \vee \bot \equiv F$ and $F \wedge \bot \equiv \bot$ (unsatisfiability rules);

11) $F \vee \neg F \equiv \top$ and $F \wedge \neg F \equiv \bot$.

Lemma 4.3

For any formulas F, G, and H, where x does not occur free in H, we have

1) $\neg(\forall x\ F) \equiv \exists x\ \neg F$;

2) $\neg(\exists x\ F) \equiv \forall x\ \neg F$;

3) $(\forall x\ F) \wedge (\forall x\ G) \equiv \forall x\ (F \wedge G)$;

4) $(\exists x\ F) \vee (\exists x\ G) \equiv \exists x\ (F \vee G)$;

5) $\forall x \forall y\ F \equiv \forall y \forall x\ F$;

6) $\exists x \exists y\ F \equiv \exists y \exists x\ F$;

7) $(\forall x\ F) \wedge H \equiv \forall x\ (F \wedge H)$;

8) $(\forall x\ F) \vee H \equiv \forall x\ (F \vee H)$;

9) $(\exists x\ F) \wedge H \equiv \exists x\ (F \wedge H)$;

10) $(\exists x\ F) \vee H \equiv \exists x\ (F \vee H)$.

Lemma 4.4

If one replaces a subformula G of a formula F by an equivalent (to G) formula H, then the resulting formula is equivalent to F.

4.5.5 Substitution of (Bound) Variables, Normal Forms

We have seen two ways of modifying formulas through substitution:

- Substitution of a *free variable* through a *term*.
- Substitution of a *bound variable* through another variable symbol.

The former is only a syntactic modification:

Definition 4.32. *For a formula F, a variable x and a term t, $F[x/t]$ denotes the formula obtained from F by substituting every free occurrence of x by t.*

We can substitute a simple variable by an arbitrary term:

Example. Let

$$F = \forall x\ P(x, y) \vee (\exists y\ Q(y) \wedge \neg P(y, y))$$

The first occurrence of y and the last two occurrences of y are free. Because $f(a, b, c)$ is a term, we can substitute all free y by this term:

$$F[y/f(a, b, c)] = \forall x\ P(x, f(a, b, c)) \vee (\exists y\ Q(y) \wedge \neg P(f(a, b, c), f(a, b, c)))$$

The other substitution that we learned is called *bound substitution*. Whereas the substitution of free variables is simply a syntactic rule that allows to construct new formulas (without any semantic meaning), bound substitution is a way to retrieve an equivalent formula from a given formula, and hence has a semantic meaning:

Lemma 4.5

For a formula G in which y does not occur, we have

- $\forall x\ G \equiv \forall y\ G[x/y]$,
- $\exists x\ G \equiv \exists y\ G[x/y]$.

The reason why we need bound substitution is, that we sometimes want our formulas to be in a specific format. An example for such a format is called *rectified* form:

Definition 4.33. *A formula F is in **rectified** form if:*

- *No variable in F occurs both as a bound and as a free variable*
- *All bound variables in F that appear directly after a quantifier symbol are distinct.*

Another format is called *prenex form*:

Definition 4.34. *A formula of the form*

$$Q_1 x_1\ Q_2 x_2\ \cdots Q_n x_n\ G,$$

*where the Q_i are arbitrary quantifiers ($\forall$ or $\exists$) and G is a formula free of quantifiers, is said to be in **prenex form**.*

Theorem 7

For every formula there is an equivalent formula in prenex form.

For a formula F one can construct an equivalent formula in prenex form with the following steps:

1. Transform F into an equivalent formula F' that is in *rectified* form.
2. Apply a sequence of equivalences of Lemma 4.2 and Lemma 4.3 to move all quantifiers to the beginning of the formula.

Example. We want to transform $F = \forall y\ (\exists z\ P(x,y,z) \wedge \forall x\ \neg Q(x))$ into prenex form.

$$\begin{aligned}
F &\equiv \forall y\ (\exists z\ P(x,y,z) \wedge \forall u\ \neg Q(u)) && \text{(bound substitution)}\\
&\equiv \forall y\ (\exists z\ (P(x,y,z) \wedge \forall u\ \neg Q(u))) && (9)\\
&\equiv \forall y\ \exists z\ (P(x,y,z) \wedge \forall u\ \neg Q(u)) && \text{(omit brackets)}\\
&\equiv \forall y\ \exists z\ (\forall u\ \neg Q(u) \wedge P(x,y,z)) && (\wedge\text{-commutativity})\\
&\equiv \forall y\ \exists z\ (\forall u\ (\neg Q(u) \wedge P(x,y,z))) && (7)\\
&\equiv \forall y\ \exists z\ \forall u\ \underbrace{(\neg Q(u) \wedge P(x,y,z))}_{=:G} && \text{(omit brackets)}
\end{aligned}$$

In the first step we have made a bound substitution of x by u, because x occurs both free (first occurrence of x) and bound in F. After that, we have a rectified formula. The numbers (7) and (9) refer to Lemma 4.3.

It is important to note that in general, a substitution of a free variable is not an equivalence transformation:

Example. Let $F := P(x)$ and $F' := F[x/y] = P(y)$. Then $F \not\equiv F'$. To see this, consider the structure $\mathcal{A}$ where:

$$U^{\mathcal{A}} = \{0, 1\}, \quad P^{\mathcal{A}}(x) = 1 :\Leftrightarrow x = 1, \quad x^{\mathcal{A}} = 1, \quad y^{\mathcal{A}} = 0$$

$\mathcal{A}$ is suitable for both F and F' but obviously $\mathcal{A} \vDash F$ while $\mathcal{A} \nvDash F'$.

