Direct proof

Prove the following results directly.

1.1 9 is not a prime number.

1.2 11 is a prime number.

1.3 For all real numbers x and y we have the triangle inequality $|x + y| \leq |x| + |y|$.
Hint: consider (four) cases depending on the signs of x and y.

1.4 For all real numbers x and y we have Bernoulli's inequality $|x - y| \geq |x| - |y|$.
Hint: the preceding exercise may help.

Contradiction

Prove the following results by contradiction.

2.1 The equation $x^6 + 1 = 0$ has no real solutions.

2.2 $\log_2 19$ is not an integer.

2.3 $2^{\frac{1}{3}}$ is irrational.

Induction

Prove the following results using mathematical induction.

3.1 $1 + 4 + 9 + ... + n^2 = \frac{1}{6}n(n + 1)(2n + 1)$ for all natural numbers $n \geq 1$.

3.2 $1 + 8 + 27 + ... + n^3 = [\frac{1}{2}n(n + 1)]^2$ for all natural numbers $n \geq 1$.

3.3 $n^2 + n$ is even for all natural numbers $n \geq 1$.

3.4 $n^3 - n$ is divisible by 6 for all natural numbers $n \geq 1$.

3.5 $n! \leq n^n$ for all natural numbers $n \geq 1$.

3.6 $2^n > n^3$ for all natural numbers $n \geq 10$.

3.7 If $x \geq 0$, then $(1 + x)^n \geq 1 + x^n$ for all natural numbers $n \geq 1$.

3.8 Define a sequence a_n recursively as follows: $a_0 = 0$, $a_1 = 1$, and for all $n \geq 2$ $a_n = 5a_{n-1} - 6a_{n-2}$. Prove that $a_n = 3^n - 2^n$ for all natural numbers $n \geq 0$.

3.9 The nth Fibonacci number is less than 2^n (see wikipedia for the definition).

Propositional calculus

Use truth tables to prove the following are tautologies.

4.1 Contrapositive: $(p \to q) \leftrightarrow (\neg q \to \neg p)$

4.2 $(\neg p \to (q \wedge \neg q)) \to p$

4.3 $(p \to q) \leftrightarrow (\neg p \vee q)$

Essay fun

In a few words explain how the following are related to proofs by contradiction.

5.1 4.1

5.2 4.2

Quantifiers

Negate each expression. Make sure to propagate $\neg$ all the way into the formula.

6.1 $(\forall x)[p(x) \to (q(x) \wedge r(x))]$

6.2 $(\exists y)[p(y) \vee (\forall x)[q(x) \to \neg r(x)]]$

6.3 $(\forall x)(\exists y)(\forall z)[p(x, y) \leftrightarrow q(y, z)]$

6.4 Look up the statement of Goldbach's Conjecture. Negate it.

6.5 Look up in your calculus book the definition of continuity at a point. Write it out symbolically. Then negate it.

Separation Axiom Schema

Use Separation to demonstrate that the following collections are sets. You may assume that $\mathbf{Z}$ and $\mathbf{R}$ are sets.

7.1 Positive even integers.

7.2 Real roots of a polynomial on one variable with real coefficients.

7.3 Critical points of a differentiable function.

Subsets

Prove the following.

8.1 $(\forall A)[\varnothing \subseteq A]$

8.2 $(\forall A)[(A \subseteq \varnothing) \to (A = \varnothing)]$

Operations on sets

Prove, or disprove by counterexample.

9.1 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

9.2 $(A \subseteq C \wedge B \subseteq D) \Rightarrow (B \setminus C \subseteq D \setminus A)$

9.3 $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$

9.4 $A \setminus (B \setminus C) = (A \setminus B) \setminus (A \setminus C)$

More on sets

10.1 Prove that for all sets A and B we have $(A \cup B) \setminus B \subseteq A$. Use a counterexample to show that subset the other way need not generally hold.

10.2 One of the following sets $(A \cup B) \setminus C$ and $A \cup (B \setminus C)$ is always a subset of the other. Determine which way and prove it. Give a counterexample to show that subset the other way may not hold.

