Exam topics

1. Basic structures: sets, lists, functions
   (a) Sets { }: write all elements, or define by condition
   (b) Set operations: $A \cup B$, $A \cap B$, $A \backslash B$, A^c
   (c) Lists ( ): Cartesian product $A \times B$
   (d) Functions $f : A \to B$ defined by any input-output rule
   (e) Injective function: $\forall a_1, a_2 \in A$: $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
   (f) Surjective function: $\forall b \in B$, $\exists a \in A$ with $f(a) = b$
   (g) A, B have same cardinality: there is a bijection $f : A \to B$
   (h) A is countable: there is a bijection $f : \mathbb{N} \to A$
2. Formal logic
   (a) Statements: definitely true or false
   (b) Conditional (open) statement $P(x)$: true/false depends on variable x
   (c) Logical operations: *and*, *or*, *not*, *implies*
   (d) Truth tables and logical equivalence
   (e) Implication $P \Rightarrow Q$ equivalent to: contrapositive $not(Q) \Rightarrow not(P)$;
   independent from: converse $Q \Rightarrow P$; inverse $not(P) \Rightarrow not(Q)$
   (f) Negate implication: $not(P \Rightarrow Q)$ is equivalent to: P *and* $not(Q)$
   (g) Quantifiers: $\forall$ for all , $\exists$ there exists;
   (h) Negate quantifiers: $not(\forall x, P(x))$ is equivalent to: $\exists x, not(P(x))$
   (i) Logical equivalences and set equations
   (j) Logic in mathematical language versus everyday language
3. Methods of proof (can be combined)
   (a) Direct proof
   (b) Proof by cases
   (c) Proof of the contrapositive
   (d) Proof by contradiction
   (e) Proof by induction (also complete induction)
4. Axioms of a Group $(G, *)$ (All variables below mean elements of G.)
   (a) Closure: $a * b \in G$.
   (b) Associativity: $(a * b) * c = a * (b * c)$
   (c) Identity: There is e with $e * a = a$ and $a * e = a$ for all a.
   (d) Inverses: For each a, there is some b with $a * b = e$ and $b * a = e$.
   Extra axioms
   (e) Commutativity: $a * b = b * a$.
   (f) Distributivity of times over plus: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.
5. Divisibility of integers (All variables below mean integers.)
   (a) Divisibility: $a|b$ means $b = ac$ for some $c \in \mathbb{Z}$

(b) Properties of divisibility:
- $a \mid b, c \implies a \mid mb{+}nc$ for all m, n
- $a|b$ and $b|c \implies a|c$.
- $a|b$ and $b|a \implies a = \pm b$.

(c) Prime and composite
- Test: a is composite $\Longrightarrow a$ has prime factor $p \leq \sqrt{a}$.

(d) Greatest common divisor $\gcd(a, b)$; relatively prime means $\gcd(a, b) = 1$.

(e) Division Lemma: $a = qb + r$ with remainder $0 \leq r < b$.

(f) Euclidean Algorithm computes remainders $a > b > r_1 > \cdots > r_k > 0$.
- Computes $\gcd(a, b) = r_k$.
- Finds m, n with $\gcd(a, b) = ma + nb$.

(g) Consequences of $\gcd(a, b) = ma + nb$
- Find integer solutions (x, y) to equation $ax + by = c$, if $\gcd(a, b) \mid c$.
- If $e|a$ and $e|b$, then $e| \gcd(a, b)$.
- Euclid's Lemma: If $c \mid ab$ and $\gcd(c, a) = 1$, then $c|b$.
- Prime Lemma: If p is prime with $p \mid ab$, then $p|a$ or $p|b$.
- For $\bar{a} \in \mathbb{Z}_n$, find multiplicative inverse $\bar{b} = \bar{a}^{-1}$, i.e $ab \equiv 1 \pmod{n}$.

(h) Fundamental Theorem of Arithmetic
- $n > 1$ is a product of primes uniquely, except for rearranging factors.
- There is a unique list of powers $s_1, s_2, s_3, \ldots \geq 0$ with: $n = 2^{s_1} 3^{s_2} 5^{s_3} 7^{s_4} 11^{s_5} \cdots$.