Hands-On 3

3.1. Structures
For the formula $F \equiv \forall x(\exists y\ (P(x, y) \land P(y, x)) \to P(f(x, y), f(y, x)))$ give a structure $\mathcal{A}$, which is

(a) not suitable for F

(b) suitable and a model for F

(c) suitable but not a model for F

3.2. Free Variables
For each formula, determine which variables are free and which are bound. For each bound variable, determine the quantifier to which it is bound.

(a) $\forall x \exists y\ Q(x) \lor P(f(y)) \lor \forall y\ R(x)$

(b) $\forall x\ (\exists y\ Q(x) \lor P(f(y))) \lor \forall y\ R(x)$

(c) $\forall x \exists y\ \ (Q(x) \lor P(f(y)) \lor \forall y\ R(x))$

3.3. Syntax
For each formula, decide if it is a formula, a statement about formulas or syntactically incorrect. P, Q, R are a predicates, x, y, z are variables and f, g, h are functions.

(a) $P(f(x)) \lor Q(g(y)) \vDash R(h(z))$

(b) $P(x) \equiv \forall x\ (Q(x) \lor \exists f\ P(f(x)))$

(c) $\forall x\ P(x) \to (Q(x) \lor Q(f(z)))$

(d) $P(f(x) \land f(y)) \to P(f(x))$

(e) $(P(x) \vDash Q(x)) \lor (Q(x) \vDash P(x))$

(f) $\forall x\ P(x) \leftrightarrow Q(x) \equiv \exists x\ P(x) \to Q(x)$

3.4. Logical Consequences
For each logical consequence, decide if it true or false. If it is false, give a counterexample (that is, an example of the formulas F and G, aswell as an appropriate structure).

(a) $(\forall x\ F) \lor G \vDash \forall x\ (F \lor G)$

(b) $\forall x\ (F \lor G) \vDash (\forall x\ F) \lor G$

(c) $(\forall x\ F) \land G \vDash \forall x\ (F \land G)$

(d) $\forall x\ (F \land G) \vDash (\forall x\ F) \land G$

3.5. Prenex Form
Consider the formula $F \equiv \forall x\ (P(x) \lor \exists x\ Q(f(x))) \land \exists y\ R(g(y, x))$.

(a) Bring F into a rectified form.

(b) Bring F into a prenex form. You can use the result of the previous subtask.

3.6. Tautologies

(a) Which of the following formulas are tautologies?
If they are, prove it by using the equivalences from Lemma 4.2, 4.3 and 4.5.
You can also use the the fact, that $F \vee \exists y\ \neg F$ is a tautology.
You can try to prove this yourself or find it in the solutions of exercise 13.3 a) (not in this script).
If they aren't, prove it by showing an counterexample (give an interpretation under which the formula is false).

(1) $\exists x\ (P(x) \to \forall x\ P(x))$

(2) $\exists x\ P(x) \vee \forall x\ P(x)$

(3) $(\forall x\ (P(x) \to Q(x)) \wedge P(y)) \to Q(y)$

(b) Prove that the following statements are true:

(1) "There exists a student, such that, if this student passes the exam, then everyone passes the exam."

(2) "If every planet is flat and the earth is a planet, then the earth is also flat"

3.7. Challenge

(a) For any formulas F,G and H, where x does not occur free in H:
Prove this equivalence: $(\exists x\ F) \vee H \equiv \exists x\ (F \vee H)$.

(b) (1) Extend the syntax and the semantics of predicate logic to include the equality symbol "=", where $t_1 = t_2$ is true if and only if the term t_1 has the same value as the term t_2.

(2) Consider the Universe G and the function $f(x, y) = x * y$.
Using only the function f, describe the following sentences as formulas.
($\forall$, $\exists$, $\wedge$, $\vee$, $\neg$, $=$, parentheses and variables are all allowed aswell).

(i) $\langle G; * \rangle$ is a monoid.

(ii) $\langle G; * \rangle$ is a group.

4.6 Solutions

4.6.1 Solutions for Hands-On 1

1.1 Soundness And Completeness Of Proof Systems

(a) The system is complete but not sound.

Proof. To see that it is complete, let $s \in \mathcal{S}$ such that $\tau(s) = 1$. Hence, s contains at most one 0. Set $p = s$ and we get $\phi(s, p) = 1$ because if s contains at most one 0, it also contains at most two 0. To show that the system is unsound, we give a counterexample: $s = 001$ is not true under τ because it contains more than one 0. Nevertheless $p = s$ is a valid proof for s. □

(b) The system is sound but not complete.

Proof. To show soundness, let $s \in \mathcal{S}$ and $p \in \mathcal{P}$ such that $\phi(s, p) = 1$. Because p has exactly one 0 and $d(s, p) = 3$, s must contain exactly one 1, thus $\tau(s) = 1$.
To disprove completeness, we again give a counterexample: $s = 111$ is true, because it contains at least one 1. But there is no proof for s, because if such a p would exist, it would have the form $p = 000$ in order to satisfy the first condition of ϕ. But then the second condition is violated, which is a contradiction. □

1.2 Finding The Verification Function

If we can choose $p \in \mathbb{N}^4$, the answer is simple: $\phi(n, p) = 1$ only if $p = (p_1, p_2, p_3, p_4)$ and it holds that:

- p_i is prime (for $1 \leq i \leq 4$).
- $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \mid n$

Claim

Π is complete.