The power set

11.1 Determine the power set of a set with 4 elements. Sketch it as a lattice.

Properties of power sets

Prove, or disprove by counterexample.

12.1 $(A \subseteq B) \Leftrightarrow (\mathscr{P}(A) \subseteq \mathscr{P}(B))$

12.2 $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cup \mathscr{P}(B)$

12.3 $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$

12.4 $\mathscr{P}(A \setminus B) = \mathscr{P}(A) \setminus \mathscr{P}(B)$

Cartesian product

Prove, or disprove by counterexample.

13.1 $A \times C \subseteq B \times D \Leftrightarrow A \subseteq B \wedge C \subseteq D$

13.2 $(A \setminus B) \times (C \setminus D) = (A \times C) \setminus (B \times D)$

Forward images

Suppose $f\colon X \to Y$ is a function and $A, B \subseteq X$. Prove the following statements.

14.1 $A \subseteq B \Rightarrow f_*(A) \subseteq f_*(B)$ (is the converse true?)

14.2 $f_*(A \cup B) = f_*(A) \cup f_*(B)$

14.3 $f_*(A \cap B) \subseteq f_*(A) \cap f_*(B)$ (is containment the other way true?)

14.4 $f_*(A) \setminus f_*(B) \subseteq f_*(A \setminus B)$ (is containment the other way true?)

Inverse images

Suppose $f\colon X \to Y$ is a function and $C, D \subseteq Y$. Prove the following statements.

15.1 $C \subseteq D \Rightarrow f^*(C) \subseteq f^*(D)$ (is the converse true?)

15.2 $f^*(C \cup D) = f^*(C) \cup f^*(D)$

15.3 $f^*(C \cap D) = f^*(C) \cap f^*(D)$

15.4 $f^*(C \setminus D) = f^*(C) \setminus f^*(D)$

Functions

Prove the following.

16.1 $f\colon \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ is neither one-to-one nor onto.

16.2 $f\colon [0, \infty) \to [0, \infty)$ given by $f(x) = x^2$ is one-to-one and onto.

16.3 Composition of two injective functions is injective.

16.4 Composition of two surjective functions is surjective.

Compositional inverses

For the following functional formulas, try to come up with an appropriate domain and co-domain that would make the resulting function of a real variable invertible. Give a recipe for the compositional inverse.

17.1 $x \mapsto x + 2$

17.2 $x \mapsto 2x$

17.3 $x \mapsto e^x$

Equivalence relations

18.1 Define two points in $\mathbf{R}^2$ to be related when their distance to the origin is the same. Prove that this is an equivalence relation and describe geometrically the equivalence classes.

18.2 Define two points in $\mathbf{R}^2 \setminus \{0\}$ to be related when one is a nonzero scalar multiple of the other. In other words $[x, y] \sim [x', y'] \Leftrightarrow (\exists c \in \mathbf{R} \setminus \{0\})[[x, y] = [cx', cy']]$. Prove that this is an equivalence relation and describe geometrically the equivalence classes.

18.3 Define two points in $\mathbf{R}^2$ to be related whenever the distance between them is rational. Show which axioms of an equivalence relation are satisfied and which violated.

Indexed families of sets

19.1 For $s \in \mathbf{R}$ define $A_s = \{x \in \mathbf{R}\colon x > -s \wedge x < s\}$. For which s do we have $A_s = \varnothing$? Find $\bigcap_{s>0} A_s$, $\bigcup_{s\in\mathbf{R}} A_s$, and $\bigcup_{s<1} A_s$.

Ordered sets

20.1 Let $S = \{x \in \mathbf{Q}\colon (\exists n \in \mathbf{N})[x = 1/n]\}$. If they exist, what are $\min S$ and $\max S$? For S as a subset of $\mathbf{Q}$, same question for $\sup S$ and $\inf S$.

20.2 Let $C = \{x \in \mathbf{Q}\colon x^2 < 2\}$. Does C have a minimum? Maximum? If we consider C as a subset of $\mathbf{R}$ what are $\sup C$ and $\inf C$?