6. Equivalence relation $\cong$ on a set S

(a) Defining properties:
- Reflexive: $a \equiv a$
- Symmetric: If $a \equiv b$, then $b \equiv a$.
- Transitive: If $a \equiv b$ and $b \equiv c$, then $a \equiv c$

(b) Equivalence class $[a] = \{b \in S \mid b \cong a\}$. Following are logically the same:
- $a \cong b$
- $a \in [b]$
- $[a] = [b]$, the same set

7. Clock arithmetic $\mathbb{Z}_n$

(a) Modular equivalence: $a \equiv b \pmod{n}$ means $n \mid a{-}b$. Class $\overline{a} = [a]$.

(b) Equivalence class $\overline{a} = [a]$. $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n{-}1}\}$

(c) Modular addition and multiplication satisfy all usual rules of algebra

(d) Modular division: $\overline{a}^{\,-1} = \overline{b}$, where $\overline{a}\overline{b} = \overline{1}$, provided $\gcd(a, n) = 1$.

(e) In $\mathbb{Z}_p$ with p prime, every $\overline{a} \neq \overline{0}$ has $\overline{a}^{\,-1} \in \mathbb{Z}_p$.

8. Limits

(a) Real number axioms: commutative group axioms for $+$, $\cdot$; distribuitive law' axioms of order $<$.

(b) Completeness: If $S \subset \mathbb{R}$ has upper bound, then $\mathrm{lub}(S) = \sup(S) \in \mathbb{R}$.

(c) Convergent sequence $\lim\limits_{n\to\infty} a_n = \ell$: $\forall \epsilon{>}0, \exists N,\ n \geq N \Rightarrow |a_n{-}\ell| < \epsilon$

(d) Divergent sequence (a_n): $\forall \ell, \exists\, \epsilon{>}0, \forall N, \exists\, n{\geq}N$ with $|a_n{-}\ell| \geq \epsilon$.

(e) Infinite limit $\lim\limits_{n\to\infty} a_n = \infty$: $\forall B, \exists N,\ n \geq N \Rightarrow a_n > B$.

(f) Thm: If (a_n) increasing bounded sequence, then (a_n) convergent.

1. (a) Use a multiplication table to find all values $a \in \mathbb{Z}_7$ for which the equation

$$x^2 = a$$

has a solution $x \in \mathbb{Z}_7$. For each such a, list all of the solutions x.

   (b) Find all solutions $x \in \mathbf{Z}_7$ to the equation $x^2 + \overline{2}x + \overline{6} = \overline{0}$.

2. Use quantifiers to express what it means for a sequence $(x_n)_{n\in\mathbb{N}}$ to *diverge*. You cannot use the terms *not* or *converge*.

3. Suppose $A, B \subseteq \mathbb{R}$ are bounded and non-empty. Show that $\sup(A \cup B) = \max\{\sup(A), \sup(B)\}$.

4. Let A, B be sets, and suppose there is a surjection $f : A \to B$. Prove that there is an injection $g : B \to A$.

5. Use the formal definition of limit to prove the following.

   (a) $\lim_{n\to\infty} \frac{n^2+3}{2n^3-4} = 0$

   (b) $\lim_{n\to\infty} \frac{4n-5}{2n+7} = 2$

   (c) $\lim_{n\to\infty} \frac{n^3-3n}{n+5} = +\infty$

   (d) $\lim_{n\to\infty} \frac{n^2-7}{1-n} = -\infty$

6. For each of the following, determine if $\sim$ defines an equivalence relation on the set S. If it does, prove it and describe the equivalence classes. If it does not, explain why.

   (a) $S = \mathbb{R} \times \mathbb{R}$. For (a, b) and $(c, d) \in S$, define $(a, b) \sim (c, d)$ if $3a + 5b = 3c + 5d$.

   (b) $S = \mathbb{R}$. For $a, b \in S$, $a \sim b$ if $a < b$.

   (c) $S = \mathbb{Z}$. For $a, b \in S$, $a \sim b$ if $a \mid b$.