Proof. Let $n \in \mathbb{N}$ such that $\tau(n) = 1$. Therefore s has at least four prime factors. Then choose $p = (p_1, p_2, p_3, p_4)$ where the p_i are four prime factors of n ($1 \leq i \leq 4$). But then the product of those prime factors divides p and hence $\phi(n, p) = 1$. □

Claim

Π is sound.

Proof. Let $n \in \mathbb{N}, p \in \mathbb{N}^4$ such that $\phi(n, p) = 1$. But then, n is dividable by the product of four primes p_i stored in p. By the definition of the *divides* relation, there exists a $k \in \mathbb{N}$ such that: $n = k \cdot (p_1 \cdot p_2 \cdot p_3 \cdot p_4)$. This means that n has four prime factors and hence $\tau(n) = 1$. □

The problem if we only have $\mathcal{P} = \mathbb{N}$ is, that we somehow need to encode 4 natural numbers in a single natural number. We remember from Theorem 3.16, that there exists a bijection $f \colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, given by the definition:

$$f(n) = (k, m), \quad \text{where: } \begin{cases} t > 0 \text{ is the smallest integer such that } \binom{t+1}{2} > n \\ k + m = t - 1 \\ m = n - \binom{t}{2} \end{cases} \tag{$*$}$$

The tuples $f(0), f(1), f(2), \ldots$ correspond to the enumeration of the diagonals in the $\mathbb{N}^2$-plane. Note, that the tuples $f(n)$ can be efficiently computed by solving the equations in $(*)$.
By using the bijection f, we can construct a function $g \colon \mathbb{N}^4 \to \mathbb{N}$ as follows:

$$g(x) = (z_1, z_2, z_3, z_4), \quad \text{where } \left\{ \begin{matrix} (z_1, z_2) = f(y_1) \\ (z_3, z_4) = f(y_2) \end{matrix} \right\}, \quad \text{where } (y_1, y_2) = f(x).$$

We first apply $f(x)$ to get a tuple (y_1, y_2) and then apply f again on the two entries y_1 and y_2 to receive a 4-tuple (z_1, z_2, z_3, z_4).

Claim

g is bijective.

Proof. We need to show that g is injective and surjective.

- **Injectivity:** Let $x, y \in \mathbb{N}$ and $x \neq y$. Hence $f(x) = (a_1, a_2) \neq (b_1, b_2) = f(y)$ because f is injective. But then for some $i \in 1, 2$ we have $a_i \neq b_i$ which - again by injectivity of f - implies that $f(a_i) \neq f(b_i)$. Thus the 4-tuples $g(x)$ and $g(y)$ cannot be equal.✓
- **Surjectivity:** Let $(z_1, z_2, z_3, z_4) \in \mathbb{N}^4$ be arbitrary. Because f is surjective, there exists a y_1 such that $f(y_1) = (z_1, z_2)$ and a y_2 such that $y_2 = (z_3, z_4)$. By the same reason, there exists an x such that $f(x) = (y_1, y_2)$.✓

□

We define our verification function as follows:

$$\phi(n, p) = 1 :\Leftrightarrow \text{ All of the three hold: } \begin{cases} g(p) = (p_1, p_2, p_3, p_4) \\ p_i \text{ is prime (for } 1 \leq i \leq 4) \\ p_1 \cdot p_2 \cdot p_3 \cdot p_4 \mid n \end{cases}$$

Since g is a bijection, we can always encode the four primes in a single number p. The proof that the proof system is still sound and complete under this verification function, stays the same as in the case where $\mathcal{P} = \mathbb{N}^4$.

1.3 Finding the truth function

We first have to introduce some notation: Let $x = x_1, x_2, x_3, x_4, x_5 \in \{0, 1\}^5$, that is we denote the i-th bit of x by $x_i \in \{0, 1\}$. We call the set of indices $\mathcal{I} = \{1, 2, 3, 4, 5\}$. For every x, we can partition $\mathcal{I}$ into two disjoint subsets $x^{(0)}$ and $x^{(1)}$ as follows:

$$x^{(0)} := \{i \in \mathcal{I} | x_i = 0\}, \quad x^{(1)} := \{i \in \mathcal{I} | x_i = 1\}, \quad x^{(0)} \cup x^{(1)} = \mathcal{I}$$

Next we define our truth function:

$$\tau(s) = 1 :\Leftrightarrow |s^{(0)}| \geq 3.$$

In words: s is true if it contains at least three 0.

Claim

Π is complete.

Proof. Let $s \in \mathcal{S}$ be arbitrary such that $\tau(s) = 1$. Therefore s may contain 3, 4 or 5 zeros. We make a case distinction:

- $s^{(0)} = 5$.
  Then $s = 00000$ and for example $p = 11110$ is a valid proof, because the hamming distance of p and s is 4, and p has only one 0.✓
- $s^{(0)} = 4$.
  Then we choose $p = 11111$ and s and p differ at exactly 4 positions.✓
- $s^{(0)} = 3$.
  We choose a $p \in \mathcal{P}$ such that $p^{(1)} = s^{(0)}$ and for the remaining two positions $\mathcal{I} \setminus s^{(0)}$ in p we set one to 1 and one to 0. Therefore p consists of four 1 and one 0. p and s differ in the three positions $s^{(0)}$ (because s contains only 0 and p contains only 1 at those positions), and at the position where we set p to 0. This leads to a total difference of 4 positions. ✓

□

Claim

Π is sound.