20.3 Prove that if $m \in B$ and m is an upper bound for B, $m = \max B$.

20.4 Prove that if A is a nonempty finite linearly ordered set, then A has a maximum.

20.5 Suppose A is a set with at least two elements. Prove that the partial order $\subseteq$ on $\mathscr{P}(A)$ is not a well order.

Quotient sets

21.1 Suppose $\sim$ is an equivalence relation on a set A and let $A/\!\sim$ denote the quotient set (the set of equivalence classes). Define the natural projection $\pi\colon A \to A/\!\sim$ by $\pi(x) = [x]$. Prove that for any set B and a function $f\colon A \to B$ that "respects" $\sim$, i.e. such that $(\forall x \in A)(\forall y \in A)[x \sim y \Rightarrow f(x) = f(y)]$, there exists a unique function $\varphi\colon A/\!\sim \to B$ such that $f = \varphi \circ \pi$.

Hint: To define the value of φ on an equivalence class, pick an element in the class and use its value under f. Then show that φ is "well defined" (independent of choice of element).

Partial inverses

22.1 Let $S = \{x \in \mathbf{R}\colon x \geq 0\}$ and let $f\colon \mathbf{R} \to S$ be given by $f(x) = x^2$. Find a function $s\colon S \to \mathbf{R}$ such that $f \circ s$ is the identity function on S.

22.2 Show that any s as above is not unique. How many of them are there?

22.3 Let $i\colon \mathbf{Z} \to \mathbf{Q}$ be the usual inclusion: $i(n) = n/1$. Find a function $f\colon \mathbf{Q} \to \mathbf{Z}$ such that $f \circ i$ is the identity on $\mathbf{Z}$.

22.4 Show that any f as above is not unique. How many of them are there?

Universal properties

Suppose A and B are sets. Sketch diagrams of functions to illustrate your proofs.

23.1 Define projections $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ by $\pi_A([x, y]) = x$ and $\pi_B([x, y]) = y$.

Prove that $A \times B$ and the two projections are *universal* among pairs of functions from a set to A and B.

In other words, prove that for any set C and functions $f_A\colon C \to A$ and $f_B\colon C \to B$, there exists a unique function $\varphi\colon C \to A \times B$ such that $f_A = \pi_A \circ \varphi$ and $f_B = \pi_B \circ \varphi$.

23.2 Let $i_A\colon A\to A\cup B$, $i_B\colon B\to A\cup B$, $j_A\colon A\cap B\to A$, and $j_B\colon A\cap B\to B$ denote the natural inclusions.

Prove that $A\cap B$ and its two inclusions into A and B are *universal* among pairs of functions from a set to A and B which define the same function to $A\cup B$.

In other words, prove that for any set C and functions $f_A\colon C\to A$ and $f_B\colon C\to B$ such that $i_A\circ f_A = i_B\circ f_B$, there exists a unique function $\varphi\colon C\to A\cap B$ such that $f_A = j_A\circ\varphi$ and $f_B = j_B\circ\varphi$.

23.3 With the same notation as in the preceding problem, show that $A\cup B$ and the two inclusions of A and B into it are *co-universal* among functions from A and B to a set that agree on $A\cap B$.

In other words, prove that for any set C and functions $g_A\colon A\to C$ and $g_B\colon B\to C$ whose restrictions to $A\cap B$ are equal (in other words $g_A\circ j_A = g_B\circ j_B$), there exists a unique function $\psi\colon A\cup B\to C$ such that its restrictions to A and B are g_A and g_B (in other words $\psi\circ i_A = g_A$ and $\psi|_B\circ i_B = g_B$).

Transitive sets

24.1 A set A is transitive $\Leftrightarrow (\forall a)(\forall x)[x\in a\wedge a\in A\to x\in A]$.

24.2 If A is a transitive set, then $\cup A\subseteq A$.

24.3 If A is a transitive set, then so is $\mathscr{P}(A)$.

Natural numbers ($\mathbf{N}$)

24.1 $n>0\Rightarrow(\exists k)[n=k^+]$

Binary relations

24.1 Define two points in $\mathbf{R}^2$ to be related when their distance to the origin is the same. Prove that this is an equivalence relation and describe geometrically the equivalence classes.