   (d) $S = \mathbb{R} \times \mathbb{R}$. For (a, b) and $(c, d) \in S$, define $(a, b) \sim (c, d)$ if $\lceil a\rceil = \lceil c\rceil$ and $\lceil b\rceil = \lceil d\rceil$. Here $\lceil x\rceil$ is the smallest integer greater than or equal to x.

7. Consider Z_n.

   (a) Under what conditions on n does every nonzero element have a multiplicative inverse? How about an additive inverse?

   (b) Does every nonzero element have a multiplicative inverse in Z_{21}?

   (c) Does 5 have a multiplicative inverse in Z_{21}? Explain why or why not. If it does, find 5^{-1}.

   (d) Solve the equation $5x - 14 = 19$ in $\mathbb{Z}_{21}$.

8. Let $A = \{a, b, c\}$ and $B = \{a, x\}$. List all elements of

   (a) $A \cup B$

   (b) $A \cap B$

   (c) $A \backslash B$

   (d) $A \times B$

   (e) Power set of A

9. Let $S(n) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid max\{x, y\} = n\}$. Prove that $S(3) \cap S(5)$ is the empty set.

10. Let $f : \mathbb{N} \to \mathbb{N}$, given by $f(n) = |n - 4|$.

    (a) Prove that f is surjective

    (b) Prove that f is not injective

11. Let $f : A \to B$ and $g : B \to A$ be functions satisfying $f(g(x)) = x$ for all $x \in B$. Prove that f is surjective.

12. Describe a concrete bijection from $\mathbb{N}$ to $\mathbb{N} \times \{1, 2, 3\}$. Briefly tell why it is injective and surjective.

13. Make a truth table for not $(A \vee B) \implies A \wedge B$. Find a shorter logically equivalent expression.

14. Find the negations of the following statements:

    (a) $(A \vee B) \wedge (B \vee C)$

    (b) $A \implies (B \wedge C)$

    (c) $\forall x \ \exists y \ (P(x) \vee (\text{not } Q(y)))$

1. (a) Use a multiplication table to find all values $a \in \mathbb{Z}_7$ for which the equation

$$x^2 = a$$

has a solution $x \in \mathbb{Z}_7$. For each such a, list all of the solutions x.

Solution. We only need to look at the diagonal of the multiplication table for $\mathbb{Z}_7$. Then the equation $x^2 = a$ has a solution $x \in \mathbb{Z}_7$ if and only if $a \in \{\overline{0}, \overline{1}, \overline{2}, \overline{4}\}$. When $a = \overline{0}$, the only solution is $x = \overline{0}$. When $a = \overline{1}$, the solutions are $x = \overline{1}$ and $x = \overline{6}$. When $a = \overline{2}$, the solutions are $x = \overline{3}$ and $x = \overline{4}$. When $a = \overline{4}$, the solutions are $x = \overline{2}$ and $x = \overline{5}$.

(b) Find all solutions $x \in \mathbf{Z}_7$ to the equation $x^2 + \overline{2}x + \overline{6} = \overline{0}$.

Solution. Adding $\overline{2}$ to both sides, the given equation is equivalent to $x^2 + \overline{2}x + \overline{1} = \overline{2}$. We can factor the left-hand side to get

$$(x + \overline{1})^2 = \overline{2}.$$

It follows from part (a) that $x + \overline{1} = \overline{3}$ or $x + \overline{1} = \overline{4}$, and hence $x = \overline{2}$ or $x = \overline{3}$.

2. Use quantifiers to express what it means for a sequence $(x_n)_{n\in\mathbb{N}}$ to *diverge*. You cannot use the terms *not* or *converge*.