Proof. By contradiction, assume that $\phi(s,p) = 1$ and $\tau(s) = 0$ for some $s \in \mathcal{S}, p \in \mathcal{P}$. Because we assumed that $\tau(s) = 0$, we conclude that $|s^{(0)}| \leq 2$. But then the hamming distance between p and s can be at most 3, by setting the only available 0 of p to a position where s is not 0 already. But this means that it is impossible to find a p that differs at 4 positions and thus $\phi(s,p) = 0$ which is a contradiction. Hence, Π is sound. □

1.4 Correct Rules (Challenge)

Let $K = \{R_1, \ldots, R_m\}$ be a calculus.

1. K is sound $\quad\Rightarrow\quad$ R_i is correct (for $1 \leq i \leq m$).

   Proof. Assume (by contradiction) that K is sound but there exists a rule $R \in K$ that is not correct and is defined as:

   $$M \vdash_R F$$

   Consider the derivation $M \vdash_K F$ that consists of a single step in which the rule R got applied. Because K is sound by assumption, we have $M \vDash F$. But because we only used the rule R which is incorrect by assumption, we have $M \nvDash F$ which is a contradiction. □

2. R_i is correct (for $1 \leq i \leq m$) $\quad\Rightarrow\quad$ K is sound.

   Proof. Let $M \vdash_K G$ be an arbitrary derivation of length n (for some n) in K. During this derivation, we construct a sequence of sets $M_0, \ldots, M_n$ that we get by deriving G from M. Consider an arbitrary derivation step where we derived $N \vdash_{R_j} G_i$ from some $N \subseteq M_{i-1}$. Because all rules are correct, we have $N \vDash G_i$, or in our newly introduced notation: $N \vDash \{G_i\}$. Because $N \subseteq M_{i-1}$ we have $M_{i-1} \vDash \{G_i\}$ by Lemma 1. Next, we apply Lemma 2 and get $M_{i-1} \vDash M_{i-1} \cup \{G_i\}$. But $M_{i-1} \cup \{G_i\} =: M_i$ (by Definition 4.5) and hence we have:

   $$M_{i-1} \vDash M_i \quad (\text{for } 1 \leq i \leq n).$$

   Note that $M_n = M_{n-1} \cup \{G\}$ and hence $M_n \vDash G$. Because of transitivity of $\vDash$ we conclude:

   $$M = M_0 \vDash M_1 \vDash \ldots \vDash M_n \vDash G \quad\Rightarrow\quad M \vDash G$$

   □

1.5 Soundness And Completeness Of Logical Calculi

(a) Let $K_1 = \{R_1\}$ where $\{F\} \vdash_{R_1} F$.

Claim

K_1 is sound.

Proof. Let $M = \{F_1, \ldots F_n\}$ be an arbitrary set of formulas. The only ways to apply a derivation rule, is to pick an arbitrary $F_i \in M$ and applying the rule: $\{F_i\} \vdash_{R_1} F_i$. Since such a step only generates a formula, that is already in M, every *derivation*[7] will end up deriving a formula $F_i \in M$:

$$M \vdash_{K_1} F_i \quad \text{for some } i \in \{1, \ldots, n\}.$$

But obviously $M \vDash F_i$, because if $\mathcal{A} \vDash M$, then $\mathcal{A} \vDash F_i$ for all $F_i \in M$ □

[7] Here, we mean an arbitrary sequence of applications of derivation rule, according to Definition 6.19.

Claim

K_1 is not complete.

Proof. Assume it is. But then we should be able to derive $\{A\} \vdash_{K_1} A \vee B$, because $\{A\} \vDash A \vee B$. But we have already seen above, that we cannot derive new formulas from any starting set M, hence we will never derive $A \vee B$ and therefore: $\{A\} \nvdash_{K_1} A \vee B$. □

(b) Let $K_2 = \{R_2\}$ where $\vdash_{R_2} F$.

Claim

K_2 is complete.

Proof. Let M be set of formulas and F be an formula such that $M \vDash F$. Obviously $M \vdash_{K_2} F$, namely by the derivation consisting of a single step: $\vdash_{R_2} F$. □

Note that in a derivation, we always choose only a subset of formulas in M to apply a derivation rule. Here we used the empty set, because our only rule R_2 demands this format.

Claim

K_2 is not sound.

Proof. We can derive $\vdash_{K_2} A$, but obviously $\nvDash A$, because $\mathcal{A}(A) = 0$ if $\mathcal{A} = \{A = 0\}$. □

4.6.2 Solutions for Hands-On 2

2.1 Propositional Logic

(a) To the definition of syntax we add the following statement:

$$\text{If } F \text{ and } G \text{ are formulas, then } (F \downarrow G) \text{ is also a formula.}$$

To the definition of semantics we add the following:

$$\mathcal{A}((F \downarrow G)) = 1 \text{ if and only if } \mathcal{A}(F) = 0 \text{ and } \mathcal{A}(G) = 0.$$

(b) Notice that a given interpretation can be both suitable and not suitable depending on the formula.