24.2 Define two points in $\mathbf{R}^2\setminus\{0\}$ to be related when one is a nonzero scalar multiple of the other. In other words $[x,y]\sim[x',y']\Leftrightarrow(\exists c\in\mathbf{R}\setminus\{0\})[[x,y]=[cx',cy']]$. Prove that this is an equivalence relation and describe geometrically the equivalence classes.

24.3 Define two points in $\mathbf{R}^2$ to be related whenever the distance between them is rational. Show which axioms of an equivalence relation are satisfied and which violated.

24.4 Give concrete examples (other than the one above) of binary relations that among reflexive, symmetric, and transitive, satisfy two but not all three of the properties. All possibilities.

24.5 Prove that if A is a set, the relation $\subseteq$ is a partial order on any subset of the power set $\mathscr{P}(A)$. Make a diagram for this partial order on $\mathscr{P}(\{0,1,2\})$ by listing all elements of the power set and drawing arrows between those that are related. Try to make it look æsthetically pleasing, be creative.

24.6 Define a relation on $\mathbf{Z}\times(\mathbf{Z}\setminus\{0\})$ by $[a,b]\sim[c,d]\Leftrightarrow ad=bc$. Prove that this is an equivalence relation.

24.7 Construct an equivalence relation on $\mathbf{N}$ with two finite equivalence classes and two infinite ones.

Binary operations

Let A be a set. Define the symmetric difference of $B, C \in \mathscr{P}(A)$ by $(B \cup C) \setminus (B \cap C)$.

19.1 What is the unit of the symmetric difference?

19.2 What is the unit of intersection, considered as an operation on $\mathscr{P}(A)$?

19.3 (extra credit) Prove that the symmetric difference is associative.

Integers ($\mathbf{Z}$)

24.1 For $[a,b],[c,d] \in \mathbf{N} \times \mathbf{N}$ define $[a,b] \sim [c,d] \Leftrightarrow a+d = b+c$. Show that $\sim$ is an equivalence relation.

Notes: The equivalence classes are called integers and their set is denoted by $\mathbf{Z}$. Think of the equivalence class of $[a,b]$ as $a-b$. Think of $\mathbf{N}$ as included in $\mathbf{Z}$ via $n \mapsto [n,0]$.

24.2 Define addition on $\mathbf{Z}$ by $[a,b]+[c,d] = [a+c, b+d]$. Show that $+$ is *well defined* (independent of the choice of representatives for each equivalence class) and agrees with addition on $\mathbf{N}$.

Hint: Replace one of the ordered pairs by an equivalent one and show that the sums are equivalent. Doing that for the other pair is similar and you can put the two results together, since $\sim$ is transitive.

24.3 Define multiplication on $\mathbf{Z}$ by $[a,b] \cdot [c,d] = [ac+bd, ad+bc]$. Show that $\cdot$ is well defined and agrees with multiplication on $\mathbf{N}$.

24.4 Prove that every integer has an additive inverse.

24.5 Define $[a,b] \leq [c,d] \Leftrightarrow a+d \leq b+c$. Show that this is well defined and a linear order on $\mathbf{Z}$ which agrees with the linear order on $\mathbf{N}$.

Rationals ($\mathbf{Q}$)

25.1 For $[a,b],[c,d] \in \mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ define $[a,b] \sim [c,d] \Leftrightarrow ad = bc$. Show that $\sim$ is an equivalence relation.

Notes: The equivalence classes are called rational numbers and their set is denoted by $\mathbf{Q}$. Think of the equivalence class of $[a,b]$ as a/b. Think of $\mathbf{Z}$ as included in $\mathbf{Q}$ via $k \mapsto [k,1]$.

25.2 Define multiplication on $\mathbf{Q}$ by $[a,b] \cdot [c,d] = [ac, bd]$. Show that $\cdot$ is well defined and agrees with multiplication on $\mathbf{Z}$.