Solution. A sequence $(x_n)_{n\in\mathbb{N}}$ *diverges* if for every $L \in \mathbb{R}$ there is some $\epsilon > 0$ such that for all $N \in \mathbb{N}$ there is some natural number $n \geq N$ for which $|x_n - L| \geq \epsilon$. In terms of quantifiers this is

$$\forall L \in \mathbb{R}\ \exists \epsilon > 0\ \forall N \in \mathbb{N}\ \exists n \geq N, |x_n - L| \geq \epsilon.$$

3. Suppose $A, B \subseteq \mathbb{R}$ are bounded and non-empty. Show that $\sup(A \cup B) = \max\{\sup(A), \sup(B)\}$.

Solution. First note that since A and B are both bounded and non-empty, the same is true of $A \cup B$ and so $\sup(A \cup B) \in \mathbb{R}$ exists. It follows immediately from Beck Proposition 8.50 that $\sup(A \cup B) \geq \max\{\sup(A), \sup(B)\}$, since A and B are both subsets of $A \cup B$. We need to prove the reverse inequality. For sake of contradiction, suppose $\sup(A \cup B) > \max\{\sup(A), \sup(B)\}$. Then neither $\sup(A)$, nor $\sup(B)$ can be an upper bound for $A \cup B$. So there is some $x \in A \cup B$ with $x > \sup(A)$ and $x > \sup(B)$. But $x \in A \cup B$ implies that $x \in A$ or $x \in B$, so this cannot happen.

4. Let A, B be finite sets, and suppose there is a surjection $f : A \to B$. Prove that there is an injection $g : B \to A$ such that $f \circ g : B \to B$ is the identity function.

   Solution. Let $b \in B$, we want to define $g(b) \in A$. Since f is surjective, it follows that $f^{-1}(b)$ is a non-empty set. Let $a \in f^{-1}(b)$ be any element of this set, and declare $g(b) = a$. We obviously have that $f \circ g$ is the identity, since $f(g(b)) = f(a) = b$ for all $b \in B$. To show g is injective, suppose there are $b, b' \in B$ with $g(b) = g(g')$. Let $a = g(b)$ denote this common value. Then by construction of g, we have $a \in f^{-1}(b)$ and $a \in f^{-1}(b')$. Applying f to a therefore gives $f(a) = b$ and $f(a) = b'$, and so $b = b'$.

5. Use the formal definition of limit to prove the following.

   (a) $\lim_{n\to\infty} \dfrac{n^2+3}{2n^3-4} = 0$

   Solution. Let $\varepsilon > 0$ be given, aribitrary. Define $N = \max\{3, \dfrac{2}{\varepsilon} + 2\}$. Let $n \geq N$, $n \in \mathbb{N}$ be arbitrary. Then,

$$
\begin{aligned}
\left|\frac{n^2+3}{2n^3-4} - 0\right| &= \frac{n^2+3}{2n^3-4} && \text{(since } n \geq 3\text{)} \\
&\leq \frac{n^2+3n^2}{2n^3-4n^2} && \text{(We increased the numerator and decreased the denominator,} \\
& && \text{keeping in mind } 2n^3 - 2n^2 > 0, \text{ as } n > 2\text{)} \\
&= \frac{2}{n-2} && \text{(Factor and cancel out common terms)} \\
&\leq \frac{2}{N-2} && (n \geq N) \\
&\leq \varepsilon && (N \geq \frac{2}{\varepsilon} + 2)
\end{aligned}
$$

   Thus, $\forall \varepsilon > 0$, $\exists N$ such that $\forall n > N$ with $n \in \mathbb{N}$, $\left|\dfrac{n^2+3}{2n^3-4} - 0\right| < \varepsilon$. Thus, indeed $\lim_{n\to\infty} \dfrac{n^2+3}{2n^3-4} = 0$.

   (b) $\lim_{n\to\infty} \dfrac{4n-5}{2n+7} = 2$

Solution. Let $\varepsilon > 0$ be given, aribitrary. Define $N = \dfrac{1}{\varepsilon}$. Let $n \geq N$, $n \in \mathbb{N}$ be arbitrary. Then,

$$\begin{aligned}
\left|\frac{4n-5}{2n+7} - 2\right| &= \frac{19}{2n+7} && \text{(since } n > 0) \\
&< \frac{19}{2n} && \text{(We decreased the denominator,} \\
&< \frac{1}{n} && \\
&\leq \frac{1}{N} && (n \geq N) \\
&= \varepsilon && (N = \frac{1}{\varepsilon})
\end{aligned}$$

Thus, $\forall \varepsilon > 0$, $\exists N$ such that $\forall n > N$ with $n \in \mathbb{N}$, $\left|\dfrac{4n-5}{2n+7} - 2\right| < \varepsilon$. Thus, indeed $\lim\limits_{n\to\infty} \dfrac{4n-5}{2n+7} = 0$.