	$A \wedge (B \vee \neg A) \wedge \neg C$	$A \vee \neg A \vee B$	$A \vee \neg D$
$\mathcal{A} = \{A = 0, B = 0, C = 1, D = 1\}$	suitable, not a model	suitable, model	suitable, not a model
$\mathcal{A} = \{A = 0, D = 0\}$	not suitable	not suitable	suitable, model
$\mathcal{A} = \{A = 1, B = 1, C = 0\}$	suitable, model	suitable, model	not suitable

(c) (1) $\mathcal{A} = \{A = 1, B = 1, C = 1, D = 0\}$ is a model for M.
Another solution is $\mathcal{A} = \{A = 0, B = 1, C = 1, D = 0\}$

(2) N is unsatisfiable. We show this with an proof by contradiction.
Suppose N was satisfiable and $\mathcal{A}$ is a model for N.
Then we have $\mathcal{A}(A \to B) = 1$, $\mathcal{A}(C \wedge D) = 1$, $\mathcal{A}(C \to A) = 1$ and $\mathcal{A}(B \to \neg D) = 1$.
Then $\mathcal{A}(C) = 1$ and $\mathcal{A}(D) = 1$ follows from $\mathcal{A}(C \wedge D) = 1$.
Then $\mathcal{A}(A) = 1$ follows from $\mathcal{A}(C) = 1$ and $\mathcal{A}(C \to A) = 1$.
Then $\mathcal{A}(B) = 1$ follows from $\mathcal{A}(A) = 1$ and $\mathcal{A}(A \to B) = 1$.
Then $\mathcal{A}(\neg D) = 1$ follows from $\mathcal{A}(B) = 1$ and $\mathcal{A}(B \to \neg D) = 1$.
Then $\mathcal{A}(D) = 0$ follows from $\mathcal{A}(\neg D) = 1$.
But this is a contradiction, because we derived both $\mathcal{A}(D) = 1$ and $\mathcal{A}(D) = 0$.
Thus, N must be unsatisfiable.

(d) We have to show the following:

Claim

$$F \vDash G \quad \Leftrightarrow \quad F \to G \text{ is a tautology}$$

Proof.

- "⇒"
  Let $\mathcal{A}$ be any interpretation suitable for both F and G, thus also suitable for $F \to G$.

  Case 1 $\mathcal{A}(F) = 1$.
  Then, by assumption $F \vDash G$ we have $\mathcal{A}(G) = 1$.
  Therefore we have $\mathcal{A}(\neg F \vee G) = 1$, because $\mathcal{A}(G) = 1$.
  This is exactly $\mathcal{A}(F \to G) = 1$.

  Case 2 $\mathcal{A}(F) = 0$.
  Then we have $\mathcal{A}(\neg F) = 1$.
  Therefore we have $\mathcal{A}(\neg F \vee G) = 1$, because $\mathcal{A}(\neg F) = 1$.
  This shows again $\mathcal{A}(F \to G) = 1$.
  We have shown for all cases that $\mathcal{A}(F \to G) = 1$ for any suitable interpretation $\mathcal{A}$. Therefore, $F \to G$ is a tautology.

- "$\Leftarrow$"
  If $F \to G$ is a tautology, then any interpretation $\mathcal{A}$ suitable for F and G is a model for $F \to G$, i.e., $\mathcal{A}(F \to G) = 1$.
  Therefore, $\mathcal{A}(\neg F \vee G) = 1$.

  Let $\mathcal{B}$ be an interpretation suitable for both F and G, which is a model for F, i.e, $\mathcal{B}(F) = 1$.
  By the assumption the following must also hold for $\mathcal{B}$:
  $\mathcal{B}(\neg F \vee G) = 1$.
  Since $\mathcal{B}(\neg F) = 0$, we have that $\mathcal{B}(\neg F \vee G)$ is equal to 1 only if $\mathcal{B}(G) = 1$.
  This shows, that every suitable interpretation for F and G, which is a model for F, is also an model for G, thus $F \vDash G$.

  □

(e) The statement is indeed false, but the given proof is incorrect. $\mathcal{A}$ is not a correct counterexample, because $\mathcal{A}$ is not suitable for the right side. The definition of $F \vDash G$ requires an interpretation which is suitable for both F and G. This will be more important in predicate logic. A correct counterexample would be: $\mathcal{A} = \{A = 1, B = 0, C = 1\}$

(f) (1) CNF
(2) CNF
(3) DNF
(4) Both in CNF and DNF
(5) Not in a normal form

(g) After determining the function table we can construct the formulas in CNF and DNF.

A	B	C	$(A \to (B \wedge C)) \wedge B$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

DNF:

$$(\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge B \wedge C)$$

CNF:

$$(A \vee B \vee C) \wedge (A \vee B \vee \neg C) \wedge (\neg A \vee B \vee C) \wedge (\neg A \vee B \vee \neg C) \wedge (\neg A \vee \neg B \vee C)$$

2.2 The Resolution Calculus

(a) We show the following:

Claim

The resolution calculus is not complete.

Proof. To do so, it suffices to provide two formulas F and G such that $F \vDash G$ but $\mathcal{K}(F) \nvdash_{\text{Res}} \mathcal{K}(G)$. For example $G := A \vee B$ is a logical consequence of $F := A$ which can be easily verified by looking at the truth tables. But there is no way to derive $\mathcal{K}(A \vee B)$ from $\mathcal{K}(A)$ because we cannot apply $\vdash_{\text{res}}$. (The only way to pick two clauses on the left side, is to pick $K_1 = \mathcal{K}(A)$ and $K_2 = \mathcal{K}(A)$. But those do not provide a resolvent as described in Definition 4.26.) □

(b) We have to show the following:

Claim

$$M \vDash F \quad \Leftrightarrow \quad M \cup \{\neg F\} \text{ is unsatisfiable.}$$

Proof. Let $M = \{G_1, \ldots, G_k\}$.

$$\begin{aligned} M \vDash F &\Leftrightarrow (G_1 \wedge \cdots \wedge G_k) \vDash F \\ &\Leftrightarrow (G_1 \wedge \cdots \wedge G_k) \rightarrow F \text{ is a tautology} \\ &\Leftrightarrow \neg(G_1 \wedge \cdots \wedge G_k) \vee F \text{ is a tautology} \\ &\Leftrightarrow \neg(\neg(G_1 \wedge \cdots \wedge G_k) \vee F) \text{ is unsatisfiable} \\ &\Leftrightarrow (G_1 \wedge \cdots \wedge G_k) \wedge \neg F \text{ is unsatisfiable} \\ &\Leftrightarrow M \cup \{\neg F\} \text{ is unsatisfiable} \end{aligned}$$

□

An alternative proof is as follows:

Proof.