Note: This definition, and the one below it, make sense, since $b \neq 0 \wedge d \neq 0 \Rightarrow bd \neq 0$.

25.3 Define addition on $\mathbf{Q}$ by $[a,b]+[c,d] = [ad+bc, bd]$. Show that $+$ is well defined and agrees with addition on $\mathbf{Z}$.

25.4 Prove that every rational number has an additive inverse and that every nonzero rational number has a multiplicative inverse.

25.5 Show that $[a,b] \sim [-a,-b]$, so that for each equivalence class we can always choose a representative with the second entry (think denominator) positive. Define $[a,b] \leq [c,d] \Leftrightarrow ad \leq bc$, where we assume $b > 0 \wedge d > 0$. Show that this is well defined and a linear order on $\mathbf{Q}$ which agrees with the linear order on $\mathbf{Z}$.

Reals ($\mathbf{R}$)

26.1 Prove that rationals are real, i.e. given $a \in \mathbf{Q}$, show that $\{b \in \mathbf{Q} \colon b < a\}$ is a Dedekind cut.

More precisely $i \colon \mathbf{Q} \to \mathbf{R}$ given by $i(a) = \{b \in \mathbf{Q} \colon b < a\}$ is an inclusion.

26.2 Show that the linear order on $\mathbf{R}$ given by $\subseteq$ of Dedekind cuts agrees with $\leq$ on $\mathbf{Q}$.

26.3 Show that $+$ on $\mathbf{R}$ agrees with $+$ on $\mathbf{Q}$.

26.4 Show that $-$ on $\mathbf{R}$ agrees with $-$ on $\mathbf{Q}$.

26.5 Suppose $A \subseteq \mathbf{R}$, $A \neq \varnothing$, and $(\exists y \in \mathbf{R})[x \in A \Rightarrow y \leq x]$. Prove A has an infimum in $\mathbf{R}$.

Hint: Apply the Least Upper Bound Property to the set $\{-x\colon x \in A\}$.

Extended reals

Affinely extended reals $[-\infty, +\infty]$ is the set of all initial segments in $\mathbf{Q}$. Nonempty proper initial segments of $\mathbf{Q}$ are reals (Dedekind cuts). The empty initial segment is denoted $-\infty$ and all of $\mathbf{Q}$ is denoted ∞.

27.1 Generalize the Least Upper Bound Property, by proving that all subsets of $[-\infty, +\infty]$ have a supremum and an infimum in $[-\infty, +\infty]$.

Divisibility

For $a, b \in \mathbf{N}$ we will say that a divides b (notation: $a|b$) whenever $(\exists q \in \mathbf{N})[b = aq]$.

25.1 Prove that divisibility is a partial order on $\mathbf{N}$.

25.2 If $a, b \in \mathbf{N}$, what are the usual interpretations for the supremum and the infimum of $\{a, b\} \subseteq \mathbf{N}$ under divisibility.

25.3 Prove one of your assertions in the preceding problem.

Algebraic structures

25.1 Prove that in groups the unit is unique. And so is the inverse of an element.

25.2 In the ring of integers $\mathbf{Z}$ which elements have multiplicative inverses?

25.3 For a set X let S_X be the set of all invertible functions $X \to X$ (*permutations*). Prove that S_X is a group under composition (*the symmetric group*).

25.4 Prove that if X has at most two elements, S_X is commutative.

25.5 Extra credit: Prove the converse.

Hint: For X with at least three elements try some *transpositions* (permutations that switch two distinct elements but leave everything else fixed). You may use the usual *cycle* notation (a, b) for the transposition that swaps a and b and leaves all other elements of X fixed.

25.6 Extra credit: Prove that if X is a set, then $\mathscr{P}(X)$ is a ring with symmetric difference playing the role of addition and intersection the role of multiplication.

(If you didn't do the previous extra credit problem on the symmetric difference, you may either assume that symmetric difference is associative or prove it now to pick up the previous extra credit.)