(c) $\lim\limits_{n\to\infty} \dfrac{n^3 - 3n}{n+5} = +\infty$

Solution. Let $M > 0$ be given, aribitrary. Define $N = \sqrt{6M+3}$. Let $n \geq N$, $n \in \mathbb{N}$ be arbitrary. Then,

$$\begin{aligned}
\frac{n^3 - 3n}{n+5} &\geq \frac{n^3 - 3n}{n+5n} && \text{(since } n \geq 1) \\
&= \frac{n^3 - 3n}{6n} && \\
&= \frac{n^2 - 3}{6} && \\
&\geq \frac{N^2 - 3}{6} && (n \geq N) \\
&= M && (N = \sqrt{6M+3})
\end{aligned}$$

Thus, $\forall M > 0$, $\exists N$ such that $\forall n > N$ with $n \in \mathbb{N}$, $\dfrac{n^3 - 3n}{n+5} \geq M$. Thus, indeed $\lim\limits_{n\to\infty} \dfrac{n^3 - 3n}{n+5} = +\infty$.

(d) $\lim\limits_{n\to\infty} \dfrac{n^2 - 7}{1-n} = -\infty$

Solution. Let $M < 0$ be given, aribitrary. Define $N = 7 - M$. Let $n \geq N$, $n \in \mathbb{N}$ be arbitrary. Then,

$$\begin{aligned}
\frac{n^2-7}{1-n} &< \frac{n^2-7}{-n} && (\text{since } n > 7,\ \text{thus } n^2 - 7 > 0) \\
&\leq \frac{n^2-7n}{-n} && (\text{since the denominator is negative and } n > 7, \\
& && \text{decreasing the numerator, while still keeping it positive }) \\
&= 7 - n \\
&\leq 7 - N && (n \geq N) \\
&= M && (N = 7 - M)
\end{aligned}$$

Thus, $\forall M < 0$, $\exists N$ such that $\forall n > N$ with $n \in \mathbb{N}$, $\dfrac{n^2-7}{1-n} \leq M$. Thus, indeed $\lim\limits_{n\to\infty} \dfrac{n^2-7}{1-n} = -\infty$.

6. For each of the following, determine if $\sim$ defines an equivalence relation on the set S. If it does, prove it and describe the equivalence classes. If it does not, explain why.

(a) $S = \mathbb{R} \times \mathbb{R}$. For (a,b) and $(c,d) \in S$, define $(a,b) \sim (c,d)$ if $3a + 5b = 3c + 5d$.

Solution. The relation $\sim$ as defined above is indeed an equivalence relation, since it satisfies reflexivity, symmetry and transitivity, as shown below.

- Reflexivity: Let $(a,b) \in S$. Then $3a + 5b = 3a + 5b$, and therefore $(a,b) \sim (a,b)$.
- Symmetry: Let $(a,b), (c,d) \in S$ such that $(a,b) \sim (c,d)$. Then $3a + 5b = 3c + 5d$. This is equivalent to $3c + 5d = 3a + 5b$, which implies $(c,d) \sim (a,b)$.
- Transitivity: Let $(a,b), (c,d), (e,f) \in S$, such that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $3a + 5b = 3c + 5d$ and $3c + 5d = 3e + 5f$. By transitivity of equality for real numbers we have $3a + 5b = 3e + 5f$, and therefore $(a,b) \sim (e,f)$.

The equivalence classes are the lines $3x + 5y = c$, i.e. each equivalence class is a line with slope $-\dfrac{3}{5}$ and the different equivalence classes have different $y-$intercepts (given by $\dfrac{c}{5}$).

(b) $S = \mathbb{R}$. For $a, b \in S$, $a \sim b$ if $a < b$.

Solution. The relation defined by $a \sim b$ if $a < b$ is not an equivalence relation, since it does not satisfy reflexivity. Namely, $a \nsim a$, since $a \nless a$.