- "⇒"
  Let $\mathcal{A}$ be an arbitrary interpretation suitable for both M and F (and hence also for $\neg F$).

  Case 1 $\mathcal{A} \vDash M$.
  Then, by assumption we have $\mathcal{A} \vDash F$ and hence $\mathcal{A}(\neg F) = 0$. But then, we conclude that $\mathcal{A} \nvDash M \cup \{\neg F\}$, because $\mathcal{A}$ is not a model for one of these formulas.

  Case 2 $\mathcal{A} \nvDash M$.
  Then $\mathcal{A} \nvDash M \cup \{\neg F\}$ (trivially).

  Because $\mathcal{A}$ was an arbitrary interpretation and $\mathcal{A} \nvDash M \cup \{\neg F\}$, the set $M \cup \{\neg F\}$ is unsatisfiable. ✓
- "⇐"
  Assume $M \cup \{\neg F\}$ is unsatisfiable. Let $\mathcal{A}$ be an arbitrary interpretation, such that $\mathcal{A} \vDash M$. Note, that then $\mathcal{A}(\neg F) = 0$, because otherwise we would have $\mathcal{A} \vDash M \cup \{\neg F\}$ which would contradict our assumption. Hence $\mathcal{A}(F) = 1$ and therefore $M \vDash F$. ✓

□

(c) ***Proof.*** We use the results from the previous subtask: $M = \{A\}, F = A \vee B$ and $M \cup \{\neg F\} = \{A, \neg A \wedge \neg B\}$. Remember, that we can always associate a set of formulas with a single formula that is the conjunctions of all formulas in the set:

$$G := A \wedge (\neg A \wedge \neg B)$$

According to (b), it suffices to show that G is unsatisfiable. G is already in CNF, therefore the clauses are:

$$\mathcal{K}(G) = \{\{A\}, \{\neg A\}, \{\neg B\}\}$$

Obviously, the first two clauses provide a resolvent:

$$\{\{A\}, \{\neg A\}\} \vdash_{res} \emptyset$$

which concludes the proof. Note, that it is not necessary to involve all clauses in a derivation. The clause $\{B\}$ for example was not used at all. □

4.6.3 Solutions for Hands-On 3

3.1 Structures

(a) $U^{\mathcal{A}} = \mathbb{N}$ and none of the functions, predicates and variables are defined.

(b) $U^{\mathcal{A}} = \mathbb{Z}$
$P^{\mathcal{A}}(x, y)$ is always 0
$f^{\mathcal{A}}(x, y) = 1337$
$y^{\mathcal{A}} = 42$
The left side of the implication is always 0, because $P^{\mathcal{A}}(x, y)$ is always 0. Therefore the whole implication is true for all x.

(c) $U^{\mathcal{A}} = \mathbb{Z}$
$P^{\mathcal{A}}(x, y) = 1$ if and only if $x \geq y$
$f^{\mathcal{A}}(x, y) = x - y$
$y^{\mathcal{A}} = 42$
We can see that the left side of the implication is always true, because there always exists a y, such that $x \geq y$ and $y \geq x$. The right side is not true for all x, where $x = 0$ is such an example. Therefore the whole implication is not true for all x.

3.2 Free Variables
In each formula there are 3 quantifier, 3 occurrences of x and 3 occurrences of y.

(a)

$$\underset{\downarrow 1}{\forall x}\underset{\downarrow 1}{\exists y}\ Q(\underset{\downarrow 2}{x}) \vee P(f(\underset{\downarrow 2}{y})) \vee \underset{\downarrow 3}{\forall y}\ R(\underset{\downarrow 3}{x})$$

- Occurrence 1 of directly follows the first ∀ quantifier and is hence bound to it.
- Occurrence 2 of is bound to the first ∀ quantifier.
- Occurrence 3 of is free.

- Occurrence 1 of y directly follows the ∃ quantifier and is hence bound to it.
- Occurrence 2 of y is free.
- Occurrence 3 of y directly follows the second ∀ quantifier and is hence bound to it.

(b)

$$\underset{\downarrow 1}{\forall x}(\underset{\downarrow 1}{\exists y}\ Q(\underset{\downarrow 2}{x}) \vee P(f(\underset{\downarrow 2}{y}))) \vee \underset{\downarrow 3}{\forall y}\ R(\underset{\downarrow 3}{x})$$

- Occurrence 1 of x directly follows the first ∀ quantifier and is hence bound to it.
- Occurrence 2 of x is bound to the first ∀ quantifier.
- Occurrence 3 of x is free.

- Occurrence 1 of y directly follows the ∃ quantifier and is hence bound to it.
- Occurrence 2 of y is free.
- Occurrence 3 of y directly follows the second ∀ quantifier and is hence bound to it.

(c)

$$\underset{\downarrow 1}{\forall x}\underset{\downarrow 1}{\exists y}\ (Q(\underset{\downarrow 2}{x}) \vee P(f(\underset{\downarrow 2}{y})) \vee \underset{\downarrow 3}{\forall y}\ R(\underset{\downarrow 3}{x}))$$

- Occurrence 1 of x directly follows the first ∀ quantifier and is hence bound to it.
- Occurrence 2 of x is bound to the first ∀ quantifier.
- Occurrence 3 of x occurrence of x is bound to the first ∀ quantifier.

- Occurrence 1 of y directly follows the ∃ quantifier and is hence bound to it.
- Occurrence 2 of y is bound to the ∃ quantifier.
- Occurrence 3 of y directly follows the second ∀ quantifier and is hence bound to it.

3.3 Syntax

(a) $\vDash$ is not allowed inside formulas. This is a statement about formulas.

(b) Incorrect. (again, $\equiv$ is not allowed inside formulas)

(c) Formula.

(d) Syntactically incorrect, as we're not allowed to use logical operators between two terms.

(e) Incorrect. This is not even a valid statement about formulas.

(f) Statement about formulas.

3.4 Logical Consequences

(a) This statement is false. We provide the following counterexample:
$F \equiv P(x)$
$G \equiv Q(x)$
$U^{\mathcal{A}} = \mathbb{N}$
$P^{\mathcal{A}}(x)$ is false for all x
$Q^{\mathcal{A}}(x)$ is true if and only if $x > 3$
$x^{\mathcal{A}} = 5$
Notice that the variable x in $Q(x)$ occurs free on the left side, but bound on the right side. $\mathcal{A}$ is suitable for both sides and a model for the left side, but not a model for the right side.

(b) This statement is false. We provide the following counterexample:
$F \equiv P(x)$
$G \equiv Q(x)$
$U^{\mathcal{A}} = \mathbb{N}$
$P^{\mathcal{A}}(x)$ is true if and only if x is even
$Q^{\mathcal{A}}(x)$ is true if and only if x is odd
$x^{\mathcal{A}} = 4$
Notice that the variable x in $Q(x)$ occurs free on the left side, but bound on the right side. Because of this, a suitable interpretation $\mathcal{A}$ must assign a value to x. $\mathcal{A}$ is suitable for both sides and a model for the left side, but not a model for the right side.

(c) This statement is false. We provide the following counterexample:
$F \equiv P(x)$
$G \equiv Q(x)$
$U^{\mathcal{A}} = \mathbb{N}$
$P^{\mathcal{A}}(x)$ is true for all x
$Q^{\mathcal{A}}(x)$ is true if and only if $x > 3$
$x^{\mathcal{A}} = 5$
Notice that the variable x in $Q(x)$ occurs free on the left side, but bound on the right side. $\mathcal{A}$ is suitable for both sides and a model for the left side, but not a model for the right side.

(d) This statement is correct.

3.5 Prenex Form

(a) $F \equiv \forall u\ (P(u) \vee \exists z\ Q(f(z))) \wedge \exists y\ R(g(y,x))$

(b)
$\equiv \forall u(\exists z\ (P(u) \vee Q(f(z)))) \wedge \exists y\ R(g(y,x))$ (Lm 4.2, Rule 2 and Lm 4.3, Rule 10)
$\equiv \forall u(\exists z\ (P(u) \vee Q(f(z))) \wedge \exists y\ R(g(y,x)))$ (Lm 4.3, Rule 7)
$\equiv \forall u(\exists z\ ((P(u) \vee Q(f(z))) \wedge \exists y\ R(g(y,x))))$ (Lm 4.3, Rule 9)
$\equiv \forall u(\exists z(\exists y\ ((P(u) \vee Q(f(z))) \wedge R(g(y,x)))))$ (Lm 4.2, Rule 2 and Lm 4.3, Rule 9)
$\equiv \forall u \exists z \exists y\ ((P(u) \vee Q(f(z))) \wedge R(g(y,x)))$ (omit brackets)

3.6 Tautologies

(a) (1) This formula is a tautology:
Let $F := \forall x\ P(x)$

$$
\begin{aligned}
&\exists x\ (P(x) \to \forall x\ P(x)) \\
&\equiv \exists x\ (\neg P(x) \vee \forall x\ P(x)) && \text{(Def. of } \to\text{)} \\
&\equiv \exists x\ \neg P(x) \vee \forall x\ P(x) && \text{(Lm 4.3, Rule 10)} \\
&\equiv \neg(\forall x\ P(x)) \vee \forall x\ P(x) && \text{(Lm 4.3, Rule 1)} \\
&\equiv \neg(F) \vee F && \text{(Substitution with } F\text{)} \\
&\equiv F \vee \neg F && \text{(Lm 4.2, Rule 2)} \\
&\equiv \top && \text{(Lm 4.2, Rule 11)}
\end{aligned}
$$

(2) This formula is not a tautology. This formula is false under the interpretation $\mathcal{A}$, where $U^{\mathcal{A}} = \mathbb{N}$ and $P^{\mathcal{A}}(x)$ is false for all x.