(c) $S = \mathbb{Z}$. For $a, b \in S$, $a \sim b$ if $a \mid b$.

Solution. The relation defined by $a \sim b$ if $a \mid b$ is not an equivalence relation, since it does not satisfy symmetry. Namely, $a \sim b$ does not necessarily imply $b \sim a$. For example, $2 \mid 8$, but $8 \nmid 2$.

(d) $S = \mathbb{R} \times \mathbb{R}$. For (a, b) and $(c, d) \in S$, define $(a, b) \sim (c, d)$ if $\lceil a \rceil = \lceil c \rceil$ and $\lceil b \rceil = \lceil d \rceil$. Here $\lceil x \rceil$ is the smallest integer greater than or equal to x.

Solution. The relation $\sim$ as defined above is indeed an equivalence relation, since it satisfies reflexivity, symmetry and transitivity, as shown below.

- Reflexivity: Let $(a, b) \in S$. Then $\lceil a \rceil = \lceil a \rceil$ and $\lceil b \rceil = \lceil b \rceil$, and therefore $(a, b) \sim (a, b)$.
- Symmetry: Let $(a, b), (c, d) \in S$ such that $(a, b) \sim (c, d)$. Then $\lceil a \rceil = \lceil c \rceil$ and $\lceil b \rceil = \lceil d \rceil$. This is equivalent to $\lceil c \rceil = \lceil a \rceil$ and $\lceil d \rceil = \lceil b \rceil$, which implies $(c, d) \sim (a, b)$.
- Transitivity: Let $(a, b), (c, d), (e, f) \in S$, such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $\lceil a \rceil = \lceil c \rceil$ and $\lceil b \rceil = \lceil d \rceil$, as well as $\lceil c \rceil = \lceil e \rceil$ and $\lceil d \rceil = \lceil f \rceil$. By transitivity of equality for real numbers we have $\lceil a \rceil = \lceil e \rceil$ and $\lceil b \rceil = \lceil f \rceil$, and therefore $(a, b) \sim (e, f)$.

The equivalence classes are squares in the plane $\mathbb{R}^2$ with sides parallel to the coordinate axes, in particular, they are sets of the form $(i, i + 1] \times (j, j + 1]$ (Cartesian product of intervals), where the ordered pair $(i, j) \in \mathbb{Z}^2$.

7. Consider Z_n.

(a) Under what conditions on n does every nonzero element have a multiplicative inverse? How about an additive inverse?

Solution. Every nonzero element in $\mathbb{Z}_n$ has a multiplicative inverse if n is prime. Indeed, if n is prime, $\gcd(n, m) = 1$ $\forall m \in \mathbb{Z}$ such that $0 < m < n$, and therefore by Bezout's Lemma there exist integers x, y such that $nx + my = 1$, thus $my \equiv 1 \mod n$, i.e. $\bar{m} \cdot \bar{y} = 1$, which implies that $\bar{m}^{-1} = \bar{y}$.

Every element in $\mathbb{Z}_n$ does have an additive inverse $\forall n \in \mathbb{N}$.

(b) Does every nonzero element have a multiplicative inverse in Z_{21}?

Solution. No, one can check that $\bar{3}$ and $\bar{7}$ do not have multiplicative inverses in $\mathbb{Z}_{21}$.

(c) Does 5 have a multiplicative inverse in Z_{21}? Explain why or why not. If it does, find 5^{-1}.

Solution. One can express $\gcd(5,21)$ in the form $5x+21y$ for some integers x,y by applying the Euclidean Algorithm, $21 = 4\cdot 5+1$, therefore $5\cdot(-4)+21\cdot 1 = 1$, thus $\bar{5}^{-1} = \bar{17}$. (Note that the equivalence classes $\bar{-4} = \bar{17}$.)

(d) Solve the equation $5x - 14 = 19$ in $\mathbb{Z}_{21}$.

Solution. The equation $\bar{5}x - \bar{14} = \bar{19}$ is equivalent to $\bar{5}x = \bar{12}$, which, using that $\bar{5}^{-1} = \bar{17}$ yields $x = \bar{12}\cdot\bar{17} = \bar{15}$.