(3) This formula is a tautology:
Let $G := \neg P(y) \vee Q(y)$

$$
\begin{aligned}
&(\forall x\ (P(x) \to Q(x)) \wedge P(y)) \to Q(y) \\
&\equiv \neg(\forall x\ (\neg P(x) \vee Q(x)) \wedge P(y)) \vee Q(y) && \text{(Def. of } \to\text{)} \\
&\equiv (\neg\forall x\ (\neg P(x) \vee Q(x)) \vee \neg P(y)) \vee Q(y) && \text{(Lm 4.2, Rule 8)} \\
&\equiv \neg\forall x\ (\neg P(x) \vee Q(x)) \vee (\neg P(y) \vee Q(y)) && \text{(Lm 4.2, Rule 3)} \\
&\equiv \exists x\ \neg(\neg P(x) \vee Q(x)) \vee (\neg P(y) \vee Q(y)) && \text{(Lm 4.3, Rule 1)} \\
&\equiv \exists y\ \neg(\neg P(y) \vee Q(y)) \vee (\neg P(y) \vee Q(y)) && \text{(Lm 4.5)} \\
&\equiv \exists y\ \neg(G) \vee (G) && \text{(Substitution with } G\text{)} \\
&\equiv G \vee \exists y\ \neg G && \text{(Lm 4.2, Rule 2)} \\
&\equiv \top && \text{(Exercise 13.3 a))}
\end{aligned}
$$

(b) (1) From the previous subtask we know, that $\exists x\ (P(x) \to \forall x\ P(x))$ is a tautology.
That means, that the formula is true for every suitable structure, in particular for the structure $\mathcal{A}$:
$U^{\mathcal{A}}$ is the set of all the student who take the exam.
$P^{\mathcal{A}}(x)$ is true if and only if student x passes the exam.
The valid formula under $\mathcal{A}$ exactly translates to the sentence:
"There exists a student, such that, if this student passes the exam, then everyone passes the exam.".

(2) From the previous subtask we know, that $(\forall x\ (P(x) \to Q(x)) \wedge P(y)) \to Q(y)$ is a tautology.
That means, that the formula is true for every suitable structure, in particular for the structure $\mathcal{A}$:
$U^{\mathcal{A}}$ is the set of all stars and planets in the physical universe
$P^{\mathcal{A}}(x)$ is true if and only if x is a planet
$Q^{\mathcal{A}}(x)$ is true if and only if x is flat
$y^{\mathcal{A}}$ is the earth
The valid formula under $\mathcal{A}$ exactly translates to the sentence:
"If every planet is flat and the earth is a planet, then the earth is also flat" .

3.7 (Challenge)

(a) We have to show the following:

Claim

For any formulas F,G and H, where x does not occur free in H:
$(\exists x\ F) \vee H \equiv \exists x\ (F \vee H)$.

Proof. We have to show that every structure $\mathcal{A}$ that is a model for $(\exists x\ F) \vee H$ is also a model for $\exists x\ (F \vee H)$, and vice versa.

Recall that the definition of the semantics of a formula $\exists x\ G$ for a structure $\mathcal{A}$ is that, for some $u \in U$, $\mathcal{A}_{[x \to u]}(G) = 1$.

We first prove the first direction, i.e., $(\exists x\ F) \vee H \vDash \exists x\ (F \vee H)$.
Suppose that $\mathcal{A}((\exists x\ F) \vee H) = 1$ and hence that

(i) $\mathcal{A}(\exists x\ F) = 1$ or that

(ii) $\mathcal{A}(H) = 1$.

Recall that (i) means that $\mathcal{A}_{[x \to u]}(F) = 1$ for some $u \in U$, and (ii) means that $\mathcal{A}_{[x \to u]}(H) = 1$ for some $u \in U$. (This is because x does not occur free in H and hence for all $u \in U$: $\mathcal{A}_{[x \to u]}(H) = \mathcal{A}(H)$).
Therefore $\mathcal{A}_{[x \to u]}(F \vee H) = 1$ for some $u \in U$, which means that $\mathcal{A}(\exists x\ (F \vee H)) = 1$, which was to be proved.

We now prove the other direction, i.e., $\exists x\ (F \vee H) \vDash (\exists x\ F) \vee H$.
Suppose that $\mathcal{A}(\exists x\ (F \vee H)) = 1$, i.e., for some $u \in U$, $\mathcal{A}_{[x \to u]}(F \vee H) = 1$ and hence that

(i) $\mathcal{A}_{[x \to u]}(F) = 1$ for some $u \in U$ or that

(ii) $\mathcal{A}_{[x \to u]}(H) = 1$ for some $u \in U$.

By definition, (i) means that $\mathcal{A}(\exists x\ F) = 1$. Moreover, because x does not occur free in H, by (ii) we have $\mathcal{A}_{[x \to u]}(H) = \mathcal{A}(H) = 1$ for all $u \in U$.
Therefore, $\mathcal{A}((\exists x\ F) \vee H) = 1$, which was to be proved. □

(b) (1) To the definition of syntax we add the following statement:

If t_1 and t_2 are terms, then $(t_1 = t_2)$ is a formula.

To the definition of semantics we add the following:

If F is of the form $(t_1 = t_2)$ for terms t_1 and t_2, then $\mathcal{A}(F) = 1$ if and only if $\mathcal{A}(t_1) = \mathcal{A}(t_2)$.

(2) For the monoid we have to describe associativity and the neutral element. For the group we have to describe the inverse element aswell.

(i) $\forall a \forall b \forall c\ (f(f(a,b),c) = f(a,f(b,c))) \wedge \exists e \forall a\ (f(a,e) = f(e,a) \wedge f(e,a) = a)$

(ii) $\forall a \forall b \forall c\ (f(f(a,b),c) = f(a,f(b,c))) \wedge$
$\exists e\ (\forall a\ (f(a,e) = f(e,a) \wedge f(e,a) = a) \wedge \forall a \exists b\ (f(a,b) = f(b,a) \wedge f(b,a) = e))$