8. Let $A = \{a,b,c\}$ and $B = \{a,x\}$. List all elements of

   (a) $A \cup B$

   (b) $A \cap B$

   (c) $A \backslash B$

   (d) $A \times B$

   (e) Power set of A

Solution. $A\cup B = \{a,b,c,x\}$, $A\cap B = \{a\}$, $A\backslash B = \{b,c\}$, $A\times B = \{(a,a),(a,x),(b,a),(b,x),(c,a),(c,x)\}$, Power set of A is $\{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a,b\},\ \{b,c\},\ \{a,c\},\ \{a,b,c\}\}$.

9. Let $S(n) = \{(x,y) \in \mathbb{R}\times\mathbb{R} \mid max\{x,y\} = n\}$. Prove that $S(3)\cap S(5)$ is the empty set.

Solution. Assume the contrary: let $(a,b) \in S(3)\cap S(5)$. Then $max\{a,b\} = 3$ and $max\{a,b\} = 5$, but $3 \neq 5$, hence our assumption leads to a contradiction. Therefore the intersection is empty.

10. Let $f : \mathbb{N} \to \mathbb{N}$, given by $f(n) = |n-4|$.

   (a) Prove that f is surjective

   (b) Prove that f is not injective

Solution. Given $y \in \mathbb{N}$, $f(y+4) = |y+4-4| = y$ since $y \geq 0$, which shows that f is surjective. $f(1) = 3 = f(7)$, hence f is not injective.

11. Let $f : A \to B$ and $g : B \to A$ be functions satisfying $f(g(x)) = x$ for all $x \in B$. Prove that f is surjective.

Solution. First attempt: Assume f is not surjective. Then there is a $b \in B$ such that there are no $a \in A$ with $f(a) = b$. Let $c = g(b)$, then $f(c) = f(g(b)) = b$ by assumption, hence we found a $c \in A$ with $f(c) = b$ which contradicts with the assumption.

Second attempt: Given $b \in B$, let $a = g(b)$, and compute $f(a) = f(g(b)) = b$ by assumption. Since b was arbitrary, this shows that f is surjective.

12. Describe a concrete bijection from $\mathbb{N}$ to $\mathbb{N} \times \{1, 2, 3\}$. Briefly tell why it is injective and surjective.

Solution. By division lemma, given n, there is a unique q and r with $0 \leq r < 3$ with $n = 3 \cdot q + r$, we could define $f(n)$ by $f(n) = (q, r + 1)$. Then f has the inverse function given by $g(a, b) = 3 \cdot a + b$. Check that $f(g(a, b)) = (a, b)$ and $g(f(n)) = n$.

13. Make a truth table for not $(A \vee B) \implies A \wedge B$. Find a shorter logically equivalent expression.

Solution. Consider all possibilities for simultaneous truth values for A and B:

A	B	not $(A \vee B)$	$A \wedge B$	not $(A \vee B) \implies$ not A
T	T	F	T	T
T	F	F	F	T
F	T	F	F	T
F	F	T	F	F

We see that the only time the expression is False is when both A and B are False, hence this expression is logically equivalent to $A \vee B$.

14. Find the negations of the following statements:

(a) $(A \vee B) \wedge (B \vee C)$

(b) $A \implies (B \wedge C)$

(c) $\forall x \ \exists y \ (P(x) \vee (\text{not } Q(y)))$

Solution. $\text{not}((A \vee B) \wedge (B \vee C)) \equiv \text{not}(A \vee B) \vee \text{not}(B \vee C) \equiv (\text{not}A \wedge \text{not}B) \vee (\text{not}B \wedge \text{not}C)$

$\text{not}(A \implies (B \wedge C)) \equiv \text{not}(\text{not}A \vee (B \wedge C)) \equiv A \wedge \text{not}(B \wedge C) \equiv A \wedge (\text{not}B \vee \text{not}C)$

$\text{not}(\forall x \ \exists y \ (P(x) \vee (\text{not } Q(y)))) \equiv \exists x \ \forall y \ (\text{not}P(x)) \wedge Q(y)$